

LIFTING LAWS AND ARITHMETIC INVARIANT THEORY

AARON POLLACK

ABSTRACT. In this paper we discuss *lifting laws* which, roughly, are ways of “lifting” elements of the open orbit of one prehomogeneous vector space to elements of the minimal nonzero orbit of another prehomogeneous vector space. We prove a handful of these lifting laws, and show how they can be used to help solve certain problems in arithmetic invariant theory. Of the results contained in this article are twisted versions of certain parametrization theorems of Bhargava.

CONTENTS

1. Introduction	1
2. Lifting laws: Introduction	6
3. Statement of twisted orbit parametrizations	9
4. Preliminaries	15
5. The first lifting law for W_J	27
6. The lifting law for $J \oplus J$	34
7. The second lifting law for W_J	49
8. Lower rank lifting laws	58
References	64

1. INTRODUCTION

Suppose F is a field, G a reductive group over F , and V an F -linear finite dimensional representation of G . The study of the orbits of $G(F)$ on $V(F)$ falls under the heading of *invariant theory*. When $F = \mathbf{C}$ is the field of complex numbers, the study of such orbits is geometric invariant theory. When $F = \mathbf{Q}$ is the field of rational numbers, following [BG14, BGW15], the consideration of these orbits is called arithmetic invariant theory. One can also replace the field F by other rings, such as the integers \mathbf{Z} , and again consider the orbits of $G(\mathbf{Z})$ on $V(\mathbf{Z})$ (if G and V have a structure over the integers.) This too falls under the heading of arithmetic invariant theory. That the study of the orbits $G(\mathbf{Z})$ on $V(\mathbf{Z})$ is a rich and useful subject was made evident in the seminal papers [Bha04a, Bha04b, Bha04c, Bha08] of Bhargava.

1.1. Twisted orbit parametrizations. The main results of this paper are twisted versions of the results of [Bha04a] and [Bha04b]. Recall that in [Bha04a], Bhargava found five explicit orbit parametrizations $G(\mathbf{Z}) \backslash V(\mathbf{Z})$. The central example of [Bha04a] is $G(\mathbf{Z}) = \mathrm{SL}_2(\mathbf{Z}) \times \mathrm{SL}_2(\mathbf{Z}) \times \mathrm{SL}_2(\mathbf{Z})$ acting on $V(\mathbf{Z}) = \mathbf{Z}^2 \otimes \mathbf{Z}^2 \otimes \mathbf{Z}^2$, the triple tensor product of the defining two-dimensional representation of SL_2 . Roughly, it is proved in *loc. cit.* that the orbits parametrize pairs $(S, (I_1, I_2, I_3))$ where S is a quadratic ring, i.e., a commutative ring that is free of rank two as a \mathbf{Z} -module, and I_j are fractional S -ideal classes whose product $I_1 I_2 I_3 = 1$ in the class group of S .

The four other examples considered in [Bha04a] are as follows:

- (1) $G(\mathbf{Z}) = \mathrm{SL}_2(\mathbf{Z})$, $V(\mathbf{Z}) = \mathrm{Sym}^3(\mathbf{Z}^2)$;
- (2) $G(\mathbf{Z}) = \mathrm{SL}_2(\mathbf{Z}) \times \mathrm{SL}_2(\mathbf{Z})$, $V(\mathbf{Z}) = \mathbf{Z}^2 \otimes \mathrm{Sym}^2(\mathbf{Z}^2)$;

This work partially supported by the NSF through grant DMS-1401858 and the Schmidt Fund at the IAS.

- (3) $G(\mathbf{Z}) = \mathrm{SL}_2(\mathbf{Z}) \times \mathrm{SL}_4(\mathbf{Z})$, $V(\mathbf{Z}) = \mathbf{Z}^2 \otimes \wedge^2(\mathbf{Z}^4)$;
(4) $G(\mathbf{Z}) = \mathrm{SL}_6(\mathbf{Z})$, $V(\mathbf{Z}) = \wedge^3(\mathbf{Z}^6)$.

Bhargava parametrized the orbits $G(\mathbf{Z})$ on $V(\mathbf{Z})$ in the above cases in terms of tuples (S, M, \dots) where S is again a quadratic ring, M is a certain type of finite S -module, the \dots represents that there is possibly some auxiliary data, and all this data is taken modulo certain equivalences.

The above examples (G, V) of [Bha04a] are all integral models of *prehomogeneous vector spaces* (PVSs). Recall that a pair (G, V) of a linear algebraic group G over a field F and a finite dimensional F -rational representation V of G is a PVS if there is a (necessarily unique) G -invariant Zariski open $V^{\mathrm{open}} \subseteq V$ for which $V^{\mathrm{open}}(\overline{F})$ consists of one $G(\overline{F})$ orbit, where \overline{F} is an algebraic closure of F . The results of [Bha04a, Bha04b, Bha04c, Bha08] were preceded by work of Wright-Yukie [WY92] and Kable-Yukie [KY97]. In the paper [WY92], the authors parametrize orbits $G(F) \backslash V(F)^{\mathrm{open}}$ where (G, V) are certain PVSs and F is a field, in terms of finite étale extensions of F . The groups G in *loc. cit.* are all split. In [KY97], the authors consider similar orbit problems, where now the group G is no longer split. The proofs in [WY92, KY97] are Galois-cohomological in nature.

Following [Bha04a, Bha04b, Bha04c, Bha08], there has been much activity in the realm of orbit parametrizations and their applications. For instance, the reader may see [GS14, BG14, BGW15, Tan08, BH16, Woo14, Tho13, BHK16] for many orbit parametrizations, although this list is not meant to be complete. While there has been work giving parametrizations $G(\mathbf{Z}) \backslash V(\mathbf{Z})$ over the integers and more general base rings (e.g., [Woo11]) when the group G is split, and parametrizations $G(F) \backslash V(F)$ over fields when G is not split, there has been little work (e.g., some parts of [GS14]) on orbit parametrizations $G(\mathbf{Z}) \backslash V(\mathbf{Z})$ when G is not split. The main results of this article are of this latter form.

We first give a twisted version of the results of Bhargava from [Bha04a]. To setup the result, suppose A is one of the following¹ types of ring:

- (1) \mathbf{Z} ;
- (2) $\mathbf{Z} \times \mathbf{Z}$;
- (3) an order in an étale cubic extension of \mathbf{Q} ;
- (4) $\mathbf{Z} \times Q$, where Q is an order in a quaternion algebra over \mathbf{Q} ;
- (5) an order in a central simple algebra of degree 3 over \mathbf{Q} .

If A is as above, then there is a cubic polynomial action of $\mathrm{GL}_2(A)$ on $W_A := \mathbf{Z} \oplus A \oplus A \oplus \mathbf{Z}$, and this is an integral model for a PVS. For instance, when $A = \mathbf{Z}$, this is the action of $\mathrm{GL}_2(\mathbf{Z})$ on its symmetric cube representation, $\mathrm{Sym}^3(\mathbf{Z}^2)$. When $A = \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}$, this is the action of $\mathrm{GL}_2(\mathbf{Z})^3$ on $\mathbf{Z}^2 \otimes \mathbf{Z}^2 \otimes \mathbf{Z}^2$. These two examples were considered in [Bha04a]. In general, one can think of the action of $\mathrm{GL}_2(A)$ on $W_A = \mathbf{Z} \oplus A \oplus A \oplus \mathbf{Z}$ as a twisted symmetric cube representation. See section 4.4 for more details.

The group $\mathrm{GL}_2(A)$ has a degree 6 norm map; define $\mathrm{SL}_2(A)$ to be its kernel. The first result parametrizes the orbits $W_A^{\mathrm{open}} / \mathrm{SL}_2(A)$ in terms of quadratic rings S and certain $S \otimes A$ -modules. To be more precise, suppose $I \subseteq (S \otimes A)_{\mathbf{Q}}$, where for any \mathbf{Z} -module M , $M_{\mathbf{Q}} := M \otimes_{\mathbf{Z}} \mathbf{Q}$. We say that I is an $S \otimes A$ fractional ideal if

- SI is contained in I ;
- IA is contained in I ;
- $I = b_1A + b_2A$, $b_1, b_2 \in (S \otimes A)_{\mathbf{Q}}$, is free of rank two as an A -module.

We are careful with the right and left actions of S and A above, since A need not be commutative. We say that I is *oriented* if it comes equipped with an $\mathrm{SL}_2(A)$ orbit of bases $(b_1, b_2) \mathrm{SL}_2(A)$.

Theorem 1.1.1. *There is an explicit bijection, to be given below, between the orbits $W_A^{\mathrm{open}} / \mathrm{SL}_2(A)$ and triples of data $(S, I, \beta) / \sim$ where*

¹These rings A all have a degree 3 norm map. For instance, in the final case, this map is the reduced norm of the central simple algebra.

- S is an oriented quadratic ring with nonzero discriminant;
- I is an oriented fractional $S \otimes A$ -ideal;
- $\beta \in (S_{\mathbf{Q}})^{\times}$;
- the pair (I, β) is **balanced**.

This data is taken modulo the equivalence $(S, I, \beta) \sim (S', I', \beta')$ if there exists an orientation preserving $\varphi : S \xrightarrow{\sim} S'$ and $x \in (S' \otimes A_{\mathbf{Q}})^{\times}$ such that $I' = x\varphi(I)$ and $\beta' = n_{A \otimes S'_{\mathbf{Q}}/S'_{\mathbf{Q}}}(x)\varphi(\beta)$. Here $\varphi(I)$ means that both the fractional ideal I and its orientation are pushed forward via φ .

In the theorem, that S is oriented means that a generator of the rank one \mathbf{Z} -module S/\mathbf{Z} has been chosen. Furthermore, $n_A : A \rightarrow \mathbf{Z}$ is a certain cubic norm on A , and $n_{A \otimes S_{\mathbf{Q}}/S_{\mathbf{Q}}}$ is its extension to $A \otimes S_{\mathbf{Q}} \rightarrow S_{\mathbf{Q}}$. The condition that the pair (I, β) is balanced means, very roughly, that the norm $n_{A \otimes S_{\mathbf{Q}}/S_{\mathbf{Q}}}(I)$ is the principal fractional S -ideal generated by β . See section 3 for the precise definition.

In the cases when A is split, i.e., when $A = \mathbf{Z}, \mathbf{Z} \times \mathbf{Z}, \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}, \mathbf{Z} \times M_2(\mathbf{Z}),$ and $M_3(\mathbf{Z})$, Theorem 1.1.1 gives the five orbit parametrizations of Bhargava from [Bha04a]. The nonsplit cases are new. Furthermore, although we have stated Theorem 1.1.1 over the base ring \mathbf{Z} , below we prove it for a more general class of base rings. We also mention that Theorem 1.1.1 is proved uniformly in the ring A , even though there appear to be five cases. When the ring A is an order in an étale cubic extension of \mathbf{Q} , Gan-Savin [GS14] also considered the above orbit problem, although only classified the orbits over fields.

Theorem 1.1.1 is suggested by some of the beautiful arguments of Bhargava-Ho [BH16]. Namely, if one considers the orbit problems in Theorem 1.1.1, with the integers \mathbf{Z} replaced by a field, then certain arguments in [BH16, section 6], when specialized to degenerate cases, should yield a parametrization of these orbits. (The arguments of [BH16] are quite different from our own, however.) It is an interesting question if the arguments suggested by [BH16] can be made to work over the integers. Instead of attempting to use the more geometric techniques of *loc. cit.*, the proof of Theorem 1.1.1 blends twisted versions of some of the constructions of [Bha04a], together with what we call “lifting laws”, which are discussed below. To a first approximation, the lifting laws take the place of the solving of equations in [Bha04a], although they also have many useful technical consequences.

The second main result is a twisted version of the parametrizations from [Bha04b]. To setup this result, suppose C is one of the following² rings:

- (1) \mathbf{Z} ;
- (2) an order in an étale quadratic extension of \mathbf{Q} ;
- (3) an order in a quaternion algebra over \mathbf{Q} .

In each case, there is a involution $\tau : C \rightarrow C$, which is the identity in the case $C = \mathbf{Z}$ and nontrivial in the other cases. If $m \in M_3(C)$, set $m^* = {}^t m^\tau$, the conjugate transpose of m . Define $H_3(C) = \{h \in M_3(C) : h^* = h\}$, the Hermitian 3×3 matrices over C . The group $\mathrm{GL}_3(C)$ acts on $H_3(C)$ via $h \cdot m = m^* h m$, and then $\mathrm{GL}_2(\mathbf{Z}) \otimes \mathrm{GL}_3(C)$ acts on $\mathbf{Z}^2 \otimes H_3(C)$. Here the $\mathrm{GL}_2(\mathbf{Z})$ action on \mathbf{Z}^2 is the usual one, twisted by the determinant. These actions are integral models of PVSs.

Similarly to the above, $\mathrm{GL}_3(C)$ has a degree 6 norm map, coming from the reduced norm on $M_3(C)$. Denote by $\mathrm{SL}_3(C)$ the kernel of this degree 6 norm on $\mathrm{GL}_3(C)$. There is likewise a notion of an oriented $T \otimes C$ -ideal, where T is a cubic ring, i.e., T is commutative ring that is free of rank 3 as a \mathbf{Z} -module. We have the following result.

Theorem 1.1.2. *There is an explicit bijection, to be given below, between the orbits $(\mathbf{Z}^2 \otimes H_3(C))^{open} / \mathrm{GL}_2(\mathbf{Z}) \times \mathrm{SL}_3(C)$ and triples of data $(T, I, \beta) / \sim$ where*

- T is a cubic ring with nonzero discriminant;

²These are integral models of the associative composition algebras.

- I is an oriented fractional $T \otimes C$ -ideal;
- $\beta \in (T_{\mathbf{Q}})^{\times}$;
- the pair (I, β) is **balanced**.

These data are taken modulo the equivalence \sim , with $(T, I, \beta) \sim (T', I', \beta')$ if there exists $\varphi : T \xrightarrow{\sim} T'$ and $x \in (T' \otimes C_{\mathbf{Q}})^{\times}$ such that $I' = x\varphi(I)$, $\beta' = xx^{\tau}\varphi(\beta)$. Here $\varphi(I)$ means that both the fractional ideal and its orientation are pushed forward via φ .

Our remarks regarding Theorem 1.1.2 are nearly identical to those following Theorem 1.1.1. First, the balanced condition very roughly means that $n_{T_{\mathbf{Q}} \otimes C / T_{\mathbf{Q}}}(I)$ is the principal fractional T -ideal generated by β . See section 3 for the precise condition. Second, the split cases of Theorem 1.1.2, namely when $C = \mathbf{Z}, \mathbf{Z} \times \mathbf{Z}$ and $M_2(\mathbf{Z})$ are the orbit parametrizations of Bhargava from [Bha04b]. When $C = R$ or $R \times R$ is split, but the ground ring \mathbf{Z} has been replaced by a more general ring R , these parametrizations are due to Wood [Woo14]. In fact, when $C = R$ or $R \times R$, Wood considers the orbits of $\mathrm{GL}_n(C)$ on the PVS $R^2 \otimes H_n(C)$ for general n . Next, we again mention that in the text below, we prove Theorem 1.1.2 both uniformly in C and over more general base rings than the integers. The nonsplit cases of Theorem 1.1.2 are new.

As with Theorem 1.1.1, Theorem 1.1.2 is suggested by some of the arguments of [BH16, section 5], which when specialized to degenerate cases should yield a parametrization, over fields, of the orbits considered in Theorem 1.1.2. Again, the arguments suggested by *loc. cit.* are quite different from our own. For the proof of Theorem 1.1.2, we blend twisted versions of constructions in [Bha04b], some ideas from [Woo14], and lifting laws.

As mentioned, one of the key ingredients in the proof of the results above is what we call a *lifting law*, and in fact this paper is as much about lifting laws as it is about the parametrizations Theorem 1.1.1 and Theorem 1.1.2 above. Roughly speaking, a lifting law is a way of “lifting” an element in an orbit of one PVS to an element in the minimal nonzero orbit of another. Since the precise definition of a lifting law and its relevance might seem strange to a non-expert, we defer a discussion of lifting laws to section 2 below. In section 2, we will define precisely what we mean by a lifting law, and also give the motivating examples for this definition.

1.2. Other results. While the main results in this paper are the twisted orbit parametrizations Theorem 1.1.1 and Theorem 1.1.2, we also give a few other results.

First, we use lifting laws to solve the orbit parametrization problems considered in Theorems 1.1.1 and 1.1.2 when the base ring \mathbf{Z} is replaced by a field. This is Theorem 5.2.1 and Theorem 6.2.6 below. These parametrizations when the base ring is a field are due to Wright-Yukie [WY92], Kable-Yukie [KY97], and Taniguchi [Tan08], whose methods are all via Galois cohomology. Of course, the more general form of Theorems 1.1.1 and 1.1.2 proved below covers this case when the base ring is a field. However, the proofs we give in Theorem 5.2.1 and Theorem 6.2.6 are not specializations of the arguments used to prove Theorems 1.1.1 and 1.1.2, and we feel that the arguments we use are sufficiently interesting to merit their inclusion. In any case, several of the technical results used to prove Theorem 5.2.1 and Theorem 6.2.6 are needed in the proof of Theorems 1.1.1 and 1.1.2.

In this context, we also mention two other results, the work of Kato-Yukie [KY16] and the recent National University of Singapore master’s thesis of Tan [Tan16]. Note that, in Theorem 1.1.2 and then again in Theorem 6.2.6, the composition algebra C is associative. In the work [KY16], the authors overcome the difficulty of non-associativity and succeed in parametrizing the orbits on the PVS $H_3(C)^2$ when C is an octonion algebra. Tan, in [Tan16], solves a variant of the orbit problem considered in [KY97]. Tan uses formulas of [Bha04b] to associate a twisted composition algebra to a non-degenerate element $(A, B) \in H_3(K)^2$, where K is a quadratic étale extension of the ground field F . The works of Kato-Yukie [KY16] and Tan [Tan16] associate different (and more interesting) data to elements in $H_3(C)^2$ than we associate to such elements in Theorem 6.2.6.

While in sections 5 and 6 we discuss both lifting laws and their application to arithmetic invariant theory, in sections 7 and 8 we only consider lifting laws. In section 7, we give a lifting law that is a variant of a result of Gan and Savin from [GS14]. See the beginning of section 7 for more details. The lifting laws in sections 5, 6, and 7 start with an element of the open orbit of some prehomogeneous vector space, and lift it to an element of the minimal orbit of another prehomogeneous vector space. In section 8, we consider a few examples of lifting laws where one starts with elements in one of the non-open orbits of a prehomogeneous vector space.

This paper uses various algebraic devices and group representations, such as cubic norm structures, composition algebras, and the Freudenthal construction, with which the reader might not already be familiar. In section 4 we discuss all of this background information. After section 4, the remaining sections are almost entirely self-contained, and only rely on section 4. The exception to this statement is that section 7 also uses results from section 5. Thus after section 4, the other sections may (almost) be read in any order.

We now briefly re-summarize the layout of the paper. In section 2, we define and give an introduction to lifting laws, by way of more familiar examples. In section 3, we give precise statements of our main results on twisted orbit parametrizations, which imply Theorems 1.1.1 and 1.1.2. In section 4, we discuss all the algebraic preliminaries needed for the rest of the paper. In section 5 (resp. section 6) we solve a class of orbit problems that includes those considered in Theorem 1.1.1 (resp. Theorem 1.1.2). In section 7 we give a variant of a result of Gan-Savin from [GS14], while in section 8 we give some “lower rank” lifting laws.

1.3. A note on the proofs. The lifting laws are, in essence, complicated polynomial identities on certain prehomogeneous vector spaces. To prove them, we often make crucial use of prehomogeneity, in the following way. Suppose the vector space V is prehomogeneous for the action of the group G , and suppose P_1, P_2 are polynomial functions $V \rightarrow W$ from V to another G -representation W . To prove $P_1(v) = P_2(v)$ for all $v \in V$, it suffices to prove this equality over an algebraic closure k of F , and then by Zariski density to prove the identity on the open orbit for $G(k)$ on $V(k)$. To prove $P_1 = P_2$ on the open orbit, it then suffices to verify $P_1(v_0) = P_2(v_0)$ for some well-chosen v_0 , and to prove that P_1 and P_2 are suitably equivariant for the action of G . (From the equivariance one obtains $P_1(v) = P_1(gv_0) = gP_1(v_0) = gP_2(v_0) = P_2(v)$.) This sort of argument will be used frequently below without detailed explanation.

1.4. Acknowledgments. We hope it is clear to the reader that this paper owes its existence to the extraordinary papers [Bha04a, Bha04b] of Bhargava. We also single out the beautiful works of Gross-Savin [GS98] and Bhargava-Ho [BH16], from which the author first learned of various exotic algebraic structures and their relevance for automorphic forms and arithmetic invariant theory. It is a pleasure to thank Wee Teck Gan, Benedict Gross, Wei Ho, and Gordan Savin for their very helpful comments on and conversations about an earlier version of this manuscript. We also thank the anonymous referee, whose comments on this paper have (hopefully) significantly improved the exposition, and whose remarks regarding section 7 led to a substantially simpler treatment of the lifting law in this section.

1.5. Notation. Throughout the entire paper, *we only work in characteristic 0*. We will always write F for our ground field, a field of characteristic 0, and R will denote a subring of F . For an R -module M , M_F denotes $M \otimes_R F$. The letter C will always denote a composition algebra over F or R , J will denote a cubic norm structure over F or R , and A will denote a cubic norm structure that is also compatibly an associative F or R -algebra. We write E for a finite étale extension of F , which will always either be a quadratic or cubic extension. We often write S or T for a particular subring of E , that is a finite R -module, although sometimes the letters S and T will have different meanings. The letter k will usually denote an arbitrary field of characteristic 0, often a large extension field of F such as an algebraic closure.

We write V_3 for the defining representation of GL_3 on row or column vectors (depending on the context.) We write V_2 or W_2 for the defining representation of GL_2 on row or column vectors, again depending on context. (In general, we use the notation W_* for vector spaces that come equipped with a symplectic form, and V_* for spaces that do not.)

2. LIFTING LAWS: INTRODUCTION

While this paper is about the results Theorems 1.1.1 and 1.1.2 above, it is also about lifting laws, which is the main technical ingredient that we use to prove these results. The purpose of this section is to give an introduction to lifting laws. We begin by motivating the definition of a lifting law by considering the parametrization of the non-degenerate orbits of $\mathrm{SL}_2(\mathbf{Z})^3$ on $\mathbf{Z}^2 \otimes \mathbf{Z}^2 \otimes \mathbf{Z}^2$ in [Bha04a]. Then, we give the precise definition of a lifting law and mention its connection to the theta correspondence in automorphic forms. Finally, we give two other examples of how lifting laws connect to arithmetic invariant theory: the parametrization of cubic rings by binary cubic forms and the parametrization of quaternion orders by ternary quadratic forms. We remark that subsections 2.1 and 2.3 are more or less special cases of the lifting laws discussed below in sections 5 and 7, respectively.

2.1. Bhargava's cubes and ideal classes in quadratic rings. Consider the parametrization in [Bha04a] of the $G(\mathbf{Z}) = \mathrm{SL}_2(\mathbf{Z}) \times \mathrm{SL}_2(\mathbf{Z}) \times \mathrm{SL}_2(\mathbf{Z})$ orbits on the non-degenerate elements of $V(\mathbf{Z}) = \mathbf{Z}^2 \otimes \mathbf{Z}^2 \otimes \mathbf{Z}^2$. Recall that the parametrization given in [Bha04a] is in terms of quadratic rings $S = \mathbf{Z}[\tau]$ and a balanced triple (I_1, I_2, I_3) of fractional S -ideals. That the triple (I_1, I_2, I_3) is balanced³ means that the product of the ideals $I_1 I_2 I_3$ is contained in S , and the product of the norms of the ideals $N(I_1)N(I_2)N(I_3) = 1$.

Denote by e_1, f_1 a basis for the first copy of \mathbf{Z}^2 in $V(\mathbf{Z})$, and similarly e_2, f_2 , and e_3, f_3 bases for the second and third copy of \mathbf{Z}^2 in $V(\mathbf{Z})$. Suppose one is given a balanced triple (I_1, I_2, I_3) of fractional S -ideals. Choose a \mathbf{Z} -basis α_1, β_1 for I_1 , α_2, β_2 for I_2 , and α_3, β_3 for I_3 . Then associated to this data, one considers the pure tensor

$$(1) \quad (\alpha_1 e_1 + \beta_1 f_1) \otimes (\alpha_2 e_2 + \beta_2 f_2) \otimes (\alpha_3 e_3 + \beta_3 f_3)$$

in $V(\mathbf{Z}) \otimes S_{\mathbf{Q}}$. Since the triple (I_1, I_2, I_3) is balanced, all the products $\alpha_1 \alpha_2 \alpha_3$, $\alpha_1 \alpha_2 \beta_3$, $\alpha_1 \beta_2 \alpha_3$ etc are in S . Hence, there exists v and v_0 in $V(\mathbf{Z})$ so that

$$(2) \quad (\alpha_1 e_1 + \beta_1 f_1) \otimes (\alpha_2 e_2 + \beta_2 f_2) \otimes (\alpha_3 e_3 + \beta_3 f_3) = \tau v + v_0 \in V(\mathbf{Z}) \otimes_{\mathbf{Z}} S = \tau V(\mathbf{Z}) \oplus V(\mathbf{Z}).$$

The parametrization of the $G(\mathbf{Z})$ orbits on $V(\mathbf{Z})$ in [Bha04a] proceeds through this construction: one associates to the balanced triple (I_1, I_2, I_3) the $G(\mathbf{Z})$ -orbit $G(\mathbf{Z})v$.

To have the possibility of parametrizing the orbits of $G(\mathbf{Z})$ on $V(\mathbf{Z})$ via triples of balanced ideals, one must be able to invert this construction. Thus given $v \in V(\mathbf{Z})$, one asks the following question: Does there exist a quadratic ring $S = \mathbf{Z}[\tau]$, and $v_0 \in V(\mathbf{Z})$, so that $\tilde{v} = \tau v + v_0$ is explicitly given as a pure tensor in

$$V'(\mathbf{Q}) := V(\mathbf{Q}) \otimes_{\mathbf{Q}} S_{\mathbf{Q}} \approx V(\mathbf{Q}) \oplus V(\mathbf{Q})?$$

Answering this question is the many equations that must be solved on page 235 of *loc. cit.*, and is a crucial step in the argument.

Set $G' = \mathrm{SL}_2(S_{\mathbf{Q}}) \times \mathrm{SL}_2(S_{\mathbf{Q}}) \times \mathrm{SL}_2(S_{\mathbf{Q}})$, which then acts on V' . Suppose S and v_0 are such that $\tilde{v} = \tau v + v_0$ is a pure tensor in V' . Because \tilde{v} is a pure tensor in V' , the stabilizer in G' of the line $S_{\mathbf{Q}}\tilde{v}$ is a parabolic subgroup of G' . Thus, another way of phrasing this question is the following: Given $v \in V(\mathbf{Q})$, does there exist a quadratic extension $S_{\mathbf{Q}}$ of \mathbf{Q} and a $v_0 \in V_0(\mathbf{Q}) = V(\mathbf{Q})$ so that the stabilizer of the line $\mathbf{Q}\tilde{v}$ in $V'(\mathbf{Q})$ is (essentially) a parabolic subgroup of G' ? More informally,

³More generally, if $\beta \in (S_{\mathbf{Q}})^{\times}$, and (I_1, I_2, I_3) are a triple of fractional S -ideals, one says that the data $((I_1, I_2, I_3), \beta)$ is balanced if $I_1 I_2 I_3 \subseteq \beta S$ and $N(I_1)N(I_2)N(I_3) = N(\beta)$.

can the element $v \in V(\mathbf{Q})$ be “lifted” to a pure tensor \tilde{v} in $V'(\mathbf{Q})$? This discussion motivates the definition of a lifting law, which we now give.

2.2. Definition of lifting law. Suppose that F is a field, (G, V) is a PVS over F , and $v \in V(F)$ is not 0.

Definition 2.2.1. A lifting law for G, V and v is the data of another finite-dimensional F -linear G -representation V_0 , an element $v_0 \in V_0$, and an action of a (bigger) linear algebraic F -group G' on $V' = V \oplus V_0$ so that

- (1) the G -linear action on $V' = V \oplus V_0$ factors through G' ,
- (2) the stabilizer S in G' of the line $F\tilde{v}$, where $\tilde{v} = (v, v_0)$, satisfies $P' \supseteq S \supseteq [P', P']$, where P' is a parabolic subgroup of G' .

The second condition roughly means that $\tilde{v} = (v, v_0)$ is in the minimal nonzero orbit of G' on V' . Note that in the definition, the data (G', V', v_0) , and in particular the group G' , depends on the element $v \in V(F)$.

The sort of lifting problem considered in Definition 2.2.1 is familiar from the theta correspondence, especially in the context of exceptional groups. In this setting, the above lifting problem arises when computing the restriction of a theta function on one group G'_1 to a smaller group G_1 . The reader may see, for instance, work of Gross-Savin [GS98], Gan [Gan00a, Gan08], Lucianovic [Luc03], or Weissman [Wei06] for some examples of these computations.

As a simple example of a lifting law, suppose q is a non-degenerate quadratic form on the vector space V , $G = \mathrm{SO}(V, q)$ is the special orthogonal group preserving this quadratic form, and $v \in V$ satisfies $q(v) = \alpha \neq 0$. Set $V_0 = F$, the trivial representation of G , with quadratic form $q_0(x) = \alpha x^2$. Put on $V' = V \oplus V_0$ the quadratic form $q' = q \perp (-q_0)$, i.e., $q'((x, x_0)) = q(x) - \alpha x_0^2$ for $x \in V$ and $x_0 \in V_0$. With this quadratic form, V' becomes a representation of the group $G' = \mathrm{SO}(V', q')$, and it is clear that the $G = \mathrm{SO}(V, q)$ -action on V' preserves q' , and thus factors through the bigger orthogonal group G' . Furthermore, the lifted vector $\tilde{v} = (v, 1)$ satisfies $q'(\tilde{v}) = 0$, and thus the stabilizer of the line $F\tilde{v}$ is a parabolic subgroup of G' . Thus the association of V', q' and \tilde{v} to the vector $v \in V$ is a lifting law.

Observe that in the situation of the previous paragraph, the orbits of $G = \mathrm{SO}(V, q)$ on $V \setminus \{0\}$ are parametrized by the value of the quadratic form q , i.e., $v_1 = gv_2$ for some $g \in \mathrm{SO}(V, q)$ if and only if $q(v_1) = q(v_2)$. Furthermore, it is the value of q on v that is the key input into the definition of the quadratic form q' on V' that enables one to lift v to an isotropic vector \tilde{v} in V' . Thus this lifting law for orthogonal groups has something to do with the invariant theory of $\mathrm{SO}(V, q)$ acting on its defining representation V .

In fact, lifting laws are connected to many problems in arithmetic invariant theory, and are no doubt recognizable to experts in this context as well. To make clear the ideas, we now give two more “classical” examples of lifting laws.

2.3. Binary cubic forms and cubic rings. Recall that classically, binary cubic forms parametrize cubic rings. This parametrization goes back at least to [DF64]. In this subsection, we briefly give the example of the lifting law that is related to this parametrization. The example in this subsection is essentially from [GGJ02, Lemma 3.3] or [Gan00b, Proposition 6.9], but see also [HMS98] and [GS98].

Consider the action of $G = \mathrm{GL}_2(F)$ on the space $V = \mathrm{Sym}^3(F^2) \otimes \det^{-1}$ of binary cubic forms $q(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$. Here the action is given by $(q \cdot g)(x, y) = \det(g)^{-1}q(g(x, y)^t)$. As is well-known, the orbits of this action parametrize cubic F -algebras L , and the parametrization works over the integers and not just fields. See for instance [GGS02] or [Bha04b]. The R -algebra T associated to the binary cubic form q is specified by saying it has basis $1, \omega, \theta$, with multiplication table

$$(3) \quad \omega\theta = -ad; \quad \omega^2 = -ac + a\theta - b\omega; \quad \theta^2 = -bd + c\theta - d\omega.$$

Conversely, if T is a cubic ring over the integral domain R , and $1, \omega, \theta$ is a basis of T as a free R -module of rank three, as in [GGJ02, GL09] one says that $(1, \omega, \theta)$ is a *good basis* if $\omega\theta \in R$. One can then show that there exists $a, b, c, d \in R$ so that ω, θ obey the above multiplication table.

From the point of view of cubic rings, the multiplication table (3) is perhaps a little mysterious. However, from the point of view of lifting laws, this multiplication can be understood conceptually. Suppose T is a cubic ring over R and $L = T_F$ is étale over F . As mentioned in the introduction, there is a cubic polynomial action of $\mathrm{GL}_2(L)$ on $V' := W_L = F \oplus L \oplus L \oplus F$. Set $G' = \{g \in \mathrm{GL}_2(L) : \det(g) \in F^\times\}$, and let G' act on V' by $vg = \det(g)^{-1}v \cdot g$, where $v \cdot g$ is the cubic polynomial action of $\mathrm{GL}_2(L)$ on W_L .

The following claim is essentially [GGJ02, Lemma 3.3] or [Gan00b, Proposition 6.9].

Claim 2.3.1. *Suppose that there exists a, b, c, d so that ω, θ obey the multiplication table (3). Then the stabilizer of the line $F(a, -\omega, \theta, d) \subseteq V'$ in G' is a parabolic subgroup of G' . Conversely, suppose there exists $a, d \in F$ so that the stabilizer of the line $F(a, -\omega, \theta, d) \subseteq V'$ in G' is a parabolic subgroup of G' . Set $b = \mathrm{tr}_{L/F}(-\omega)$ and $c = \mathrm{tr}_{L/F}(\theta)$. Then ω, θ obey the multiplication table (3).*

The claim suggests that good bases for cubic rings may be understood conceptually in terms of lifting laws. To make this precise, set $V_0 = M_2(F)$ the 2×2 matrices over F , with $G = \mathrm{GL}_2(F)$ action given by right translation: $m \cdot g = mg$ if $m \in M_2(F)$ and $g \in \mathrm{GL}_2(F)$. Then, $G \subseteq G'$, and as a G -module, $V' \simeq V \oplus V_0$. Furthermore, one can choose this isomorphism of G -modules so that

$$\tilde{v} := (a, -\omega, \theta, d) \mapsto (v, v_0) = (ax^3 + bx^2y + cxy^2 + dy^3, 1_2) \in V \oplus V_0.$$

Thus, finding a good basis for the cubic ring T is the same as finding $\tilde{v} = (v, v_0) \in V \oplus V_0 \simeq V'$ with the line $F\tilde{v}$ in V' stabilized by a parabolic subgroup of G' . Thus the association of cubic rings with binary cubic forms is closely connected to a lifting law.

The above lifting law is used in an automorphic setting in, for instance, [Gan00b] and [GGJ02]. Implicit in [GS14] is a generalization of the above lifting law, and in section 7 below we give a further extension of this lifting law.

2.4. Ternary quadratic forms and quaternion orders. As is well-known, ternary quadratic forms $q(x, y, z) = ax^2 + by^2 + cz^2 + dyz + ezx + fxy$, modulo the action of GL_3 , parametrize quaternion algebras up to isomorphism. When the coefficients of the ternary quadratic form a, b, c, d, e, f are in some ring R as opposed to a field, the orbits of $\mathrm{GL}_3(R)$ on them parametrize quaternion orders over R ; see [GL09] and [Voi11].

As with the case of binary cubic forms and cubic rings, the parametrization of quaternion orders over R by ternary quadratic forms uses the notion of a *good basis*. More precisely, suppose $q(x, y, z)$ is a ternary quadratic form, as above. As always, assume R is an integral domain with fraction field F of characteristic 0. Let GL_3 act on the right of ternary quadratic forms via $(q \cdot g)(x, y, z) = \det(g)q({}^t g^{-1}(x, y, z)^t)$ for $g \in \mathrm{GL}_3(R)$. One associates to $q(x, y, z)$ a quaternion order Q over R with basis $1, v_1, v_2, v_3$, as follows. First, denote by e_1, e_2, e_3 the standard basis of $V_3 = R^3$ (row vectors). We have a quadratic form q on V_3 via $q(xe_1 + ye_2 + ze_3) = q(x, y, z)$, for x, y, z in R . Set $Q = \mathrm{Clif}^+(V_3, q)$, the even part of the Clifford algebra associated to (V_3, q) , and $v_1 = e_2e_3, v_2 = e_3e_1, v_3 = e_1e_2$. Then Q is a quaternion order over R , and the basis v_1, v_2, v_3 satisfies the multiplication table

$$\begin{aligned} v_2v_3 &= av_1^*; \\ v_3v_1 &= bv_2^*; \\ v_1v_2 &= cv_3^* \\ (4) \quad v_1v_1^* &= bc; v_2v_2^* = ca; v_3v_3^* = ab. \end{aligned}$$

Here $*$ is the involution on Q .

Conversely, if Q is a quaternion order over R (assumed to be free of rank 4 over R), and $1, v_1, v_2, v_3$ is a basis of Q as a free R -module, one says that (v_1, v_2, v_3) is a *good basis* (see [GL09]) if there exist $a, b, c \in R$ so that the v_i obey the multiplication table above. Then every quaternion ring Q over R admits a good basis [GL09], and their parametrization through ternary quadratic forms in *loc. cit.* proceeds through the use of good bases.

