Automorphism-invariant Integral Forms in Griess Algebras

by

Gregory G. Simon

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)
in the University of Michigan
2016

Doctoral Committee:

Professor Robert L. Griess, Jr., Chair
Professor Jonathon I. Hall, Michigan State University
Professor John R. Stembridge
Professor James D. Wells
Professor Michael E. Zieve

DEDICATION

Dedicated to my family, especially my wife and the family I gained through her, my mother, my father, my stepmother, my grandmothers, and my sisters. Your love and support were and are invaluable and irreplaceable.

ACKNOWLEDGMENTS

I want to first and foremost thank my advisor, Dr. Robert Griess, for his suggesting the main problem solved in this dissertation and for innumerable suggestions and ideas given throughout. This dissertation benefited also from the supportive atmosphere at the University of Michigan by both professors and fellow students. I want to thank Gabriel Frieden for suggesting Gauss' Lemma, which turned out to be very powerful and helpful. I also want to thank Dr. Karen Smith for her advice and support.

TABLE OF CONTENTS

LIST OF APPENDICES

ABSTRACT

Automorphism-invariant Integral Forms in Griess Algebras

by

Gregory G. Simon

Chair: Robert L. Griess, Jr.

Motivated by the existence of group-invariant integral forms in various vertex operator algebras, we classify maximal automorphism-invariant integral forms in some small-dimensional Griess algebras, which are certain finite-dimensional commutative, nonassociative algebras arising in the theory of vertex operator algebras. An integral form of a rational algebra is the integer span of a basis of the algebra that is closed under the algebra product. The main method is the development of "integral form detector functions" and an investigation of their properties. Each of the small Griess algebras we analyzed – the eight Norton-Sakuma algebras and three others – have unique maximal automorphism-invariant integral forms. This provides a canonically defined lattice and subring inside these algebras.

CHAPTER 1

Introduction

1.1 Motivation and background

In 1982, Robert L. Griess, Jr., provided the first construction of the monster simple group $\mathbb{M}$ as a group of automorphisms of a 196884-dimensional commutative nonassociative algebra $\mathcal{B}$ [Gri82]. In subsequent years, this construction was simplified and analyzed in a number of papers, including several by Jacques Tits [Tit83a, Tit83b, Tit84, Tit85] and by John H. Conway [Con85]. In particular, Conway discovered an association between a distinguished set of idempotents (called axes) in $\mathcal{B}$ and a conjugacy class of involutions in $\mathbb{M}$ (called the 2A conjugacy class, or called the set of τ-involutions of $\mathcal{B}$). Simon Norton [Nor96] studied the subalgebras in $\mathcal{B}$ generated by two axes, and he was the first to state many facts about these algebras. He stated that the isomorphism type of the algebra generated by two axes only depended on the conjugacy class in $\mathbb{M}$ of the product of the associated involutions. He gave eight such algebras, labeled by the name of the relevent conjugacy class:

$$2A,\ 2B,\ 3A,\ 3C,\ 4A,\ 4B,\ 5A,\ \text{and } 6A.$$

He worked out the structure coefficients in each algebra.

In 1988, Frenkel, Lepowsky, and Meurman [FLM88] showed that $\mathcal{B}$ was the degree two piece of an infinite-dimensional graded representation of $\mathbb{M}$ called the moonshine module, denoted $V^\natural = \bigoplus_{n=0}^{\infty} V_n^\natural$, which has the structure of a vertex operator algebra (VOA). The moonshine module was used by Borcherds to resolve the moonshine conjectures – which were a family of conjectures relating the representation theory of $\mathbb{M}$ and modular forms. For certain vertex operator algebras (for those V with $\dim V_0 = 1$ and $\dim V_1 = 0$), the degree two piece V_2 will inherit the structure of a commutative nonassociative algebra, and this is known as a *(generalized) Griess algebra*. The adjective *generalized* is included to emphasize the distinction between the degree two piece of some general VOA with the original Griess algebra, the original 196884-dimensional algebra and the degree two piece of the moonshine module. It was shown by Miyamoto [Miy96] that the link between axes in $\mathcal{B}$ and involutions in $\mathbb{M}$ could be understood in the more general context of VOAs as a link between involutive automorphisms of the vertex operator algebra and distinguished idempotents in a generalized Griess algebra (or more precisely, Miyamoto considered 'rational conformal vectors with central charge 1/2' also known as 'Ising vectors' which correspond to two times these idempotents). In 2007, Sakuma [Sak07] showed that in any generalized Griess algebra for a suitably nice vertex operator algebra, there are only eight possibilities for the subalgebra generated by two distinct axes, and so the eight studied by Norton represent all possible isomorphism types of such algebras. These eight algebras are known as the *Norton-Sakuma algebras*.