Good bases for quaternion orders are closely connected to a lifting law. Namely, set $G = \mathrm{GL}_3$, $V = \mathrm{Sym}^2(V_3)^\vee \otimes \det = H_3(F)$, so that elements $v \in V(F)$ correspond to ternary quadratic forms. Here we have identified $\mathrm{Sym}^2(V_3)^\vee$ with $H_3(F)$, the Hermitian 3×3 matrices over the constant associative composition algebra F . The implied action of $\mathrm{GL}_3(F)$ on $H_3(F)$ is $h \cdot g = \det(g)g^{-1}h^t g^{-1}$. The pair (G, V) is a PVS. If $v \in V^{open}$ corresponds to the quaternion algebra Q_F , set $V' = H_3(Q_F)$ and define $G' = \{(\delta, m) \in \mathrm{GL}_1(F) \times \mathrm{GL}_3(Q_F) : \delta^2 = N_6(m)\}$. Here $N_6(m)$ is the degree six reduced norm on $M_3(Q_F)$, and G' acts on $H_3(Q_F)$ via $h \mapsto \delta m^{-1} h^* m^{-1}$. Clearly $V \hookrightarrow V'$, and as a representation of $\mathrm{GL}_3(F)$, $V' = V \oplus V_0$, where $V_0 = M_3(F)$ with $\mathrm{GL}_3(F)$ action given by right translation, $m \mapsto mg$.

Now, suppose $q(x, y, z) = ax^2 + by^2 + cz^2 + dyz + ezx + fxy$ is as above. As an element of $H_3(F)$, $q(x, y, z)$ corresponds to

$$v = \begin{pmatrix} a & \frac{f}{2} & \frac{e}{2} \\ \frac{f}{2} & b & \frac{d}{2} \\ \frac{e}{2} & \frac{d}{2} & c \end{pmatrix}.$$

Suppose (v_1, v_2, v_3) is the good basis of the quaternion algebra Q corresponding to $q(x, y, z)$, so that the v_i satisfy the multiplication table (4). Define

$$\tilde{v} = \begin{pmatrix} a & v_3 & v_2^* \\ v_3^* & b & v_1 \\ v_2 & v_1^* & c \end{pmatrix},$$

so that $\tilde{v} \in H_3(Q_F)$. Then the stabilizer of the line $F\tilde{v}$ in G' is a parabolic subgroup of G' . In terms of the decomposition $V' = V \oplus V_0 \simeq H_3(F) \oplus M_3(F)$, one can choose this isomorphism so that $\tilde{v} = (v, v_0)$, with $v_0 = 1_3 \in M_3(F)$. Thus good bases in the setting of quaternion orders naturally correspond to lifting laws.

We remark that an application of this correspondence to automorphic forms is given in [Luc03]. For the reader familiar with Tits' so-called second construction of cubic norm structures, the above decomposition $H_3(Q) = H_3(F) \oplus M_3(F)$ is a special case of this. In fact, quite generally, Tits' construction can be regarded as a lifting law.

3. STATEMENT OF TWISTED ORBIT PARAMETRIZATIONS

In the introduction, we gave rough statements of the main results Theorem 1.1.1 and Theorem 1.1.2. The purpose of this section is to give precise statements of the more general versions of these results that we prove below. The proofs will be given in subsections 5.3 and 6.3, once the relevant lifting laws and necessary technical facts have been proved. In the first part of this section, we discuss Theorem 1.1.1, while in the second part of this section we discuss Theorem 1.1.2.

3.1. Twisted orbit parametrization yielding quadratic rings. In this subsection we assume R is an integral domain, with fraction field F of characteristic 0. We will shortly insist that R satisfies an additional property, but for now we only assume these properties of R .

3.1.1. Algebraic preliminaries. The first parametrization theorem concerns the nondegenerate orbits of $\mathrm{GL}_2(A)$ on $W_A = R \oplus A \oplus A \oplus R$, for certain R -algebras A . We begin by describing which R -algebras A are considered. We introduce one non-standard piece of terminology.

Definition 3.1.1. Suppose A is an associative F -algebra. We say that a pair $(A, n_A : A \rightarrow F)$ is an **associative cubic norm structure** (ACNS) over F if it is one of the following:

- (1) $A = F$, with $n_A : F \rightarrow F$ given by $x \mapsto x^3$;
- (2) $A = F \times F$, with $n_A : F \times F \rightarrow F$ given by $(x, y) \mapsto xy^2$;
- (3) $A = E$, where E is a cubic étale extension of F , with $n_A = n_{E/F} : E \rightarrow F$ the usual degree three norm map;
- (4) $A = F \times Q$, where Q is a quaternion F -algebra, with $n_A : F \times Q \rightarrow F$ given by $(x, y) \mapsto xn_{Q/F}(y)$ where $n_{Q/F} : Q \rightarrow F$ is the (degree two) reduced norm map;
- (5) A a central simple F algebra of degree 3, with $n_A : A \rightarrow F$ the (degree three) reduced norm map.

When $R = F$ is a field, these are the set of R -algebras that will be considered in the orbit parametrizations.

In all of the cases above, there is a quadratic polynomial map $\# : A \rightarrow A$, which we write $y \mapsto y^\#$, that is uniquely determined by the property $y^\# = n_A(y)y^{-1}$ when y is invertible. This map is called the *adjoint*. To state the explicit orbit parametrization Theorem 3.1.7 below (and for nearly everything else besides), we will need to use this adjoint map. To see that $y \mapsto n_A(y)y^{-1}$ extends to a polynomial map on all of A , one need only verify this when A is split. In these cases, the adjoint map is given by the following rule in each of the cases above:

- (1) $A = F$, with $x^\# = x^2$;
- (2) $A = F \times F$, with $(x, y)^\# = (y^2, xy)$
- (3) $A = F \times F \times F$, with $\#$ the map $(\lambda_1, \lambda_2, \lambda_3) \mapsto (\lambda_2\lambda_3, \lambda_3\lambda_1, \lambda_1\lambda_2)$.
- (4) $A = F \times Q$, where Q is a quaternion F -algebra, with $(x, y)^\# = (n_Q(y), xy^*)$. Here n_Q is the degree two reduced norm map on Q , and y^* the conjugate of $y \in Q$, so that $yy^* = n_Q(y)$ for all $y \in Q$.
- (5) $A = M_3(F)$, with $x \mapsto x^\#$ the adjoint map on 3×3 matrices.

There is an analogous notion of an associative cubic norm structure over R .

Definition 3.1.2. Suppose A is an associative R -algebra, that is free of finite rank over R . We say a pair $(A, n_A : A \rightarrow R)$ is an **associative cubic norm structure** over R if $A_F = A \otimes_R F$, with the induced $n_{A_F} : A_F \rightarrow F$, is an ACNS over F , and $y^\# \in A \subseteq A_F$ for all $y \in A$.

For the rest of this subsection, A denotes⁴ an ACNS over R . For such an A , the algebra $M_2(A)$ has a degree 6 (reduced) norm map $\det_6 : M_2(A) \rightarrow R$, with $\mathrm{GL}_2(A)$ being the preimage of R^\times . One can define a cubic polynomial action of $\mathrm{GL}_2(A)$ on the R -module $W_A := R \oplus A \oplus A \oplus R$, which will be discussed in detail in subsection 4.4. As mentioned in the introduction, this action makes $W_A \otimes_R F$ a PVS for the action of $\mathrm{GL}_2(A_F)$.

There is a quartic form $q : W_A \rightarrow R$, whose definition is essentially due to Freudenthal. The action of $\mathrm{GL}_2(A_F)$ on W_{A_F} preserves this quartic form, up to scaling: $q(v \cdot g) = \det_6(g)^2 q(v)$, where $\det_6 : \mathrm{GL}_2(A_F) \rightarrow F^\times$ is the degree 6 (reduced) norm map. The open orbit $W_{A_F}^{\mathrm{open}}$ for the action of $\mathrm{GL}_2(A_F)$ consists of those $v \in W_{A_F}$ with $q(v) \neq 0$.

3.1.2. Orbit problem. We now begin the description of the orbit problem. We will parametrize the orbits of a certain group G on W_A^{open} in terms of quadratic rings S over R and certain $S \otimes A$ -modules.

To define the group G , set $G_1 = \mathrm{GL}_1(R) \times \mathrm{GL}_2(A)$. Let $(\lambda, g) \in \mathrm{GL}_1(R) \times \mathrm{GL}_2(A)$ act on $v \in W_A$ by $v \mapsto \lambda^{-1}(v \cdot g)$. Define $G \subseteq G_1$ to consist of the pairs (λ, g) where $\lambda^3 = \det_6(g)$. The group G acts on W_A by the restriction of the G_1 action.

We now briefly discuss quadratic rings S over R . For the rest of this subsection, we will additionally assume that the ring R satisfies $\frac{x^2+x}{2}$ is in R for all $x \in R$. For such a ring, every quadratic ring S over R , i.e., every commutative R -algebra that is free of rank two over R , is of the form $S = S_D = R[y]/(y^2 - Dy + \frac{D^2-D}{4})$, where D is congruent to a square modulo $4R$. If S is a

⁴The reader unfamiliar with cubic norm structures might take $R = \mathbf{Z}$ and A an order in a degree three field extension of \mathbf{Q} to get a sense for the definitions and constructions below.

quadratic ring over R , and $(1, \tau)$ is a basis of S , we say that $(1, \tau)$ is a *good basis* of S if τ satisfies a quadratic equation $\tau^2 - D\tau + \frac{D^2-D}{4}$ for some $D \in R$ (necessarily a square modulo $4R$). We write $E := S_D \otimes_R F = F[y]/(y^2 - D)$, and denote by ω the image of y in E .

3.1.3. Balanced modules. As mentioned, the orbits of G on W_A will be parametrized in terms of certain $S \otimes A$ modules. To describe which modules show up, we need to make a few definitions. We consider a class of $S_D \otimes_R A = S \otimes_R A$ modules $I \subseteq A_E$ as follows.

Definition 3.1.3. If $I \subseteq E \otimes A$, we say that I is an $S \otimes A$ -fractional ideal if

- I is closed under left multiplication by S and right multiplication by A ;
- I is free of rank 2 as an A -module;
- $I_F = E \otimes A$ is free of rank one as an A_E -module.

If a fractional $S \otimes A$ -ideal I comes equipped with an A -basis, $I = b_1A \oplus b_2A$, we may define its norm as follows.

Definition 3.1.4. Suppose $(\tau, 1)$ is a good basis of S , and $I = b_1A \oplus b_2A$, with $b_1, b_2 \in E \otimes A$. Then, there is a unique $g \in M_2(A_F)$ so that $(b_1, b_2) = (\tau \otimes 1, 1 \otimes 1)g$. Define the **norm** of the data $(I, (b_1, b_2))$ as $N(I; \tau, (b_1, b_2)) = \det_6(g)$ where g is as above. Concretely, if $b_1 = \tau \otimes m_{11} + 1 \otimes m_{21}$ and $b_2 = \tau \otimes m_{12} + 1 \otimes m_{22}$, with $m_{ij} \in A_F$, then the norm $N(I; \tau, (b_1, b_2))$ is defined to be $\det_6\left(\begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}\right)$. The norm of I depends on the data τ, b_1, b_2 .

The orbits of G on W_A^{open} will be parametrized by what are called *balanced* fractional $S \otimes A$ -ideals. To define the notion of balanced, and to then state the explicit bijection Theorem 3.1.7 below, we need to define a certain cubic polynomial map $! : A^2 \rightarrow W_A$. Thus suppose $(x, y) \in A^2$. Associated to the pair (x, y) is the element

$$(5) \quad (x, y)! := (n_A(x), x^\#y, y^\#x, n_A(y)) \in W_A.$$

Note that if $a \in A$, then $(ax, ay)! = n_A(a)(x, y)! \in W_A$. The fact that W_A receives a cubic polynomial map from A^2 with this property is the sense that in which W_A can be thought of as twisted symmetric cube representation of $\mathrm{GL}_2(A)$.

One always has $q((x, y)!) = 0$, and in fact, $(x, y)!$ is in the minimal nonzero orbit for the action $\mathrm{GL}_2(A_F)$ on W_{A_F} . Base-changing the map (5) from A to A_E , one obtains a map $! : A_E^2 \rightarrow W_A \otimes E$ given by the same formula as in (5).

We can now define the notion of a balanced fractional $S \otimes A$ -ideal.

Definition 3.1.5. Suppose $\beta \in E^\times$, and I is an $S \otimes A$ -fractional ideal with A -basis b_1, b_2 , and $\tau \in S$ is such that $(\tau, 1)$ is a good basis of S . We say the data $(I, (b_1, b_2), \tau, \beta)$ is **balanced** if

$$(6) \quad \beta^{-1}(x, y)! = \beta^{-1}(n_{A_E}(x), x^\#y, y^\#x, n_{A_E}(y)) \in W_A \otimes S \subseteq W_A \otimes E$$

for all $x, y \in I$ and if $N(I; \tau, (b_1, b_2)) = N_{E/F}(\beta)$. Here n_{A_E} denotes the E -linear extension of $n_A : A \rightarrow F$ to $n_{A_E} : A_E \rightarrow E$.

The condition $\beta^{-1}(x, y)! \in W_A \otimes S$ for all $x, y \in I$ implies that $n_{A_E}(x) \in \beta S$ for all $x \in I$. When $A = R \times R \times R$, $R \times M_2(R)$, and $M_3(R)$, the condition $n_{A_E}(x) \in \beta S$ for all $x \in I$ is in fact equivalent to the condition (6).

It is a fact that $\beta^{-1}(x, y)! \in W_A \otimes S$ for all $x, y \in I$ if and only if $\beta^{-1}(b_1, b_2)! \in W_A \otimes S$. Suppose that I is a fractional $S \otimes A$ -ideal, with A -basis $b = (b_1, b_2)$, and $\beta \in E^\times$. Set

$$X(I, b, \beta) := \beta^{-1}b! \in W_{A_E} = W_A \otimes_R E.$$

The element $X(I, b, \beta)$ is the analogue of the pure tensor in (1).

Finally, we define an equivalence relation on data (I, b, β) .

Definition 3.1.6. The triple (I, b, β) is said to be *equivalent* to the triple (I', b', β') if there exists $x \in A_E^\times$ so that $I' = xI$, $b' = xb$, and $\beta' = n_{A_E}(x)\beta$. We write $[(I, b, \beta)]$ for the associated equivalence class.

The non-degenerate orbits of G on W_A will be parametrized in terms of equivalence classes of balanced data (I, b, β) .

3.1.4. The explicit bijection. Suppose that $\tau, 1$ is a good basis for S and that (I, b, β) is a balanced fractional $S \otimes A$ -ideal. Then there are $v, v' \in W_A$ so that $\beta^{-1}b' = X(I, b, \beta) = \tau v + v' \in W_A \otimes S$. One thus obtains a map from balanced data (I, b, β) to $v \in W_A$:

$$(I, b, \beta) \mapsto X(I, b, \beta) = \tau v + v' \mapsto v \in W_A.$$

Note the similarity of this map with those in [Bha04a] and the construction of subsection 2.1. It will be checked below that the v so obtained is in W_A^{open} . We can now state the parametrization theorem.

Theorem 3.1.7. *The map $(I, (b_1, b_2), \tau, \beta) \mapsto v$ induces a bijection between $v \in W_A$ with $q(v) = D \neq 0$ and balanced data $(I, (b_1, b_2), \tau, \beta)$ up to equivalence, with $\tau^2 - D\tau + \frac{D^2 - D}{4} = 0$. This bijection is equivariant for the action of the group G , with $(\lambda, g) \in G$ acting on the data $((b_1, b_2), \omega, \beta)$ by*

$$[((b_1, b_2), \omega, \beta)] \mapsto [((b_1, b_2)g, \lambda\omega, \beta)].$$

Here $[((b_1, b_2), \tau, \beta)]$ means that the data is taken up to equivalence.

Note that Theorem 3.1.7 implies Theorem 1.1.1 of the introduction, by restricting to the action of $\mathrm{SL}_2(A) \subseteq G$. Below we will also describe explicitly the inverse map $v \mapsto [(I, (b_1, b_2), \tau, \beta)]$. This will involve producing the element $X = \tau v + v'$ from the element $v \in W_A$, which will be the lifting law in this context.

3.2. Twisted orbit parametrization yielding cubic rings. In this subsection we assume R is an integral domain, with fraction field F of characteristic 0. (We no longer assume $x^2 + x \in 2R$ for all $x \in R$.) We will state a precise and more general version of Theorem 1.1.2 of the introduction. This theorem will parametrize the non-degenerate orbits of (essentially) $\mathrm{GL}_2(R) \times \mathrm{GL}_3(C)$ on $H_3(C)^2 = R^2 \otimes H_3(C)$, for an associative composition ring C . The orbits will be parametrized in terms cubic R -algebras T and certain $T \otimes C$ -modules. We discuss each of these pieces in turn: composition rings, the module $H_3(C)$, cubic R -algebras, and the $T \otimes C$ -modules that arise.

3.2.1. Composition rings. We begin by discussing associative composition algebras.

Definition 3.2.1. Suppose C is an associative F -algebra. We say that $(C, n_C : C \rightarrow F)$ is an **associative composition algebra** (ACA) if C is one of the following:

- (1) $C = F$, with $n_C : F \rightarrow F$ given by $x \mapsto x^2$;
- (2) $C = E$, with E a quadratic étale extension of F , and $n_C = n_{E/F} : E \rightarrow F$ the (degree two) norm map;
- (3) C is a quaternion F -algebra, with $n_C : C \rightarrow F$ the (degree two) reduced norm map.

If C is such an F -algebra, then C has the standard involution $\sigma : C \rightarrow C$ that satisfies $n_C(x) = x\sigma(x)$. If C is an associative R -algebra, that is free of finite rank as an R -module, then we say that $(C, n_C : C \rightarrow R)$ is an ACA over R if $(C_F, n_{C_F} : C_F \rightarrow F)$ is an ACA over F and C is stable under the involution σ on C_F .

Throughout the rest of this subsection, C will denote⁵ an ACA over R . We set $H_3(C) = \{h \in M_3(C) : h^* = h\}$ the Hermitian 3×3 matrices with coefficients in C . Here $*$: $M_3(C) \rightarrow M_3(C)$ is

⁵The reader may wish to take $R = \mathbf{Z}$ and C an order in a quadratic extension of \mathbf{Q} to get a sense for the definitions and constructions below.

$x \mapsto {}^t x^\sigma$, the transpose conjugate. In coordinates, $H_3(C)$ consists of the elements

$$\begin{pmatrix} c_1 & a_3 & a_2^\sigma \\ a_3^\sigma & c_2 & a_1 \\ a_2 & a_1^\sigma & c_3 \end{pmatrix}$$

with $c_1, c_2, c_3 \in R$ and $a_1, a_2, a_3 \in C$. There is an action of $\mathrm{GL}_3(C)$ on $H_3(C)$ via $h \cdot m = m^* h m$, for $h \in H_3(C)$ and $m \in \mathrm{GL}_3(C)$. From now on, we will often abuse notation and write $*$, instead of σ , for the involution on C .

3.2.2. Binary cubic forms and cubic rings. We now give various facts and reminders that concern the relationship between binary cubic forms and cubic rings. See, for instance, [GGS02] (and also subsection 4.1.3) for more details.

Suppose we have the binary cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ with a, b, c, d in the base ring R . The based cubic R -algebra T determined by f is a free R -module of rank 3, with basis $1, \omega, \theta$. The multiplication table in T is

- $\omega\theta = -ad$;
- $\omega^2 = -ac + a\theta - b\omega$;
- $\theta^2 = -bd + c\theta - d\omega$.

Denote $L = T \otimes_R F$, and set $\omega_0 = \omega + \frac{b}{3}$ and $\theta_0 = \theta - \frac{c}{3}$, so that $\mathrm{tr}_{L/F}(\omega_0) = \mathrm{tr}_{L/F}(\theta_0) = 0$. The basis $(1, \omega, \theta)$ of T is called a *good basis*.

3.2.3. Orbit problem. For the rest of this subsection, R, F and C will be as above. The letter T will denote a cubic ring over R , and $L = T \otimes_R F$.

Set $G_1 = \mathrm{GL}_1(R) \times \mathrm{GL}_2(R) \times \mathrm{GL}_3(C)$, which acts on the right of $V := V_2(R) \otimes H_3(C)$. Here $V_2(R) = R^2$ is the row vectors with coefficients in R and the action of GL_2 action is the usual right action of matrices on row vectors. The group $\mathrm{GL}_3(C)$ acts on the right of $H_3(C)$ by $h \mapsto m^* h m$ for $h \in H_3(C)$ and $m \in \mathrm{GL}_3(C)$. Finally, $\lambda \in \mathrm{GL}_1(R)$ acts on V by scaling by λ . We denote by $G \subseteq G_1$ the group of triples $(\lambda, g, m) \in \mathrm{GL}_1(R) \times \mathrm{GL}_2(R) \times \mathrm{GL}_3(C)$ with $\lambda = \det(g)^{-1}$ and $\det(g)^2 = N_6(m)$, where $N_6(m)$ is the degree 6 reduced norm on $M_3(C)$. Then G also acts on V by restriction of the action of G_1 . One has that the pair $(G(F), V(F))$ is a PVS. We will consider the orbits of G on V^{open} .

3.2.4. Balanced modules. Let $C_L = C \otimes_R L$. We consider $T \otimes C$ submodules $I \subseteq L \otimes C$. We make a few definitions.

Definition 3.2.2. If $I \subseteq L \otimes C$. We say I is a $T \otimes C$ -fractional ideal if

- I is closed under left multiplication by T and right multiplication by C ;
- I is free of rank 3 as a C -module;
- $I \otimes_R F$ is free of rank one as an $L \otimes C$ -module.

Definition 3.2.3. Suppose I is a $T \otimes C$ fractional ideal, and b_1, b_2, b_3 is an ordered basis of I i.e., that $I = b_1 C + b_2 C + b_3 C$ inside $L \otimes C$, where b_1, b_2, b_3 are in $L \otimes C$. Then $(b_1, b_2, b_3) = (1 \otimes 1, \omega \otimes 1, \theta \otimes 1)g$ for some unique $g \in M_3(C_F)$. We define the norm of the ideal I , $N(I; (b_1, b_2, b_3); (1, \omega, \theta))$, with respect to the data (b_1, b_2, b_3) and $(1, \omega, \theta)$ to be $N_6(g)$. Of course, this norm depends on the choice of the good basis $(1, \omega, \theta)$ and the choice of ordered basis (b_1, b_2, b_3) .

We now define when the based fractional ideal $I, (b_1, b_2, b_3)$ is balanced.

Definition 3.2.4. Suppose $\beta \in L^\times$, and the good basis $(1, \omega, \theta)$ of T is fixed. The data $((I, (b_1, b_2, b_3)), \beta)$ is said to be **balanced** if $y^\sigma x \in \beta C \otimes_R T$ for all x, y in I and $N((I, (b_1, b_2, b_3))) = N_{L/F}(\beta)$. Here $\sigma : L \otimes C \rightarrow L \otimes C$ is the L -linear extension of $\sigma : C \rightarrow C$.

Set $b = (b_1, b_2, b_3) \in (C_L^3)$, a row vector. If $I = b_1C + b_2C + b_3C$ and $\beta \in L^\times$, we set $X_{I,b,\beta} = \beta^{-1}b^*b \in H_3(C) \otimes T = H_3(C_T)$. In coordinates,

$$X_{I,b,\beta} = \beta^{-1}b^*b = \beta^{-1} \begin{pmatrix} n_C(b_1) & b_1^*b_2 & b_1^*b_3 \\ b_2^*b_1 & n_C(b_2) & b_2^*b_3 \\ b_3^*b_1 & b_3^*b_2 & n_C(b_3) \end{pmatrix}.$$

One sees easily that $X_{I,b,\beta}$ is in $H_3(C) \otimes T \subseteq H_3(C) \otimes L$ if and only if $\beta^{-1}y^\sigma x \in C \otimes_R T$ for all $x, y \in I$. The element $X_{I,b,\beta}$ is, by construction, a ‘‘pure tensor’’ in $H_3(C) \otimes L$, just like the element $X(I, b, \beta)$ was in subsection 3.1.

We now define an equivalence relation on based fractional $T \otimes C$ ideals. Suppose $I = b_1C + b_2C + b_3C \subseteq C_L$ is a $C_T = C \otimes_R T$ -fractional ideal, and $\beta \in L^\times$ is a unit. We fix the good basis $(1, \omega, \theta)$ of T . Now say that (b_1, b_2, b_3, β) is equivalent to $(b'_1, b'_2, b'_3, \beta')$ if there exists $x \in C_L^\times$ so that

$$(b'_1, b'_2, b'_3, \beta') = (xb_1, xb_2, xb_3, n_C(x)\beta).$$

It is clear that if (b_1, b_2, b_3, β) is equivalent to $(b'_1, b'_2, b'_3, \beta')$, then $X_{I,b,\beta} = X_{I',b',\beta'}$.

If the data $(I, (b_1, b_2, b_3), \beta)$ is balanced, then since $X_{I,b,\beta}$ is in $H_3(C_T) = H_3(C) \otimes_R T$, there are A, B, D in $H_3(C)$ so that

$$(7) \quad X_{b,\beta} = -A\theta + B\omega + D.$$

Associated to a based-balanced $T \otimes C$ -module $(I, (b_1, b_2, b_3), \beta)$, and the good basis $(1, \omega, \theta)$ of T , one thus obtains a pair $(A, B) \in H_3(C)^2$ by equality (7). Again, it is clear that the association $(I, (b_1, b_2, b_3), \beta) \mapsto (A, B)$ descends to the level of equivalence classes. It will be checked below that if $L = T \otimes_R F$ is étale, then this pair (A, B) is in V^{open} .

We can now state the orbit parametrization theorem.

Theorem 3.2.5. *Suppose that $L = T_F$ is étale. Then the association*

$$(T, (1, \omega, \theta), (I, (b_1, b_2, b_3)), \beta) \mapsto (A, B)$$

induces a bijection between based-balanced fractional $T \otimes C$ -ideals and pairs (A, B) in V^{open} . These bijections are equivariant for the action of the group G : If $h = (\lambda, m, g) = (\det(g)^{-1}, m, g)$ with $N_6(m) = \det(g)^2$ is in G , then h acts on the data via

$$[((\omega_0, \theta_0), (b_1, b_2, b_3), \beta)] \mapsto [((\omega_0, \theta_0)g, (b_1, b_2, b_3)m, \beta)].$$

Here, $[((\omega_0, \theta_0), (b_1, b_2, b_3), \beta)]$ means that the data (b_1, b_2, b_3, β) is taken up to equivalence.

Note the similarity of the map above with those of [Bha04b]. Below, we will also explicitly give the inverse map. As with Theorem 3.1.7, constructing the inverse will involve producing the good basis $(1, \omega, \theta)$ and the element $X = -A\theta + B\omega + D$ out of the pair (A, B) , which will involve the lifting law in this context.

Remark 3.2.6. In the context of Theorem 3.1.7, constructing $X = \tau v + v'$ from $v \in W_A$, and showing that X is abstractly ‘‘rank one’’ (this is the general stand-in for being a pure tensor), is easy. This is done in Theorem 5.1.1. Similarly, in the context of Theorem 3.2.5, constructing $X = -A\theta + B\omega + D$ from the pair (A, B) and proving that X is rank one is again easy. This is done in the (first part) of Theorem 6.1.2. Both Theorem 5.1.1 and 6.1.2 occur in the context of arbitrary cubic norm structures. Where we use the hypotheses that A is an associative cubic norm structure, and C is an associative composition algebra, is to write the rank one elements X as ‘‘pure tensors’’ in a precise way. Writing X as a pure tensor is what is needed for the orbit parametrizations. These *refined* lifting laws, which write the rank one elements X as pure tensors, are Theorem 5.1.4 and Theorem 6.1.10 below.

4. PRELIMINARIES

In this section, we discuss the algebraic preliminaries needed for the various other sections, such as composition algebras, cubic norm structures, certain reductive groups and representations related to these objects, and facts pertaining to the association of binary cubic forms with cubic rings. To ease the burden on the reader, all the necessary preliminaries are given in this section, even though some of this is a repetition of the algebraic preliminaries given in prior sections.

In subsection 4.1 we discuss quadratic and cubic rings over a base ring R , and composition algebras. (As always in this paper, R is an integral domain with fraction field F of characteristic 0.) In subsection 4.2 we discuss cubic norm structures over F and R , and in subsection 4.3 we discuss the Freudenthal construction W_J for general cubic norm structures J . Finally, in subsection 4.4, we discuss some facts and constructions related to the Freudenthal construction that apply when $J = A$ is an associative cubic norm structure. Subsections 4.1, 4.2 and 4.3 consist entirely of a review of well-known material. Subsection 4.4 contains some algebraic constructions and facts related to these objects that may be new, or at least, for which we were not able to find a reference⁶.

The reader only interested in the results of section 6 can skip subsection 4.1.1, subsection 4.3 and subsection 4.4. The reader only interested in the results of section 5 can skip subsection 4.1.3.

4.1. Quadratic and cubic rings. In this subsection we discuss quadratic and cubic rings over a base ring R , and composition algebras.

4.1.1. *Quadratic rings over R .* We now discuss quadratic rings over base rings R , satisfying some property. In this paragraph, we assume that R

- is an integral domain, with fraction field F of characteristic 0;
- $\frac{x^2+x}{2} \in R$ for all $x \in R$.

Definition 4.1.1. A commutative R -algebra S is said to be a quadratic ring over R if S is a free of rank 2 as an R -module.

We parametrize quadratic rings over R : Define

$$\text{QuadRing}(R) := \{D \in R : D \equiv \square \text{ modulo } 4R\} / ((R^\times)^2).$$

If $D \in \text{QuadRing}(R)$, then $\frac{D^2-D}{4} \in R$ and set $S_D = R[x]/(x^2 - Dx + \frac{D^2-D}{4})$. The S_D are exactly the quadratic rings over R , up to isomorphism.

To see this, suppose $S = R[x]/(x^2 + ax + b)$ is some quadratic ring over R . Set $D = a^2 - 4b$. Then $D \in \text{QuadRing}(R)$. Set $y = x - 2b + \frac{a^2+a}{2}$. Then $y^2 - Dy + \frac{D^2-D}{4} = 0$, and thus $S \simeq S_D$, so every quadratic ring appears. Furthermore, one can check $S_D \hookrightarrow S_{D'}$ if and only if $D = \alpha^2 D'$ for some $\alpha \in R$, and thus $S_D \cong S_{D'}$ implies D and D' define the same class in $\text{QuadRing}(R)$.

4.1.2. *Composition algebras.* We now discuss composition algebras. A composition F -algebra C is a not-necessarily associative unital F -algebra C , for which there exists a non-degenerate quadratic form $n_C : C \rightarrow F$ that satisfies the identity $n_C(xy) = n_C(x)n_C(y)$ for all $x, y \in C$. If such an n_C exists, it is unique, and is called the norm on the composition algebra. Composition algebras have an involution, $x \mapsto x^*$ that is order-reversing and satisfies $x + x^* = \text{tr}_C(x) \in F$ and $n_C(x) = xx^*$. In a composition algebra, one always has the identity $\text{tr}_C(a_1(a_2a_3)) = \text{tr}_C((a_1a_2)a_3)$, for $a_i \in C$, even though the multiplication may not be associative.

Composition F -algebras always have dimensions 1, 2, 4, or 8, and are, respectively, F , a quadratic étale extension of F , a quaternion algebra, or an octonion algebra. The composition algebras C for

⁶We have recently learned of a forthcoming work by Wei Ho and Matthew Satriano that will consider a generalization of the space V_A constructed in subsection 4.4.

which the multiplication is associative are precisely the ones of dimensions 1, 2 or 4. For more on composition algebras see the books [SV00] or [KMRT98].

By a composition ring C , we mean a unital R -algebra C for which $C_F := C \otimes_R F$ is a composition F -algebra, such that C is closed under the involution $*$, and for which the norm and trace form n_C, tr_C on C_F are R -valued on C . We will also call such rings C composition R -algebras.

4.1.3. Binary cubic forms and cubic rings. We now give various facts and reminders that concern the relationship between binary cubic forms and cubic rings. See, for instance, [GGS02] for more details.

Suppose $f(x, y)$ is a binary cubic form over R , i.e., $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ with a, b, c, d in the base ring R . Associated to f is a based cubic R -algebra T . The R -algebra T determined by f is a free R -module of rank 3, with basis $1, \omega, \theta$, that satisfies the multiplication table

- $\omega\theta = -ad$;
- $\omega^2 = -ac + a\theta - b\omega$;
- $\theta^2 = -bd + c\theta - d\omega$.

Set $L = T \otimes_R F$, a cubic ring over F . For readers wanting to understand this multiplication table from the point of view of the Freudenthal construction discussed below, we note that the above algebraic relations in T are determined by the fact that $(a, -\omega, \theta, d)$ is rank one in W_L , and $\text{tr}(-\omega) = b$, $\text{tr}(\theta) = c$. This is essentially the lifting law in subsection 2.3.

Set $\omega_0 = \omega + \frac{b}{3}$ and $\theta_0 = \theta - \frac{c}{3}$, so that $\text{tr}_{L/F}(\omega_0) = \text{tr}_{L/F}(\theta_0) = 0$. We record the multiplication table for $(1, \omega_0, \theta_0)$ in L . We have

- $\omega_0\theta_0 = \frac{b}{3}\theta_0 - \frac{c}{3}\omega_0 + \left(\frac{bc}{9} - ad\right)$;
- $\omega_0^2 = a\theta_0 - \frac{b}{3}\omega_0 + 2\left(\left(\frac{b}{3}\right)^2 - a\frac{c}{3}\right)$;
- $\theta_0^2 = \frac{c}{3}\theta_0 - d\omega_0 + 2\left(\left(\frac{c}{3}\right)^2 - d\frac{b}{3}\right)$.

The F -algebra L possesses a unique quadratic polynomial map $\# : L \rightarrow L$, that satisfies $y^\# = n_{L/F}(y)y^{-1}$ for y in L invertible. This fact was mentioned in section 3.1 and will be discussed in much more generality in section 4.2. For later use, we record that $\omega^\# = a\theta$ and $\theta^\# = -d\omega$. Associated to the quadratic polynomial map $\#$ is a symmetric bilinear map $\times : L \otimes L \rightarrow L$ defined by $x \times y = (x + y)^\# - x^\# - y^\#$. Again, this map will be put in much more context in subsection 4.2. For now, we also record that $\omega \times \theta = ad - bc + b\theta - c\omega$. To compute $\omega \times \theta$, one uses the identity $x^\# \times x = \text{tr}(x^2)x - x^3$. Furthermore,

$$\begin{aligned} \omega_0^\# &= (\omega + b/3)^\# = a\theta - \frac{b}{3}\omega - \frac{2}{9}b^2 \\ &= a\theta_0 - \frac{b}{3}\omega_0 + a\left(\frac{c}{3}\right) - \left(\frac{b}{3}\right)^2, \end{aligned}$$

$$\begin{aligned} \theta_0^\# &= (\theta - c/3)^\# = \frac{c}{3}\theta - d\omega - \frac{2}{9}c^2 \\ &= \frac{c}{3}\theta_0 - d\omega_0 + d\left(\frac{b}{3}\right) - \left(\frac{c}{3}\right)^2, \end{aligned}$$

and

$$\begin{aligned} \omega_0 \times \theta_0 &= (\omega + b/3) \times (\theta - c/3) = \frac{2}{3}b\theta - \frac{2}{3}c\omega + ad - \frac{5}{9}bc \\ &= \frac{2}{3}b\theta_0 - \frac{2}{3}c\omega_0 + ad - \left(\frac{b}{3}\right)\left(\frac{c}{3}\right). \end{aligned}$$

Binary cubic forms possess a quartic invariant, the discriminant. If $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$, then the discriminant of f is

$$Q(f) = -27a^2d^2 + 18adbc + b^2c^2 - 4ac^3 - 4db^3.$$

We remark that this discriminant can be easily understood in the context of the Freudenthal construction, see section 4.3. Namely, the binary cubic $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ corresponds to the element $(a, \frac{b}{3}, \frac{c}{3}, d)$ in the Freudenthal construction W_F , for the trivial cubic norm structure on F . (This is the structure from Example 4.2.6, case (3).) We set $q_f = q((a, b/3, c/3, d))$. Then the discriminant $Q(f) = -27q_f$. Indeed,

$$\begin{aligned} -27q_f &= -\frac{1}{3}q((3a, b, c, 3d)) \\ &= -\frac{1}{3}\{(9ad - 3bc)^2 + 12ac^3 + 12db^3 - 12b^2c^2\} \\ &= -3(3ad - bc)^2 - 4ac^3 - 4db^3 + 4b^2c^2 \\ &= -27a^2d^2 + 18adbc + b^2c^2 - 4ac^3 - 4db^3. \end{aligned}$$

One has the equality

$$\text{disc}(1, \omega, \theta) := \det \begin{pmatrix} \text{tr}(1) & \text{tr}(\omega) & \text{tr}(\theta) \\ \text{tr}(\omega) & \text{tr}(\omega^2) & \text{tr}(\omega\theta) \\ \text{tr}(\theta) & \text{tr}(\theta\omega) & \text{tr}(\theta^2) \end{pmatrix} = \det \begin{pmatrix} 3 & -b & c \\ -b & b^2 - 3ac & -3ad \\ c & -3ad & c^2 - 2bd \end{pmatrix} = Q(f).$$

The left action of GL_2 on binary cubic forms is $(g \cdot f)(x, y) = \det(g)^{-1}f((x, y)g)$. With this action, one has $q(g \cdot f) = \det(g)^2q(f)$, and $\begin{pmatrix} \omega_0 \\ \theta_0 \end{pmatrix} \mapsto g \begin{pmatrix} \omega_0 \\ \theta_0 \end{pmatrix}$. This latter identity, $\begin{pmatrix} \omega_0 \\ \theta_0 \end{pmatrix} \mapsto g \begin{pmatrix} \omega_0 \\ \theta_0 \end{pmatrix}$, has the following meaning: Set $f' = (g \cdot f)(x, y) = a'x^3 + b'x^2y + c'xy^2 + d'y^3$, denote $(T', (1, \omega', \theta'))$ the based cubic ring associated to f' , and set $\omega'_0 = \omega' + \frac{b'}{3}$, $\theta'_0 = \theta' - \frac{c'}{3}$. Then one can identify T with T' so that $\begin{pmatrix} \omega'_0 \\ \theta'_0 \end{pmatrix} = g \begin{pmatrix} \omega_0 \\ \theta_0 \end{pmatrix}$ inside L .

4.2. Cubic norm structures. In this subsection we discuss cubic norm structures. For completeness, and to fix notation, we begin with the definition of a cubic norm structure. However, readers not familiar with cubic norm structures might wish to proceed first to the examples, and only then come back to the definition if desired.

Definition 4.2.1. (See for example [PR86].) Let J be a finite dimensional F vector space. A *cubic norm structure* on J consists of the data of an element $1 \in J$, a cubic polynomial map $N : J \rightarrow F$, a quadratic polynomial map $\# : J \rightarrow J$, and a non-degenerate symmetric pairing $(\ , \) : J \otimes J \rightarrow F$, that are subject to the following requirements.

- $(x\#)\# = N(x)x$;
- $N(1) = 1$, $1\# = 1$, $1 \times x = (1, x) - x$ for all $x \in J$;
- One has $(x, y) = (1, 1, x)(1, 1, y) - (1, x, y)$ and

$$N(x + y) = N(x) + (x\#, y) + (x, y\#) + N(y)$$

for all $x, y \in J$.

Here $x \times y := (x + y)\# - x\# - y\#$, and (x, y, z) is the polarization of the norm form N , i.e.,

$$(x, y, z) := N(x + y + z) - N(x + y) - N(x + z) - N(y + z) + N(x) + N(y) + N(z)$$

is the unique symmetric trilinear form on J satisfying $(x, x, x) = 6N(x)$. The notation $\text{tr}(x) := (1, x)$ and $\text{tr}(x, y) := (x, y)$ is also used. The map N is called the norm on J , while the map $\#$ is called the adjoint.

It follows from these requirements that $(x \times y, z) = (x, y, z) = (x, y \times z)$. For x, y in J , one sets

$$U_x y := -x^\# \times y + (x, y)x.$$

One has $N(U_x y) = N(x)^2 N(y)$.

One can also replace F by a subring R , and J by a finite, free R -module. We will sometimes be in this slightly more general situation.

Remark 4.2.2. Suppose J is an F vector space, and one has a quadratic polynomial map $\# : J \rightarrow J$, a cubic polynomial map $n : J \rightarrow F$, a non-degenerate symmetric pairing $J \otimes_F J \rightarrow F$, and an element $1 \in J$. As above, define $x \times y = (x + y)^\# - x^\# - y^\#$. To check that this data defines a cubic norm structure on J , it suffices to check that

- $1 \times x = (1, x) - x$;
- $(x^\#)^\# = n(x)x$;
- $(x, x^\#) = 3n(x)$;
- the trilinear form $(x, y \times z)$ is symmetric in x, y, z .

The key examples of cubic norm structures are as follows.

Example 4.2.3. Suppose $J = A$ is a central simple F -algebra of degree 3. One defines $1 \in J$ to be the identity in A , and $N(x)$ to be the reduced norm of $x \in A$. The pairing (x, y) is $(x, y) = \text{tr}(xy)$, where the trace on the right is the reduced trace of A . For $x \in A$ invertible, $x^\# = N(x)x^{-1}$, and in fact this map extends to a quadratic polynomial map on all of A . For $x, y \in A$, one has the identity $U_x y = xyx$.

Example 4.2.4. Suppose C is a composition algebra. Set $J = H_3(C)$, the 3×3 Hermitian matrices with elements in C . Elements of J are of the form

$$x = \begin{pmatrix} c_1 & a_3 & a_2^* \\ a_3^* & c_2 & a_1 \\ a_2 & a_1^* & c_3 \end{pmatrix}$$

with $c_i \in F$ and $a_i \in C$. The element 1 for J is just the 3×3 identity matrix 1_3 . The norm on J is

$$N(x) = c_1 c_2 c_3 - c_1 n_C(a_1) - c_2 n_C(a_2) - c_3 n_C(a_3) + \text{tr}_C(a_1 a_2 a_3)$$

and the adjoint on J is

$$x^\# = \begin{pmatrix} c_2 c_3 - n_C(a_1) & a_2^* a_1^* - c_3 a_3 & a_3 a_1 - c_2 a_2^* \\ a_1 a_2 - c_3 a_3^* & c_1 c_3 - n_C(a_2) & a_3^* a_2^* - c_1 a_1 \\ a_1^* a_3^* - c_2 a_2 & a_2 a_3 - c_1 a_1^* & c_1 c_2 - n_C(a_3) \end{pmatrix}.$$

One has $\text{tr}(x) = (1, x) = c_1 + c_2 + c_3$ and $(x, x') = \text{tr}(xx' + x'x)/2 = \sum_i c_i c'_i + \sum_j (a_j, a'_j)$ where $(a_j, a'_j) = n_C(a_j + a'_j) - n_C(a_j) - n_C(a'_j) = \text{tr}_C(a_j^* a'_j)$. If C is associative, then for $x, y \in J = H_3(C)$ one has the identity $U_x y = xyx$.

Example 4.2.5. Suppose $K = F$ or a quadratic étale extension of F , and B is a central simple K algebra, with involution of the second kind $*$. That is, we assume $* : B \rightarrow B$ is an order-reversing involution that induces the unique involution on K over F . (So, if $K = F$, this involution on K is the identity.) Set J to be $B^{*=1}$, the F -subspace of B fixed by the involution $*$. From example 4.2.3, B is a cubic norm structure over K . Restricting the norm, adjoint, and pairing to J makes J a cubic norm structure over F . If $C = K$ is a commutative associative composition algebra, $B = M_3(C)$, with involution $*$ being conjugate transpose, then J is the cubic norm structure $H_3(C)$ from example 4.2.4.

There are also degenerate versions of some of the above examples.

Example 4.2.6. Suppose $J = A$ is one of the following associative F -algebras:

- (1) $A = E$, a cubic étale F -algebra;
- (2) $A = F \times C$, for C an associative composition algebra;
- (3) $A = F$.

(When $C = K$ is a quadratic étale F -algebra, there is overlap between cases (1) and (2).) In each case, let 1 for J be the identity of the algebra A . In case (1), let the trace pairing and norm on E be the usual trace pairing and norm, and $x^\# = N(x)x^{-1}$ for x invertible. (Again, this extends as a polynomial map to all of E .) In case (2), set $N((\alpha, x)) = \alpha n_C(x)$ for $\alpha \in F$ and $x \in C$, $(\alpha, x)^\# = (n_C(x), \alpha x^*)$, and $((\alpha, x), (\beta, y)) = \alpha\beta + (x, y)$. In case (3), define $N(x) = x^3$, $x^\# = x^2$, and $(x, y) = 3xy$, where here $x, y \in F$.

We introduce one non-standard piece of terminology.

Definition 4.2.7. Suppose J is a cubic norm structure. We say J is an *associative cubic norm structure* if $J = A$ is as in Example 4.2.3 or Example 4.2.6. In this case, one has the identities $xx^\# = x^\#x = N(x)$, $(xy)^\# = y^\#x^\#$, $N(xy) = N(x)N(y)$, and $U_xy = xyx$.

All of the above constructions and definitions have generalizations to the case when F is replaced by a subring R , and one assumes J is finite and free over R .

There is also a weaker notion a *cubic norm pair*, which we now define. (This notion will only be used in section 6.)

Definition 4.2.8. Suppose J, J^\vee are finite dimensional F vector spaces in perfect duality by a pairing $(,) : J \otimes J^\vee \rightarrow F$. The structure of a cubic norm pair on J, J^\vee is the data of cubic polynomial maps $N_J : J \rightarrow F$, $N_{J^\vee} : J^\vee \rightarrow F$, and quadratic polynomial maps $\#_J : J \rightarrow J^\vee$ and $\#_{J^\vee} : J^\vee \rightarrow J$ that are subject to the following requirements:

- (1) One has

$$N_J(x + y) = N_J(x) + (y, x^{\#_J}) + (x, y^{\#_J}) + N_J(y)$$

for all $x, y \in J$ and similarly for N_{J^\vee} .

- (2) One has $(x^{\#_J})^{\#_{J^\vee}} = N_J(x)x$ for all $x \in J$ and similarly $(y^{\#_{J^\vee}})^{\#_J} = N_{J^\vee}(y)y$ for all $y \in J^\vee$.

One sets

$$x \times_J y := (x + y)^{\#_J} - x^{\#_J} - y^{\#_J}$$

if $x, y \in J$ and similarly for J^\vee . One has $(x, y \times z) = (z, x \times y) = (x, y, z)$ for $x, y, z \in J$ if (x, y, z) denotes the polarization of the norm form, and again similarly for J^\vee .

Obviously, every cubic norm structure gives rise to a cubic norm pair with $J^\vee = J$.

We now define the rank of elements of J .

Definition 4.2.9. Suppose J is a cubic norm structure. All elements of J have rank at most 3. An element x has rank at most 2 if $N_J(x) = 0$. An element x has rank at most 1 if $x^\# = 0$. Finally, 0 is the unique element of rank 0.

For more on cubic norm structures, see, for example, [KMRT98] or [McC04].

4.2.1. *Identities for cubic norm structures.* We give several identities valid in cubic norm structures. These identities will be used throughout the paper. First, one has the relations

$$\begin{aligned} x \times (x^\# \times y) &= n(x)y + (x, y)x^\#, \\ x^\# \times (x \times y) &= n(x)y + (x^\#, y)x, \\ (x \times y)^\# + x^\# \times y^\# &= (x, y^\#)x + (x^\#, y)y. \end{aligned}$$

Recall that the cubic norm structure J is said to be *special* if there exists an associative algebra W , and an inclusion $J \subseteq W$ so that $U_xy = xyx$. Here the multiplication on the right hand side of this equality is that of W . If J is special, then one has $xx^\# = x^\#x = n(x)$. Linearizing this

identity gives $x(x \times y) + yx^\# = (x^\#, y)$ and similarly $(x \times y)x + x^\#y = (x^\#, y)$, one consequence of which is the identity $y^\#x(x \times y) = (x^\#, y)y^\# - n(y)x^\#$. One also has the identity

$$(8) \quad x \times (y \times z) = (x, y)z + (x, z)y - (yxz + zxy)$$

for special J .

4.2.2. *The group M_J .* We now define a reductive group M_J that acts on J if J is a cubic norm structure. Namely, define M_J to be the group of $(g, \lambda) \in \mathrm{GL}(J) \times \mathrm{GL}_1$ so that $N_J(gx) = \lambda N_J(x)$ for all $x \in J$. The group M_J preserves the rank of elements of J , and its action makes J into a prehomogeneous vector space. The open orbit consists of the elements of rank 3.

More generally, suppose J, J^\vee form a cubic norm pair over F . There is an analogue of the group M_J for the pair (J, J^\vee) . Define $\widetilde{M}(J, J^\vee)$ to be the group of $(\alpha, t, t^\vee, \delta) \in \mathrm{GL}_1 \times \mathrm{GL}(J) \times \mathrm{GL}(J^\vee) \times \mathrm{GL}_1$ that satisfy the following identities, for all $b \in J, c \in J^\vee$:

- $(t(b), t^\vee(c)) = \alpha\delta(b, c)$;
- $N_{J^\vee}(t^\vee(c)) = \alpha\delta^2 N_{J^\vee}(c)$;
- $N_J(t(b)) = \alpha^2\delta N_J(b)$;
- $t(b)^\#J = \alpha t^\vee(b^\#J)$ and $t^\vee(c)^\#J^\vee = \delta t(c^\#J^\vee)$.

Now, define the group $M(J, J^\vee)$ to be the subgroup of $\widetilde{M}(J, J^\vee)$ where $\alpha\delta = 1$. If J is a cubic norm structure, then $M_J = M(J, J)$, which makes sense because J, J is a cubic norm pair.

4.3. **The Freudenthal construction.** We now discuss the so-called Freudenthal construction associated to a cubic norm structure J . That is, to such a J , we define the space the space W_J together with its natural quartic form and symplectic pairing. We also discuss the group $H(W_J)$, that acts on W_J preserving these structures.

Suppose J is a cubic norm structure. We set

$$W_J = F \oplus J \oplus J^\vee \oplus F = F \oplus J \oplus J \oplus F.$$

We write typical elements of W_J as (a, b, c, d) . The space W_J carries a symplectic pairing

$$\langle (a, b, c, d), (a', b', c', d') \rangle := ad' - (b, c') + (c, b') - da'$$

The space W_J also carries a natural quartic form (due to Freudenthal), given by

$$q((a, b, c, d)) = (ad - (b, c))^2 + 4an(c) + 4dn(b) - 4(b^\#, c^\#).$$

Polarizing the quartic form q , there is a symmetric 4-linear form (w, x, y, z) on W_J normalized by the condition $(v, v, v, v) = 2q(v)$ for v in W_J . Since the symplectic pairing is non-degenerate, there is a symmetric trilinear form $t : W_J \times W_J \times W_J \rightarrow W_J$ normalized by the identity

$$\langle w, t(x, y, z) \rangle = (w, x, y, z).$$

Finally, for $v \in W_J$, set $v^\flat = t(v, v, v)$. If $v = (a, b, c, d)$, then $v^\flat = (a^\flat, b^\flat, c^\flat, d^\flat)$, where

- $a^\flat = -a^2d + a(b, c) - 2n(b)$;
- $b^\flat = -2c \times b^\# + 2ac^\# - (ad - (b, c))b$;
- $c^\flat = 2b \times c^\# - 2db^\# + (ad - (b, c))c$;
- $d^\flat = ad^2 - d(b, c) + 2n(c)$;

One has the following fact.

Lemma 4.3.1. *For $v \in W_J$, one has $\langle v, v^\flat \rangle = 2q(v)$ and $(v^\flat)^\flat = -q(v)^2v$.*

We now define the rank of elements of W_J .

Definition 4.3.2. All elements of W_J have rank at most 4. An element v of W_J has rank at most 3 if $q(v) = 0$. An element v of W_J has rank at most 2 if $(v, v, v, w) = 0$ for all $w \in W_J$. Equivalently, v has rank at most 2 if $v^\flat = 0$. An element v has rank at most 1 if $(v, v, v', w) = 0$ for all $w \in W_J$ and $v' \in W_J$ satisfying $\langle v, v' \rangle = 0$. Equivalently, v has rank at most 1 if $t(v, v, w) \in Fv$ for all $w \in W_J$. Finally, 0 is the unique element of rank 0.

4.3.1. *The group $H(W_J)$.* Let W_J be as above. We now define a group $H(W_J)$ that acts on W_J . We define the group $H(W_J)$ to be the subgroup of $g \in \mathrm{GSp}(W_J; \langle \cdot, \cdot \rangle)$ satisfying $q(gv) = \nu(g)^2 q(v)$ for all $v \in W_J$. Here $\nu(g) \in \mathrm{GL}_1$ is the similitude of g in $\mathrm{GSp}(W_J)$.

We define some maps on W_J that are in $H(W_J)$.

- For $X \in J$, define

$$n_J(X)(a, b, c, d) = (a, b + aX, c + b \times X + aX^\#, d + (c, X) + (b, X^\#) + an(X))$$

and similarly for $Y \in J^\vee = J$ define

$$\bar{n}_J(Y) = n_{J^\vee}(Y)(a, b, c, d) = (a + (b, Y) + (c, Y^\#) + dn(Y), b + c \times Y + dY^\#, c + dY, d).$$

- For $\lambda \in \mathrm{GL}_1$, define

$$m(\lambda)(a, b, c, d) = (\lambda^2 a, \lambda b, c, \lambda^{-1} d).$$

- More generally, for $m = (\alpha, t, t^\vee, \delta) \in \widetilde{M}(J, J)$, define

$$m(a, b, c, d) = (\alpha a, t(b), t^\vee(c), \delta d).$$

- Define $w_J(a, b, c, d) = (d, -c, b, -a)$.

The following proposition is well-known, the only nontrivial piece being for the maps $n_J(X), n_{J^\vee}(Y)$. (See [Spr06, Lemma 2.3] for this nontrivial piece.)

Proposition 4.3.3. *The above maps are all elements of $H(W_J)$.*

The action of $H(W_J)$ preserves the ranks of elements of W_J , and makes it into a prehomogeneous vector space. The elements of rank 4 of W_J form the open orbit. All elements of rank 1 of W_J are in the same $H(W_J)$ orbit.

One has the following fact.

Lemma 4.3.4. *If $v = (a, b, c, d) \in W_J$ is rank one, then $b^\# = ac$, $c^\# = db$, and $(b, c) = 3ad$. If either a or d is nonzero, then the first two conditions imply v is rank one.*

All rank one elements of W_J are in the $H(W_J)$ -orbit of the element $(1, 0, 0, 0)$. More generally, arbitrary nonzero elements v of $H(W_J)$ are in the $H(W_J)$ -orbit of elements of the form $(1, 0, c, d)$.

Lemma 4.3.5. *Every nonzero element v of W_J can be moved to one of the form $(1, 0, c, d)$ by applying operators $n_J(X), \bar{n}_J(Y)$, and $m(\lambda)$.*

A proof of the previous two lemmas may be found in [GS05, Proposition 11.2, Corollary 11.3].

From the definitions, if $g \in H(W_J)$, one obtains $(gv)^\flat = \nu(g)g(v^\flat)$ and similarly $t(gv_1, gv_2, gv_3) = \nu(g)gt(v_1, v_2, v_3)$.

4.4. **Particulars for associative cubic norm structures.** In this subsection we give more preliminaries that apply specifically to the case that $J = A$ is an associative cubic norm structure. Throughout this subsection, A is assumed to be an associative cubic norm structure. We write n or n_A for the cubic norm map $A \rightarrow F$.

We first note the following. Suppose $u, v \in A$ and $n(u)n(v) \in F^\times$. Then if one sets $\alpha = n(u), \delta = n(v)$, $t(b) = vbu^\#, t^\vee(c) = ucv^\#$, the map $L(u, v) := m(\alpha, t, t^\vee, \delta)$ is in $\widetilde{M}(A, A)$.

4.4.1. *The quadratic map R .* Define a map $R : W_A \rightarrow M_2(A)$ via

$$v = (a, b, c, d) \mapsto R(v) = \begin{pmatrix} ad + 2cb - (c, b) & 2b^\# - 2ac \\ 2db - 2c^\# & -ad + (b, c) - 2bc \end{pmatrix}.$$

Proposition 4.4.1. *One has $R(v)^2 = q(v)1_2$ for all $v \in W_A$.*

Proof. Computing the $(1, 2)$ entry of $R(v)^2$, one obtains

$$\begin{aligned} R(v)_{12}^2 &= (ad + 2cb - (b, c))(2b^\# - 2ac) + (2b^\# - 2ac)(-ad + (b, c) - 2bc) \\ &= 2cb(2b^\# - 2ac) + (2b^\# - 2ac)(-2bc) \\ &= 0. \end{aligned}$$

Similarly, the $(2, 1)$ entry of $R(v)^2 = 0$. We thus must compute the diagonal entries of $R(v)^2$. The $(1, 1)$ entry is

$$\begin{aligned} R(v)_{11}^2 &= (ad - (b, c) + 2cb)^2 + 4(b^\# - ac)(db - c^\#) \\ &= (ad - (b, c))^2 + 4E \end{aligned}$$

where

$$\begin{aligned} E &= (ad - (b, c))cb + cbc + (b^\# - ac)(db - c^\#) \\ &= an(c) + dn(b) - \left(\text{tr}(cb)cb - (cb)^2 + (cb)^\# \right) \\ &= an(c) + dn(b) - \text{tr}((cb)^\#) \end{aligned}$$

since for all x in A we have

$$x^2 - \text{tr}(x)x + \text{tr}(x^\#) - x^\# = 0.$$

Thus $R(v)_{11}^2 = q(v)$. Similarly, $R(v)_{22}^2 = q(v)$. This completes the proof. \square

We will sometimes have desire to use the more symmetrical-looking matrix $S(v) := \frac{1}{2}R(v) \begin{pmatrix} & -1 \\ 1 & \end{pmatrix}$. If $v = (a, b, c, d)$, then

$$(9) \quad S(v) := \frac{1}{2}R(v) \begin{pmatrix} & -1 \\ 1 & \end{pmatrix} = \begin{pmatrix} b^\# - ac & ad - cb - \text{tr}(ad - cb)/2 \\ ad - bc - \text{tr}(ad - bc)/2 & c^\# - db \end{pmatrix}.$$

From Proposition 4.4.1 one obtains the identity $S(v)J_2S(v) = -\frac{q(v)}{4}J_2$, where $J_2 = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$.

Example 4.4.2. Suppose $A = F \times F \times F$ and $v = (a, b, c, d)$, with $b = (b_1, b_2, b_3)$, $c = (c_1, c_2, c_3)$. The element v is a $2 \times 2 \times 2$ cube, as considered in [Bha04a]. Then $S(v) \in M_2(A) = M_2(F) \times M_2(F) \times M_2(F)$, and one has $S(v) = (q_1, q_2, q_3)$ with

$$\begin{aligned} q_1 &= \begin{pmatrix} b_2b_3 - ac_1 & \frac{-b_1c_1 + b_2c_2 + b_3c_3 - ad}{2} \\ \frac{-b_1c_1 + b_2c_2 + b_3c_3 - ad}{2} & c_2c_3 - db_1 \end{pmatrix} \\ q_2 &= \begin{pmatrix} b_3b_1 - ac_2 & \frac{-b_2c_2 + b_3c_3 + b_1c_1 - ad}{2} \\ \frac{-b_2c_2 + b_3c_3 + b_1c_1 - ad}{2} & c_3c_1 - db_2 \end{pmatrix}, \\ q_3 &= \begin{pmatrix} b_1b_2 - ac_3 & \frac{-b_3c_3 + b_1c_1 + b_2c_2 - ad}{2} \\ \frac{-b_3c_3 + b_1c_1 + b_2c_2 - ad}{2} & c_1c_2 - db_3 \end{pmatrix}. \end{aligned}$$

The q_i are 2×2 symmetric matrices, or equivalently, binary quadratic forms. These are (essentially) the 3 quadratic forms associated to v from [Bha04a]. Since one always has $mJ_2m^t = \det(m)J_2$ for $m \in M_2(F)$, the identity $S(v)JS(v) = -\frac{q(v)}{4}J$ is the statement that the 3 quadratic forms q_i have the same discriminant, which is equal to the discriminant of v .

We record how $R(v)$ behaves under the action of certain elements of $H(W_A)$.

Proposition 4.4.3. *Suppose $v \in W_A$, $X \in A$, and $m, n \in A$ with $n_A(m)n_A(m) \in R^\times$. Then $R(n(X)v) = \begin{pmatrix} 1 & \\ X & 1 \end{pmatrix} R(v) \begin{pmatrix} 1 & \\ -X & 1 \end{pmatrix}$, $R(w_A(v)) = \begin{pmatrix} -1 & \\ & 1 \end{pmatrix} R(v) \begin{pmatrix} & \\ 1 & -1 \end{pmatrix}$, and*

$$\begin{aligned} R(L(m, n)v) &= n_A(m)n_A(n) \begin{pmatrix} m & \\ & n \end{pmatrix} R(v) \begin{pmatrix} m^{-1} & \\ & n^{-1} \end{pmatrix} \\ &= \begin{pmatrix} m & \\ & n \end{pmatrix} R(v) \begin{pmatrix} n_A(n)m^\# & \\ & n_A(m)n^\# \end{pmatrix}. \end{aligned}$$

Proof. These are all direct computations. \square

The vanishing of $R(v)$, or equivalently $S(v)$, characterizes elements of W_A of rank at most 1.

Lemma 4.4.4. *For $v \in W_A$, one has $S(v) = 0$ if and only if v has rank at most 1.*

Proof. Clearly $S(0) = 0$, and one computes $S((1, 0, c, d)) = \begin{pmatrix} -c & -d/2 \\ -d/2 & c^\# \end{pmatrix}$. The lemma then follows by the equivariance result of Proposition 4.4.3. The lemma also follows right away from [GS05, Proposition 11.2]. \square

4.4.2. *Rank one elements.* We now say a bit more about rank one elements of W_A . Suppose $\ell = (s, t) \in A^2$ is a row vector. We define $\ell^\dagger \in W_A$ to be the element

$$\ell^\dagger = (s, t)^\dagger := (n(s), s^\#t, t^\#s, n(t)).$$

Similarly, if $\eta \in A^2$ is a column vector, we define

$$\eta^\dagger = \begin{pmatrix} u \\ v \end{pmatrix}^\dagger = (n(u), vu^\#, uv^\#, n(v)).$$

Note that the order of multiplication in the “ b ” and “ c ”-components has been switched. We have the following lemma.

Lemma 4.4.5. *For $\ell \in A^2$ a row vector, and $\eta \in A^2$ a column vector, ℓ^\dagger and η^\dagger are rank at most one, and one has $\langle \ell^\dagger, \eta^\dagger \rangle = n_A(\ell \begin{pmatrix} 1 & \\ & -1 \end{pmatrix} \eta)$.*

Proof. That ℓ^\dagger and η^\dagger are rank at most one follows from Lemma 4.4.4. Suppose $\ell = (s, t)$ and $\eta = \begin{pmatrix} u \\ v \end{pmatrix}$. Then

$$\begin{aligned} \langle \ell^\dagger, \eta^\dagger \rangle &= \langle (n(s), s^\#t, t^\#s, n(t)), (n(u), vu^\#, uv^\#, n(v)) \rangle \\ &= n(s)n(v) - (s^\#t, uv^\#) + (t^\#s, vu^\#) - n(t)n(u) \\ &= n(sv) - ((sv)^\#, tu) + (sv, (tu)^\#) - n(tu) \\ &= n(sv - tu) \end{aligned}$$

and the lemma follows. \square

4.4.3. *The $\mathrm{GL}_2(A)$ -action on W_A .* In this paragraph we define a right and left $\mathrm{GL}_2(A)$ action on W_A , that preserves the symplectic and quartic forms, up to similitude. We will give the details for the left action; the right action is completely analogous.

We begin by constructing a space V_A , with a left $\mathrm{GL}_2(A)$ action, that comes equipped with a map $V_A \rightarrow W_A$. We will then show that this map is an isomorphism.

We consider $W_2 \otimes A$ to be the 2×1 column vectors with coefficients in A , an A bi-module.

Definition 4.4.6. We first define V_{A_F} . Denote by S_3 the symmetric group on three letters. The vector space V_{A_F} is defined to be the S_3 invariants of the quotient of $(W_2 \otimes A_F)^{\otimes 3}$ by the subspace spanned by $xa \otimes xa \otimes xa - n(a)x \otimes x \otimes x$ for $x \in W_2 \otimes A_F$ and $a \in A_F$. That is, set

$$I_{A_F} := (\langle xa \otimes xa \otimes xa - n(a)x \otimes x \otimes x : x \in W_2 \otimes A_F, a \in A_F \rangle),$$

the subspace spanned by $xa \otimes xa \otimes xa - n(a)x \otimes x \otimes x$ for $x \in W_2 \otimes A_F$ and $a \in A_F$, and

$$V_{A_F} := (((W_2 \otimes A_F) \otimes (W_2 \otimes A_F) \otimes (W_2 \otimes A_F)) / I_{A_F})^{S_3}.$$

We define V_A to be the image of $(A^2 \otimes A^2 \otimes A^2)^{S_3}$ in V_{A_F} .

Note that since $\mathrm{GL}_2(A_F)$ preserves the submodule I_{A_F} , and since the $\mathrm{GL}_2(A_F)$ and S_3 actions commute on $(W_2 \otimes A_F)^{\otimes 3} / I_{A_F}$, $\mathrm{GL}_2(A_F)$ acts on the left of V_{A_F} . The group $\mathrm{GL}_2(A)$ preserves the module V_A inside V_{A_F} .

A map $V_A \rightarrow W_A$ is defined as follows. We map $x \otimes x \otimes x$ to x^\dagger . Linearizing this, suppose $x_i = \begin{pmatrix} u_i \\ v_i \end{pmatrix}$ in $W_2 \otimes A$. Recall the symmetric trilinear form on A that satisfies the identities $(x, x, x) = 6n(x)$, $(x, y, z) = \mathrm{tr}(x \times y, z)$. Then we map

$$\sum_{\sigma \in S_3} \sigma(x_1 \otimes x_2 \otimes x_3) \mapsto (\alpha(x_1, x_2, x_3), \beta(x_1, x_2, x_3), \gamma(x_1, x_2, x_3), \delta(x_1, x_2, x_3))$$

where

- $\alpha(x_1, x_2, x_3) = (u_1, u_2, u_3)$
- $\beta(x_1, x_2, x_3) = v_1(u_2 \times u_3) + v_2(u_3 \times u_1) + v_3(u_1 \times u_2)$
- $\gamma(x_1, x_2, x_3) = u_1(v_2 \times v_3) + u_2(v_3 \times v_1) + u_3(v_1 \times v_2)$
- $\delta(x_1, x_2, x_3) = (v_1, v_2, v_3)$.

Note that this does define a map on V_A , since $\alpha(x_1a, x_2a, x_3a) = n(a)\alpha(x_1, x_2, x_3)$, $\beta(x_1a, x_2a, x_3a) = n(a)\beta(x_1, x_2, x_3)$ etcetera.

Lemma 4.4.7. *Suppose x, y, z are in $W_2 \otimes A$ and a_1, a_2, a_3, a are in A . Then in $(W_2 \otimes A_F)^{\otimes 3} / I_{A_F}$, one has the following equalities:*

- (1) $\sum_{\sigma \in S_3} \sigma(xa_1 \otimes xa_2 \otimes xa_3) = (a_1, a_2, a_3)x \otimes x \otimes x$;
- (2) $xa \otimes ya \otimes z = x \otimes y \otimes za^\#$;
- (3) $xa_1 \otimes ya_2 \otimes z + xa_2 \otimes ya_1 \otimes z = x \otimes y \otimes z(a_1 \times a_2)$.

Proof. The first item follows from linearizing the identity $xa \otimes xa \otimes xa = n(a)x \otimes x \otimes x$, and the third item follows from the second by linearization. Thus, we prove the second statement.

To do this, fix x, y, z in $W_2 \otimes A$, and consider the map $A \rightarrow (W_2 \otimes A_F)^{\otimes 3} / I_{A_F}$ given by

$$a \mapsto xa \otimes ya \otimes z - x \otimes y \otimes za^\#.$$

Since this is a polynomial map from A to a finite dimensional F vector space, to check that it is identically 0, it suffices to check that it is 0 on the Zariski dense set of a with $n(a) \neq 0$. But now in $(W_2 \otimes A_F)^{\otimes 3} / I_{A_F}$, one has

$$n(a) \left(x \otimes y \otimes za^\# \right) = xa \otimes ya \otimes za^\# a = n(a) (xa \otimes ya \otimes z),$$

and the lemma follows. \square

Fix the standard basis $e = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $f = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ of W_2 .

Proposition 4.4.8. *The map $V_{A_F} \rightarrow W_{A_F}$ is a linear isomorphism, which induces an isomorphism of R -modules $V_A \rightarrow W_A$.*

Proof. We check that the map $V_A \rightarrow W_A$ is an isomorphism by seeing that it is surjective, and checking the bound $\dim_F V_{A_F} \leq 2 + 2 \dim_F A_F$.

To see the surjectivity, note that for $a \in R$ and $b \in A$, $ae \otimes e \otimes e \mapsto (a, 0, 0, 0)$, and

$$bf \otimes e \otimes e + e \otimes bf \otimes e + e \otimes e \otimes bf \mapsto (0, b, 0, 0)$$

and similarly the elements $(0, 0, c, 0)$, $(0, 0, 0, d)$ are in the image of $V_A \rightarrow W_A$.

It follows from Lemma 4.4.7 that the elements

- $ae \otimes e \otimes e, a \in F$;
- $bf \otimes e \otimes e + e \otimes bf \otimes e + e \otimes e \otimes bf, b \in A_F$;
- $ce \otimes f \otimes f + f \otimes ce \otimes f + f \otimes f \otimes ce, c \in A_F$;
- $df \otimes f \otimes f, d \in F$

span V_{A_F} . The dimension bound, and thus the proposition, follows. \square

As a consequence of Proposition 4.4.8, we obtain a left $\mathrm{GL}_2(A)$ action on W_A by transport of structure. Note that by the definition of this action, we have $(g\eta)^! = g \cdot \eta^!$, if $g \in \mathrm{GL}_2(A)$ and $\eta \in A^2$ is a column vector.

We next need to check that the induced action of $\mathrm{GL}_2(A)$ on W_A preserves the symplectic and quartic form. First, a lemma.

Lemma 4.4.9. *The element $\begin{pmatrix} 1 & \\ X & 1 \end{pmatrix}$ of $\mathrm{GL}_2(A)$ acts on W_A as $n(X)$, $\begin{pmatrix} m & \\ & n \end{pmatrix}$ acts on W_A as $L(m, n)$, and $\begin{pmatrix} & \\ -1 & 1 \end{pmatrix}$ acts on W_A as w_A .*

Proof. These are all direct computations that follow from Lemma 4.4.7 and the definitions. For example, $\begin{pmatrix} m & \\ & n \end{pmatrix}$ acts on $(0, b, 0, 0)$ as

$$\sum_{cyc} e \otimes e \otimes bf \mapsto \sum_{cyc} me \otimes me \otimes nbf = \sum_{cyc} e \otimes e \otimes nbm^\# f = (0, nbm^\#, 0, 0).$$

\square

Denote by $P \subseteq \mathrm{GL}_2(A_F)$ the subgroup consisting of elements of the form $\begin{pmatrix} * & 0 \\ & * \end{pmatrix}$.

Lemma 4.4.10. *The group $\mathrm{GL}_2(A_F)$ is generated by P and $J_2 = \begin{pmatrix} & \\ -1 & 1 \end{pmatrix}$.*

Proof. We give a direct proof. Suppose $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is in $\mathrm{GL}_2(A_F)$. We first check that we may assume c is invertible. Multiplying g on the right by J_2 , we may assume $\mathrm{rank} d \geq \mathrm{rank} c$. Now, consider $g^{-1} = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$. We get that $cq + ds = 1$, and thus

$$1 = n(cq + ds) = n(c)n(q) + (c^\#d, sq^\#) + (d^\#c, qs^\#) + n(d)n(s).$$

Now, if d is rank 3, we are done, and if $c = 0$, then d is rank three. If both c and d are rank at most 1, then $n(cq + ds) = 0$, so we cannot have this case. Thus we may assume d is rank two, and c is rank two or rank one. We conclude that not both of $c^\#d$ and $d^\#c$ are 0. It follows that we can find $y \in A_F$ and $\lambda \in \mathrm{GL}_1(F)$ so that $\lambda(c^\#d, y) + \lambda^2(d^\#c, y^\#) \neq 0$. Indeed, if this is 0 for all λ and fixed y , then $(c^\#d, y) = 0$ and $(d^\#c, y^\#) = 0$, and if these are 0 for all y , then $c^\#d = 0$ and $d^\#c = 0$. Hence, there exists $x = \lambda y$ for which $n(c + dx) \neq 0$, and thus $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & \\ x & 1 \end{pmatrix} = \begin{pmatrix} * & \\ c+dx & * \end{pmatrix}$ has an invertible entry in the bottom row.

Thus, we've shown that we can multiply g by elements of P and J_2 so that the bottom right entry of g is invertible. Now, multiply $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ on the right by $\begin{pmatrix} 1 & \\ x & 1 \end{pmatrix}$, where $x = -d^{-1}c$. One obtains an element in $P^{op} = \begin{pmatrix} * & \\ 0 & * \end{pmatrix}$. Conjugation by J_2 moves P^{op} to P , thus completing the lemma. \square

For $m \in M_2(A)$, denote by $\det(m)$ the degree 6 reduced norm on $M_2(A)$.

Corollary 4.4.11. *The action of $\mathrm{GL}_2(A)$ on W_A induced by the isomorphism $V_A \rightarrow W_A$ and the natural action of $\mathrm{GL}_2(A)$ on V_A preserves the symplectic and quartic form on W_A . That is, $\langle g \cdot v, g \cdot w \rangle = \det(g) \langle v, w \rangle$ and $q(g \cdot v) = \det(g)^2 q(v)$ for all $v, w \in W_A$.*

Proof. This follows immediately from Lemmas 4.4.9 and 4.4.10. \square

Note that since V_A is defined polynomially, it is a module for $M_2(A)$. We will require the following fact below.

Corollary 4.4.12. *Suppose $m \in M_2(A)$, and $x, y \in V_A$. Then $\langle mx, my \rangle = \det(m) \langle x, y \rangle$ and $q(mx) = \det(m)^2 q(x)$.*

Proof. The difference $\langle mx, my \rangle - \det(m)\langle x, y \rangle$ is 0 for all $m \in \mathrm{GL}_2(A) \subseteq M_2(A)$. Since $\mathrm{GL}_2(A)$ is Zariski dense in $M_2(A)$, the identity follows. The second identity is similar. \square

Recall the element $R(v) \in M_2(A)$ defined for $v \in W_A$.

Lemma 4.4.13. *For $g \in \mathrm{GL}_2(A)$, we have $R(g \cdot v) = \det(g)gR(v)g^{-1}$. Here $g \cdot v$ is the left action of $\mathrm{GL}_2(A)$ on W_A .*

Proof. This follows immediately from Lemma 4.4.9 and Proposition 4.4.3. \square

All of the above constructions and proofs can be made analogously for the right action of $\mathrm{GL}_2(A)$ on row vectors A^2 , which then induces a right action of $\mathrm{GL}_2(A)$ on W_A . We state explicitly the ‘‘right’’ version of the previous lemma. Set $R_r(v) = J_2 R(v) J_2^{-1}$, where $J_2 = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$. We have the following.