Although often considered over fields of characteristic zero, the axioms defining vertex algebras involve only the integers and therefore make sense over any commutative ring [Bor86, Kac98, GL13]. In particular, there has been some recent progress studying integral forms in vertex algebras.

For an algebra (not necessarily associative) over a field of characteristic zero (meaning a vector space A with a bilinear map $A \times A \to A$), an integral form is defined to be the $\mathbb{Z}$-span of a basis of the algebra which is closed under the algebra product. For example, $\mathbb{Z}^n$ is an integral form in $\mathbb{R}^n$ and $\mathrm{Mat}_{n\times n}(\mathbb{Z})$ is an integral form in $\mathrm{Mat}_{n\times n}(\mathbb{C})$, both for any positive integer n. The definition for an integral form in a vertex algebra is analogous. There are at least two inequivalent definitions for integral forms (also called a $\mathbb{Z}$-forms) for a vertex algebra. In

[McR14], an integral form of a vertex algebra V is defined to be an additive subgroup $V_{\mathbb{Z}}$ of V such that $V_{\mathbb{Z}}$ is a vertex subalgebra (over $\mathbb{Z}$) of V and the map $k \otimes_{\mathbb{Z}} V_{\mathbb{Z}} \to V$ given by $\lambda \otimes v \mapsto \lambda v$ is a vector space isomorphism. In [DG12] and [GL13], an integral form is defined for a vertex operator algebra that invokes the grading and the Virasoro vector, which are not available in the vertex algebra setting. Of particular interest are integral forms of a vertex operator algebra V which are invariant under some subgroup G of $\mathrm{Aut}(V)$. For such an integral form $V_{\mathbb{Z}}$, we can form the vertex algebra $V_{\mathbb{Z}} \otimes_{\mathbb{Z}} k$ over any field k and produce an infinite sequence of representations of $k[G]$, given by the graded components of $V_{\mathbb{Z}} \otimes_{\mathbb{Z}} k$. In this way, we could potentially study moonshine-like phenomena over arbitrary fields. This also can increase our understanding of vertex (operator) algebras in general over arbitrary fields. When these integral forms of vertex operator algebras intersect with the generalized Griess algebra, the result is an integral form of this algebra in the classical sense. So in this document, we study the integral forms in several small generalized Griess algebras – in particular inside the Norton-Sakuma algebras. More precisely, we study the integral forms preserved by the action of G (called G-invariant integral forms, or *GIIF*s for short), where G is the subgroup of the automorphism group of the algebra generated by the distinguished involutions mentioned above.

So this sets forth the following goal: given a finite-dimensional algebra A (which is not necessarily associative) over a field k of characteristic zero, and a subgroup $G \subseteq \mathrm{Aut}(A)$, try to understand the integral forms of A which are preserved by the action of G.

1.2 Statement of the main result

Throughout this document, a *rng* is an abelian group R with a $\mathbb{Z}$-bilinear product $R \times R \to R$. A *ring* is a rng with an element 1_R that is both a left and right multiplicative identity element, and a *k-algebra* is ring that is a k-vector space and the algebra product is k-bilinear. In particular, none of these products are necessarily associative.

Let a be an element in an algebra V. For a scalar μ, define $V_\mu^{(a)} = \{v \in V \ : \ a \cdot v = \mu v\}$ to be the subspace of μ-eigenvectors of the adjoint action of a.

Definition 1.2.1. Let k be a field of characteristic zero, and V a commutative k-algebra. An element $a \in V$ is an *axis* if:

(i) $V_1^{(a)} = \mathrm{span}_k(a)$. In particular, $a \cdot a = a$.

(ii) The algebra decomposes as $V = V_1^{(a)} \oplus V_0^{(a)} \oplus V_{1/4}^{(a)} \oplus V_{1/32}^{(a)}$. In other words the map $\mathrm{ad}(a) : V \to V$ defined by $v \mapsto a \cdot v$ is diagonalizable with eigenvalues from the set $\{1, 0, 1/4, 1/32\}$.

(iii) The eigenspaces $V_\lambda^{(a)}$ satisfy the Virasoro fusion rules: $V_\lambda^{(a)} \cdot V_\mu^{(a)} \subseteq \sum\limits_{\nu \in \lambda \star \mu} V_\nu^{(a)}$ where $\star : \{0, 1, \frac{1}{4}, \frac{1}{32}\}^2 \to \mathscr{P}(\{0, 1, \frac{1}{4}, \frac{1}{32}\})$ is given by the table below.