Lemma 4.4.14. *The element $\begin{pmatrix} 1 & X \\ & 1 \end{pmatrix}$ acts on the right of W_A as the map $n(X)$; the element $J_2 = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$ acts on the right of W_A as $-w_A$, i.e., $(a, b, c, d) \cdot J_2 = (-d, c, -b, a)$; and the element $\begin{pmatrix} m & \\ & n \end{pmatrix}$ acts on the right of W_A as the map $R(m, n)$, with*

$$(a, b, c, d) \cdot R(m, n) = (n_A(m)a, m^\#bn, n^\#cm, n_A(n)d).$$

For $g \in \mathrm{GL}_2(A)$, we have $R_r(v \cdot g) = \det(g)g^{-1}R_r(v)g$. Here $v \cdot g$ is the right action of $\mathrm{GL}_2(A)$ on W_A .

Definition 4.4.15. Suppose R is a semisimple ring, by which we mean R is a subring of a finite product of fields $k = \prod_i k_i$. Assume $A = A_R$ is an associative cubic norm structure over R . Then, we define $V_{A_k} = \prod_i V_{A_{k_i}}$ together with its associated $\mathrm{GL}_2(A_k) = \prod_i \mathrm{GL}_2(A_{k_i})$ -action, and we have a k -linear isomorphism of V_{A_k} with $W_{A_k} = \prod_i W_{A_{k_i}}$. We define V_{A_R} to be the image of $(W_2(A_R)^{\otimes 3}/I_A)^{S_3}$ in V_{A_k} , and then we similarly have an R -linear isomorphism of V_{A_R} with W_{A_R} .

4.4.4. An invariant of rank one elements of W_{A_F} . All the rank one lines in W_{A_F} are in the same $\mathrm{GL}_2(A_F)$ orbit, but that there is slight extra invariant of the rank one elements of W_{A_F} , that distinguishes different $\mathrm{GL}_2(A_F)$ -orbits. This invariant measures how far a rank one element is from one of the form ℓ^1 or η^1 . We will now define this invariant.

Suppose k is a field, $A = A_k$ is an associative cubic norm structure over k , and $v \in W_A$ is rank one. Then there is a row vector $\ell \in A^2$ so that $\langle \ell^1, v \rangle \neq 0$, and similarly a column vector $\eta \in A^2$ so that $\langle v, \eta^1 \rangle \neq 0$. The following lemma says that these elements of k^\times give well-defined classes in $k^\times/n(A^\times)$, and in fact this class is the same if one uses row vectors or column vectors.

Lemma 4.4.16. *Suppose k is a field, $A = A_k$ is an associative cubic norm structure over k , and $v \in W_A$ is rank one. Then, there an element $\lambda \in k^\times$ so that*

$$(10) \quad \{ \langle \ell^1, v \rangle : \ell \in A^2 \text{ row vector} \} \cap k^\times = \lambda n(A^\times) = \{ \langle v, \eta^1 \rangle : \eta \in A^2 \text{ column vector} \} \cap k^\times.$$

As a consequence of the lemma, we can make the following definition.

Definition 4.4.17. Suppose k is a field, A is an associative cubic norm structure over k , and v in W_A is rank one. We define $\lambda(v) \in k^\times/n(A^\times)$ to be the class of λ determined by Lemma 4.4.16. Similarly, if $k = \prod_i k_i$ is a finite product of fields, A is an associative cubic norm structure over k , and $v = \prod_i v_i \in W_A$ is rank one in every component, then we define $\lambda(v) = \prod_i \lambda(v_i)$ in $\prod_i k_i^\times/n(A_{k_i}^\times) = k^\times/n(A^\times)$.

Proof of Lemma 4.4.16. Suppose $r \in A$. Since $(r\ell)^1 = n(r)\ell^1$ and $(\eta r)^1 = n(r)\eta^1$, the sets on the left and right side of (10) are $n(A^\times)$ -cosets.

Since all rank one lines are in the same $\mathrm{GL}_2(A)$ -orbit, there is $\lambda_1, \lambda_2 \in k^\times$, and η_1, ℓ_2 a column vector and a row vector in A^2 , so that $v = \lambda_1 \eta_1^1 = \lambda_2 \ell_2^1$. Now, suppose $v = \lambda_1 \eta_1^1$. Then for any $\ell \in A^2$ a row vector, $\langle \ell^1, v \rangle = \lambda_1 n(\ell J_2 \eta_1)$, where $J_2 = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$. Hence it follows that the set on the

left of (10) forms a single $n(A^\times)$ -coset, and this coset is represented by λ_1 . Similarly for the set on the right of (10); it forms a single $n(A^\times)$ -coset represented by λ_2 .

It remains to prove that λ_1 and λ_2 represent the same class in $k^\times/n(A^\times)$. This is clear if either the “ a ” or “ d ”-components of v are nonzero, and in general it follows from this and the $\mathrm{GL}_2(A)$ action. \square

In the following lemma, and below, a primitive vector of $W_2(A_F)$ is a vector which may be completed to an A_F -basis of $W_2(A_F)$.

Lemma 4.4.18. *Suppose $\eta \in W_2(A_F)$, and $\eta^! \neq 0$ in W_{A_F} . Then η is primitive.*

Proof. Write $\eta = \begin{pmatrix} u \\ v \end{pmatrix}$. Since $\eta^! \neq 0$, by acting by $\mathrm{GL}_2(A_F)$, we may assume $\eta^! = \gamma(1, 0, 0, 0)$ for some $\gamma \in F^\times$. But then $n(u) \in F^\times$, so η is primitive. \square

5. THE FIRST LIFTING LAW FOR W_J

Suppose A is an associative cubic norm structure, over the field F or over a subring R of F . Then the group $\mathrm{GL}_2(A)$ acts on W_A , as shown in the previous section. Denote by $\mathrm{SL}_2(A)$ the subgroup of $\mathrm{GL}_2(A)$ that is kernel of the degree 6 norm map. Equivalently, $\mathrm{SL}_2(A)$ is the subgroup of $\mathrm{GL}_2(A)$ that acts on W_A with similitude 1. The purpose of this section is to parametrize the orbits of $\mathrm{SL}_2(A)$ on W_A , over the field F and over a subring R of F . We begin by proving two lifting laws, one for general cubic norm structures J and another more precise lifting law for associative cubic norm structures A . We then use the second of these lifting laws to parametrize the orbits of $\mathrm{SL}_2(A)$ on W_A .

The lifting laws are proved in subsection 5.1. In subsection 5.2, we parametrize the orbits of $\mathrm{SL}_2(A)$ on W_A over a field F , and in subsection 5.3 we parametrize the orbits over a subring R of F . The main result of this section is Corollary 5.3.8, which implies Theorem 3.1.7.

5.1. The lifting law. In this subsection, we state the two lifting laws. The first lifting law applies to the general case of W_J with J a cubic norm structure, while the second lifting law applies to the case W_A with A an associative cubic norm structure, but gives more information.

Here is the first lifting law. It is likely known to experts in Freudenthal triple systems.

Theorem 5.1.1. *Let J be a cubic norm structure over the field F . Suppose $v \in W_J$ has $q(v) \neq 0$, and suppose $F \subseteq k$ is an extension of fields, and $\omega \in k$ satisfies $\omega^2 = q(v)$ in F . The elements $\omega v \pm v^b$ in $W_J \otimes_F k = W_{J_k}$ are rank one. In fact, one has the equality*

$$(11) \quad 3t(\omega v + v^b, \omega v + v^b, x) = \langle x, \omega v + v^b \rangle (\omega v + v^b)$$

for all $x \in W_{J_k}$ and similarly for $\omega v - v^b$.

Proof. Note that the fact that $\omega v + v^b$ is rank one follows immediately from (11), which gives more information. So, we must check (11).

As mentioned, this result is likely known to experts in Freudenthal triple systems. For instance, it follows by a one-line computation from the definition of a Freudenthal triple system and [Spr06, Lemma 4.4]. One can also give a simple proof using prehomogeneity and equivariance for the action of group $H(W_{J_k})$. Indeed, it is immediately seen that both sides of (11) change in the same way under the action of $H(W_{J_k})$, thus it suffices to check the equality (11) at a single non-degenerate v in W_J . For instance, if one takes $v = (a, 0, 0, d)$, both sides of (11) are easy to compute, and they are seen to be equal. \square

For v, ω as in Theorem 5.1.1, set $X(v) = (\omega v + v^b)/2$ and $\overline{X(v)} = (-\omega v + v^b)/2$. Note that $\langle X(v), \overline{X(v)} \rangle = \omega q(v)$.

We give a complement to the lifting law, which explains the way in which the rank one lift $X(v)$ of v is unique.

Lemma 5.1.2. *Suppose k is a field, E is an étale extension of k , $\omega \in E$ satisfies $\omega^2 \in k$ and $1, \omega$ are linearly independent over k . Additionally, suppose J is a cubic norm structure over k , $v_1, v_2 \in W_J$ with $q(v_1) \neq 0$, and $X = \omega v_1 + v_2 \in W_J \otimes_k E$ is rank one. Then there is $t \in k^\times$ so that $(t^{-1}\omega)^2 = q(v_1)$ and $v_2 = tv_1^\flat$. Consequently, $t^{-1}X = (t^{-1}\omega)v_1 + v_1^\flat$.*

Proof. By equivariance and passing to the algebraic closure, we may assume $v_1 = (a, 0, 0, d)$ with $a, d \in k^\times$. Write $v_2 = (a', b', c', d')$, so $X = (\omega a + a', b', c', \omega d + d')$. Then since X is rank one, $(b')^\# = (\omega a + a')c'$, $(c')^\# = (\omega d + d')b'$, and $3(\omega a + a')(\omega d + d') = (b', c')$.

From the first equation, we deduce $c' = 0$, and from the second that $b' = 0$. We then get from the third equation that $\omega(ad' + a'd) + (a'd' + \omega^2(ad)) = 0$. Since a, d are in k^\times , there exists $t \in k$ so that $a' = -ta^2d$, $d' = tad^2$, and we then get that $\omega^2 = t^2(ad)^2$. Note that if t is in some extension field of k , and $v_2 = tv_1^\flat$, then necessarily $t \in k$. Since $(a, 0, 0, d)^\flat = (-a^2d, 0, 0, ad^2)$ and $q((a, 0, 0, d)) = (ad)^2$, we obtain $\omega^2 = t^2q(v_1)$ and $v_2 = tv_1^\flat$. Because $1, \omega$ are assumed linearly independent, $t \neq 0$, and thus $t \in k^\times$. The lemma follows. \square

Suppose F is a field, J is a cubic norm structure over F , E is an étale quadratic extension of F , and $X \in W_J \otimes_F E = W_{J_E}$ is rank 1. Say X is *admissible* if $X = (\omega v + v^\flat)/2$ for some $\omega \in E^\times \setminus F^\times$ and $v \in W_J$ with $\omega^2 = q(v)$. Below we will need to understand when λX is admissible, for $\lambda \in E^\times$.

Lemma 5.1.3. *Let the notation be as above, and assume $X = (\omega v + v^\flat)/2$ is admissible. If $\mu \in E^\times$, $\mu = \alpha + \beta\omega$ with $\alpha, \beta \in F$, then*

$$\mu n_{E/F}(\mu)X = (n_{E/F}(\mu)\omega)(\alpha v + \beta v^\flat)/2 + n_{E/F}(\mu)(\alpha v^\flat + q(v)\beta v)/2$$

is admissible. In particular, one has the identities

$$(12) \quad q(\alpha v + \beta v^\flat) = (\alpha^2 - q(v)\beta^2)^2 q(v)$$

and

$$(13) \quad (\alpha v + \beta v^\flat)^\flat = (\alpha^2 - q(v)\beta^2)(\alpha v^\flat + q(v)\beta v).$$

Proof. The admissibility of $\mu n_{E/F}(\mu)X$ follows from the identities (12) and (13), and these identities are familiar from the theory of Freudenthal triple systems. For example, (13) is [Spr06, Lemma 4.5]. The reader can check these identities themselves by observing that both sides of (12) and (13) are equivariant under the action of $g \in H(W_J)$ with $\nu(g) = 1$, and then checking them for $v = (a, 0, 0, d)$. (This is essentially how (13) is proved in [Spr06].) For $v = (a, 0, 0, d)$,

$$\alpha v + \beta v^\flat = ((\alpha - \beta ad)a, 0, 0, (\alpha + \beta ad)d),$$

and (12), (13) follow. \square

We now give the more precise lifting law that applies when A is an associative cubic norm structure.

Theorem 5.1.4. *Let A be an ACNS over F . Suppose $v \in W_A$ has $q(v) \neq 0$, $E = F[x]/(x^2 - q(v))$, and denote by ω the image of x in E . Set $X(v) = (\omega v + v^\flat)/2$ in $W_A \otimes_F E$, and $\overline{X(v)} = (-\omega v + v^\flat)/2$, and recall the element $R(v) \in M_2(A)$ that satisfies $R(v)^2 = q(v)$. Then for all column vectors $\eta \in A_E^2$, one has*

$$\left(\left(\frac{\omega + R(v)}{2} \right) \eta \right)^\flat = \langle X(v), \eta^\flat \rangle \overline{X(v)}$$

in $W_A \otimes E$. Similarly, if $\ell \in A_E^2$ is a row vector, and $R_r(v) = J_2 R(v) J_2^{-1}$ (see Lemma 4.4.14 and the discussion preceding it), then

$$\left(\ell \left(\frac{\omega + R_r(v)}{2} \right) \right)^\flat = \langle \ell^\flat, \overline{X(v)} \rangle X(v).$$

Remark 5.1.5. In Theorem 5.1.1, which takes place in the context of arbitrary cubic norm structures, the element $X(v)$ was proved to be rank one. Theorem 5.1.4 proves a stronger statement in the special case when the cubic norm structure is an ACNS. Namely, Theorem 5.1.4 gives an explicit decomposition of $X(v)$ as a “pure tensor”, i.e., as an explicit scalar times the shriek (!) of an element of A_E^2 .

Proof of Theorem 5.1.4. The equality in question is polynomial in nature, and thus by prehomogeneity it suffices to check equivariance of both sides and to check it for particular v 's. The equivariance is immediate using $R(gv) = gR(v)g^{-1}$, $gX(v) = X(gv)$ for $g \in \mathrm{SL}_2(A)$. A short computation verifies the identity when $v = v_0 = (a, 0, 0, d)$, in which case $R(v) = \begin{pmatrix} ad & \\ & -ad \end{pmatrix}$. \square

5.2. Orbits over a field. In this subsection, we assume F is a field, and A is an associative cubic norm structure over F . We parametrize the orbits of $\mathrm{SL}_2(A)$ on the elements of W_A with rank 4.

More precisely, suppose $v \in W_A$ has $q(v) \neq 0$. Define $E = E_{q(v)} = F[x]/(x^2 - q(v))$, denote ω the image of x in E , and denote by $y \mapsto \bar{y}$ the nontrivial involution on E , so that $\bar{\omega} = -\omega$. Now, let $X(v) = (\omega v + v^b)/2$ in $W_A \otimes_F E = W_{A_E}$. Associate to v the invariants $q(v)$ and $\lambda(X(v)) \in E^\times/n(A_E^\times)$. This latter invariant λ was defined in Definition 4.4.17. The purpose of this subsection is to prove the following theorem. Many of the instances of this theorem are closely related to results of Wright-Yukie [WY92] and Kable-Yukie [KY97], which were proven by means of Galois cohomology.

Theorem 5.2.1. *For $v \in W_A$ with $q(v) \neq 0$, the invariant $\lambda(v) := \lambda(X(v))$ satisfies $n_{E/F}(\lambda) \in F^\times \cap n_{A_E}(A_E^\times)$. The association $v \mapsto (E_{q(v)}, \omega, \lambda(X(v)))$ defines a bijection between $\mathrm{SL}_2(A)$ orbits on the rank 4 elements of W_A and triples (E, ω, λ) of this kind, up to isomorphism. An isomorphism of a triple (E, ω, λ) with (E', ω', λ') is an F -algebra isomorphism $\phi : E \rightarrow E'$ satisfying $\phi(\omega) = \omega'$ and $\phi(\lambda) = \lambda'$.*

Proof. Note that we have

$$\langle X(v), \overline{X(v)} \rangle = \frac{1}{4} \langle \omega v + v^b, -\omega v + v^b \rangle = \frac{2\omega}{4} \langle v, v^b \rangle = \omega q(v) \in E^\times.$$

It follows that $X(v)$ is nonzero in every component of W_{A_E} , and thus the invariant $\lambda(v)$ is defined.

That $n_{E/F}(\lambda(v))$ is a norm from $n(A_E)$ follows quickly from the lifting law. Indeed, set $U = \frac{\omega + R(v)}{2}$ in $M_2(A_E)$, and suppose $\eta \in A_E^2$ is a column vector with $\langle X(v), \eta^! \rangle = \lambda(v) \in E^\times$. Then since $\lambda(\overline{X(v)}) = \overline{\lambda(X(v))}$, there is a row vector $\ell \in A_E^2$ with $\langle \ell^!, \overline{X(v)} \rangle = \overline{\lambda(v)}$. Hence

$$n(\ell J_2 U \eta) = \langle \ell^!, (U\eta)^! \rangle = \langle X(v), \eta^! \rangle \langle \ell^!, \overline{X(v)} \rangle = \lambda(v) \overline{\lambda(v)},$$

proving that $n_{E/F}(\lambda(v))$ is in $F^\times \cap n_{A_E}(A_E^\times)$. Here we have used Lemma 4.4.5 for the first equality and the lifting law Theorem 5.1.4 for the second.

Suppose now $v' = g \cdot v$ with $g \in \mathrm{SL}_2(A)$. Then $q(v) = q(v')$, and $(v')^b = (g \cdot v)^b = \nu(g) (g \cdot v^b) = g \cdot v^b$. Hence $g \cdot X(v) = \omega g \cdot v + g \cdot v^b = X(v')$. It follows that v and v' have isomorphic invariants.

Before we complete the proof of the theorem, we give some necessary intermediate results. \square

Proposition 5.2.2. *Suppose $v \in W_A$ is non-degenerate, i.e., $q(v) \neq 0$. Then, there exists $\lambda \in E^\times$ and a primitive vector v_0 in $W_2(A_E)$ for which $X(v) = \lambda v_0^!$. Furthermore, if one sets*

$$v_1 = \left(\frac{\omega - R(v)}{2\omega} \right) v_0,$$

then $R(v)v_1 = -\omega v_1$ and $\lambda v_1^! = X(v)$.

Proof. We have already established the first part of the proposition. Now, let v_1 be as in the statement. Then $R(v)v_1 = -\omega v_1$, and by the lifting law,

$$\begin{aligned} \lambda v_1^\dagger &= -\frac{\lambda}{\omega^3} \left(\left(\frac{-\omega + R(v)}{2} \right) v_0 \right)^\dagger \\ &= -\frac{\lambda}{\omega^3} \langle X(v), v_0^\dagger \rangle X(v) \\ &= \frac{1}{\omega^3} \langle X(v), \overline{X(v)} \rangle X(v) \\ &= X(v). \end{aligned}$$

This completes the proof. \square

We can now establish the fact that if $v, v' \in W_A$ have isomorphic invariants, then they are in the same $\mathrm{SL}_2(A)$ orbit, as stated in the following lemma.

Lemma 5.2.3. *Suppose $v, v' \in W_A^{rk=4}$ have isomorphic invariants, so that in particular $q(v) = q(v') \neq 0$. Then, there is $g \in \mathrm{SL}_2(A)$ with $g \cdot v = v'$.*

Proof. Since v, v' have isomorphic invariants, we may write $\lambda v_1^\dagger = \lambda v_0^\dagger = X(v)$ and $\lambda(v_1')^\dagger = \lambda(v_0')^\dagger = X(v')$, where $v_0, v_0' \in W_2(A_E)$ are primitive, $\lambda \in E^\times$, and v_1, v_1' are as in the Proposition 5.2.2.

Since v_0, v_0' are primitive, there exists $\tilde{g} \in \mathrm{GL}_2(A_E)$ satisfying $\tilde{g}v_0 = v_0'$. Write $\tilde{g} = g_1 - \omega g_\omega$, with $g_* \in M_2(A)$, and set $g = g_1 + g_\omega R(v)$. Then $g \in M_2(A)$. We have

$$\begin{aligned} g \cdot X(v) &= \lambda g \cdot v_0^\dagger = \lambda g \cdot v_1^\dagger \\ &= \lambda ((g_1 + g_\omega R(v))v_1)^\dagger \\ &= \lambda ((g_1 - g_\omega \omega)v_1)^\dagger \\ &= \lambda \tilde{g} \cdot v_1^\dagger = \tilde{g} \cdot X(v) \\ &= X(v'). \end{aligned}$$

Hence $g \cdot v = v'$ and $g \cdot v^b = (v')^b$. Thus, since $q(v) = q(v')$,

$$2q(v) = 2q(v') = \langle v', (v')^b \rangle = \langle g \cdot v, g \cdot v^b \rangle = \det(g) \langle v, v^b \rangle = 2 \det(g) q(v).$$

This proves $\det(g) = 1$, and in particular $g \in M_2(A)$ is actually invertible and in $\mathrm{SL}_2(A)$. This completes the proof. \square

Finally, to complete the proof of Theorem 5.2.1, we must check that every (E, ω, λ) with $n_{E/F}(\lambda) \in F^\times \cap n(A_E^\times)$ arises as an actual invariant of some $v \in W_A$ of rank 4. To see that these invariants do all arise, first set $v = (0, 1, 0, d)$, with $d \in F^\times$. Write $d^{1/2}$ for the image of x in $F[x]/(x^2 - d)$; one has $\omega = 2d^{1/2}$. Then $X(v) = (1, d^{1/2}, d, d^{3/2})$, and thus $\lambda(X(v)) = 1$. Hence, all invariants $(E, \omega, 1)$ appear.

Now, suppose $\lambda \in E^\times$ satisfies $n_{E/F}(\lambda) \in F^\times \cap n(A_E^\times)$. Then from Corollary 5.1.3, we know $\lambda n(\lambda) X(v) = X(v')$ for some $v' \in W_A$ with $q(v') \neq 0$. But $\lambda(X(v')) = \lambda n(\lambda)$, which represents the same class as λ since $n(\lambda) \in n(A_E^\times)$. Hence all classes (E, ω, λ) arise, as desired. This completes the proof of Theorem 5.2.1.

5.3. Balanced modules and integral orbits. In this subsection we parametrize the orbits of essentially $\mathrm{GL}_2(A)$ on W_A , when A is an ACNS over the integral domain R . More precisely, we prove Theorem 3.1.7, and thus Theorem 1.1.1 of the introduction.

In this subsection, we assume R is an integral domain, with fraction field F of characteristic 0, and R satisfies $\frac{x^2+x}{2}$ is in R for all $x \in R$. The characterization of quadratic rings over R is as discussed in paragraph 4.1.1: these quadratic rings are of the form $S_D = R[y]/(y^2 - Dy + \frac{D^2-D}{4})$,

where D is congruent to a square modulo $4R$; we denote τ_D or τ the image of y in S_D . If S is a quadratic ring over R , and $(1, \tau)$ is a basis of S as an R -module, we say that $(1, \tau)$ is a *good basis* of S if τ satisfies a quadratic equation $\tau^2 - D\tau + \frac{D^2-D}{4}$ for some $D \in R$ (necessarily a square modulo $4R$).

The letter A denotes an ACNS over R . There is a cubic polynomial action of $\mathrm{GL}_2(A)$ on W_A , which we take to be the action on the right. Set $G_1 = \mathrm{GL}_1(R) \times \mathrm{GL}_2(A)$. Let $(\lambda, g) \in \mathrm{GL}_1(R) \times \mathrm{GL}_2(A)$ act on $v \in W_A$ by $v \mapsto \lambda^{-1}(v \cdot g)$. We define $G \subseteq \mathrm{GL}_2(A)$ to be the pairs (λ, g) where $\lambda^3 = \det_6(g)$.

5.3.1. *Preliminaries.* We now give the various preliminaries that we will need, much of which is a repetition of facts and notations from above.

Suppose $v \in W_A$ has $q(v) = D \neq 0$. We set $E = F[x]/(x^2 - q(v))$ and let ω denote the image of x in E . Of course, S_D is a subring of E . We define $X(v) \in W_A \otimes_R E$ as

$$X(v, \omega) = X(v) = \frac{\omega v + v^\flat}{2} = \frac{q(v) + \omega}{2}v + \frac{v^\flat - q(v)v}{2} = \tau_D v + \frac{v^\flat - q(v)v}{2}.$$

By using the formula for v^\flat from Lemma 4.3.1, one checks easily that the assumption that $x^2 + x \in 2R$ for all $x \in R$ implies $\frac{v^\flat - q(v)v}{2}$ is in W_A . Hence, $X(v) \in W_A \otimes S_D$. Similarly, one defines $X(v, -\omega) = \overline{X(v)} = \frac{-\omega v + v^\flat}{2}$, which is also in $W_A \otimes S_D$. One has the equality $\langle X(v, \omega), X(v, -\omega) \rangle = \omega^3$.

Set $S(v) \in \frac{1}{2}M_2(A)$ as in subsection 4.4, and $R_r(v) = 2JS(v)$, where $J = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$. One has $R_r(v)^2 = q(v) = D$. We also record the equivariance property of $R_r(v)$: $R_r(v \cdot g) = \det(g)g^{-1}R_r(v)g$ for $g \in \mathrm{GL}_2(A)$.

We need two other pieces of notation: if $\ell = (s, t) \in A^2$ is a row vector, set $\ell^\# = (n(s), s^\#t, t^\#s, n(t))$ in W_A . Furthermore, set

$$\epsilon = \epsilon(v) = \frac{\omega + R_r(v)}{2\omega} = \frac{1}{2} + \frac{1}{2\omega}R_r(v).$$

Finally, note that

$$\omega\epsilon = \frac{\omega + R_r(v)}{2} = \frac{\omega + q(v)}{2} + \frac{R_r(v) - q(v)}{2} = \tau_D + \frac{R_r(v) - q(v)}{2} = \tau_D - \frac{D}{2} + JS(v).$$

Using again that $x^2 + x \in 2R$ for all $x \in R$, one checks that $\frac{R_r(v) - q(v)}{2} = -\frac{D}{2} + JS(v)$ is in $M_2(A)$.

We these notations behind us, we can restate the lifting law, Theorem 5.1.4: For all row vectors $\ell \in A_F^2$,

$$\omega^3(\ell\epsilon(v))^\# = \langle \ell^\#, X(v, -\omega) \rangle X(v)$$

in $W_A \otimes E$. If $\ell \in A^2$, then both sides are in $W_A \otimes S_D$.

Set $\Omega = \Omega(v) = \frac{q(v) + R_r(v)}{2}$. Then $\Omega(v) \in M_2(A)$, and satisfies $\Omega^2 - D\Omega + \frac{D^2-D}{4} = 0$. Thus Ω defines an action of S_D on the column vectors A^2 .

5.3.2. *Balanced modules.* We consider a class of $S_D \otimes A = S \otimes A$ modules $I \subseteq A_E$ as follows.

Definition 5.3.1. If $I \subseteq E \otimes A$, we say that I is an $S \otimes A$ -fractional ideal if

- I is closed under left multiplication by S and right multiplication by A ;
- I is free of rank 2 as an A -module;
- $I_F = E \otimes A$ is free of rank one as an A_E -module.

If $(\tau, 1)$ is a good basis of S , and $I = b_1A \oplus b_2A$ with $b_1, b_2 \in E \otimes A$, define the **norm** of I $N(I; \tau, (b_1, b_2)) = \det_6(g)$ where $g \in M_2(A_F)$ is the unique matrix with $(b_1, b_2) = (\tau \otimes 1, 1 \otimes 1)g$. Explicitly, if $b_1 = \tau m_{11} + m_{21}$ and $b_2 = \tau m_{12} + m_{22}$, with $m_{ij} \in A_F$, define $N(I; \tau, (b_1, b_2)) = \det_6 \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}$. This definition does depend on the good basis $(\tau, 1)$ of S and on the A -basis (b_1, b_2) of I .

If $\beta \in E^\times$, and $I, \tau, (b_1, b_2)$ are as above, we say the data $(I, (b_1, b_2), \tau, \beta)$ is **balanced** if $\beta^{-1}(x, y)^! \in W_A \otimes S$ for all $x, y \in I$ and $N(I; \tau, (b_1, b_2)) = N_{E/F}(\beta)$.

Suppose $(I, (b_1, b_2), \beta, \tau)$ is data as above. Set

$$X(I, b, \beta) := \beta^{-1}b^! \in W_{A_E} = W_A \otimes_R E.$$

It is clear that $X(I, b, \beta) \in W_A \otimes S$ if and only if $\beta^{-1}(x, y)^! \in W_A \otimes S$ for all $x, y \in I$. We next define an equivalence relation on data (I, b, β) .

Definition 5.3.2. The triple (I, b, β) is said to be *equivalent* to the triple (I', b', β') if there exists $x \in A_E^\times$ so that $I' = xI$, $b' = xb$, and $\beta' = n_{A_E}(x)\beta$.

It is clear that if (I, b, β) is equivalent to (I', b', β') , then $X(I, b, \beta) = X(I', b', \beta')$. The converse is also true, as the following lemma proves.

Lemma 5.3.3. *If $X(I, b, \beta) = X(I', b', \beta')$, then there exists $x \in A_E^\times$ so that $b' = xb$ and $\beta' = n_{A_E}(x)\beta$.*

Proof. Since $b = (\tau, 1)g$, b is primitive, and thus there is $h \in \text{GL}_2(A_E)$ so that $b_0 = bh = (1, 0)$. Set $b_1 = b'h = (s, t)$. Then $\beta^{-1}b_0^! = (\beta')^{-1}b_1^!$ yields that $\beta' = n(s)\beta$, so $s \in A_E^\times$, and then that $t = 0$. Hence $\beta' = n(s)\beta$ and $b_1 = sb_0$. The lemma follows. \square

The following equivalent criterion for a module to be balanced is useful.

Lemma 5.3.4. *Suppose I is a fractional $S \otimes A$ -ideal, $b = (b_1, b_2)$ is an A basis of I , and $\beta \in E^\times$. Suppose moreover that $(1, \tau)$ is a good basis of S , and set $\omega = \tau - \bar{\tau}$. Recall $X = X(I, b, \beta) = \beta^{-1}b^!$. Then $\langle X, \bar{X} \rangle = \omega^3 \frac{\det_6(g)}{N_{E/F}(\beta)}$. It follows that if $X \in W_A \otimes S$, the triple (I, b, β) is balanced if and only if $\langle X, \bar{X} \rangle = \omega^3$.*

Proof. We have

$$\langle X, \bar{X} \rangle = \frac{1}{N_{E/F}(\beta)} \langle (\tau, 1)^! \cdot g, (\bar{\tau}, 1)^! \cdot g \rangle = \frac{\det_6(g)}{N_{E/F}(\beta)} (\tau - \bar{\tau})^3 = \omega^3 \frac{\det_6(g)}{N_{E/F}(\beta)}.$$

The lemma follows. \square

The elements of W_A^{open} parametrize pairs (S, M) , where S is a quadratic ring over R and M is an equivalence class of based balanced modules (I, b, β) . First, a technical lemma.

Lemma 5.3.5. *Suppose $v \in W_A$ is rank 4 and recall the element $\epsilon = \epsilon(v)$ of $M_2(A_E)$. Then, there is $\eta \in A_F^2$ (column vectors) and $\ell \in A_F^2$ (row vectors) so that $\ell\epsilon\eta$, in A_E , is actually in A_E^\times .*

Proof. For all row vectors x and column vectors y in A_E^2 , one has $n_{A_E}(xJ_2y) = \langle x^!, y^! \rangle$. Thus

$$\omega^3 n_{A_E}(\ell\epsilon\eta) = \langle \omega^3(\ell\epsilon)^!, (J_2^{-1}\eta)^! \rangle = \langle \ell^!, X(v, -\omega) \rangle \langle X(v, \omega), (J_2^{-1}\eta)^! \rangle.$$

This latter term can be made to lie in E^\times for appropriate choices of ℓ, η , since $\langle X(v, \omega), X(v, -\omega) \rangle \in E^\times$. To see this, first note that since $\langle X(v, \omega), X(v, -\omega) \rangle \in E^\times$ there is $\ell_1 \in A_E^2$ with $\langle \ell_1^!, X(v, \omega) \rangle \in E^\times$. Now, set $\ell = \text{tr}_{E/F}(\ell_1\epsilon)$, taking the trace $\text{tr}_{E/F}(\cdot)$ individually on each of the two entries of $\ell_1\epsilon$. Then one computes $\ell\epsilon = \ell_1\epsilon$. Hence

$$\langle \ell^!, X(v, -\omega) \rangle X(v) = \omega^3(\ell\epsilon)^! = \omega^3(\ell_1\epsilon)^! = \langle \ell_1^!, X(v, -\omega) \rangle X(v),$$

from which it follows that $\langle \ell^!, X(v, -\omega) \rangle \in E^\times$. Similarly one finds an $\eta \in A_F^2$ with $\langle X(v, \omega), (J_2^{-1}\eta)^! \rangle \in E^\times$. The lemma follows. \square

Given a row vector $\ell \in A_F^2$, one defines a map $\Phi^\ell : A^2 \rightarrow A_E$ from the column vectors A^2 to A_E via $\Phi^\ell(\eta) = \ell\eta$. Note that Φ^ℓ is an $S \otimes A$ module map, with S acting on the left of the column vectors A^2 via $\Omega(v)$ and A acting on the right of them by multiplication $A \otimes A \rightarrow A$. The previous lemma implies that ℓ can be chosen so that $\Phi^\ell(A_F^2)$ contains a unit of A_E . By dimension count, it follows that for this ℓ , Φ^ℓ is an A_E -module isomorphism $A_F^2 \rightarrow A_E$.

Choose any such ℓ as above, and set $I(\ell) = \Phi^\ell(A^2)$, $b(\ell) = \ell\epsilon = (b_1, b_2)$, so that $b_1 = \Phi^\ell((1, 0)^t)$ and $b_2 = \Phi^\ell((0, 1)^t)$. Set $\beta(\ell) = \omega^{-3}\langle \ell^!, X(v, -\omega) \rangle$. One has $\beta(\ell) \in E^\times$ (from the proof of Lemma 5.3.5, for example). We claim $(I(\ell), b(\ell), \beta(\ell))$ is balanced. Indeed, the lifting law gives $\beta(\ell)^{-1}(b(\ell))^! = X(v)$ is in $W_A \otimes S$, and thus that $(I(\ell), b(\ell), \beta(\ell))$ is balanced follows from Lemma 5.3.4.

From the above remarks, and an application of the lifting law and Lemma 5.3.3, we see that $v \mapsto (I(\ell), b(\ell), \beta(\ell))$ yields an equivalence class of based balanced modules. There is also a map in the other direction

$$(I, b, \beta) \mapsto X(I, b, \beta) = \tau v + v' \mapsto v \in W_A.$$

Lemma 5.3.6. *If (I, b, β) as above is balanced, and $X(I, b, \beta) = \tau v + v'$, then $q(v) = \omega^2$ and in particular v is rank 4.*

Proof. Since (I, b, β) is a balanced triple, one has $\langle X(I, b, \beta), \overline{X(I, b, \beta)} \rangle = \omega^3$. This implies that $X(I, b, \beta) = \frac{\omega v + v_2}{2}$ is *admissible*, meaning that $q(v) = \omega^2$ and $v_2 = v^b$.

To see this, note that by construction, $X = X(I, b, \beta) = (\omega v + v_2)/2$ is rank one. We have $\langle X, \overline{X} \rangle = \frac{\omega}{2}\langle v, v_2 \rangle = \omega^3$. Since $\omega v = X(v) - \overline{X(v)}$ is the difference of two rank one elements with pairing landing in E^\times , v is rank 4. Thus we may apply Lemma 5.1.2 to obtain $\omega^2 = t^2 q(v)$ and $v_2 = tv^b$ for some $t \in F^\times$. We obtain

$$\omega^3 = \langle X(v), \overline{X(v)} \rangle = \frac{\omega}{2}\langle v, v_2 \rangle = \frac{\omega}{2}\langle v, tv^b \rangle = t\omega q(v) = \omega^3/t.$$

Hence $t = 1$ and thus X is admissible, as claimed. \square

From the lifting law, the composition of the two maps is the identity, if one starts with v in W_A . We will check that the composition of the two maps is also the identity if you start with a based balanced module (I, b, β) .

Theorem 5.3.7. *The maps $v \mapsto (I, (b_1, b_2), \tau, \beta)$ and $(I, (b_1, b_2), \tau, \beta) \mapsto v$ define inverse bijections between $v \in W_A$ with $q(v) = D \neq 0$ and data $(I, (b_1, b_2), \tau, \beta)$ up to equivalence, with $\tau^2 - D\tau + \frac{D^2 - D}{4} = 0$. This bijection is equivariant for the action of G_1 , with $(\lambda, g) \in \text{GL}_1(R) \times \text{GL}_2(A)$ acting on the data via*

$$((b_1, b_2), \omega, \beta; \ell) \mapsto ((b_1, b_2)g, \det(g)\lambda^{-2}\omega, \lambda^3 \det(g)^{-1}\beta; \ell g).$$

Here $((b_1, b_2), \tau, \beta; \ell)$ means that the data is computed using the row vector $\ell \in A_F^2$.

Proof. From Lemma 5.3.6, if $X(I, b, \beta) = \tau v + v'$, then $X(I, b, \beta) = X(v, \omega)$ and $q(v) = D$. Now, take $\ell \in A_F^2$ so that $\beta(\ell) = \omega^{-3}\langle \ell^!, X(v, -\omega) \rangle$ is in E^\times . Then $(I(\ell), b(\ell), \beta(\ell))$ is a balanced triple. We have

$$\beta(\ell)^{-1}(\ell\epsilon(v))^! = X(v) = X(I, b, \beta) = \beta^{-1}b^!.$$

It follows from Lemma 5.3.3 then that $b = x\ell\epsilon(v)$ for some $x \in A_E^\times$.

We check that the action maps agree. Let $R_I \in M_2(A)$ denote the action of ω on I . Then, since b_1, b_2 is a basis for the free A -module I , R_I is the unique matrix in $M_2(A)$ satisfying $\omega b = bR_I$. But we have

$$bR_I = \omega b = \omega x\ell\epsilon(v) = x\ell\epsilon(v)R(v) = bR(v).$$

It follows that $R_I = R(v)$, so that the action maps $R_I, R(v)$ agree, so we write $\epsilon = \epsilon(v)$ for the common element of $M_2(A_E)$.

Now, set $b_0 = \text{tr}_{E/F}(b) \in A_F^2$. Then $b_0\epsilon = b$, as is immediately checked. Thus by the lifting law,

$$\beta X(v) = \beta X(I, b, \beta) = b^! = (b_0\epsilon)^! = \beta(b_0)X(v).$$

It follows that $\beta(b_0) = \beta \in E^\times$. Thus the triple $(I(\ell), b(\ell), \beta(\ell))$ is equivalent to the triple $(I(b_0), b(b_0), \beta(b_0))$, and this latter triple is equal to (I, b, β) . Thus the composition $(I, b, \beta) \mapsto v \mapsto (I', b', \beta')$ is the identity as well.

Now for the equivariance. Set $h = (\lambda, g) \in G_1$. From $R_r(\lambda^{-1}(v \cdot g)) = \lambda^{-2} \det_6(g) g^{-1} R_r(v) g$, one computes $\epsilon(v \cdot h) = g^{-1} \epsilon(v) g$. From the definition of the action of h on ω , one gets $X(\omega, v) \mapsto \lambda^{-3} \det_6(g) (X(\omega, v) \cdot g)$. The results on (b_1, b_2) and β follow. This completes the proof of the theorem. \square

The following corollary is immediate, and implies Theorem 3.1.7.

Corollary 5.3.8. *The action of $G \subseteq G_1$ on the data $((b_1, b_2), \omega, \beta)$ is*

$$((b_1, b_2), \omega, \beta; \ell) \mapsto ((b_1, b_2)g, \lambda\omega, \beta; \ell g).$$

6. THE LIFTING LAW FOR $J \oplus J$

Suppose C is an associative composition algebra over F . The purpose of this section is to parametrize the orbits of $\text{SL}_3(C)$ on $H_3(C)^2$, and to solve the analogous problem over a subring R of F . Over a field, a closely-related parametrization problem was solved in [Tan08, KY97, WY92], albeit by very different methods. The integral theory involves a notion of “balanced” module, following [Bha04b], and also uses some ideas from [Woo14]. We begin by proving a general lifting law, that applies to the prehomogeneous vector space $J \oplus J = V_2 \otimes J$ for an arbitrary cubic norm structure J . Then when $J = H_3(C)$, we prove a refined lifting law. We use the refined lifting law to solve the orbit parametrization problems.

The lifting laws are proved in subsection 6.1. In subsection 6.2, we parametrize the orbits over a field F , and in subsection 6.3, we parametrize the orbits over a subring R of F . The main result of this section is Corollary 6.3.8, which implies Theorem 3.2.5.

6.1. The lifting law. In this subsection we give the lifting law for the prehomogeneous vector space J^2 , where J is a cubic norm structure over the ring R . We also give a more explicit lifting law when $J = H_3(C)$ for an associative composition ring C over R .

6.1.1. The representation space. We begin with a description of the representation space $J^2 = V_2 \otimes J$. We write a typical element of J^2 as (A, B) , and then the (left) GL_2 action is

$$g \cdot \begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} pA + qB \\ rA + sB \end{pmatrix}$$

if $g = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$.

Recall the group M_J , which is the group of $(g, \lambda) \in \text{GL}(J) \times \text{GL}_1$ satisfying $n(gX) = \lambda n(X)$ for all $X \in J$. Then M_J also acts on J^2 via $g \cdot (A, B) = (gA, gB)$, and this action commutes with the action of GL_2 to give a $\text{GL}_2 \times M_J$ action on J^2 , under which J^2 becomes a prehomogeneous vector space.

6.1.2. The discriminant invariant. To the element (A, B) of J^2 , we assign the binary cubic form

$$f_{(A,B)}(x, y) = n_J \left((x, y) \begin{pmatrix} A \\ B \end{pmatrix} \right) = n_J(Ax + By) = n(A)x^3 + (A^\#, B)x^2y + (A, B^\#)xy^2 + n(B)y^3,$$

and the degree 12 discriminant polynomial $Q((A, B)) := Q(f_{(A,B)})$; see subsection 4.1.3. Here $n_J : J \rightarrow R$ is the cubic norm on J . If $g \in \text{GL}_2$, then $f_{g \cdot (A,B)} = \det(g)(g \cdot f_{(A,B)})$ (recall that the action $g \cdot f$ is twisted by $\det(g)^{-1}$.) Hence $Q(g \cdot (A, B)) = \det(g)^6 Q((A, B))$. If $m = (g, \lambda) \in M_J$, then $f_{(m \cdot (A,B))}(x, y) = \lambda f_{(A,B)}(x, y)$ and hence $Q(m \cdot (A, B)) = \lambda^4 Q((A, B))$.

Associated to the binary cubic $f_{(A,B)}$ is a cubic R -ring T with good basis $(1, \omega, \theta)$, and thus to every pair (A, B) in J^2 is associated a cubic ring with good basis.

6.1.3. *The lifting law for J .* We now give the lifting law for general cubic norm structures J . Suppose $(A, B) \in J^2$ has associated based cubic ring $T, (1, \omega, \theta)$. Consider $J_T = J \otimes_R T$, and put on J_T the cubic norm structure over T , with norm and adjoint extended T -linearly from J to J_T . That is, $(U \otimes \lambda)^\# = U^\# \otimes \lambda^2$ and $n(U \otimes \lambda) = \lambda^3 n(U)$, for $U \in J$ and $\lambda \in T$. Set

$$X = X(A, B, \omega, \theta) := -A\theta + B\omega + A^\# \times B^\#,$$

an element of J_T . The first part of the lifting law below will be that X is rank one in J_T .

Remark 6.1.1. With $X = X(A, B, \omega, \theta)$ as above, we have

$$\mathrm{tr}_{T/R}(X) = 3A^\# \times B^\# - (A, B^\#)A - (A^\#, B)B.$$

In Kato-Yukie [KY16], the authors parametrize the orbits of $\mathrm{GL}_2 \times M_J$ on $J \oplus J$, where $J = H_3(C)$ with C an octonion algebra. Associated to the non-degenerate pair (A, B) , Kato-Yukie assign an embedding $L := T \otimes_R F \hookrightarrow J^\dagger$, where J^\dagger is an isotope of J . This isotope J^\dagger of [KY16] is precisely the isotope specified by the element $\mathrm{tr}_{T/R}(X)$ of J .

We will define an element $Y = Y(A, B, \omega, \theta)$ of J_T^\vee associated to A, B, ω, θ , which will also turn out to be rank one. To do this, first define an R -bilinear map $\times_T : J_T \otimes J_T \rightarrow J_T^\vee$ via

$$(U_1 \otimes \lambda_1) \times_T (U_2 \otimes \lambda_2) = (U_1 \times U_2) \otimes (\lambda_1 \times \lambda_2).$$

We set $Y = Y(A, B, \omega, \theta) := \frac{1}{2}X(A, B, \omega, \theta) \times_T X(A, B, \omega, \theta)$, an element of J_T^\vee .

More precisely, if V is any R -module, the map $\times : J \otimes_R J \rightarrow J^\vee$ extends to a map

$$(14) \quad (J \otimes_R V) \otimes_R (J \otimes_R V) \rightarrow J^\vee \otimes_R (V \otimes_R V).$$

Then $\times : J_T \otimes J_T \rightarrow J_T^\vee$ is the composition of the map (14) for $V = T$ with the multiplication map $T \otimes_R T \rightarrow T$, and \times_T is the composition of the map (14) with the map $\times : T \otimes_R T \rightarrow T$. We similarly have maps $\# : J_T^\vee \rightarrow J_T$ and $\times_T : J_T^\vee \otimes J_T^\vee \rightarrow J_T$.

Here is the lifting law.

Theorem 6.1.2. *The elements $X(A, B, \omega, \theta) \in J_T$ and $Y(A, B, \omega, \theta) \in J_T^\vee$ are rank one. Furthermore, the pairing $(X(A, B, \omega, \theta), Y(A, B, \omega, \theta))$, a priori in T , lies in R and one has*

$$(X(A, B, \omega, \theta), Y(A, B, \omega, \theta)) = Q((A, B)).$$

Before proving the lifting law, we record the following lemma, which will be used in the proof of Theorem 6.1.2.

Lemma 6.1.3. *Define two 4-linear maps $J_T \otimes J_T \otimes J_T \otimes J_T \rightarrow J_T$ via*

$$m_1(w, x, y, z) = (w \times x) \times_T (y \times z) + (w \times z) \times_T (y \times x)$$

and

$$m_2(w, x, y, z) = (x \times_T z) \times (w \times_T y).$$

Then $m_1 = m_2$. Consequently, if $x \in J_T$, then $(x \times_T x)^\# = 4x^\# \times_T x^\#$.

Proof. The first part of the lemma follows immediately from the identity

$$(\lambda_1 \lambda_2) \times (\lambda_3 \lambda_4) + (\lambda_1 \lambda_4) \times (\lambda_3 \lambda_2) = (\lambda_2 \times \lambda_4)(\lambda_1 \times \lambda_3)$$

for $\lambda_1, \lambda_2, \lambda_3, \lambda_4 \in T$.

The second claim of the lemma is a direct consequence of the first, as $(x \times_T x)^\# = \frac{1}{2}m_2(x, x, x, x)$ while $4x^\# \times_T x^\# = \frac{1}{2}m_1(x, x, x, x)$. \square

We compute $Y(A, B, \omega, \theta)$ more explicitly.

Lemma 6.1.4. *Suppose $f_{(A,B)}(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$, and that this binary cubic form corresponds to the based cubic ring T , $(1, \omega, \theta)$. Then*

(15)

$$Y(A, B, \omega, \theta) = (c\theta - 3d\omega - c^2 + bd)A^\# + (-b\theta + c\omega + bc - 3ad)A \times B + (3a\theta - b\omega - b^2 + ac)B^\#.$$

Proof. One has

$$\begin{aligned} Y(A, B, \omega, \theta) &= \frac{1}{2}X(A, B, \omega, \theta) \times_T X(A, B, \omega, \theta) \\ &= \frac{1}{2}(-A\theta + B\omega + A^\# \times B^\#) \times_T (-A\theta + B\omega + A^\# \times B^\#) \\ &= 2A^\#\theta^\# - (A \times B)(\omega \times \theta) - (A \times (A^\# \times B^\#))(\theta \times 1) + 2B^\#\omega^\# \\ &\quad + (B \times (A^\# \times B^\#))(\omega \times 1) + 2(A^\# \times B^\#)^\# \\ &= 2A^\#(-d\omega) - (A \times B)(ad - bc + b\theta - c\omega) - (aB^\# + cA^\#)(c - \theta) + 2B^\#(a\theta) \\ &\quad - (dA^\# + bB^\#)(b + \omega) + 2(-ad(A \times B) + bdA^\# + acB^\#). \end{aligned}$$

Here we have used the identities $W \times (W^\# \times Z) = n(W)Z + (W, Z)W^\#$ and $(u \times v)^\# + u^\# \times v^\# = (u, v^\#)u + (u^\#, v)v$. Hence we obtain the formula (15). \square

Proof of Theorem 6.1.2. That X is rank one follows by direct computation from the multiplication table of T . Indeed, one has

$$\begin{aligned} X^\# &= (A^\# \times B^\#)^\# + adA \times B - bdA^\# - acB^\# \\ &\quad + (cA^\# + aB^\# - A \times (A^\# \times B^\#))\theta + (-dA^\# - bB^\# + B \times (A^\# \times B^\#))\omega. \end{aligned}$$

This then gives 0 by the general identities $W \times (W^\# \times Z) = n(W)Z + (W, Z)W^\#$ and $(u \times v)^\# + u^\# \times v^\# = (u, v^\#)u + (u^\#, v)v$ used above.

That Y is rank one then follows from Lemma 6.1.3. We must still evaluate (X, Y) . This can be proved by a somewhat tedious, but entirely straightforward computation using the multiplication table of T . \square

The following two lemmas provide a complement to the lifting law. They explain the sense in which the rank one ‘‘lift’’ X of (A, B) is unique.

Lemma 6.1.5. *Suppose $T, (1, \omega, \theta)$ is a good-based cubic ring, $A, B \in J$, and $X' = -A\theta + B\omega + C$ is rank one in J_T . Suppose $n(Ax + By)$ is not identically 0 and $\delta \in J$ is such that $X' + \delta$ is rank one. Then, $\delta = 0$.*

Proof. We have $0 = (X' + \delta)^\# = X' \times \delta + \delta^\#$. Hence, since $1, \omega, \theta$ are F -linearly independent, $A \times \delta = 0 = B \times \delta$. Hence $(Ax + By) \times \delta = 0$ in $J \otimes_F F(x, y)$, where $F(x, y)$ is the field of rational functions in x, y . But $Ax + By$ is invertible in $J \otimes_F F(x, y)$, since $n(Ax + By) \neq 0$. Thus the lemma follows from the fact that $z \times \delta = 0$ implies $\delta = 0$, when z is invertible.

This latter fact is a consequence of the identity

$$z^\# \times (z \times \delta) = n(z)\delta + (z^\#, \delta)z = n(z)\delta + \frac{1}{2}(z, z \times \delta)z.$$

\square

Lemma 6.1.6. *Suppose $T, (1, \omega, \theta)$ is a good-based cubic ring, $A, B \in J$, and $X' = -A\theta + B\omega + C$ is rank one in J_T . Set $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ the binary cubic form associated to ω, θ , $f'(x, y) = n(Ax + By)$ the binary cubic associated to the pair (A, B) . Assume A, B, C are linearly independent in J , and $f(x, y) \neq 0$. Then there exists $t \in F$ so that $f'(x, y) = tf(x, y)$.*

In other words, if $-A\theta + B\omega + C$ is rank one in J_T , then the data $(T, (1, \omega, \theta))$ is essentially the based cubic ring associated to (A, B) .

Proof of Lemma 6.1.6. To check that $f' = tf$, it suffices to first act by $\mathrm{SL}_2(F)$ on (ω_0, θ_0) and (A, B) so that the coefficients of x^3 and y^3 in $f(x, y)$ are both not zero and X' stays invariant. (Every nonzero orbit of $\mathrm{SL}_2(F)$ on binary cubics contains an element with $ad \neq 0$.) So by using the action of $\mathrm{SL}_2(F)$, we may assume $ad \neq 0$.

Now, using the multiplication table for $(1, \omega, \theta)$ and taking $(X')^\#$, one finds

$$(X')^\# = \left(cA^\# + aB^\# - A \times C \right) \theta + \left(-dA^\# - bB^\# + B \times C \right) \omega \\ + \left(C^\# - bdA^\# - acB^\# + (ad)(A \times B) \right) 1.$$

Since $1, \omega, \theta$ are linearly independent, each of the terms in parentheses is 0. Consequently,

$$\begin{aligned} n(A)C + (A^\#, C)A &= A^\# \times (A \times C) \\ &= A^\# \times (cA^\# + aB^\#) \\ (16) \qquad \qquad \qquad &= 2cn(A)A + aA^\# \times B^\# \end{aligned}$$

and similarly

$$(17) \qquad \qquad \qquad n(B)C + (B^\#, C)B = 2bn(B)B + dA^\# \times B^\#.$$

Multiplying (16) by d , (17) by a and subtracting, one obtains

$$(18) \qquad (n(A)d - n(B)a)C + d((A^\#, C) - 2cn(A))A + a(2bn(B) - (B^\#, C))B = 0.$$

Since A, B, C are assumed linearly independent in J , we deduce $n(A)d = n(B)a$. Pairing the coefficient of θ in $(X')^\#$ with A , we get

$$2cn(A) + a(A, B^\#) = 2(A^\#, C)$$

and similarly pairing the coefficient of ω in $(X')^\#$ with B we get

$$3bn(B) + d(A^\#, B) = 2(B^\#, C).$$

Plugging these into the coefficients of A and B in (18) we get

$$2d(a(A, B^\#) - cn(A)) = 0, \qquad a(bn(B) - d(A^\#, B)) = 0.$$

Since $ad \neq 0$, this completes the proof. \square

6.1.4. The lifting law for $J = H_3(C)$. Suppose now that C is a composition ring over R , and that C is associative. Then $J = H_3(C)$ is a cubic norm structure, and $\mathrm{GL}_3(C)$ acts on J via $m \cdot h = mhm^*$, for $m \in \mathrm{GL}_3(C)$ and m^* the conjugate transpose of m . We now extend the lifting law Theorem 6.1.2 to a more precise lifting law.

Let $(A, B) \in J^2$ be fixed. Define a map $S_r : T \rightarrow M_3(C)$ by $S_r(1) = 1$, $S_r(\omega) = -A^\#B$, $S_r(\theta) = B^\#A$ and extending R -linearly, and another R -linear map $S_\ell : T \rightarrow M_3(C)$ via $S_\ell(\lambda) = S_r(\lambda)^*$ for $\lambda \in T$. The maps S_r, S_ℓ are R -algebra homomorphisms, and in fact $X = X(A, B, \omega, \theta)$ and $Y = Y(A, B, \omega, \theta)$ are eigenvectors for the action of $S_\gamma(T)$. This claim is verified in the following proposition. The maps S_γ are closely related to constructions in [Woo14].

Proposition 6.1.7. *The maps $S_r, S_\ell : T \rightarrow M_3(C)$ are R algebra homomorphisms, and if $\lambda \in T$, then $S_\ell(\lambda)X = \lambda X = X S_r(\lambda)$.*

Proof. First we check that S_r is a ring homomorphism. It is clear that $S_r(\omega)S_r(\theta) = -ad = S_r(\theta)S_r(\omega)$. Next we check that $S_r(\omega)^2 = S_r(\omega^2)$. This amounts to the identity

$$(19) \qquad \qquad \qquad A^\#BA^\#B = -n(A)(A, B^\#) + n(A)B^\#A + (A^\#, B)A^\#B.$$

Equation (19) is a polynomial identity, and thus by Zariski density it suffices to prove it when $n(A) \neq 0$. When this is the case, (19) is equivalent to

$$(20) \qquad \qquad \qquad BA^\#B + (A, B^\#)A = AB^\#A + (A^\#, B)B$$

by multiplying (19) on the left by A , dividing by $n(A)$, and rearranging. But now both sides of (20) are equal to $(A \times B)^\#$, since one has $(x \times y)^\# = (x^\#, y)y + U_x y^\#$, and $U_x z = xzx$. The proof that $S_r(\theta)^2 = S_r(\theta^2)$ is essentially identical.

Now, since T is commutative and $S_\ell = S_r^*$, S_ℓ is also a ring map. To prove that $\lambda X = X S_r(\lambda)$ for $\lambda \in T$, one must only check this for $\lambda = \omega$ and $\lambda = \theta$. From (8), one obtains

$$(21) \quad A^\# \times B^\# = \left((A, B^\#) - AB^\# \right) A = \left((A^\#, B) - BA^\# \right) B.$$

Hence,

$$\begin{aligned} X S_r(\omega) &= \left(A\theta - B\omega - (A, B^\#)A + AB^\#A \right) (A^\#B) \\ &= aB\theta - BA^\#B\omega - acB + adA. \end{aligned}$$

Likewise one computes

$$\omega X = \omega(-A\theta + B\omega + bB - BA^\#B) = adA - acB + aB\theta - BA^\#B\omega,$$

so $\omega X = X S_r(\omega)$. The proof that $\theta X = X S_r(\theta)$ is similar.

Since $X = X^*$, the equation $\lambda X = X S_r(\lambda)$ implies $\lambda X = S_\ell(\lambda)X$. \square

Before giving the extended lifting law for $J = H_3(C)$, we give one additional preparation. *From now on we assume that the pair (A, B) is non-degenerate*, i.e. that $Q((A, B)) \neq 0$, or equivalently that $L = T \otimes_R F$ is a cubic étale F -algebra.

Definition 6.1.8. Suppose given two copies T_1, T_2 of the R -algebra T , by which we mean given two R -algebras T_1, T_2 and R -algebra isomorphisms $\iota_j : T \rightarrow T_j$, for $j = 1, 2$. Let $\{v_\alpha\}$ be a basis of T , and $\{w_\alpha\}$ the dual basis in $L = T \otimes F$ for the trace form. Define

$$\epsilon(T_1, T_2) := \sum_{\alpha} \iota_1(v_\alpha) \otimes \iota_2(w_\alpha) \in T_1 \otimes_R T_2 \otimes F.$$

Then $\epsilon(T_1, T_2)$ is independent of the choice of basis $\{v_\alpha\}$. When $T_1 = S_r(T), T_2 = T$, $\iota_1 = S_r$ and ι_2 is the identity, we set $\epsilon := \epsilon(S_r(T_1), T)$, so $\epsilon \in M_3(C) \otimes L$.

With this definition, one has the following lemma.

Lemma 6.1.9. *Suppose $T_1, T_2, \iota_1, \iota_2$ are as in Definition 6.1.8. Then $\iota_1(x)\epsilon(T_1, T_2) = \epsilon(T_1, T_2)\iota_2(x)$ for all $x \in T$.*

Proof. It suffices to check the identity for the elements of a basis of $T \otimes F$ over F , and thus we may assume x is invertible in $T \otimes F$. Now, let v_α, w_α be as in Definition 6.1.8. Then we have

$$\begin{aligned} \iota_1(x)\epsilon(T_1, T_2) &= \sum_{\alpha} \iota_1(x)\iota_1(v_\alpha) \otimes \iota_2(w_\alpha) \\ &= \sum_{\alpha} \iota_1(xv_\alpha) \otimes \iota_2(x^{-1}w_\alpha)\iota_2(x) \\ &= \epsilon(T_1, T_2)\iota_2(x) \end{aligned}$$

since $x^{-1}w_\alpha$ is the basis dual to xv_α , and $\epsilon(T_1, T_2)$ is independent of the choice of basis. \square

Finally, with these preparations, we can state the lifting law. Write $V_3(C) = C^3$ to be row vectors with entries in our associative composition ring C . In the lifting law Theorem 6.1.2, $X(A, B, \omega, \theta)$ is shown to be rank one. In Theorem 6.1.10, we now show explicitly the way in which $X(A, B, \omega, \theta)$ is a ‘‘pure tensor’’.

Theorem 6.1.10. *Let $\epsilon, X = X(A, B, \omega, \theta), Y = Y(A, B, \omega, \theta)$, and $Q((A, B))$ be as above. Then for all $v \in V_3(C)$, one has*

$$(22) \quad Q((A, B))(v\epsilon)^*(v\epsilon) = (vYv^*)X.$$

Before giving the proof, we give various preparations. Observe that

$$-A\theta_0 + B\omega_0 = \begin{pmatrix} \omega_0 & \theta_0 \end{pmatrix} \begin{pmatrix} & 1 \\ -1 & \end{pmatrix} \begin{pmatrix} A \\ B \end{pmatrix}.$$

Hence under the action of GL_2 , $g \cdot (A, B) = (A', B')$, which induces $(\omega_0, \theta_0) \mapsto (\omega'_0, \theta'_0)$, the expression $-A\theta_0 + B\omega_0$ gets multiplied by $\det(g)^2$. Similarly one has that the quantity $-AS_r(\theta_0) + BS_r(\omega_0)$, which is in $H_3(C_F)$, gets multiplied by $\det(g)^2$ under the action of GL_2 on A, B . It is thus convenient to write X and Y above in terms of $-A\theta_0 + B\omega_0$ and $-AS_r(\theta_0) + BS_r(\omega_0)$, which we will now do.

Lemma 6.1.11. *One has the equality*

$$X = -\frac{1}{2}(AS(\theta_0) - BS(\omega_0)) - A\theta_0 + B\omega_0.$$

Proof. From (21) one gets

$$(23) \quad A^\# \times B^\# = \frac{1}{2}(cA - AB^\#A) + \frac{1}{2}(bB - BA^\#B),$$

and thus

$$\begin{aligned} X &= -A(\theta_0 + c/3) + B(\omega_0 - b/3) + \frac{1}{2}(cA - AB^\#A) + \frac{1}{2}(bB - BA^\#B) \\ &= -A\theta_0 + B\omega_0 - \frac{1}{2}AB^\#A + \frac{c}{6}A - \frac{1}{2}BA^\#B + \frac{b}{6}B \\ &= -\frac{1}{2}(AS(\theta_0) - BS(\omega_0)) - A\theta_0 + B\omega_0. \end{aligned}$$

This completes the proof. \square

Define

$$Y_0 = Y_0(A, B, \omega, \theta) = (3(A\theta_0 - B\omega_0))^\# + (3(A\theta_0 - B\omega_0)) \times (3(AS(\theta_0) - BS(\omega_0))).$$

Lemma 6.1.12. *One has $Y_0 = -3Y$.*

Proof. We have

$$\begin{aligned} (A(3\theta_0) - B(3\omega_0))^\# &= A^\#(3c\theta_0 - 9d\omega_0 + 2c^2 - 6db) - (A \times B)(3b\theta_0 - 3c\omega_0 + bc - 9ad) \\ &\quad + B^\#(9a\theta_0 - 3b\omega_0 + 2b^2 - 6ac) \end{aligned}$$

Additionally, we have $S(3\theta_0) = 3B^\#A - c$, $S(3\omega_0) = -3A^\#B + b$, $AS(3\theta_0) - BS(3\omega_0) = 3(AB^\#A + BA^\#B) - (cA + bB)$. Applying (23) yields

$$AS(3\theta_0) - BS(3\omega_0) = -6A^\# \times B^\# + 2cA + 2bB.$$

Using this, one gets

$$A \times (AS(3\theta_0) - BS(3\omega_0)) = -2cA^\# + 2bA \times B - 6aB^\#$$

and

$$B \times (AS(3\theta_0) - BS(3\omega_0)) = -6dA^\# + 2cA \times B - 2bB^\#.$$

We obtain

$$\begin{aligned} Y_0 &= A^\#(-3c\theta_0 + 9d\omega_0 + 2c^2 - 6bd) - A \times B(-3b\theta_0 + 3c\omega_0 + bc - 9ad) \\ &\quad + B^\#(-9a\theta_0 + 3b\omega_0 + 2b^2 - 6ac) \\ &= A^\#(-3c\theta + 9d\omega + 3c^2 - 3bd) - A \times B(-3b\theta + 3c\omega + 3bc - 9ad) \\ &\quad + B^\#(-9a\theta + 3b\omega + 3b^2 - 3ac). \end{aligned}$$

Comparing with (15), we get $Y_0 = -3Y$, as desired. \square

If $m \in \mathrm{GL}_3(C)$, and $\mu \in \mathrm{GL}_1$, we get a map on $H_3(C) = J$ via $h \mapsto \mu m h m^*$. Let $[\mu, m]$ denote the corresponding element of M_J . Denote by $N(m)$ the degree 6 reduced norm on $H_3(C)$. One has $N(m) = n(mm^*)$.

Proposition 6.1.13. *The element $[\mu, m] \in M_J$ changes the quantities $f(x, y) = n(Ax + By)$, $\omega_0, \theta_0, X, Y_0, \epsilon$ as follows:*

- (1) $f(x, y) \mapsto \mu^3 N(m) f(x, y)$;
- (2) $\omega_0 \mapsto \mu^3 N(m) \omega_0$;
- (3) $\theta_0 \mapsto \mu^3 N(m) \theta_0$;
- (4) $X \mapsto \mu^4 N(m) m X m^*$;
- (5) $Y_0 \mapsto \mu^8 N(m)^3 (m^*)^{-1} Y_0 m^{-1}$;
- (6) $\epsilon \mapsto (m^*)^{-1} \epsilon m^*$.

Under the action of $g \in \mathrm{GL}_2$, the quantities $f(x, y) = n(Ax + By)$, $\omega_0, \theta_0, X, Y_0, \epsilon$ change as follows:

- (1) $f(x, y) \mapsto f((x, y)g) = \det(g) (\det(g)^{-1} f((x, y)g))$;
- (2) $\begin{pmatrix} \omega_0 \\ \theta_0 \end{pmatrix} \mapsto \det(g) g \begin{pmatrix} \omega_0 \\ \theta_0 \end{pmatrix}$;
- (3) $X \mapsto \det(g)^2 X$;
- (4) $Y_0 \mapsto \det(g)^4 Y_0$;
- (5) $\epsilon \mapsto \epsilon$.

Proof. These are straightforward computations, especially by using the equivariance properties of the expression $A\theta_0 - B\omega_0$. \square

Finally, set

$$V = V(1, \omega, \theta) = \mathrm{tr}_{L/F} \left(\begin{pmatrix} 1 \\ \omega \\ \theta \end{pmatrix} \begin{pmatrix} 1 & \omega & \theta \end{pmatrix} \right) = \begin{pmatrix} \mathrm{tr}(1) & \mathrm{tr}(\omega) & \mathrm{tr}(\theta) \\ \mathrm{tr}(\omega) & \mathrm{tr}(\omega^2) & \mathrm{tr}(\omega\theta) \\ \mathrm{tr}(\theta) & \mathrm{tr}(\theta\omega) & \mathrm{tr}(\theta^2) \end{pmatrix}.$$

Suppose x_i, y_j are in T , $(1, \omega, \theta)m = (x_1, x_2, x_3)$ and $(1, \omega, \theta)n = (y_1, y_2, y_3)$, with $m, n \in M_3(R)$. Then $(\mathrm{tr}_{T/R}(x_i y_j)) = {}^t m V n$. It follows that $Q(f)\epsilon = \det(V)\epsilon$ is a polynomial in $1, \omega, \theta, A$, and B .

Proof of Theorem 6.1.10. Multiplying both sides of (22) by $Q(f)$, this identity becomes a polynomial identity in A, B, ω, θ and v . Thus to prove the lifting law, it suffices to check that both sides of (22) behave the same way under the action of $\mathrm{GL}_2 \times M_J$, and that one has the equality for all v in a particular non-degenerate case.

For the equivariance, suppose $(g, [\mu, m]) \in \mathrm{GL}_2 \times M_J$ acts on A, B as defined above. Define an action of $\mathrm{GL}_3(C)$ on $V_3(C)$ by $v \mapsto v m^*$. Under these actions, one finds using Proposition 6.1.13 that both of (22) change via

$$Z \mapsto \det(g)^6 \mu^{12} N(m)^4 m Z m^*.$$

For the non-degenerate case, take $A = 1$ and $B = \mathrm{diag}(d, -d, 0)$ for some nonzero $d \in F$. Then $f(x, y) = x^3 - d^2 x y^2 = x(x - dy)(x + dy)$, $Q(f) = 4d^6$, so the pair (A, B) is non-degenerate. We have $S_r(\omega) = \mathrm{diag}(-d, d, 0)$, $S_r(\theta) = \mathrm{diag}(0, 0, -d^2)$. We identify L with $F \times F \times F$ via the map that takes $\omega \mapsto (-d, d, 0)$ and $\theta \mapsto (0, 0, -d^2)$. This is an F -algebra isomorphism.

Since we can compute ϵ in any basis, take the basis $\epsilon_1 = (1, 0, 0)$, $\epsilon_2 = (0, 1, 0)$, $\epsilon_3 = (0, 0, 1)$ of L . This basis is self-dual, and we have $S_r(\epsilon_1) = \mathrm{diag}(1, 0, 0)$, $S_r(\epsilon_2) = \mathrm{diag}(0, 1, 0)$, $S_r(\epsilon_3) = \mathrm{diag}(0, 0, 1)$. We obtain

$$\epsilon = \begin{pmatrix} (1, 0, 0) & & \\ & (0, 1, 0) & \\ & & (0, 0, 1) \end{pmatrix} =: E.$$

We now compute X . One obtains

$$\begin{aligned} X &= (0, 0, d^2)1 + \begin{pmatrix} (-d^2, d^2, 0) & & \\ & (d^2, -d^2, 0) & \\ & & 0 \end{pmatrix} - d^2 \begin{pmatrix} 1 & & \\ & 1 & \\ & & 0 \end{pmatrix} \\ &= d^2(-2, -2, 1)E. \end{aligned}$$

Thus

$$Y = \frac{1}{2}X \times_T X = d^4(-2, -2, 1)^{\#} \frac{1}{2}E \times_T E = d^4(-2, -2, 4)E.$$

Suppose $v = (v_1, v_2, v_3)$, with v_1, v_2, v_3 in the composition algebra C . For our choice of (A, B) , we see that both $Q(f)(v\epsilon)^*(v\epsilon)$ and $(vYv^*)X$ are equal to $4d^6(n(v_1), n(v_2), n(v_3))E$. This completes the proof. \square

In the next subsection, we will consider the orbit problem for the action of $\mathrm{GL}_2(R) \times \mathrm{SL}_3(C)$ on $H_3(C)^2$ when $R = F$ is a field. Before doing this, we finish this subsection with a preparatory result.

The following proposition says that Y is also an eigenvector for the action of $S(T)$.

Proposition 6.1.14. *Let R, T, Y be as above, and drop (for this proposition) our running assumption that $Q((A, B)) \neq 0$, so that instead T can be arbitrary. One has $S_r(\lambda)Y = \lambda Y = YS_\ell(\lambda)$ for all λ in T .*

Note that right and left have been switched.

Proof of Proposition 6.1.14. Since $YS_\ell(\lambda) = (S_r(\lambda)Y)^*$, it suffices to check that $S_r(\theta)Y = \theta Y$ and $S_r(\omega)Y = \omega Y$.

From the identities of subsection 4.2.1, one has $B^{\#}A(A \times B) = bB^{\#} - dA^{\#}$ and $B^{\#}AB^{\#} = -d(A \times B) + cB^{\#}$. Thus

$$\begin{aligned} S_r(\theta)Y &= (c\theta - 3d\omega - c^2 + bd)(aB^{\#}) + (-b\theta + c\omega + bc - 3ad)(bB^{\#} - dA^{\#}) \\ &\quad + (3a\theta - b\omega - b^2 + ac)(-d(A \times B) + cB^{\#}) \\ &= (db\theta - dc\omega - dbc + 3ad^2)A^{\#} + (-3ad\theta + db\omega + db^2 - dac)A \times B \\ &\quad + ((4ac - b^2)\theta - 3ad\omega - 2abd)B^{\#}. \end{aligned}$$

Computing θY using $\theta^2 = -bd + c\theta - d\omega$ and $\omega\theta = -ad$, one obtains the same expression, and thus $\theta Y = S_r(\theta)Y$, as desired.

The proof of the equality $S_r(\omega)Y = \omega Y$ is similar; for completeness, we give the details. From the identities of subsection 4.2.1, one obtains $-A^{\#}BA^{\#} = -bA^{\#} + a(A \times B)$, $-A^{\#}B(A \times B) = -cA^{\#} + aB^{\#}$, $-A^{\#}B(B^{\#}) = -dA^{\#}$. Thus

$$\begin{aligned} S_r(\omega)Y &= (c\theta - 3d\omega - c^2 + bd)(-bA^{\#} + a(A \times B)) + (-b\theta + c\omega + bc - 3ad)(-cA^{\#} + aB^{\#}) \\ &\quad + (3a\theta - b\omega - b^2 + ac)(-dA^{\#}) \\ &= (-3ad\theta + (4bd - c^2)\omega + 2adc)A^{\#} + (ac\theta - 3ad\omega - ac^2 + abd)A \times B \\ &\quad + (-ab\theta + ac\omega + abc - 3a^2d)B^{\#}. \end{aligned}$$

Using now that $\omega^2 = -ac + a\theta - b\omega$, one finds for ωY the same expression, and thus $S_r(\omega)Y = \omega Y$. This completes the proof. \square

6.2. Orbits over a field. In this subsection, $R = F$ is a field. An element $(A, B) \in H_3(C)^2$ is said to be non-degenerate if $Q((A, B)) \neq 0$. In this subsection we use the lifting law to parametrize the orbits of $\mathrm{SL}_3(C)$ on the non-degenerate elements of $H_3(C)^2$.

6.2.1. *The invariant $\mu(X)$.* Before stating the parametrization theorem, we associate to a non-degenerate pair (A, B) two invariants. The first invariant is the cubic étale F -algebra L , determined by $f_{(A,B)}(x, y) = n(Ax + By)$, together with its good basis $1, \omega, \theta$. The second invariant involves the rank one element $X = X(A, B, \omega, \theta) = -A\theta + B\omega + A^\# \times B^\#$. Note that if $v \in V_3(C_L)$, then v^*v in $H_3(C_L)$ is rank one; the second invariant associated to (A, B) measures how far X is from a “pure tensor” v^*v in $H_3(C_L)$.

In the following lemma and also below, we say a vector v in $V_3(A)$, for an associative composition algebra A , is *primitive* if v can be extended to a basis of $V_3(A)$.

Lemma 6.2.1. *Suppose k is a field, A is an associative composition algebra over k , and Y in $H_3(A)$ is rank one. Then, there exists a primitive column vector $v_0 \in V_3(A)$ and an element $\mu \in k^\times$ so that $Y = \mu v_0 v_0^*$. This element μ is unique up to multiplication by an element of $n(A^\times)$.*

Proof. First assume that a primitive v_0 and a $\mu \in k^\times$ has been found; we check the uniqueness of μ . To do this, note that $v^*Yv = \mu n(v^*v_0)$. Since v_0 is primitive, by definition $v_0 = g \cdot (1, 0, 0)^*$ for some $g \in \text{GL}_3(A)$, and thus there is v so that $n(v^*v_0) = 1$. Hence $\{v^*Yv : v \in V_3(A)\} \cap k^\times$ is nonempty. The formula $v^*Yv = \mu n(v^*v_0)$ then shows that

$$\{v^*Yv : v \in V_3(A)\} \cap k^\times = \mu n(A^\times),$$

which implies the desired uniqueness property.