$\star$	1	0	$\frac{1}{4}$	$\frac{1}{32}$
1	1	0	$\frac{1}{4}$	$\frac{1}{32}$
0	0	$1, 0$	$\frac{1}{4}$	$\frac{1}{32}$
$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$1, 0$	$\frac{1}{32}$
$\frac{1}{32}$	$\frac{1}{32}$	$\frac{1}{32}$	$\frac{1}{32}$	$1, 0, \frac{1}{4}$

Note that $\mathscr{P}(X)$ is the powerset of X.

The properties of axes in Griess algebras have been axiomatized and studied in several different ways. Our definition of axes is less restrictive than that in e.g. [Iva09] and [IPSS10], where existence of an associative bilinear form is also required. Our definition of axes coincides with the definition of $\mathfrak{V}(4, 3)$-axes given in [HRS15a] and [HRS15b].

One can see from this table that there is a $\mathbb{Z}/2\mathbb{Z}$-grading of V given by $V_+^{(a)} \stackrel{\text{def}}{=} V_1^{(a)} \oplus V_0^{(a)} \oplus V_{1/4}^{(a)}$ and $V_-^{(a)} \stackrel{\text{def}}{=} V_{1/32}^{(a)}$. A $\mathbb{Z}/2\mathbb{Z}$-grading of an algebra yields an involution of the algebra: if we define the linear map $\tau(a) : V \to V$ by

$$\tau(a) = \begin{cases} -\mathrm{Id} & \text{on } V^{(a)}_{1/32} \\ \mathrm{Id} & \text{on } V^{(a)}_{1} \oplus V^{(a)}_{0} \oplus V^{(a)}_{1/4} \end{cases}$$

Then $\tau(a)$ is an involutive automorphism of the algebra V, called the *τ-involution* associated to the axis a.

The fusion rules also show that the fixed point subalgebra of $\tau(a)$, $V^{\tau(a)} = V^{(a)}_{+}$, itself has a $\mathbb{Z}/2\mathbb{Z}$-grading given by $\left[V^{(a)}_{1} \oplus V^{(a)}_{0}\right] \oplus [V^{(a)}_{1/4}]$. Therefore we define $\sigma(a) : V^{(a)}_{+} \to V^{(a)}_{+}$ by

$$\sigma(a) = \begin{cases} -\mathrm{Id} & \text{on } V^{(a)}_{1/4} \\ \mathrm{Id} & \text{on } V^{(a)}_{1} \oplus V^{(a)}_{0} \end{cases}$$

Then $\sigma(a)$ is an involutive automorphism of $V^{(a)}_{+}$. These are properties (M4),(M6), and (M7) in [IPSS10]. When V is a subalgebra of a generalized Griess algebra of a vertex operator algebra, the automorphisms $\tau(a)$ and $\sigma(a)$ of V equal the τ- and σ-involutions defined by Miyamoto when restricted to V [Miy03, §2].

Definition 1.2.2. An integral form of an algebra V over a field k of characteristic zero is a subrng $L \subseteq V$ such that L is the $\mathbb{Z}$-span of a k-basis of V.

Definition 1.2.3. For an $\mathbb{F}$-algebra A with basis $\{b_i : i \in I\}$, the structure coefficients of A with respect to this basis are the scalars $\alpha_{i,j,k} \in \mathbb{F}$ (where $i, j, k \in I$) defined by $b_i \cdot b_j = \sum_{k \in I} \alpha_{i,j,k} b_k$.

If the structure coefficients of a basis are all integers, then the $\mathbb{Z}$-span of that basis is an integral form of the algebra.

If $\alpha_{i,j,k}$ are the structure coefficients of a basis $\{b_i : i \in I\}$, and c is in the field $\mathbb{F}$, then it follows from the previous definition that the structure coefficients of the basis $\{cb_i : \ i \in I\}$ are given by $c\alpha_{i,j,k}$. Thus if the structure coefficients are a basis are rational numbers, then some integer multiple of this basis spans an integral form of the algebra.

Definition 1.2.4. A G-invariant integral form (GIIF) of an algebra V is an integral form L of V such that L is closed under the action of $G = \langle \tau(a) : a \text{ an axis of V} \rangle$.

A GIIF L is maximal if it is not properly contained in any other GIIF.