For the existence, we show that there exists $g \in \text{SL}_3(A)$ so that

$$gYg^* = Z = \mu e_{11} = \mu \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}.$$

Hence setting $v_0 = g^{-1}(1, 0, 0)^*$ gives the lemma, once g is found.

To find such a g , one can use uppertriangular unipotent matrices in $\text{SL}_3(A)$ to move Y to an element Z with some $Z_{ii} \neq 0$, and thus in k^\times since k is a field. Using the permutation matrices $S_3 \subseteq \text{GL}_3(A)$, one can assume $Z_{11} = \mu \in k^\times$. Then again using unipotent matrices, one can clear out the top row of Z , so that $Z_{12} = Z_{13} = Z_{21} = Z_{31} = 0$. Since Y and thus Z is rank one, we then get that $Z = \mu e_{11}$, as desired. \square

We require one more lemma before defining the invariant $\mu((A, B)) = \mu(X(A, B, \omega, \theta))$.

Lemma 6.2.2. *Assume $Q(f) \neq 0$, so that L is étale, and $X = X(A, B, \omega, \theta)$. Suppose $\sigma : L \rightarrow k$ is a map of F -algebras to a field k . Then $\sigma(X) \neq 0$. Furthermore, $n(\text{tr}_{L/F}(X)) = Q(f)$, so in particular $\text{tr}_{L/F}(X)$ in J is invertible.*

Proof. We first make some general remarks. Assume first that X is an arbitrary element of $J \otimes_F L$, for some cubic norm structure J . Extending scalars from F to some algebraic closure k of L , we can assume $L = k \times k \times k$ and $X = (X_1, X_2, X_3) \in J_k \times J_k \times J_k$. In other words, $X = X_1\epsilon_1 + X_2\epsilon_2 + X_3\epsilon_3$, with $X_i \in J_k$ and $\epsilon_1 = (1, 0, 0)$, $\epsilon_2 = (0, 1, 0)$, $\epsilon_3 = (0, 0, 1)$ the primitive idempotents in L .

Set $Y = \frac{1}{2}X \times_L X$. We find

$$Y = \frac{1}{2} \sum_{i,j} X_i \times X_j \otimes \epsilon_i \times \epsilon_j = (X_2 \times X_3)\epsilon_1 + (X_3 \times X_1)\epsilon_2 + (X_1 \times X_2)\epsilon_3$$

since $\epsilon_1 \times \epsilon_2 = \epsilon_3$, $\epsilon_1^\# = 0$ etc. Thus

$$(Y, X) = (X_1, X_2 \times X_3)\epsilon_1 + (X_2, X_3 \times X_1)\epsilon_2 + (X_3, X_1 \times X_2)\epsilon_3 = (X_1, X_2, X_3).$$

Suppose now that X is rank one. Then $X_i^\# = 0$ for all i , and hence $n(X_1 + X_2 + X_3) = (X_1, X_2 \times X_3) = (X_1, X_2, X_3)$. Thus, if X is rank one and $Y = \frac{1}{2}X \times_L X$, we have shown $(X, Y) = n(\text{tr}_{L/F}(X))$.

Applying this fact to $X = X(A, B, \omega, \theta)$, and using that for this X , $(X, Y) = Q(f)$, we obtain

$$n(\mathrm{tr}_{L/F}(X)) = (X_1, X_2, X_3) = Q(f) \neq 0.$$

In particular, each $X_i \neq 0$. It follows that $\sigma(X) \neq 0$ for any $\sigma : L \rightarrow k$ as in the statement of the lemma. \square

We record for later use the following corollary.

Corollary 6.2.3. *Suppose the pair (A, B) is non-degenerate, i.e., $Q(f) \neq 0$. Then A, B , and $A^\# \times B^\#$ are linearly independent in J .*

Proof. $A, B, A^\# \times B^\#$ are linearly dependent if and only if there exists a nonzero linear map $\ell : L \rightarrow F$ such that $\ell(X) = 0$. Since L is étale, every linear map $L \rightarrow F$ is of the form $\mathrm{tr}_{L/F}(\mu \cdot)$ for some $\mu \in L$.

Now, let k be an algebraic closure of F , and X_1, X_2, X_3 as in Lemma 6.2.2. To show $\mathrm{tr}_{L/F}(\mu X) = 0$ implies $\mu = 0$, it suffices to check that X_1, X_2, X_3 are linearly independent in k . But if one had a dependence relation between the X_i , say $X_3 = \alpha X_1 + \beta X_2$, then

$$Q(f) = (X_1, X_2, X_3) = \alpha(X_1, X_2, X_1) + \beta(X_1, X_2, X_2) = 0$$

since X_1, X_2 are rank one. Since $Q(f) \neq 0$, the corollary follows. \square

Using Lemmas 6.2.2 and 6.2.1 we can now see that X is of the form $v_0 v_0^*$ times a unit of L .

Corollary 6.2.4. *Suppose the pair (A, B) is non-degenerate. Then, there is $\mu \in L^\times$ and a primitive column vector $v_0 \in V_3(C_L)$ so that $X = \mu v_0 v_0^*$. The element μ is unique up to multiplication by $n(C_L^\times)$, and thus associated to X is a well-defined class $[\mu_X] \in L^\times / (n(C_L^\times))$.*

Proof. Since (A, B) is non-degenerate, L is an étale F -algebra, and thus a product of fields. Suppose $\sigma : L \rightarrow k$ is an F -algebra map to a field k . Then by Lemma 6.2.2, $\sigma(X) \neq 0$, and thus $\sigma(X)$ is rank one. It follows that we may apply Lemma 6.2.1 to each of the connected components of $\mathrm{Spec}(L)$, to get the existence of $\mu \in L^\times$ and v_0 in $V_3(C_L)$ a primitive vector so that $X = \mu v_0 v_0^*$. Uniqueness of μ modulo $n(C_L^\times)$ also follows. \square

Definition 6.2.5. To a non-degenerate pair $(A, B) \in J^2$, we associate its invariant, which is the triple $(L, (1, \omega, \theta), [\mu_X])$. Here $(L, (1, \omega, \theta))$ is the étale cubic F -algebra, together with its good basis $(1, \omega, \theta)$, determined by the binary cubic form $n(Ax + By)$, and the element $[\mu_X] \in L^\times / n(C_L^\times)$ is that for which $X_{(A,B)} = \mu_X v_0 v_0^*$ for some primitive vector $v_0 \in V_3(C_L)$. We say a triple $(L, (1, \omega, \theta), [\mu])$ is isomorphic to a triple $(L', (1, \omega', \theta'), [\mu'])$ if there is an F -algebra isomorphism $\phi : L \rightarrow L'$ for which $\phi(\omega) = \omega'$, $\phi(\theta) = \theta'$, and $\phi([\mu]) = [\mu']$.

We can now state the orbit parametrization theorem. Here $J = H_3(C)$ and $G = \mathrm{SL}_3(C)$, where $\mathrm{SL}_3(C) = \{m \in \mathrm{GL}_3(C) : N(m) = 1\}$. This result is closely related to work of Wright-Yukie [WY92], Kable-Yukie [KY97], and Taniguchi [Tan08].

Theorem 6.2.6. *If the pair (A, B) is non-degenerate, then $n_{L/F}(\mu(X(A, B))) \in n(C^\times)$. The invariant map of Definition 6.2.5, which associates to (A, B) the invariant $(L, (1, \omega, \theta), [\mu(X(A, B))])$, descends to a bijection between G orbits on J^2 and isomorphism classes of pairs $(L, (1, \omega, \theta), [\mu])$, where $L, (1, \omega, \theta)$ is an étale cubic F -algebra with good basis and $[\mu]$ is an element of the quotient group $L^\times / n(C_L)^\times$ for which $n_{L/F}(\mu) \in n(C^\times)$.*

Note that $\mu \in L^\times$ is only well-defined up to multiplication by an element $n_C(C_L^\times)$. Thus implicit in the statement of Theorem 6.2.6 is the fact that $n_{L/F}(n_C(C_L^\times)) \in n_C(C^\times)$. This will be proved directly below.

We will prove Theorem 6.2.6 in steps. We begin with the following lemma.

Lemma 6.2.7. *If $h \in G$, then the invariant associated to $h \cdot (A, B)$ is isomorphic to the invariant associated to (A, B) .*

Proof. If $m \in \mathrm{GL}_3(C)$ and $N(m) = 1$, then the cubic étale F -algebra L and its good basis does not change, and furthermore $X_{m \cdot (A, B)} = mX_{(A, B)}m^*$. Hence $[\mu_X]$ does not change. \square

Thus the map from G -orbits on J^2 to arithmetic invariants $(L, (1, \omega, \theta), [\mu])$ is well-defined. We now check that this map is injective.

Proposition 6.2.8. *Suppose (A, B) and (A', B') are non-degenerate elements of J^2 with invariants $(L, (1, \omega, \theta), [\mu])$ and $(L', (1, \omega', \theta'), [\mu'])$, and suppose that these invariants are isomorphic. Then (A, B) and (A', B') are in the same G -orbit.*

Proof. Write X, X' for the rank one elements of $J \otimes L$ associated to the pairs (A, B) and (A', B') , respectively. Since $L, (1, \omega, \theta)$ is isomorphic to $L', (1, \omega', \theta')$ we have $n(Ax + By) = n(A'x + B'y)$. Thus we may assume $L = L'$. We have $X = \mu v_0 v_0^*$ and $X' = \mu' v'_0 (v'_0)^*$, and by changing v'_0 if necessary, we may assume $\mu = \mu'$. Now, since v_0 and v'_0 are primitive, there is $\tilde{m} \in \mathrm{GL}_3(C_L)$ so that $\tilde{m}v_0 = v'_0$. Hence $\tilde{m}X\tilde{m}^* = X'$. Now, write $\tilde{m} = m_1 + m_\omega \omega + m_\theta \theta$, with $m_* \in M_3(C)$, and set $m = m_1 + m_\omega S_\ell(\omega) + m_\theta S_\ell(\theta)$. Then $m \in M_3(C)$, and $\tilde{m}X\tilde{m}^* = mXm^*$ by Proposition 6.1.7, from which we deduce $A' = mA m^*$ and $B' = mB m^*$. Since $n(Ax + By) = n(A'x + B'y) = N(m)n(Ax + By)$, we get $N(m) = 1$ and m is invertible. The proposition follows. \square

Say a rank one element $X \in J_L$ is *admissible* if $X = X(A, B, \omega, \theta)$ for some A, B in J . Note that if $1, \omega', \theta'$ is a good basis of L , and $X = -A'\theta' + B'\omega' + C'$ for some A', B', C' in L , then by Lemma 6.1.5, X is admissible for $(A', B', \omega', \theta')$ if and only if $n(A'x + B'y) = f_{\omega', \theta'}(x, y)$. Here $f_{\omega', \theta'}(x, y)$ is the binary cubic form associated to the good basis $1, \omega', \theta'$ of L .

Lemma 6.2.9. *Suppose $\mu \in L^\times$, and $X = X(A, B, \omega, \theta)$ is admissible. Then $\mu n_{L/F}(\mu)X$ is admissible.*

Proof. Set $X' = \mu n(\mu)X$. We have

$$\begin{aligned} X' &= n(\mu)X S_r(\mu) = -A S_r(\mu)(n(\mu)\theta) + B S_r(\mu)(n(\mu)\omega) + n(\mu)C S_r(\mu) \\ &= -A'\theta' + B'\omega' + C'. \end{aligned}$$

Here $A' = A S_r(\mu)$, $\theta' = n(\mu)\theta$ etc. Note that since the left-hand side is in $J_L \subseteq M_3(C)_L$, so is the right-hand side, and thus $A', B', C' \in J$. We have $f_{(\omega', \theta')}(x, y) = n(\mu)f_{(\omega, \theta)}(x, y)$.

Set $Y' = \frac{1}{2}X' \times_L X'$. Then $Y' = \mu^\# n(\mu)^2 Y$, and thus $(X', Y') = n(\mu)^4 (X, Y) = n(\mu)^4 Q(f) \neq 0$. It follows as in the proof of Corollary 6.2.3 that A', B', C' are linearly independent. Hence we may apply Lemma 6.1.6 to deduce that

$$n((Ax + By)S_r(\mu)) = n(A'x + B'y) = t f_{(\omega', \theta')}(x, y) = t n(\mu) n(Ax + By)$$

for some $t \in F$.

We claim $t \in F^\times$. Indeed, this is clear, since $(Ax + By)S_r(\mu)$ is invertible in $M_3(C) \otimes F(x, y)$. Hence $tX' = -A'(t\theta') + B'(t\omega') + tC'$ is admissible. But now, since tX' is admissible, we obtain

$$t^4 n(\mu)^4 Q((\omega, \theta)) = Q((t\omega', t\theta')) = \frac{1}{2}(tX', (tX') \times_L (tX')) = t^3 (X', Y') = t^3 n(\mu)^4 Q(f).$$

Hence $t = 1$ and X' is admissible. \square

As a corollary of the proof, we observe that

$$n((Ax + By)S_r(\mu)) = n(\mu)n(Ax + By)$$

for all $\mu \in T$.

To finish the proof of Theorem 6.2.6, we still must characterize the image of the invariant map.

Proposition 6.2.10. *Suppose L/F is cubic étale, $\mu \in L^\times$, and $n_{L/F}(\mu) \in n_C(C^\times)$. Then, there exists a non-degenerate pair $(A, B) \in J^2$ with invariants $(L, (1, \omega, \theta), \mu)$.*

Proof. First, we write down (A_1, B_1) with invariants $(L, (1, \omega, \theta), 1)$, then multiply the associated $X_1 = X_{(A_1, B_1)}$ by μ to find the desired pair (A, B) .

More specifically, following Bhargava [Bha04b], set

$$A_1 = \begin{pmatrix} 1 & & \\ & -a & \\ 1 & & -c \end{pmatrix}, \quad B_1 = \begin{pmatrix} & -1 & \\ -1 & -b & \\ & & -d \end{pmatrix}.$$

Then one computes

$$A_1^\# = \begin{pmatrix} ac & & a \\ & -1 & \\ a & & \end{pmatrix}, \quad B_1^\# = \begin{pmatrix} bd & -d & \\ -d & & \\ & & -1 \end{pmatrix},$$

and then

$$\begin{aligned} n(A_1x + B_1y) &= n(A_1)x^3 + (A_1^\#, B_1)x^2y + (A_1, B_1^\#)xy^2 + n(B_1)y^3 \\ &= ax^3 + bx^2y + cxy^2 + dy^3. \end{aligned}$$

Thus every $L, (1, \omega, \theta)$ arises. Furthermore, note that the top left entry of $A_1^\# \times B_1^\#$ is 1, so the same is true about $X_{(A, B)}$, and thus $\mu(X_{(A, B)}) = 1$. Thus we have checked that the invariant $(L, (1, \omega, \theta), 1)$ appears for every étale cubic L and good basis $(1, \omega, \theta)$.

To get the invariant (L, μ) , we multiply $X_{(A_1, B_1)}$ by $\mu n(\mu) = \mu n(c)$. By Lemma 6.2.9, $X = \mu n(\mu)X_{(A_1, B_1)}$ is admissible, and it has invariants $(L, [\mu n(\mu)]) = (L, [\mu])$ since $n(\mu) \in n(C)$. Multiplying X by $\mu n(\mu)$ changes the good basis, but since every good basis arises, this is irrelevant. The proposition follows. \square

If $m \in M_n(C)$, denote by $N_{2n}(m)$ the degree $2n$ reduced norm on $M_n(C)$. If $h \in H_n(C)$, denote by $n_{H_n(C)}(h)$ the degree n norm on $H_n(C)$, the Hermitian $n \times n$ matrices over the associative composition algebra C . One has $N_{2n}(m) = n_{H_n(C)}(mm^*)$.

Lemma 6.2.11. *Suppose C is an associative composition algebra, and $m \in M_n(C)$. Then the norm $n_{H_n(C)}(mm^*)$ is a norm from C .*

Proof. If C is commutative this is clear. Thus we may assume C is a quaternion algebra. Then the quantity $n_{H_n(C)}(mm^*) = N_{2n}(m)$ is the reduced norm of m in $M_n(C)$, while norms from C are the reduced norms from $C = M_1(C)$. That these two sets are the same is well-known. \square

The following proposition completes the proof of Theorem 6.2.6.

Proposition 6.2.12. *Suppose $X = X_{(A, B)}$ is admissible, and $X = \mu v^*v$, with $\mu \in L^\times$ and $v \in V_3(C_L)$. Then $n_{L/F}(\mu) = n(x)$ for some $x \in C$.*

Proof. We have $v = v_0m$ for $v_0 = (1, \omega, \theta)$ and some $m \in M_3(C)$. Set $X' = v^*v$ and $Y' = \frac{1}{2}X' \times_L X'$. Then

$$Q((A, B)) = (X, Y) = (\mu X', \mu^\# Y') = n_{L/F}(\mu)(X', Y') = n_{L/F}(\mu)n(\text{tr}_{L/F}(X')).$$

These last two quantities are equal by the proof of Lemma 6.2.2. Since $X' = v^*v = m^*v_0^*v_0m$, $\text{tr}_{L/F}(X') = m^* \text{tr}_{L/F}(v_0^*v_0)m$ and

$$n(\text{tr}_{L/F}(X')) = N_6(m)n(\text{tr}_{L/F}(v_0^*v_0)).$$

But $n(\text{tr}_{L/F}(v_0^*v_0)) = \text{disc}(1, \omega, \theta) = Q((A, B))$. Hence we obtain

$$Q((A, B)) = (X, Y) = n_{L/F}(\mu)n(\text{tr}_{L/F}(X')) = n_{L/F}(\mu)N_6(m)Q((A, B)).$$

Since $N_6(m) \in n(C)$, the proposition follows. \square

The following lemma will be used in the next subsection, and has essentially already been proved above.

Lemma 6.2.13. *Suppose $X' = -A'\theta + B'\omega + C'$ is rank one in $J \otimes_R T$, and set $Y' = \frac{1}{2}X' \times_T X'$. If $(X', Y') = \text{disc}(1, \omega, \theta) \neq 0$, then X' is admissible.*

Proof. Set $Q(\omega, \theta) = \text{disc}(1, \omega, \theta)$. We have

$$n(\text{tr}_{L/F}(X')) = (X'_1, X'_2, X'_3) = (X', Y') = Q(\omega, \theta) \neq 0.$$

Since X' is rank one, we deduce that the X'_i are linearly independent, and hence $\text{tr}_{L/F}(\mu X) = 0$ implies $\mu = 0$, from which we conclude that A', B', C' are linearly independent.

It then follows that there exists $t \in F$ so that $f'(x, y) = n(A'x + B'y) = tf_{(\omega, \theta)}(x, y)$. We must rule out the case $t = 0$. Define $C_1 \in J$ so that $X' = -A'\theta_0 + B'\omega_0 + C_1$. Then we have

$$n(-A'\theta_0 + B'\omega_0) = n(X' - C_1) = (X', C_1^\#) - n(C_1) = -(A', C_1^\#)\theta_0 + (B', C_1^\#)\omega_0 + 2n(C_1).$$

We have $\text{tr}_{L/F}(X') = 3C_1$, and thus $n(C_1) \neq 0$. Hence $n(-A'\theta_0 + B'\omega_0) \neq 0$, and so we cannot have $t = 0$.

Thus $t \in F^\times$, and $tX' = -A'(t\theta) + B'(t\omega) + tC'$ is admissible. Hence

$$t^4 Q((\omega, \theta)) = Q((t\omega, t\theta)) = \frac{1}{2}(tX', (tX') \times_T (tX')) = t^3 \frac{1}{2}(X', X' \times_T X') = t^3 Q((\omega, \theta)).$$

Hence $t = 1$, and X' is admissible. \square

Recall the element $\epsilon \in M_3(C) \otimes L$ from Definition 6.1.8. If $v_0 \in C_F^3$ (row vectors), define $\Phi^{v_0} : C_F^3 \rightarrow C_L$ (this C_F^3 being column vectors) via the formula $\Phi^{v_0}(\ell) = v_0 \epsilon \ell$. This map Φ^{v_0} is a map of right C_F -modules. The following proposition will also be used below.

Proposition 6.2.14. *There exists $v_0 \in C_F^3$ (row vectors), and $\ell_0 \in C_F^3$ (column vectors) so that $(v_0^* v_0, Y) \in L^\times$ and $(\ell_0 \ell_0^*, X) \in L^\times$. For such a v_0 , the map $\Phi^{v_0} : C_F^3 \rightarrow C_L$ is a C_F -module isomorphism.*

Proof. We already know $X = \mu u_0 u_0^*$ for some primitive column vector $u_0 \in C_L^3$ and $\mu \in L^\times$. Since $(X, Y) = Q((A, B)) \in F^\times$, taking $\tilde{v} = u_0^*$ gives $\tilde{v} Y \tilde{v}^* = (\tilde{v}^* \tilde{v}, Y) \in L^\times$. Write $\tilde{v} = v_1 + v_\omega \omega + v_\theta \theta$, with the $v_* \in C_F^3$, and set $v_0 = v_1 + v_\omega S_r(\omega) + v_\theta S_r(\theta)$. Then $v_0 Y v_0^* = \tilde{v} Y \tilde{v}^* \in L^\times$. The existence of ℓ_0 with $(\ell_0 \ell_0^*, X) \in L^\times$ is proved similarly. This proves the first part of the proposition.

For the second part, suppose $v \in C_F^3$ (row vectors) and $\ell \in C_F^3$ (column vectors). By the lifting law, we can calculate $n_C(\Phi^v(\ell))$. Indeed, we have

$$(24) \quad Q((A, B)) n_C(\Phi^v(\ell)) = Q((A, B)) \Phi^v(\ell)^* \Phi^v(\ell) = (v Y v^*)(\ell^* X \ell).$$

Furthermore, note that via the properties of ϵ , $\Phi^v(C_F^3) \subseteq C_L$ is closed under left multiplication by L and right multiplication by C , and hence is a C_L -submodule of C_L .

By (24), $n_C(\Phi^{v_0}(\ell_0)) \in L^\times$. Thus, for v_0 as above, the map $\Phi^{v_0} : C_F^3 \rightarrow C_L$ is surjective, since the image contains a unit of C_L and is closed under left C_L -multiplication. Since $\dim_F C_F^3 = \dim_F C_L = 3 \dim_F C$, Φ^{v_0} is injective as well. This completes the proof. \square

6.3. Integral orbits. Suppose that R is an integral domain, with fraction field F of characteristic 0, and C is an associative composition algebra over R . Recall that this means that C is a free R -module of finite rank, is an R -subring of an associative composition F -algebra, stable under the involution $*$, and such that $x + x^*$, xx^* are in R for all $x \in C$. In this subsection we consider the orbits of a certain group G on $H_3(C)^2$.

More precisely, set $G_1 = \text{GL}_1(R) \times \text{GL}_2(R) \times \text{GL}_3(C)$, which acts on the right of $V := V_2(R) \otimes H_3(C)$. Here $V_2(R) = R^2$ is the row vectors with coefficients in R and the action of GL_2 action is the usual right action of matrices on row vectors. The group $\text{GL}_3(C)$ acts on the right of $H_3(C)$ by $h \mapsto m^* h m$ for $h \in H_3(C)$ and $m \in \text{GL}_3(C)$. Finally, $\lambda \in \text{GL}_1(R)$ acts on V by scaling by λ . We

denote by $G \subseteq G_1$ the group of triples $(\lambda, g, m) \in \mathrm{GL}_1(R) \times \mathrm{GL}_2(R) \times \mathrm{GL}_3(C)$ with $\lambda = \det(g)^{-1}$ and $\det(g)^2 = N_6(m)$, where $N_6(m) = n(mm^*)$ is the degree 6 reduced norm on $M_3(C)$. Then G also acts on V by restriction of the action of G_1 .

We begin with a few definitions. Suppose T is a cubic ring over R and $L = T \otimes_R F$. We have $1, \omega, \theta$ a good basis of T . Let $C_L = C \otimes_R L$. We consider $T \otimes C$ submodules $I \subseteq L \otimes C$.

Definition 6.3.1. If $I \subseteq L \otimes C$, we say I is a fractional ideal if

- I is closed under left multiplication by T and right multiplication by C ;
- I is free of rank 3 as a C -module;
- $I \otimes_R F$ is free of rank one as an $L \otimes C$ -module.

Definition 6.3.2. Suppose I is a $T \otimes C$ fractional ideal, and b_1, b_2, b_3 is an ordered basis of I i.e., that $I = b_1C + b_2C + b_3C$ inside $L \otimes C$. Then $(b_1, b_2, b_3) = (1 \otimes 1, \omega \otimes 1, \theta \otimes 1)g$ for some unique $g \in M_3(C_F)$. We define $N(I; (b_1, b_2, b_3); (1, \omega, \theta)) = N_6(g) = n(g^*g)$ the norm of the ideal. Of course, this norm depends on the choice of the good basis $(1, \omega, \theta)$ and the choice of ordered basis (b_1, b_2, b_3) .

We will parametrize the orbits of G on $H_3(C)^2$ in terms of *balanced* fractional ideals. We now define when the based fractional ideal $I, (b_1, b_2, b_3)$ is balanced.

Definition 6.3.3. Suppose $\beta \in L^\times$, and the good basis $(1, \omega, \theta)$ of T is fixed. One says that the data $((I, (b_1, b_2, b_3)), \beta)$ is **balanced** if $y^*x \in \beta C \otimes_R T$ for all x, y in I and $N((I, (b_1, b_2, b_3))) = n_{L/F}(\beta)$. If the data $(I, b_1, b_2, b_3, \beta)$ is balanced, we set

$$X_{I, \beta} = \beta^{-1} b^* b \in H_3(C) \otimes T.$$

Associated to a non-degenerate pair $(A, B) \in H_3(C)^2$, one can define a based balanced $T \otimes C$ -module (I, β) as follows. First, from the non-degenerate pair (A, B) , one defines the binary cubic form $f_{(A, B)}(x, y) = n(Ax + By)$, which is associated to a good-based cubic ring $T, (1, \omega, \theta)$. Next, one has the rank one elements $X = X(A, B, \omega, \theta), Y = Y(A, B, \omega, \theta)$ in $H_3(C) \otimes T$. One has $X = -A\theta + B\omega + A^\# \times B^\#$ and $Y = \frac{1}{2}X \times_T X$. We set $S(\omega) = -A^\#B$ and $S(\theta) = B^\#A$ in $M_3(C)$.

Finally, suppose given some auxiliary $v_0 \in C^3$ (row vectors), with $v_0 Y v_0^* = (v_0^* v_0, Y)$ in L^\times . By Proposition 6.2.14, such a v_0 can always be found. Define $\beta(v_0) = \frac{(v_0^* v_0, Y)}{Q}$, $Q = Q(A, B) = \mathrm{disc}(1, \omega, \theta)$ and $\Phi^{v_0} : C^3 \rightarrow C_L$ (this C^3 being column vectors) via the formula $\Phi^{v_0}(\ell) = v_0 \ell$.

Proposition 6.3.4. Write $E_1 = (1, 0, 0)^t, E_2 = (0, 1, 0)^t, E_3 = (0, 0, 1)^t$, the standard basis of column vectors. Set $b_j = \Phi^{v_0}(E_j)$ and I the C submodule generated by these b_j , i.e., $I = \Phi^{v_0}(C^3)$. Then the data $(I, (b_1, b_2, b_3), \beta(v_0))$ is a balanced fractional $T \otimes C$ -ideal.

Proof. By Proposition 6.2.14 and its proof, $I = b_1C + b_2C + b_3C$ is a fractional $T \otimes C$ -ideal. It remains to check that the data is balanced.

Thus, suppose $g \in M_3(C)$ satisfies $(b_1, b_2, b_3) = (1, \omega, \theta)g$. By the lifting law Theorem 6.1.10, we have

$$\beta X_{A, B} = g^* \begin{pmatrix} 1 \\ \omega \\ \theta \end{pmatrix} (1 \ \omega \ \theta) g.$$

Now, take $n(\mathrm{tr}_{L/F}(\cdot))$ of both sides. On the left-hand side, one obtains $n_{L/F}(\beta)Q(A, B) \in F^\times$, by Lemma 6.2.2. On the right-hand side, one obtains $n(g^*Vg)$, with V given below the proof of Proposition 6.1.13. But

$$n(g^*Vg) = N_6(g)n(V) = N_6(g)\mathrm{disc}(1, \omega, \theta) = N_6(g)Q(A, B).$$

Since $Q(A, B) \in F^\times$, $n_{L/F}(\beta) = N_6(g)$, so the proposition follows. \square

We now define an equivalence relation on based fractional $T \otimes C$ ideals. Suppose $I = b_1C + b_2C + b_3C \subseteq C_L$ is a $C_T = C \otimes_R T$ -module, and $\beta \in L^\times$ is a unit. We fix the good basis $(1, \omega, \theta)$ of T . Now say that (b_1, b_2, b_3, β) is equivalent to $(b'_1, b'_2, b'_3, \beta')$ if there exists $x \in C_L^\times$ so that

$$(b'_1, b'_2, b'_3, \beta') = (xb_1, xb_2, xb_3, n_C(x)\beta).$$

We have the following lemma.

Lemma 6.3.5. *The tuples (b_1, b_2, b_3, β) and $(b'_1, b'_2, b'_3, \beta')$ are equivalent if and only if $X := X_{b, \beta} = X_{b', \beta'} =: X'$.*

Proof. It is clear that if the tuples are equivalent, then $X = X'$. Conversely, since by assumption the b_i span C_L as a C_F -module, b is primitive. (This follows, for example, from the identity

$$(b_1, b_2, b_3) = (1, 0, 0) \begin{pmatrix} 1 & \omega & \theta \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} g$$

with g invertible.) Thus there exists $g \in \mathrm{GL}_3(C_L)$ so that $b_0 := bg = (1, 0, 0)$. Set $b'_0 = b'g$. Then one sees easily that there exists $x \in C_L^\times$ so that $b'_0 = xb_0$ and $\beta' = n_C(x)\beta$. The result for b and b' follows. \square

Associated to a non-degenerate pair $(A, B) \in H_3(C)^2$, one can define a based balanced $T \otimes C$ -module (I, β) as above, using some choice of v_0 . Then, if one changes v_0 to a different v'_0 , the I', β' one gets from v'_0 is equivalent to the I, β obtained from v_0 . For instance, this follows from the lifting law and Lemma 6.3.5.

Conversely, associated to a based-balanced $T \otimes C$ -modules $(I, (b_1, b_2, b_3), \beta)$, one obtains a pair $(A', B') \in H_3(C)^2$ by the equality $X_{b, \beta'} = -A'\theta + B'\omega + C'$. It is clear that the association $(I, (b_1, b_2, b_3), \beta) \mapsto (A', B')$ descends to the level of equivalence classes.

Lemma 6.3.6. *If $(I, (b_1, b_2, b_3), \beta)$ is a fractional $T \otimes C$ -ideal, and, as always, L is étale, then the associated pair (A', B') is non-degenerate.*

Proof. To see this, consider the equality

$$X := X_{I, \beta} = \beta^{-1} g^* \begin{pmatrix} 1 \\ \omega \\ \theta \end{pmatrix} (1 \ \omega \ \theta) g.$$

Then if $Y = \frac{1}{2}X \times_T X$, one has

$$(X, Y) = n_{L/F}(\beta)^{-1} N_6(g) \mathrm{disc}(1, \omega, \theta) = \mathrm{disc}(1, \omega, \theta) \neq 0$$

since I, β is assumed balanced. It now follows from Lemma 6.2.13 that (A', B') is non-degenerate. \square

The following result says that the above associations between equivalence classes of based-balanced $T \otimes C$ fractional ideals and non-degenerate pairs $(A, B) \in H_3(C)^2$ are inverse to one another.

Theorem 6.3.7. *The associations*

$$(A, B) \mapsto (T, (1, \omega, \theta), (I, (b_1, b_2, b_3)), \beta)$$

and

$$(T, (1, \omega, \theta), (I, (b_1, b_2, b_3)), \beta) \mapsto (A', B')$$

define inverse bijections between non-degenerate pairs (A, B) and based-balanced fractional $T \otimes C$ -ideals. These bijections are equivariant for the action of G_1 , where $(\lambda, g, m) \in \mathrm{GL}_1(R) \times \mathrm{GL}_2(R) \times \mathrm{GL}_3(C)$ acts on the data $(T, (1, \omega, \theta), (I, (b_1, b_2, b_3)), \beta)$ via

$$((\omega_0, \theta_0), (b_1, b_2, b_3), \beta; v_0) \mapsto (\lambda^3 N_6(m) \det(g)(\omega_0, \theta_0)g, (b_1, b_2, b_3)m, (\lambda^4 N_6(m) \det(g)^2)^{-1} \beta; v_0 m).$$

Here, $((\omega_0, \theta_0), (b_1, b_2, b_3), \beta; v_0)$ means that the data (b_1, b_2, b_3, β) is computed via the element $v_0 \in C^3$.

Proof. The lifting law says that the composition $(A, B) \mapsto (b_1, b_2, b_3, \beta) \mapsto (A', B')$ is the identity.

The direction $(I, \beta) = (b_1, b_2, b_3, \beta) \mapsto (A, B) \mapsto (b'_1, b'_2, b'_3, \beta')$ is also the identity. First, we check that the action maps are the same. For this, the basis b gives rise to the action map $S_I : T \rightarrow M_3(C)$. This map by definition satisfies the identity $\lambda b = b S_I(\lambda)$ for all $\lambda \in T$. One sees that this is the same as the action map $S_{A,B} : T \rightarrow M_3(C)$ by observing $X(I, \beta) = X(A, B)$. Indeed, note that if $\lambda \in T$, then

$$X(I, \beta) S_I(\lambda) = \lambda X(I, \beta) = \lambda X(A, B) = X(A, B) S_{A,B}(\lambda).$$

Taking $\text{tr}_{L/F}$ of both sides gives $S_I = S_{A,B}$ since $\text{tr}_{L/F}(X(A, B))$ is invertible, since we have already proved in 6.3.6 that (A, B) is non-degenerate.

Since we have just checked that the actions are the same, we may compute with the ϵ defined by S_I , as opposed to $S_{A,B}$. Now, set $v_0 = \text{tr}_{L/F}(b) = (\text{tr}_{L/F}(b_1), \text{tr}_{L/F}(b_2), \text{tr}_{L/F}(b_3)) \in C_F^3$. Then $v_0 \epsilon = \text{tr}_{L/F}(b) \epsilon$ and one computes (very easily) that this latter expression is just b . Hence with this choice of v_0 , $(b_1, b_2, b_3) = (b'_1, b'_2, b'_3)$. Furthermore, since

$$\beta^{-1} b^* b = X(I, \beta) = X(A, B) = \beta(v_0)^{-1} (b')^* b' = \beta(v_0)^{-1} b^* b,$$

we get $\beta = \beta(v_0)$. Thus, the composition $(I, \beta) \mapsto (A, B) \mapsto (I', \beta')$ is the identity as well.

Finally, the equivariance follows from Proposition 6.1.13. \square

Call the fractional $T \otimes C$ -ideal *oriented* if it comes equipped with an $\text{SL}_3(C)$ -orbit of C -bases $(b_1, b_2, b_3) \text{SL}_3(C)$. The following corollary proves Theorem 3.2.5 and implies Theorem 1.1.2 of the introduction.

Corollary 6.3.8. *If $m \in \text{GL}_3(C)$ and $g \in \text{GL}_2(R)$ with $N_6(m) = \det(g)^2$, so that $h = (\det(g)^{-1}, g, m)$ is in G , then h acts on the data via*

$$((\omega_0, \theta_0), (b_1, b_2, b_3), \beta; v_0) \mapsto ((\omega_0, \theta_0)g, (b_1, b_2, b_3)m, \beta; v_0m).$$

Consequently, if $(R^\times)^2 = 1$ (e.g., if $R = \mathbf{Z}$), then the G orbits on $(R^2 \otimes H_3(C))^{\text{open}}$ parametrize (T, I, β) up to equivalence and isomorphism, where I is oriented and (I, β) is balanced.

Proof. The first part of the corollary is immediate. For the second, note that if $(I, (b_1, b_2, b_3) \text{SL}_3(C))$ is an oriented fractional $T \otimes C$ -ideal, then $N(I, (b_1, b_2, b_3))$ is well-defined in $F^\times / (R^\times)^2$. Indeed, this follows from the fact that in the equation $(b_1, b_2, b_3) = (1, \omega, \theta)g$, g is well-defined up to $g \mapsto ugg'$ where $g' \in \text{SL}_3(C)$ and $u \in \text{GL}_3(R)$. Hence if $(R^\times)^2 = 1$ and I is oriented, the notion of a balanced pair (I, β) is unambiguous. Thus the second part of the corollary follows from the first. \square

7. THE SECOND LIFTING LAW FOR W_J

The purpose of this section is to give a second lifting law for the space W_J , where J is of a certain form. More specifically, suppose that K is a quadratic étale extension of F , and B is an associative cubic norm structure over K . Furthermore, assume that B comes equipped with an involution of the second kind, i.e., an order-reversing involution $* : B \rightarrow B$, which induces the nontrivial F -linear involution on K . This involution is required to be compatible with the cubic norm structure, in the sense that $n(x^*) = n(x)^*$ and $(x^*)^\# = (x^\#)^*$. Define $J \subseteq B$ to be the F -subspace of elements fixed by $*$. Then J is a cubic norm structure over F . In this section we will discuss a second lifting law for the space W_J .

Before explaining this lifting law, we list the common examples of such pairs (J, B) .

Example 7.0.1. Here are the common examples of pairs J, B as above.

- (1) Suppose K is any quadratic étale extension of F , $B = M_3(K)$ with its usual cubic norm structure, and $*$ conjugate transpose. Then $J = H_3(K)$ is the Hermitian 3×3 matrices.

- (2) Suppose $K = F \times F$, and A is a central simple F -algebra of degree three. Then set $B = A \times A^{opp}$, with involution $*$: $(x, y^{opp}) \mapsto (y, x^{opp})$.
- (3) Suppose A is an associative cubic norm structure over F , for which the multiplication in A is commutative, and suppose that K is any étale quadratic F -algebra. Set $B = A \otimes_F K$, with involution $(a \otimes \lambda)^* = a \otimes (\lambda^*)$ for $a \in A$ and $\lambda \in K$.

Throughout this section, J, B, K, F , and $*$ are as above. In this setting, Tits defined a cubic norm structure over F on the space $U = J \oplus B$, which we will review momentarily. In this case,

$$W_U = F \oplus (J \oplus B) \oplus (J \oplus B) \oplus F = W_J \oplus B^2$$

as F -vector spaces, and in fact as modules for a large subgroup G of $H(W_J)$. In this section we investigate when an element $v \in W_J$ of rank four can be lifted to a rank one element of W_U . In case (J, B) comes from a cubic étale algebra A over F , as in the third item of Example 7.0.1, the lifting law we prove reduces to a lifting law essentially contained in [GS14].

We begin this section by reviewing the second construction of Tits. We then describe the group G that acts on W_J and B^2 ; G is essentially $\mathrm{GU}(2, B)$. After this, we prove Theorem 7.3.1, which is the lifting law in this context. Interestingly, to prove this lifting law, we use the *first* lifting laws Theorems 5.1.1 and 5.1.4 for the spaces W_J and W_B . Finally, we end this section by giving a second construction of this lifting law, that is in a sense more explicit. We also explain the relation between this more explicit construction and some of the results in [GS14].

7.1. The second construction of Tits. In this subsection, we review the so-called second construction of Tits. More precisely, suppose that $\lambda \in K^\times$, $S \in J$, and $n(S) = \lambda\lambda^*$, so that in particular S is rank three. Out of this data, one puts on $U = J \oplus B$ the norm, adjoint, and pairing as follows: For $X \in J$ and $\alpha \in B$,

- (1) $n((X, \alpha)) = n(X) - (X, \alpha S \alpha^*) + \mathrm{tr}_{K/F}(\lambda n(\alpha))$;
- (2) $(X, \alpha)^\# = (X^\# - \alpha S \alpha^*, -X\alpha + \lambda^{-1}(\alpha^*)^\# S^\#)$;
- (3) $((X, \alpha), (Y, \beta)) = (X, Y) + \mathrm{tr}_J(\alpha S \beta^* + \beta S \alpha^*)$.

It is a fact that with these definitions, U is a cubic norm structure. This is the so-called second construction of Tits. We call the above cubic norm structure $U = U(S, \lambda)$.

7.2. Group actions. In this subsection, we define an action of a large subgroup of $\mathrm{GU}(2, B)$ on W_J . Here

$$\mathrm{GU}(2, B) = \{(g, \nu(g)) \in \mathrm{GL}_2(B) \times \mathrm{GL}_1 : g^* \begin{pmatrix} & 1 \\ -1 & \end{pmatrix} g = \nu(g) \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}\}.$$

Set $G \subseteq \mathrm{GL}(2, B)$ to be

$$G = \{g \in \mathrm{GU}(2, B) : \det(g) = \nu(g)^3\},$$

where $\det(g)$ in this definition is the degree 6 reduced norm on $M_2(B)$ as a central simple K -algebra. This group acts naturally on W_J as follows. First, consider on $W_B = K \oplus B \oplus B \oplus K$ the involution $*$: $(a, b, c, d) \mapsto (a^*, b^*, c^*, d^*)$. Clearly, W_J is the fixed space of $*$ on W_B . Since $\mathrm{GL}_2(B)$ acts on W_B , we have an action of $\mathrm{GU}(2, B)$ and thus G on W_B . We will check that this action of G preserves W_J . We use the left action of $\mathrm{GL}_2(B)$ and $\mathrm{GU}(2, B)$ on W_B .

One way to check this is simply by checking it on generators for G . However, we will give a different proof, which is perhaps more enlightening, by checking that $\mathrm{GU}(2, B)$ preserves an extra K -valued Hermitian form on W_B .

On the column vectors $W_2(B)$, one has the B -valued Hermitian symplectic form

$$(25) \quad \left\langle \left(\begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} x' \\ y' \end{pmatrix} \right) \right\rangle_B = (x^*, y^*) \begin{pmatrix} & 1 \\ -1 & \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} = x^* y' - y^* x'.$$

This B -valued pairing induces on $W_2(B)^{\otimes 3}$ a K -valued Hermitian form. Namely, for $\eta_i, \eta'_j \in W_2(B)$, define

$$(26) \quad \langle \eta_1 \otimes \eta_2 \otimes \eta_3, \eta'_1 \otimes \eta'_2 \otimes \eta'_3 \rangle = (\langle \eta_1, \eta'_1 \rangle_B, \langle \eta_2, \eta'_2 \rangle_B, \langle \eta_3, \eta'_3 \rangle_B),$$

where on the right-hand side we are applying the K -valued symmetric trilinear form on B that is the polarization of the norm form.

Note that the elements of the form $\eta_1 a \otimes \eta_2 a \otimes \eta_3 a - n(a)\eta_1 \otimes \eta_2 \otimes \eta_3$ are in the radical of the form (26). That is,

$$\langle \eta_1 a \otimes \eta_2 a \otimes \eta_3 a - n(a)\eta_1 \otimes \eta_2 \otimes \eta_3, \eta'_1 \otimes \eta'_2 \otimes \eta'_3 \rangle = 0$$

for all $\eta'_1, \eta'_2, \eta'_3$. Thus, this form descends to $V_B \simeq W_B$. Furthermore, it is clear that this form is Hermitian, and that $\text{GU}(2, B)$ preserves it up to ν^3 :

$$\langle g\eta_1 \otimes g\eta_2 \otimes g\eta_3, g\eta'_1 \otimes g\eta'_2 \otimes g\eta'_3 \rangle = \nu(g)^3 \langle \eta_1 \otimes \eta_2 \otimes \eta_3, \eta'_1 \otimes \eta'_2 \otimes \eta'_3 \rangle.$$

We calculate what this form is in coordinates of W_B . For $v, v' \in W_B$, denote $\langle v, v' \rangle_K$ the Hermitian form (26), and denote $\langle v, v' \rangle$ (with no K -subscript) the usual K -valued symplectic form on W_B .

Lemma 7.2.1. *If $v, v' \in W_B$, then $\langle v, v' \rangle_K = 6\langle v^*, v' \rangle$. In particular, since G preserves both this form and the symplectic form up to $\det(g) = \nu(g)^3$, G preserves W_J .*

Proof. Recall that an element (a, b, c, d) of W_B is the image of

$$ae \otimes e \otimes e + \sum_{cyc} e \otimes e \otimes bf + \sum_{cyc} f \otimes f \otimes ce + df \otimes f \otimes f.$$

The first part of the lemma is now a simple computation. For example,

$$\begin{aligned} \langle (0, b, 0, 0), (0, 0, c', 0) \rangle_K &= \left\langle \sum_{cyc} e \otimes e \otimes bf, \sum_{cyc} f \otimes f \otimes ce \right\rangle_K \\ &= 3(1, 1, -b^*c) \\ &= -6(b^*, c) \\ &= 6\langle (0, b, 0, 0)^*, (0, 0, c, 0) \rangle. \end{aligned}$$

For the second part of the lemma, suppose $g \in \text{GU}(2, B)$. Then for all $v, v' \in W_B$ one has

$$6\nu(g)^3 \langle v^*, v' \rangle = \nu(g)^3 \langle v, v' \rangle_K = \langle gv, gv' \rangle_K = 6\langle (gv)^*, gv' \rangle = 6\det(g) \langle g^{-1}(gv)^*, v' \rangle.$$

Hence if $g \in G$ so that $\nu(g)^3 = \det_6(g)$, then $(gv)^* = g(v^*)$. It follows that G preserves W_J , as claimed. \square

From now on, we let G act on W_J as the ν^{-1} twist of the cubic polynomial action derived from the action of $\text{GL}_2(B)$ on W_B . With this action, we obtain a map $G \rightarrow H(W_J)$, preserving similitudes. Indeed, this follows immediately from Lemma 7.2.1 and the fact that the cubic polynomial action of $\text{GL}_2(B)$ on W_B preserves the symplectic and quartic form up to $\det_6(g)$ and $\det_6(g)^2$, respectively.

Since G acts on W_J and on B^2 , it acts on $W_U = W_J \oplus B^2$. The explicit identification of the right-hand side with the left-hand side is

$$v + \eta = (a, b, c, d) + \begin{pmatrix} u \\ v \end{pmatrix} \mapsto (a, (b, -u), (c, v), d).$$

Here $(b, -u)$ and (c, v) are considered elements of $U = J \oplus B$. With this choice of identification, the action of G on $W_J \oplus B^2 \simeq W_U$ preserves the symplectic and quartic form on W_U up to similitude.

Proposition 7.2.2. *Suppose $U = U(S, \lambda)$ for any S, λ as above. Then the map $G \rightarrow \text{GL}(W_U)$ defined by the action $g(v + \eta) = gv + g\eta$ preserves the symplectic and quartic form on W_U up to ν and ν^2 , respectively. That is, this action defines an embedding $G \rightarrow H(W_U)$, preserving similitudes.*

Proof. It suffices to check this on generators of G , which may be done easily. \square

7.3. The lifting law. With the above preparations, we can now state and prove the lifting law. Suppose given $v = (a, b, c, d) \in W_J$ of rank four. We ask when we can lift v to a rank one element of W_U . This question is answered by the following theorem.

Theorem 7.3.1. *Suppose $v \in W_J$ is rank four, and set $J_2 = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$.*

- (1) *If there exists (S, λ) as above, and $\eta \in B^2$, so that $v + \eta$ is rank one in $W_U \simeq W_J \oplus B^2$, then $q(v) = \omega^2$ for $\omega \in K^\times$ with $\omega^* = -\omega$.*
- (2) *Conversely, suppose $q(v) = \omega^2$ for $\omega \in K^\times$ with $\omega^* = -\omega$. Then there exists S, λ, η with $v + \eta$ rank one in $W_{U(S, \lambda)}$. More precisely, by the lifting law Theorem 5.1.4 for W_B , there exists $\lambda \in K^\times$ and $\eta \in B^2$ so that $\lambda\eta^! = \frac{-\omega v + v^b}{2}$. Then $n\left(\frac{\langle \eta, \eta \rangle_B}{\omega}\right) = (\lambda\lambda^*)^{-1}$ is invertible.*

Set $S = \left(\frac{\langle \eta, \eta \rangle_B}{\omega}\right)^{-1}$. Then $v + \eta$ is rank one in $W_{U(S, \lambda)}$. Furthermore, one has the identity $\eta S \eta^ = S(v) - \frac{\omega}{2} J_2$.*

- (3) *Finally, suppose S, λ and η are such that $v + \eta$ is rank one in $W_{U(S, \lambda)}$. Then $\lambda\eta^! = \frac{\pm\omega v + v^b}{2}$. Choose the element ω so that $\lambda\eta^! = \frac{-\omega v + v^b}{2}$. Then $\frac{\langle \eta, \eta \rangle_B}{\omega} = S^{-1}$ and $\eta S \eta^* = S(v) - \frac{\omega}{2} J_2$.*

Proof. We prove the statements in turn. Consider the first claim. Thus suppose (S, λ) are as above, and $v + \eta$ is rank one in $W_J \oplus B^2$. By equivariance, i.e., Proposition 7.2.2, we may assume $v = (1, 0, c, d)$. Then $v + \eta = (1, (0, -u), (c, v), d)$, and thus

$$(c, v) = (0, -u)^\# = (-u S u^*, \lambda^{-1}(u^*)^\# S^\#)$$

and $d = n((0, -u)) = -\text{tr}_{K/F}(\lambda n(u))$. Consequently,

$$\begin{aligned} q(v) &= d^2 + 4n(c) = \text{tr}_{K/F}(\lambda n(u))^2 - 4n(S)n(u)n(u^*) = \text{tr}_{K/F}(\lambda n(u))^2 - 4n_{K/F}(\lambda n(u)) \\ &= (\lambda n(u) - (\lambda n(u))^*)^2. \end{aligned}$$

This proves the first part.

Now consider the second claim. Thus assume $q(v) = \omega^2$ with $\omega^* = -\omega$ in K . Recall the notation $X(\pm\omega, v) = \frac{\pm\omega v + v^b}{2}$. By the lifting law for W_B , there exist $\lambda \in K^\times$ and $\eta \in B^2$ so that $\lambda\eta^! = X(-\omega, v)$. Thus

$$\omega q(v) = \langle X(\omega, v), X(-\omega, v) \rangle = \langle \lambda^*(\eta^*)^!, \lambda\eta^! \rangle = \lambda\lambda^* n(\langle \eta, \eta \rangle_B).$$

It follows that $n(\langle \eta, \eta \rangle_B / \omega) = (\lambda\lambda^*)^{-1}$, as claimed. Thus, $\langle \eta, \eta \rangle_B / \omega = S^{-1}$, with $S \in J$ and $n(S) = \lambda\lambda^*$.

We claim that with these definitions of S and λ , $v + \eta$ is rank one in $W_{U(S, \lambda)}$. To check this, we may use equivariance of these conditions under the action of $G \subseteq \text{GU}(2, B) \subseteq \text{GL}(2, B)$, the group of (g, ν) such that $\det_6(g) = \nu(g)^3$. Indeed, if $g \in G$, set $v' = gv$, $\eta' = g\eta$, $\omega' = \nu(g)\omega$. Then $\lambda(\eta')^! = \frac{-\omega'v' + (v')^b}{2}$, $\langle \eta', \eta' \rangle_B / \omega' = S^{-1}$, and $v + \eta$ is rank one if and only if $v' + \eta'$ is rank one. Thus we may assume $v = (1, 0, c, d)$, so that $v + \eta = (1, (0, -u), (c, v), d)$. We must check $-u S u^* = c, \lambda^{-1}(u^*)^\# S^\# = v$, and $\text{tr}_{K/F}(\lambda n(u)) = -d$.

For $v = (1, 0, c, d)$, one has $v^b = (-d, 2c^\#, dc, d^2 + 2n(c))$. Thus

$$(\lambda n(u), \lambda v u^\#, \lambda u v^\#, \lambda n(v)) = \lambda\eta^! = \frac{-\omega v + v^b}{2} = (-(d+\omega)/2, c^\#, (d-\omega)c/2, (-\omega d + d^2 + 2n(c))/2).$$

Immediately, we obtain $\text{tr}_{K/F}(\lambda n(u)) = -d$.

Now, since $\langle \eta, \eta \rangle_B / \omega = S^{-1}$,

$$-u \frac{(\langle \eta, \eta \rangle_B)^\#}{q(v)} u^* = -n(S)^{-1} u S u^*.$$

It is an identity in associative cubic norm structures that

$$u(\langle \eta, \eta \rangle_B)^\# u^* = u(u^*v - v^*u)^\# u^* = n(u^*)uv^\# - (vu^\#) \times (vu^\#)^* + n(u)(uv^\#)^*.$$

Thus

$$\begin{aligned} -uSu^* &= \frac{n(S)}{q(v)} \left(-u(\langle \eta, \eta \rangle_B)^\# u^* \right) \\ &= \frac{\lambda\lambda^*}{q(v)} \left((vu^\#) \times (vu^\#)^* - n(u^*)uv^\# - n(u)(uv^\#)^* \right) \\ &= \frac{1}{q(v)} \left(c^\# \times c^\# + \left(\frac{d-\omega}{2} \right)^2 c + \left(\frac{d+\omega}{2} \right)^2 c \right) \\ &= \frac{1}{q(v)} \left(\frac{d^2 + 4n(c) + \omega^2}{2} \right) c \\ &= c, \end{aligned}$$

as desired.

Next, we must check that $\lambda^{-1}(u^*)^\# S^\# = v$. But we have

$$\lambda^{-1}(u^*)^\# S^\# = \lambda^*(u^*)^\# S^{-1} = \frac{(\lambda u^\#)^*(u^*v - v^*u)}{\omega} = \frac{(\lambda n(u))^*v - (\lambda v u^\#)^*u}{\omega}.$$

But $(\lambda v u^\#)^* = (c^\#)^* = c^\# = \lambda v u^\#$, and thus $(\lambda v u^\#)^*u = \lambda n(u)v$. Thus,

$$\lambda^{-1}(u^*)^\# S^\# = \left(\frac{(\lambda n(u))^* - (\lambda n(u))}{\omega} \right) v = v.$$

Thus, we have checked that if $\lambda\eta^\dagger = X(-\omega, v)$ and $\langle \eta, \eta \rangle_B/\omega = S^{-1}$, then $v + \eta$ is rank one.

To finish the proof of the second claim, we must evaluate $\eta S \eta^* = \begin{pmatrix} uSu^* & uSv^* \\ vSu^* & vSv^* \end{pmatrix}$. We have already checked $uSu^* = -c$. Since we have already checked that $v + \eta$ is rank one, we obtain

$$(0, -du) = (c, v)^\# = (c^\# - vSv^*, -cv + \lambda^{-1}(v^*)^\# S^\#).$$

Thus $vSv^* = c^\#$. Finally, as above,

$$\begin{aligned} q(v)uSv^* &= \lambda\lambda^*u(u^*v - v^*u)^\# v^* = \lambda\lambda^* \left((uv^\#)(vu^\#)^* - 1 \times ((uv^\#)^*(vu^\#)) + n(u)n(v)^* \right) \\ &= \left(\frac{d-\omega}{2} \right) cc^\# - 1 \times \left(\left(\frac{d+\omega}{2} \right) cc^\# \right) - \left(\frac{d+\omega}{2} \right) \left(\frac{\omega d + d^2 + 2n(c)}{2} \right) \\ &= -\frac{d}{4}(d^2 + 4n(c) + \omega^2) - \frac{\omega}{2}(d^2 + 4n(c)). \end{aligned}$$

Hence $uSv^* = -d/2 - \omega/2$. Taking the conjugate, one obtains $vSu^* = -d/2 + \omega/2$. Since for $v = (1, 0, c, d)$ one has $S(v) = \begin{pmatrix} -c & -d/2 \\ -d/2 & c^\# \end{pmatrix}$, this proves $\eta S \eta^* = S(v) - \frac{\omega}{2} J_2$, completing the proof of the second claim.

We now consider the third claim. Thus suppose $S \in J$, $\lambda \in K^\times$, $n(S) = \lambda\lambda^*$. Furthermore suppose $v \in W_J$ with $q(v) = \omega^2$ and $v + \eta$ is rank one in $W_{U(S, \lambda)}$. Consider $\text{tr}_{K/F}(\lambda\eta^\dagger) := (\lambda\eta^\dagger)^* + \lambda\eta^\dagger$ in W_J . We first claim that $\text{tr}_{K/F}(\lambda\eta^\dagger) = v^\flat$.

Note that $W_J \otimes K = W_J \oplus \omega W_J = W_B$, and the action of G commutes with this decomposition. Thus the statement $\text{tr}_{K/F}(\lambda\eta^\dagger) = v^\flat$ is invariant under the G action, so we may as usual assume $v = (1, 0, c, d)$. Since $v + \eta$ is rank one, $(c, v) = (-uSu^*, \lambda^{-1}(u^*)^\# S^\#)$ and $d = -\text{tr}_{K/F}(\lambda n(u))$. One obtains from these that $\lambda v u^\# = c^\#$, $\lambda u v^\# = -(\lambda n(u))^*c$ and $\lambda n(v) = (\lambda^* n(u)^*)^2$. Thus

$$\text{tr}_{K/F}(\lambda\eta^\dagger) = (-d, 2c^\#, -dc, \text{tr}_{K/F}((\lambda n(u))^2)).$$

Now for $x \in K$, $\text{tr}(x^2) = (x + x^*)^2 - 2xx^*$, and thus

$$\text{tr}_{K/F}((\lambda n(u))^2) = (-d)^2 - 2\lambda\lambda^*n(u)n(u^*) = d^2 + 2n(-uSu^*) = d^2 + 2n(c).$$

Hence $\text{tr}_{K/F}(\lambda\eta^!) = v^b$, as desired.

We obtain that $\lambda\eta^! = \frac{-\omega x + v^b}{2}$ is rank one, for some $x \in W_J$. That $x = \pm v$ follows from the essential uniqueness of rank one lifts, Lemma 5.1.2. Namely, one applies Lemma 5.1.2 to the element $2\omega\lambda\eta^!$, and uses that $(x^b)^b = -q(x)x$ for $x \in W_J$ and $q(x^b) = q(x)^3$. Now, choose ω so that $\lambda\eta^! = \frac{-\omega v + v^b}{2}$. We must evaluate $\frac{\langle \eta, \eta \rangle_B}{\omega}$. Again, by equivariance, we may assume $v = (1, 0, c, d)$. But then

$$u^*v - v^*u = \lambda^{-1}n(u^*)S^\# - (\lambda^*)^{-1}S^\#n(u) = (\lambda^*n(u^*) - \lambda n(u))S^{-1}.$$

Since $\lambda\eta^! = \frac{-\omega v + v^b}{2}$, $(\lambda^*n(u^*) - \lambda n(u)) = \omega$, giving that $\frac{\langle \eta, \eta \rangle_B}{\omega} = S^{-1}$.

The final part of the third claim follows as the final part of the second claim. This completes the proof of the theorem. \square

Remark 7.3.2. Suppose A is a commutative associative cubic norm structure, as in the third item of Example 7.0.1. If $v \in W_A$ is rank four, then one can define $K = F[x]/(x^2 - q(v))$ and $B = A \otimes K$ as in this example. Theorem 7.3.1 then applies. Thus in the case that A is commutative, every rank four element of W_A can be lifted to a rank one element of W_U , for an appropriate U .

7.4. A more explicit construction of the lift. In Theorem 7.3.1, given $v \in W_J$ of rank four with $q(v)$ of a certain form, we produced a cubic norm structure $U = J \oplus B$ and a rank one lift $\tilde{v} = v + \eta \in W_U \simeq W_J \oplus B^2$. To give this construction one must choose $\eta \in B^2$ and $\lambda \in K^\times$ so that $\lambda\eta^! = \frac{-\omega v + v^b}{2}$. The existence of such λ, η are guaranteed by the lifting law Theorem 5.1.4. In this subsection we explain how one can construct the cubic norm structure U and the rank one lift $\tilde{v} \in W_U$ without making any choices. However, the price that is paid to do this is to first construct a space $\tilde{U} = J + B^2$ and a rank one B -module $I(v, \omega) \subseteq B^2 \subseteq \tilde{U}$. The cubic norm structure U is then given as $\tilde{U}/I(v, \omega)$. The rank one lift in W_U can then be produced more canonically, as the image of an element from $F \oplus \tilde{U} \oplus \tilde{U} \oplus F$ in $W_U = F \oplus \left(\tilde{U}/I(v, \omega)\right) \oplus \left(\tilde{U}/I(v, \omega)\right) \oplus F$.

After we describe \tilde{U} , $U = \tilde{U}/I(v, \omega)$, and the rank one lift, we explain the relation of some of these constructions to elements of [GS14]. Throughout this subsection, $v = (a, b, c, d) \in W_J$ is rank four.

7.4.1. Formulas defining the cubic norm structure on $\tilde{U}/I(v, \omega)$. We now define $I(v, \omega) \subseteq B^2$ and the explicit formulas for the norm, adjoint, and pairing on the quotient $\tilde{U}/I(v, \omega)$.

Set

$$h(v, \omega) := -\frac{\omega}{2}J_2 + S(v)$$

where recall $J_2 = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$ and

$$S(v) = \begin{pmatrix} b^\# - ac & ad - cb - \text{tr}(ad - cb)/2 \\ ad - bc - \text{tr}(ad - bc)/2 & c^\# - db \end{pmatrix}.$$

Then $h(v, \omega) \in M_2(B)$ satisfies $h(v, \omega)^* = h(v, \omega)$, where $*$ on $M_2(B)$ is the composite of matrix transpose and $*$ on B . We define $Ad(\cdot; v, \omega) : \tilde{U} \rightarrow \tilde{U}$ as follows. For $x \in J$ and a row vector $\ell \in B^2$, set

$$Ad((x, \ell); v, \omega) := (x^\# - \ell h(v, \omega)\ell^*, -x\ell + \delta(\ell; v)^*J_2)$$

where here if $\ell = (u, v)$,

$$\delta(\ell; v) := \begin{pmatrix} au^\# + u \times (vb) + cv^\# \\ bu^\# + (uc) \times v + dv^\# \end{pmatrix}.$$

The norm on \tilde{U} is defined as

$$n((x, \ell); v, \omega) := n(x) - (x, \ell h(v, \omega) \ell^*) + \text{tr}_{K/F} \left(\left\langle \frac{-\omega v + v^b}{2}, J_2^{-1} \ell^! \right\rangle \right).$$

Here, ℓ is a row vector, so if $\ell = (u, v)$, then $\ell^! = (n(u), u^\#v, v^\#u, n(v))$. Note that $\ell^!$ and $-\omega v + v^b$ live in $W_B \supseteq W_J$, not W_J .

The submodule $I(v, \omega)$ is defined to be the set of $\ell \in B^2$ for which $\ell h(v, \omega) = 0$. Equivalently, since the trace pairing on B is non-degenerate, $I(v, \omega)$ is the set of ℓ for which $\text{tr}_{B/K}(\ell h(v, \omega) (\ell')^*) = 0$ for all $\ell' \in B^2$.

A pairing $\tilde{U} \otimes \tilde{U} \rightarrow F$ is defined as follows. Suppose $(x_1, \ell_1), (x_2, \ell_2)$ are in \tilde{U} , with $x_i \in J$ and $\ell_i \in B^2$. Define

$$((x_1, \ell_1), (x_2, \ell_2); v, \omega) := (x_1, x_2) + \text{tr}_{B/K}(\ell_1 h(v, \omega) \ell_2^* + \ell_2 h(v, \omega) \ell_1^*).$$

It is clear that this lands in F , and descends to $U(v, \omega) \otimes U(v, \omega)$.

Define $Ad(\cdot, \cdot; v, \omega) : \tilde{U} \otimes \tilde{U} \rightarrow \tilde{U}$ via $Ad(y, z; v, \omega) = Ad(y + z; v, \omega) - Ad(y; v, \omega) - Ad(z; v, \omega)$. When v and ω are fixed, we abbreviate $Ad(y, z; v, \omega)$ as $y \times z$.

The above formulas do not define a cubic norm structure on \tilde{U} . However, they do define a cubic norm structure on $U = \tilde{U}/I(v, \omega)$, as stated in Theorem 7.4.1. Furthermore, these formulas have the advantage that they depend explicitly, and in fact equivariantly, on the element $v \in W_J$. We first prove that U is a cubic norm structure, by producing an isomorphism with the second Tits construction $U(S, \lambda) = J \oplus B$. We then discuss the equivariance properties of the formulas and the rank one lift.

Theorem 7.4.1. *Suppose v in W_J is rank 4, with $q(v) = \omega^2$, and $\omega \in K^\times$ with $\omega^* = -\omega$. The submodule $I(v, \omega)$ satisfies $\tilde{U} \times I(v, \omega) \subseteq I(v, \omega)$, and the norm map $n(\cdot; v, \omega)$ is well-defined on $U(v, \omega) = \tilde{U}/I(v, \omega)$. The induced adjoint $Ad(\cdot; v, \omega)$, norm, and pairing on $U(v, \omega) := \tilde{U}/I(v, \omega)$ make it a cubic norm structure. In fact, $U \simeq U(S, \lambda)$ for appropriate S, λ in the second construction of Tits.*

Proof. We explain the isomorphism $\tilde{U}/I(v, \omega) \simeq U(S, \lambda)$, from which the other statements follow.

Note that $h(v, \omega) J_2 = \frac{\omega + R(v)}{2}$, and this latter element of $M_2(B)$ occurs in the lifting law Theorem 5.1.4. Thus for a column vector η_0 in B^2 , by Theorem 5.1.4 we have

$$(h(v, \omega) J_2 \eta_0)^! = \langle X(\omega, v), \eta_0^! \rangle X(-\omega, v).$$

Here recall that $X(\pm\omega, v) = \frac{\pm\omega v + v^b}{2}$. Choose η_0 so that $\langle X(\omega, v), \eta_0^! \rangle \in K^\times$, and set $\eta = h(v, \omega) J_2 \eta_0$.

Then with $\lambda = (\langle X(\omega, v), \eta_0^! \rangle)^{-1}$, one has $\lambda \eta^! = \frac{-\omega v + v^b}{2}$. Define $S = \left(\frac{\langle \eta, \eta \rangle_B}{\omega} \right)^{-1}$ as in Theorem 7.3.1.

We now define a map $\tilde{U} \rightarrow U(S, \lambda)$ as

$$(x, \ell) \mapsto (x, \ell \eta) = (x, \ell h(v, \omega) J \eta_0).$$

Note that $\ell \eta \in B$ since ℓ is a row vector and η is a column vector. Furthermore, it is clear that by the definition of $I(v, \omega)$, this map induces a map $\tilde{U}/I(v, \omega) \rightarrow U(S, \lambda)$.

We claim that $B^2/I(v, \omega) \rightarrow B$ via $\ell \mapsto \ell \eta$ is a left B -module isomorphism. To see this, note that is injective, because if $\ell \eta = 0$, then $\ell \eta S \eta^* = 0$. But from Theorem 7.3.1, $\eta S \eta^* = h(v, \omega)$, so $\ell h(v, \omega) = 0$, so $\ell \in I(v, \omega)$. To see that $B^2/I(v, \omega) \rightarrow B$ is surjective, note that since it is a B -module map, it suffices to check that the image contains a unit of B . But if $\ell = \frac{1}{\omega} \eta^* J_2$, then $\ell \eta = \frac{1}{\omega} \langle \eta, \eta \rangle_B = S^{-1}$ is invertible. Thus $\tilde{U}/I(v, \omega) \simeq U(S, \lambda)$ is an F -linear isomorphism.

Using the fact that $h(v, \omega) = \eta S \eta^*$ and $\frac{-\omega v + v^b}{2} = \lambda \eta^!$, it is easy to check that the norm and pairing defined above on \tilde{U} factor through the map $\tilde{U} \rightarrow U(S, \lambda)$ and the norm and pairing on the

$U(S, \lambda)$. One can also show that the adjoint map $\# : \tilde{U} \rightarrow \tilde{U}$ commutes with the map $\tilde{U} \rightarrow U(S, \lambda)$. The statements of the theorem now all follow. \square

As mentioned above, the formulas for the norm, adjoint, and pairing on \tilde{U} have the advantage that they are explicitly defined in terms of $v \in W_J$, that they are suitably equivariant in v , and that they enable one to write down a rank one lift $\tilde{v} \in W_U$ somewhat more canonically than we could in Theorem 7.3.1. We now address these equivariance and lifting claims.

7.4.2. *Equivariance of formulas on \tilde{U} .* For the equivariance, we have the following theorem.

Theorem 7.4.2. *Suppose $x, x_1, x_2 \in J$ and ℓ, ℓ_1, ℓ_2 in B^2 are row vectors. Furthermore, suppose $g \in G$. Then*

- (1) *The norm is equivariant for the action of G : $n((x, \ell); gv, \nu(g)\omega) = n((x, \ell g); v, \omega)$.*
- (2) *The adjoint is equivariant for the action of G : $Ad((x, \ell); gv, \nu(g)\omega) = Ad((x, \ell g); v, \omega)g^{-1}$. The g^{-1} on the right-hand side of this equality acts by multiplication on the B^2 component in \tilde{U} and acts trivially on the J component.*
- (3) *The pairing is equivariant for the action of G :*

$$((x_1, \ell_1), (x_2, \ell_2); gv, \nu(g)\omega) = ((x_1, \ell_1 g), (x_2, \ell_2 g); v, \omega).$$

- (4) *The B submodule $I(v, \omega)$ is equivariant for the action of G : $I(gv, \nu(g)\omega) = I(v, \omega)g^{-1}$.*

Proof. Most of the statements of the theorem are straightforward checks. We explain the proof of the most difficult step, which is the equivariance of the map $\delta(\ell; v)$, which is needed to prove that the adjoint map is suitably equivariant. In fact, the map $\delta(\ell; v)$ satisfies an equivariance property for all of $\text{GL}_2(B)$: $g\delta(\ell g; v) = \delta(\ell; g \cdot v)$ for $g \in \text{GL}_2(B)$, where here $g \cdot v$ is the cubic polynomial action of $\text{GL}_2(B)$ on W_B . To check this equivariance statement, it suffices to check it on generators for $\text{GL}_2(B)$, and the only nontrivial part is the equivariance for the action of the elements $n(X)$, $X \in B$.

Suppose $\ell = (u, v)$, and recall $v = (a, b, c, d) \in W_B$. To check the equivariance for $n(X)$, one must verify the identity

$$\begin{pmatrix} 1 & \\ X & 1 \end{pmatrix} \begin{pmatrix} a(u + vX)^\# + (u + vX) \times (vb) + cv^\# \\ b(u + vX)^\# + ((u + vX)c) \times v + dv^\# \end{pmatrix} = \begin{pmatrix} a'u^\# + u \times (vb') + c'v^\# \\ b'u^\# + (uc') \times v + d'v^\# \end{pmatrix},$$

where $a' = a$, $b' = b + aX$, $c' = c + b \times X + aX^\#$, and $d' = d + (c, X) + (b, X^\#) + an(X)$. The top row of this equality is immediate, using the identity $(vX) \times (vb) = (X \times b)v^\#$. For the second row, one must prove that

- $b(u \times (vX)) + X(u \times (vb)) = (u(b \times X)) \times v$
- $X(u \times (vX)) = (uX^\#) \times v$
- $d' = d + (Xc) \times 1 + bX^\# + Xc'$.

This last identity follows from $(Xc) \times 1 = (c, X) - Xc$ and $X(b \times X) + bX^\# = (b, X^\#)$. The second identity follows from pairing each side against an arbitrary $w \in B$:

$$(w, X(u \times (vX))) = (wX, u \times (vX)) = ((wX) \times (vX), u) = (X^\#(w \times v), u) = (w, (uX^\#) \times v).$$

The first identity similarly follows by pairing against an arbitrary w in B , while now using the following claim.

Claim 7.4.3. *If b, X, v, w are in B , then $(b \times X)(v \times w) = (vb) \times (wX) + (vX) \times (wb)$.*

Proof. One obtains the claim by linearizing the identity $(v(b + X)) \times (w(b + X)) = (b + X)^\#(v \times w)$. \square

Applying the claim, one obtains

$$\begin{aligned} (w, (u(b \times X)) \times v) &= ((b \times X)(w \times v), u) = ((vb) \times (wX) + (vX) \times (wb), u) \\ &= (w, b(u \times (vX)) + X(u \times (vb))), \end{aligned}$$

finishing the proof. \square

7.4.3. The rank one lift. We now explain the lifting law from the point of view of \tilde{U} . Since $\tilde{U} = J \oplus B^2$, one has a decomposition $F \oplus \tilde{U} \oplus \tilde{U} \oplus F = W_J \oplus M_2(B)$. Explicitly, if $\ell_1, \ell_2 \in B^2$ are row vectors, $m = \begin{pmatrix} \ell_1 \\ \ell_2 \end{pmatrix} \in M_2(B)$, and $v' = (a', b', c', d') \in W_J$, then we identify $v' + m \in W_J \oplus M_2(B)$ with the element $(a', (b', -\ell_1), (c', \ell_2), d')$ in $F \oplus \tilde{U} \oplus \tilde{U} \oplus F$.

We let G act on $M_2(B)$ via left translation: $m \mapsto gm$ in $M_2(B)$. Taking the quotient of \tilde{U} by $I(v, \omega)$, we obtain a map

$$(27) \quad W_J \oplus M_2(B) \simeq F \oplus \tilde{U} \oplus \tilde{U} \oplus F \rightarrow F \oplus \left(\tilde{U}/I(v, \omega) \right) \oplus \left(\tilde{U}/I(v, \omega) \right) \oplus F \simeq W_U.$$

It is clear that this map is equivariant for the action of G on both sides. We now have the following result.

Theorem 7.4.4. *Suppose v in W_J is rank 4, with $q(v) = \omega^2$, and $\omega \in K^\times$ with $\omega^* = -\omega$. Let $\tilde{U}, I(v, \omega)$ and $U = \tilde{U}/I(v, \omega)$ be as above. Then the image of the element $\tilde{v} = v + 1_2$ in W_U under the map (27) is rank one.*

This theorem gives the somewhat more canonical rank one lift $\tilde{v} \in W_U$ of $v \in W_J$ promised above.

Proof. The cubic norm structure $U = \tilde{U}/I(v, \omega)$ was proved in Theorem 7.4.1 to be isomorphic to $U(S, \lambda)$, in the notation of that theorem. The map constructed in Theorem 7.4.1 sends $x + \ell \in J \oplus B^2$ to $(x, \ell\eta)$, where $\eta \in B^2$ is a column vector with $\lambda\eta^1 = \frac{-\omega v + v^b}{2}$. Thus if $\eta = \begin{pmatrix} u \\ v \end{pmatrix}$, the image of $v + 1_2$ under the map (27), composed with the isomorphism $U \simeq U(S, \lambda)$, is $(a, (b, -u), (c, v), d) \in W_{U(S, \lambda)}$. But this latter element was proved to be rank one in Theorem 7.3.1. This completes the proof of the theorem. \square

Remark 7.4.5. Denote ω_0 the image of the element $(1, 0) \in B^2$ in $B^2/I(v, \omega) \subseteq U$, and similarly set θ_0 the image of the element $(0, 1) \in B^2$ in $B^2/I(v, \omega) \subseteq U$. Then Theorem 7.4.4 says that $(a, b - \omega_0, c + \theta_0, d)$ is rank one in W_U . This theorem generalizes the lifting law discussed in subsection 2.3.

7.4.4. Relation with work of Gan-Savin [GS14]. We close this section by discussing the relation of the lifting laws in this section with elements of the paper [GS14].

More specifically, consider the case when the pair J and B are as in the third item of Example 7.0.1, so that $B = A \otimes_F K$, with A a commutative associative cubic norm structure. Then $A^2 \subseteq B^2$, and in fact the map $A^2 \rightarrow B^2/I(v, \omega)$ is an isomorphism of left A -modules. Indeed, both sides have the same dimension as F -vector spaces, and it is injective because $A^2 \cap I(v, \omega) = 0$. That $A^2 \cap I(v, \omega) = 0$ is immediate: If $0 = \ell h(v, \omega) = \ell S(v) - \frac{\omega}{2} \ell J_2$, then clearly $\ell = 0$, by looking at the coefficient of ω .

It follows from this fact that in this setting, one can write the formulas for the cubic norm structure $U = J \oplus B^2/I(v, \omega) \simeq A \oplus A^2$ entirely in terms of A . One obtains the following formulas. Here $v = (a, b, c, d) \in W_A$ is rank four, $x, x_1, x_2 \in A$ and $\ell, \ell_1, \ell_2 \in A^2$ are row vectors:

- (1) The norm on U is given by $n((x, \ell); v) = n(x) - (x, \ell S(v) \ell^t) + \langle v^b, J_2^{-1} \ell^t \rangle$.
- (2) The adjoint on U is given by $Ad((x, \ell); v) = (x^\# - \ell S(v) \ell^t, -x\ell + \delta(\ell; v)^t J_2)$.
- (3) The pairing on U is given by $((x_1, \ell_1), (x_2, \ell_2); v) = (x_1, x_2) + \text{tr}_{A/F}(\ell_1 S(v) \ell_2^t + \ell_2 S(v) \ell_1^t)$.

Here if $\ell = (u, v)$,

$$\delta(\ell; v) = \begin{pmatrix} au^\# + u \times (vb) + cv^\# \\ bu^\# + (uc) \times v + dv^\# \end{pmatrix}.$$

Note that the ω drops out in all of these formulas. These explicit formulas for the cubic norm structure U associated to $v \in W_A$ of rank four are (in different notation) the ones given by Gan-Savin given in [GS14, Section 10].

As in Theorem 7.4.2, the above formulas for the cubic norm structure on U are equivariant for the action of a certain subgroup $G \subseteq \mathrm{GL}_2(A)$. Namely, denote $\det_2 : \mathrm{GL}_2(A) \rightarrow \mathrm{GL}_1(A)$ the usual (degree two) determinant map, which we denote with a subscript 2 to distinguish it from the degree 6 map $\mathrm{GL}_2(A) \rightarrow \mathrm{GL}_1(F)$. Then if $G = \{g \in \mathrm{GL}_2(A) : \det_2(g) \in \mathrm{GL}_1(F)\}$, the above formulas defining the cubic norm structure on U are equivariant for the action of G . Here, the action of G on W_A is the \det_2^{-1} twist of the cubic polynomial action.

Finally, we restate the lifting law in this context, which is implicit in [GS14]. Define a map $W_A \oplus M_2(A) \rightarrow W_U$ by

$$v + m = (a', b', c', d') + \begin{pmatrix} \ell_1 \\ \ell_2 \end{pmatrix} \mapsto (a', (b', -\ell_1), (c', \ell_2), d') \in W_U.$$

Then $G \subseteq \mathrm{GL}_2(A)$ acts on $M_2(A)$ by left translation, $m \mapsto gm$, and by the action on W_A just described. This defines an action of G on W_U , and one has the following result. As above, denote by $\omega_0 = (1, 0) \in A^2 \subseteq U$ and $\theta_0 = (0, 1) \in A^2 \subseteq U$.

Theorem 7.4.6 (Gan-Savin). *Suppose $v \in W_A$ is rank 4. With the formulas defined above, U is a cubic norm structure. The action of G on W_U preserves the symplectic and quartic form on W_U up to similitude, thus giving a map $G \rightarrow H(W_U)$, preserving similitudes. The lifted element*

$$v + 1_2 = (a, b, c, d) + (0, -\omega_0, \theta_0, 0) =: (a, -\omega, \theta, d) \in W_U$$

is rank one.

8. LOWER RANK LIFTING LAWS

In this section we give a few examples of lower rank lifting laws. That is, we show how to lift elements of non-maximal rank in certain prehomogeneous spaces, i.e., elements not in the open orbit, to rank one elements of bigger prehomogeneous vector spaces. More precisely, we use the Cayley-Dickson construction to lift elements of $H_3(C)$ of rank two, for C an associative composition algebra, to rank one elements of $H_3(D)$, with D a composition algebra produced from C via the Cayley-Dickson construction. We again use the Cayley-Dickson construction to lift rank two elements of $W_{H_3(C)}$ to rank one elements of $W_{H_3(D)}$. Finally, we lift rank 3 elements of W_J to rank one elements of $W_{J \oplus B}$ by using the second Tits construction.

8.1. The Cayley-Dickson construction and rank two elements. Throughout this subsection, F is the ground field, and C is an associative composition F -algebra. In this subsection, we use the Cayley-Dickson construction to lift rank two elements of $H_3(C)$ to rank one elements of $H_3(D)$, and rank two elements of $W_{H_3(C)}$ to rank one elements of $W_{H_3(D)}$. Here $D = C \oplus C$ is a composition algebra obtained from C by the Cayley-Dickson construction.

Before stating the results, we recall the Cayley-Dickson construction. Suppose C is an associative composition algebra over F , and $\gamma \in \mathrm{GL}_1(F) = F^\times$. Define $D = C(\gamma)$ to be C^2 with addition defined component-wise and multiplication given by

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 + \gamma y_2^*y_1, y_2x_1 + y_1x_2^*).$$

The conjugation $*$ on $C(\gamma)$ is $(x, y)^* = (x^*, -y)$ and the norm is $n((x, y)) = n(x) - \gamma n(y)$. With these definitions, D is a composition F -algebra.

8.1.1. *Rank two elements of $H_3(C)$.* Denote by V_3 the vector space F^3 , considered as row-vectors, i.e., the defining (right) representation of GL_3 . For $\gamma \in F^\times$, define $U(\gamma) = H_3(C) \oplus V_3(C)$, with norm, adjoint, and pairing given as follows: If $X \in H_3(C)$ and $v \in V_3(C)$ a row vector, then

- (1) $n((X, v)) = n(X) + \gamma v X v^*$;
- (2) $(X, v)^\# = (X^\# + \gamma v^* v, -vX)$;
- (3) $\langle (X, v), (Y, w) \rangle = (X, Y) - \gamma(v, w)$ where $(v, w) = vw^* + wv^* = (v_1, w_1) + (v_2, w_2) + (v_3, w_3)$.

Via these definitions, $U(\gamma)$ becomes a cubic norm structure. In fact, $U(\gamma) \simeq H_3(C(\gamma))$, where $C(\gamma)$ is the composition algebra formed from C via the Cayley-Dickson construction.

To see that $U(\gamma) \simeq H_3(C(\gamma))$, define an F -linear map $\phi : U(\gamma) \rightarrow H_3(C(\gamma))$ via

$$\phi((X, v)) = \begin{pmatrix} c_1 & a_3 & a_2^* \\ a_3^* & c_2 & a_1 \\ a_2 & a_1^* & c_3 \end{pmatrix}$$

where $c_i = X_{ii}$ and $a_i = (a_i(X), v_i) = (X_{i+1, i+2}, v_i)$. Here the indices are taken modulo 3.

Lemma 8.1.1. *The map ϕ is an isomorphism of cubic norm structures. In particular, $U(\gamma)$ is a cubic norm structure.*

Proof. The proof is a straightforward computation. We remark that it also is easy to verify directly that $U(\gamma)$ is a cubic norm structure. \square

Here is the first lower-rank lifting law.

Theorem 8.1.2. *Suppose $X \in H_3(C)$, and there exists $\gamma \in F^\times$ and $v \in V_3(C)$ so that (X, v) is rank one in $U(\gamma)$. Then, $n(X) = 0$, so that X has rank at most 2. If X has rank exactly two, then (X, v) is rank one in $U(\gamma)$ if and only if $X^\# = -\gamma v^* v$, and given $X \in H_3(C)$ of rank two, the set of such $\gamma \in F^\times$ and $v \in V_3(C)$ so that $X = -\gamma v^* v$ is non-empty. Finally, the class of $\gamma \in F^\times / n(C^\times)$ is uniquely determined.*

Proof. Suppose one has $\gamma \in F^\times$ and $v \in V_3(C)$ so that (X, v) is rank one in $U(\gamma)$. Then $X^\# = -\gamma v^* v$, and $Xv = 0$. Since $X^\#$ is then rank one, we conclude $n(X) = 0$.

Now suppose X has rank exactly two. Then $X^\#$ has rank one, and thus we know from Lemma 6.2.1 that there exists a $v \in V_3(C)$ and a gamma in F^\times so that $-X^\# = \gamma v^* v$, and that furthermore this γ is uniquely determined in $F^\times / n(C^\times)$.

We shall require the following lemma.

Lemma 8.1.3. *Suppose $Y \in H_3(C)$, $Y \neq 0$, and $Y = \gamma w^* w$ for some $\gamma \in F^\times$ and $w \in V_3(C)$. Then w is primitive.*

Proof. By $\mathrm{GL}_3(C)$ -equivariance, we may assume

$$Y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Write $w = (w_1, w_2, w_3)$. Then from the equation $Y = \gamma w^* w$, we deduce $n(w_1) \in F^\times$, and hence w is primitive. \square

Now suppose $X^\# = -\gamma v^* v$. By the lemma, v is primitive. But we get

$$0 = n(X) = X^\# X = -\gamma v^*(vX).$$

Since v is primitive, $v^*(vX) = 0$ implies $vX = 0$. Hence $vX = 0$, and so $(X, v)^\# = 0$. This completes the proof. \square

8.1.2. *Rank two elements of $W_{H_3(C)}$.* In this subsection we consider the lifting of rank two elements of $W_{H_3(C)}$ to rank one elements of $W_{H_3(C(\gamma))} = W_{U(\gamma)}$, with notation as in the previous subsection. Before giving the lifting law, we make a definition. If $x = (a, b, c, d) \in W_{H_3(C)}$, then we define

$$S(x) = \begin{pmatrix} b^\# - ac & ad - cb - \text{tr}(ad - cb)/2 \\ ad - bc - \text{tr}(ad - bc)/2 & c^\# - bd \end{pmatrix}.$$

Here the products bc and cb are taken in $M_3(C) \supseteq H_3(C)$. Thus, $S(x)$ is an element of $M_6(C)$. This is an identical definition to that given in (9), but we restate it since $H_3(C)$ is not an associative algebra.

Denote by $W_6 = V_3 \oplus V_3$ the defining right representation of GSp_6 on row vectors, and $W_6(C) = W_6 \otimes C$. Put on $W_6(C)$ the C -valued symplectic-Hermitian form $\langle u, u' \rangle_C = uJ_6(u')^*$, where $J_6 = \begin{pmatrix} & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ -13 & & & & & \end{pmatrix}$. Thus if $v, w, v', w' \in V_3(C)$, $u = (v, w)$ and $u' = (v', w')$, then $\langle u, u' \rangle_C = v(w')^* - w(v')^* \in C$.

For $\gamma \in F^\times$, we make an identification $W_{H_3(C)} \oplus W_6(C) \simeq W_{U(\gamma)}$ via

$$(a, b, c, d) + (v, w) \mapsto (a, (b, -v), (c, w), d).$$

Here $v, w \in V_3(C)$. We have the following lifting law.

Theorem 8.1.4. *Suppose $x = (a, b, c, d) \in W_{H_3(C)}$. If there exists $\gamma \in F^\times$ and $u = (v, w) \in W_6(C)$ so that $x + u$ is rank one in $W_{U(\gamma)}$, then $x^\flat = 0$, so that x has rank at most 2. For $\gamma \in F^\times$, define the set $\text{Lift}(x, \gamma)$ as*

$$\text{Lift}(x, \gamma) := \{u \in W_6(C) : \langle u, u \rangle_C = 0, -S(x) = \gamma u^* u\}.$$

For $x \in W_{H_3(C)}$ of rank exactly two, one has $x + u$ is rank one in $W_{U(\gamma)}$ if and only if $u \in \text{Lift}(x, \gamma)$. Furthermore, given x of rank two, there exists $\gamma \in F^\times$ so that $\text{Lift}(x, \gamma)$ is non-empty, and the class of such γ is uniquely determined in $F^\times / n(C^\times)$.

To prove this result, we will use the following proposition. Define $\text{GU}_6(C) = \{g \in \text{GL}_6(C) : gJ_6g^* = \nu(g)J_6\}$, i.e., the group preserving the symplectic-Hermitian form $\langle \cdot, \cdot \rangle_C$ up to similitude. Consider the group $H(W_{H_3(C)}) \times \text{GU}_6(C)$. This group acts on $W_{U(\gamma)} = W_{H_3(C)} \oplus W_6(C)$ by letting $H(W_{H_3(C)})$ act on $W_{H_3(C)}$ and $\text{GU}_6(C)$ on $W_6(C)$; we use right actions for both of these groups. Define the group $G(\gamma, C)$ to be the subgroup of $(h, g) \in H(W_{H_3(C)}) \times \text{GU}_6(C)$ with $\nu(h) = \nu(g)$ and such that (h, g) preserves the symplectic and quartic form on $W_{U(\gamma)}$ up to this common similitude. Thus, $G(\gamma, C)$ maps to $H(W_{U(\gamma)})$ by definition.

Proposition 8.1.5. *Denote by \overline{F} an algebraic closure of F . The projections $G(\gamma, C) \rightarrow H(W_{H_3(C)})$ and $G(\gamma, C) \rightarrow \text{GU}_6(C)$ are surjections on \overline{F} -points, whose kernels are $1 \times \mu_2 \subseteq H(W_{H_3(C)}) \times \text{GU}_6(C)$ and $\mu_2 \times 1 \subseteq H(W_{H_3(C)}) \times \text{GU}_6(C)$, respectively. Furthermore, if $(h, g) \in G(\gamma, C)$, then $S(xh) = g^*S(x)g$ for all $x \in W_{H_3(C)}$.*

Proof. This proposition was essentially proved in [Pol17, Appendix A]. More specifically, when C is a quaternion algebra, all but the last statement was proved in *loc. cit.* For a general associative composition algebra, the surjectivity and kernel statements are proved identically. We take this opportunity, however, to correct a typo in [Pol17]: In equation (A.4) of *loc. cit.*, the term $\text{tr}(b \times B, c \times C)$ should be multiplied by 2. I.e., (A.4) should read

$$\text{tr}(B, C)(ad - (b, c)) + 2 \text{tr}(b \times B, c \times C) + 2 \text{tr}(B^\#, c^\# - bd) + 2 \text{tr}(C^\#, b^\# - ac).$$

(This has no affect on the arguments of [Pol17, Appendix A].)

The claim $S(xh) = g^*S(x)g$ is essentially the content of Proposition 4.4.3 or Lemma 4.4.13, but we state it again because we are now working in the context of the special cubic norm structure $H_3(C)$ instead of an associative cubic norm structure A , as was the case in Proposition 4.4.3 and Lemma 4.4.13. For the claim that $S(xh) = g^*S(x)g$, it suffices to prove this over the algebraic

closure. To do so, one first checks this claim directly for the elements called $n_\Theta(X)$, J_Θ , $m_\Theta(\lambda)$, $z_\Theta(\lambda)$ and $(M(m, \delta), ({}^m *_{m-1}))$ on page 1428 of *loc. cit.*. Assuming this for the moment, then for a general $(h, g) \in G(\gamma, C)$, the equivariance $S(xh) = g^*S(x)g$ follows from the same fact for these specific elements, plus the statement about μ_2 -kernels.

Checking that $S(xh) = g^*S(x)g$ for the elements J_Θ , $m_\Theta(\lambda)$, $z_\Theta(\lambda)$ and $(M(m, \delta), ({}^m *_{m-1}))$ is immediate from their definitions. The only nontrivial check that must be performed is for the element $n_\Theta(X)$. To do so, one must verify the following two identities. Define (a', b', c', d') via

$$(a', b', c', d') = (a, b + aX, c + b \times X + aX^\#, d + (c, X) + (b, X^\#) + an(X)).$$

Then we must check

$$(28) \quad a'd' - b'c' - \text{tr}(a'd' - b'c')/2 = ad - bc - \text{tr}(ad - bc)/2 + X(b^\# - ac)$$

and

$$(29) \quad (c')^\# - d'b' = c^\# - db + X(ad - cb - \text{tr}(ad - cb)/2) + (ad - bc - \text{tr}(ad - bc)/2)X + X(b^\# - ac)X.$$

The proof of (28) reduces to the identity $(b, X^\#) = bX^\# + X(X \times b)$, valid in special cubic norm structures. The proof of (29) follows from $c \times (b \times X) = (c, X)b + (c, b)X - (bcX + Xcb)$, again valid in special cubic norm structures, and other similar identities. \square

Proof of Theorem 8.1.4. By proposition 8.1.5, we may assume $x = (1, 0, c, d)$. With x in this form, we find $x + u = (1, (0, -v), (c, w), d)$, and this is rank one if and only if

$$(c, w) = (0, -v)^\# = (\gamma v^*v, 0)$$

and $d = n((0, -v)) = 0$. Hence $c^\# = 0$, and $d = 0$, and thus

$$(30) \quad x^\flat = (-d, 2c^\#, dc, d^2 + 2n(c)) = 0.$$

Thus if x has a rank one lift for some γ , then x has rank at most 2.

Now suppose x has rank exactly two. Then by (30), we get $d = 0$, $c^\# = 0$, and thus $S(x) = \begin{pmatrix} -c & -d/2 \\ -d/2 & c^\# \end{pmatrix} = \begin{pmatrix} -c & 0 \\ 0 & 0 \end{pmatrix}$. Furthermore, for $u = (v, w)$, we see that $x + u$ is rank one in $W_{U(\gamma)}$ if and only if $c = \gamma v^*v$ and $w = 0$. In particular $u \in \text{Lift}(x, \gamma)$. Since $c^\# = 0$, there exists $\gamma \in F^\times$ and $v \in V_3(C)$ so that $c = \gamma v^*v$, and hence for this γ , $\text{Lift}(x, \gamma)$ is non-empty. Conversely, suppose $u = (v, w) \in \text{Lift}(x, \gamma)$. Then since $S(x) = -\gamma u^*u$, $c = \gamma v^*v$ and $v^*w = 0$. Since x has rank exactly two, $c \neq 0$. Thus by Lemma 8.1.3, v is primitive and hence since $v^*w = 0$, $w = 0$. Hence $u \in \text{Lift}(x, \gamma)$ implies $x + u$ is rank one in $W_{U(\gamma)}$.

Finally, we must check that for x of rank two, γ is uniquely determined in $F^\times/n(C^\times)$. Thus suppose $x + u_1$ is rank one in $W_{U(\gamma_1)}$, and $x + u_2$ is rank one in $W_{U(\gamma_2)}$. Then $\gamma_1 u_1^* u_1 = -S(x) = \gamma_2 u_2^* u_2$. By multiplying these quantities by u on the left and u^* on the right, one obtains $\gamma_1 n(u_1 u^*) = \gamma_2 n(u_2 u^*)$ for all $u \in W_6(C)$. Since u can be chosen so that $n(u_1 u^*) \neq 0$ (as follows from equivariance and the calculation of the previous paragraph), we deduce that γ_1 and γ_2 represent the same class in $F^\times/n(C^\times)$. This completes the proof. \square

8.2. Rank three elements of W_J and the Tits construction. In this subsection we assume J, B and K are as in section 7. That is, suppose K is a quadratic étale extension of F , B is a cubic associative algebra over K with an involution of the second kind $*$ compatible with the cubic norm, and $J = B^{*=1}$. See the very beginning of section 7 for details. Given $h \in J$ of rank three, a special case of the second construction of Tits can be used to make $U(h) = J \oplus B$ into a cubic norm structure. In this subsection, we discuss how this construction can be used to lift rank 3 elements of W_J to rank one elements of $W_{U(h)}$.

First, let us recall this construction of Tits, in a somewhat special case. See subsection 7.1 for the general construction. One defines a norm, adjoint, and pairing on $U(h) = J \oplus B$ as follows: For $X, Y \in J$ and $\alpha, \beta \in B$,

- $n((X, \alpha)) = n(X) - (X, \alpha h^\# \alpha^*) + n(h) \operatorname{tr}_{K/F}(n(\alpha))$
- $((X, \alpha))^\# = (X^\# - \alpha h^\# \alpha^*, -X\alpha + (\alpha^*)^\# h)$
- $((X, \alpha), (Y, \beta)) = (X, Y) + \operatorname{tr}_J(\alpha h^\# \beta^* + \beta h^\# \alpha^*)$.

It is a fact that these formulas make $U(h)$ into a cubic norm structure⁷. In the notation of subsection 7.1, this is the special case where $(S, \lambda) = (h^\#, n(h))$.

Now, recall the group $G \subseteq \operatorname{GU}_2(B)$ from subsection 7.2. Namely, G is the subgroup of $\operatorname{GL}_2(B)$ for which $g^* \begin{pmatrix} & 1 \\ -1 & \end{pmatrix} g = \nu(g) \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$ and $\det_6(g) = \nu(g)^3$. The group G acts on the left of W_J by the ν^{-1} -twist of the restriction of the cubic polynomial action of $\operatorname{GL}_2(B)$ on W_B ; see subsection 7.2. Denote by $W_2(B) = B^2$ the 2×1 column vectors with coefficients in B . Then we identify $W_J \oplus W_2(B)$ with $W_{U(h)}$ via $x + \eta \mapsto (a, (b, -u), (c, v), d)$, where $x = (a, b, c, d)$ and $\eta = \begin{pmatrix} u \\ v \end{pmatrix}$.

Via this identification, G acts on the left of $W_{U(h)}$, and in fact one obtains a map $G \rightarrow H(W_{U(h)})$. That is, G preserves the symplectic and quartic form on $W_{U(h)}$, up to similitude. This fact was stated in Proposition 7.2.2.

Recall that we have a B -valued symplectic-Hermitian form on $W_2(B)$ defined by $\langle \eta, \eta' \rangle_B = \eta^* J_2 \eta'$, where $J_2 = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$. A vector $\eta \in W_2(B)$ is said to be *isotropic* if $\langle \eta, \eta \rangle_B = 0$. Here is the lifting law.

Theorem 8.2.1. *Suppose $x = (a, b, c, d) \in W_J$. If there exists a rank 3 h in J and an isotropic $\eta = \begin{pmatrix} u \\ v \end{pmatrix}$ in $W_2(B)$ with $x + \eta$ rank one in $W_{U(h)}$, then $q(x) = 0$, so that x has rank at most 3. Given $x \in W_J$, and $h \in J$ of rank 3, define*

$$\operatorname{Lift}(x, h) = \{ \eta \in W_2(B) : \langle \eta, \eta \rangle_B = 0, S(x) = \eta h^\# \eta^*, \frac{x^b}{2} = n(h) \eta^1 \}.$$

Suppose x has rank 3. Then if $\eta \in W_2(B)$ is isotropic, $x + \eta$ is rank one in $W_{U(h)}$ if and only if $\eta \in \operatorname{Lift}(x, h)$. Furthermore, for x of rank 3, there exists $h \in J$ with $n(h) \neq 0$ so that $\operatorname{Lift}(x, h)$ is non-empty.

Proof. Suppose $x + \eta$ is rank one in $W_{U(h)}$ for some isotropic η . Applying Lemma 4.4.13, one sees that the conditions defining $\operatorname{Lift}(x, h)$ are equivariant for the action of G . Thus by this equivariance, we may assume $x = (1, 0, c, d)$, so $x + \eta = (1, (0, -u), (c, v), d)$. Since this is rank one, $(c, v) = (0, -u)^\# = (-uh^\# u^*, (u^*)^\# h)$ and $d = n((0, -u)) = -n(h) \operatorname{tr}_{K/F}(n(u))$. Since η is isotropic, $u^* v = n(u)^* h$ is Hermitian, and thus $n(u) = n(u)^*$, so $d = -2n(h)n(u)$. Hence

$$q(x) = d^2 + 4n(c) = (-2n(h)n(u))^2 + 4n(-uh^\# u^*) = 0$$

since $n(u) = n(u)^*$. Thus x has rank at most 3.

Suppose now that x has rank exactly 3. To check that $x + \eta$ is rank one in $W_{U(h)}$ for an isotropic η if and only if $\eta \in \operatorname{Lift}(x, h)$, by equivariance for the action of G , it suffices to consider the case $x = (1, 0, c, d)$. Then recall that $x^b = (-d, 2c^\#, dc, d^2 + 2n(c))$ and $S(x) = \begin{pmatrix} -c & -d/2 \\ -d/2 & c^\# \end{pmatrix}$. Then as above, if η is isotropic, $x + \eta = (1, (0, -u), (c, v), d)$ is rank one if and only if $n(u) \in F$, $(c, v) = (-uh^\# u^*, (u^*)^\# h)$, and $d = -2n(u)n(h)$.

We check that these conditions are equivalent to η being in $\operatorname{Lift}(x, h)$. First suppose η isotropic and $x + \eta$ is rank one. Then $-d/2 = n(h)n(u)$,

$$c^\# = (-uh^\# u^*)^\# = n(h)(u^*)^\# hu^\# = n(h)vu^\#,$$

$$dc/2 = -n(h)n(u)(-uh^\# (u^*)^\#) = n(h)u(n(u)h^\# (u^*)^\#) = n(h)uv^\#,$$

⁷One can even consider this construction itself as a lifting law. We leave the formulation of such a lifting law to the interested reader.

and

$$d^2/2 + n(c) = 2n(h)^2n(u)^2 - n(u)^2n(h)^2 = n(h)n(u^2)n(h) = n(h)n(v).$$

Thus $x^b/2 = n(h)\eta^!$. Furthermore

$$\begin{aligned} \eta h^\# \eta^* &= \begin{pmatrix} u \\ v \end{pmatrix} h^\# \begin{pmatrix} u^* & v^* \end{pmatrix} = \begin{pmatrix} uh^\#u^* & uh^\#v^* \\ vh^\#u^* & vh^\#v^* \end{pmatrix} \\ &= \begin{pmatrix} uh^\#u^* & n(h)n(u) \\ n(h)n(u) & n(h)(u^*)^\#hu^\# \end{pmatrix} = \begin{pmatrix} -c & -d/2 \\ -d/2 & c^\# \end{pmatrix} \\ &= S(x). \end{aligned}$$

Conversely, suppose x is rank 3, $n(h) \neq 0$, and $\eta \in \text{Lift}(x, h)$. Then immediately $c = -uh^\#u^*$ and $d = -2n(h)n(u)$, and hence $n(u) \in F$, and thus $d = n(h)\text{tr}_{K/F}(-n(u))$. We wish to show $v = (u^*)^\#h$. If $d \neq 0$, this is easy. For the general case, however, we argue as follows. One has

$$(v - (u^*)^\#h)h^\#u^* = vh^\#u^* - n(h)n(u) = (-d/2) - (-d/2) = 0$$

and

$$(v - (u^*)^\#h)h^\#v^* = vh^\#v^* - n(h)(vu^\#)^* = c^\# - c^\# = 0.$$

Hence $(v - (u^*)^\#h)h^\#\eta^* = 0$.

Now, since x has rank exactly 3, $n(h)\eta^! = x^b/2 \neq 0$. Hence η is primitive, and so $(v - (u^*)^\#h)h^\#\eta^* = 0$ implies $(v - (u^*)^\#h)h^\# = 0$, and thus $v = (u^*)^\#h$, since $n(h) \neq 0$.

Finally, it follows from equivariance and Lemma 8.2.2 below that there exists $h \in J$ of rank three for which $\text{Lift}(x, h)$ is non-empty. This completes the proof. \square

Lemma 8.2.2. *Given $x = (1, 0, c, d)$ in W_J of rank three, there exists $h \in J$ with $n(h) \neq 0$ and $u, v \in B$ so that $(1, (0, -u), (c, v), d) \in W_{U(h)}$ is rank one. Furthermore, the element $\eta = (u, v)$ of $W_2(B)$ can be chosen to be isotropic.*

Proof. Since x is rank three, $q(x) = d^2 + 4n(c) = 0$. We break the proof up into two cases, according as to whether $d = 0$ or not.

Suppose first that $d \neq 0$. It follows that $n(c) \neq 0$. In this case, set $h = -2d^{-1}c^\#$, $u = 1$ and $v = h$. Then $(0, -1)^\# = (-h^\#, h) = (-(2/d)^2n(c)c, v) = (c, v)$ and $n((0, -1)) = -2n(h) = 2(2/d)^3n(c)^2 = d$. Thus, $x + \eta = (1, (0, -1), (c, v), d)$ is rank one in $W_{U(h)}$. It is clear that $\eta = (1, h)$ is isotropic, and thus this completes the proof of the lemma when $d \neq 0$.

Now suppose that $d = 0$. Then $n(c) = 0$, but $c^\# \neq 0$ since $x^b = (-d, 2c^\#, dc, d^2 + 2n(c)) \neq 0$ by assumption. Hence c is rank two, and $c^\#$ is rank one. We claim that we may reduce to the case that $\text{tr}(c^\#) \neq 0$. Suppose for now that c is such that $\text{tr}(c^\#) \neq 0$. Set $S = c - c^\#$. Note that $n(S) = -\text{tr}((c^\#)^2) = -\text{tr}(c^\#)^2$, since $c^\#$ is rank one. Furthermore, if $u = 1 - \frac{c^\#}{\text{tr}(c^\#)}$, then

$$uSu = \left(1 - \frac{c^\#}{\text{tr}(c^\#)}\right) (c - c^\#) \left(1 - \frac{c^\#}{\text{tr}(c^\#)}\right) = c \left(1 - \frac{c^\#}{\text{tr}(c^\#)}\right) = c,$$

where we have used the identity $(c^\#)^2 = \text{tr}(c^\#)c^\#$, since $c^\#$ is rank one. Now, set $h = (\text{tr}(c^\#))^{-1}S^\#$ and $v = (u^*)^\#h$. Since $n(u) \in F$ (in fact, $n(u) = 0$), $u^*v = n(u)h$ is in J , and thus $\eta = (u, v)$ is isotropic. Furthermore, $-h^\# = S$ and thus $-uh^\#u^* = -uh^\#u = c$. Since $n(u) = 0$, it now follows that $x + \eta = (1, (0, -u), (c, v), 0)$ is rank one in $W_{U(h)}$. This completes the proof of the lemma in case $n(c) = 0$ but $\text{tr}(c^\#) \neq 0$.

Finally, we explain the reduction to the case $\text{tr}(c^\#) \neq 0$. This follows by equivariance for the action of the group G . Indeed, if $y \in J$ with $n(y) \neq 0$, then the element $m = \begin{pmatrix} y^{-1} & \\ & y \end{pmatrix}$ of $\text{GL}_2(B)$ is in G , and $mx = (n(y)^{-1}, 0, y^{-1}cy^\#, 0)$. Furthermore, $\text{tr}((y^{-1}cy^\#)^\#) = \text{tr}(yc^\#y) = (y^2, c^\#)$. Since $c^\# \neq 0$, it follows by a Zariski density argument that there exists $y \in J$ with $n(y) \neq 0$ and

$(y^2, c^\#) \neq 0$. Scaling mx by $n(y)$ gives an element $(1, 0, c', 0)$ in the G orbit of x with $\text{tr}((c')^\#) \neq 0$. This completes the proof of the lemma. \square

REFERENCES

- [BG14] Manjul Bhargava and Benedict H. Gross, *Arithmetic invariant theory*, Symmetry: representation theory and its applications, Progr. Math., vol. 257, Birkhäuser/Springer, New York, 2014, pp. 33–54. MR 3363006
- [BGW15] Manjul Bhargava, Benedict H. Gross, and Xiaoheng Wang, *Arithmetic invariant theory II: Pure inner forms and obstructions to the existence of orbits*, Representations of reductive groups, Progr. Math., vol. 312, Birkhäuser/Springer, Cham, 2015, pp. 139–171. MR 3495795
- [BH16] Manjul Bhargava and Wei Ho, *Coregular spaces and genus one curves*, Camb. J. Math. **4** (2016), no. 1, 1–119.
- [Bha04a] Manjul Bhargava, *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.
- [Bha08] ———, *Higher composition laws. IV. The parametrization of quintic rings*, Ann. of Math. (2) **167** (2008), no. 1, 53–94.
- [BHK16] Manjul Bhargava, Wei Ho, and Abhinav Kumar, *Orbit parametrizations for K3 surfaces*, Forum Math. Sigma **4** (2016), e18, 86. MR 3519436
- [DF64] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, Translations of Mathematical Monographs, Vol. 10, American Mathematical Society, Providence, R.I., 1964.
- [Gan00a] Wee Teck Gan, *An automorphic theta module for quaternionic exceptional groups*, Canad. J. Math. **52** (2000), no. 4, 737–756.
- [Gan00b] ———, *A Siegel-Weil formula for exceptional groups*, J. Reine Angew. Math. **528** (2000), 149–181.
- [Gan08] ———, *A Siegel-Weil formula for automorphic characters: cubic variation of a theme of Snitz*, J. Reine Angew. Math. **625** (2008), 155–185.
- [GGJ02] Wee Teck Gan, Nadya Gurevich, and Dihua Jiang, *Cubic unipotent Arthur parameters and multiplicities of square integrable automorphic forms*, Invent. Math. **149** (2002), no. 2, 225–265.
- [GGS02] Wee Teck Gan, Benedict Gross, and Gordan Savin, *Fourier coefficients of modular forms on G_2* , Duke Math. J. **115** (2002), no. 1, 105–169.
- [GL09] Benedict H. Gross and Mark W. Lucianovic, *On cubic rings and quaternion rings*, J. Number Theory **129** (2009), no. 6, 1468–1478. MR 2521487
- [GS98] Benedict H. Gross and Gordan Savin, *Motives with Galois group of type G_2 : an exceptional theta-correspondence*, Compositio Math. **114** (1998), no. 2, 153–217.
- [GS05] Wee Teck Gan and Gordan Savin, *On minimal representations definitions and properties*, Represent. Theory **9** (2005), 46–93 (electronic).
- [GS14] ———, *Twisted Bhargava cubes*, Algebra Number Theory **8** (2014), no. 8, 1913–1957.
- [HMS98] Jing-Song Huang, Kay Magaard, and Gordan Savin, *Unipotent representations of G_2 arising from the minimal representation of D_4^E* , J. Reine Angew. Math. **500** (1998), 65–81.
- [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.
- [KY97] Anthony C. Kable and Akihiko Yukie, *Prehomogeneous vector spaces and field extensions. II*, Invent. Math. **130** (1997), no. 2, 315–344.
- [KY16] R. Kato and A. Yukie, *Rational orbits of the space of pairs of exceptional Jordan algebras*, ArXiv e-prints (2016).
- [Luc03] Mark William Lucianovic, *Quaternion rings, ternary quadratic forms, and Fourier coefficients of modular forms on $PGSp(6)$* , ProQuest LLC, Ann Arbor, MI, 2003, Thesis (Ph.D.)—Harvard University.
- [McC04] Kevin McCrimmon, *A taste of Jordan algebras*, Universitext, Springer-Verlag, New York, 2004.
- [Pol17] Aaron Pollack, *The spin L -function on GSp_6 for Siegel modular forms*, Compositio Mathematica **153** (2017), no. 7, 1391–1432.
- [PR86] Holger P. Petersson and Michel L. Racine, *Classification of algebras arising from the Tits process*, J. Algebra **98** (1986), no. 1, 244–279.
- [Spr06] T. A. Springer, *Some groups of type E_7* , Nagoya Math. J. **182** (2006), 259–284.

- [SV00] Tonny A. Springer and Ferdinand D. Veldkamp, *Octonions, Jordan algebras and exceptional groups*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000.
- [Tan08] Takashi Taniguchi, *On parameterizations of rational orbits of some forms of prehomogeneous vector spaces*, Manuscripta Math. **125** (2008), no. 2, 169–190.
- [Tan16] Wei Kiat Douglas Tan, *Orbits of twisted bhargava boxes*.
- [Tho13] Jack A. Thorne, *Vinberg’s representations and arithmetic invariant theory*, Algebra Number Theory **7** (2013), no. 9, 2331–2368. MR 3152016
- [Voi11] John Voight, *Characterizing quaternion rings over an arbitrary base*, J. Reine Angew. Math. **657** (2011), 113–134.
- [Wei06] Martin H. Weissman, *D_4 modular forms*, Amer. J. Math. **128** (2006), no. 4, 849–898.
- [Woo11] Melanie Matchett Wood, *Parametrizing quartic algebras over an arbitrary base*, Algebra Number Theory **5** (2011), no. 8, 1069–1094. MR 2948473
- [Woo14] ———, *Parametrization of ideal classes in rings associated to binary forms*, J. Reine Angew. Math. **689** (2014), 169–199.
- [WY92] David J. Wright and Akihiko Yukie, *Prehomogeneous vector spaces and field extensions*, Invent. Math. **110** (1992), no. 2, 283–314.

DEPARTMENT OF MATHEMATICS, INSTITUTE FOR ADVANCED STUDY, PRINCETON, NJ USA
E-mail address: aaronjp@math.ias.edu