By a discrete subgroup of a finite-dimensional rational vector space, we mean a subgroup that is discrete with respect to the unique topology making the vector space a Hausdorff topological $\mathbb{Q}$-vector space [Rud91, Theorem 1.21] . Equivalently, a discrete subgroup of a finite-dimensional rational vector space is the $\mathbb{Z}$-span of a finite set of vectors. Let W be a G-invariant discrete subgroup of a finite-dimensional $\mathbb{Q}$-algebra V with $\operatorname{rank}(W) = \dim V$. Let $\{w_i : i = 1, \ldots, \dim V\}$ be a $\mathbb{Z}$-basis of W. Then $\{w_i : i = 1, \ldots, \dim V\}$ is a $\mathbb{Q}$-linearly independent set so is also a $\mathbb{Q}$-basis of V. The structure coefficients of the algebra with respect to this basis will be rational numbers. By the discussion following Definition 1.2.3, nW will be an integral form of V for some integer n. By hypothesis, W is G-invariant, which implies that nW is G-invariant, so nW will be a GIIF of V. Therefore, a list all GIIFs of V would include an integer multiple of every G-invariant full-rank additive subgroup of V. The classification of all GIIFs of V is then a strictly harder problem than a classification of all discrete full-rank G-submodules of V.

However, we shall show that the list of *maximal* GIIFs for the Norton-Sakuma algebras is completely classifiable and similarly for several larger Griess algebras. There is a unique maximal GIIF in every Norton-Sakuma algebra except for $2A$, and in $2A$ there are three GIIFs but which are conjugate under other automorphisms. This gives a distinguished intrinsically-defined integral form inside each Norton-Sakuma algebra, which is the main result of this document:

Theorem 1.2.5. *Let V be one of the Norton-Sakuma algebras over $\mathbb{Q}$. Then there is a unique maximal $Aut(V)$-invariant integral form of V.*

Proof. This is proven case-by-case for each algebra. In Theorem 3.1.11, it is shown that there are exactly three maximal integral forms of the rational 2A Norton-Sakuma algebra, and they are conjugate under the action of the σ-automorphisms. The rational 2B algebra is isomorphic to $\mathbb{Q}^2$, so it has a unique maximal integral form, namely $\mathbb{Z}^2$ (3.1.4). There is a unique maximal GIIF in the rational Norton-Sakuma algebras of type 3C (Theorem 3.4.4), 3A (Theorem 3.3.13), 4A (Theorem 3.5.10), 4B (Theorem 3.6.8), 5A (Theorem 3.7.9), and 6A (Theorem 3.8.6).

It is an easy consequence of $G = \langle \tau(a) : \ a \text{ an axis.}\rangle$ being normal in $\mathrm{Aut}(V)$ that the set of GIIFs is invariant under the action of $\mathrm{Aut}(V)$ (Corollary 2.2.11). Therefore, if V has a unique maximal GIIF then this is also the unique maximal $\mathrm{Aut}(V)$-invariant integral form. □

In the later sections, we extend this result to several slightly larger algebras which are generated by three axes (compared to the Norton-Sakuma algebras which are generated by two axes).

Theorem 1.2.6. *Each of the following algebras has a unique maximal GIIF:*

(i) The algebra with $G \cong Sym(4)$ of shape (2B,3C), described in [IPSS10, §4.3],

(ii) The algebra with $G \cong Sym(4)$ of shape (2A,3C), described in [IPSS10, §4.4],

(iii) The 'Lam-Chen algebra' with $G \cong 3^2 : 2$, as described in [CL14].

Proof. These are proved separately, as Theorems 4.1.7, 4.2.10, and 4.3.13. □

It is unknown if every Griess algebra V has a unique maximal $\mathrm{Aut}(V)$-invariant integral form.

CHAPTER 2

General facts about integral forms

2.1 Integral form detector functions

Definition 2.1.1. For a in an finite dimensional algebra V, define $\mathrm{ad}(a)$ to be the linear function $V \to V$ given by $x \mapsto a \cdot x$.

For an endomorphism x of a finite dimensional vector space, define $\chi(x;\, t) = \det(x - tI)$ to be the characteristic polynomial of x. When it can cause no confusion, if a is in a finite dimensional algebra, $\chi(a;\, t)$ is understood to mean $\chi(\mathrm{ad}(a);\, t)$ i.e. the characteristic polynomial of $\mathrm{ad}(a)$. Similarly, $\mathrm{trace}(a) = \mathrm{Tr}(\mathrm{ad}(a))$ is the trace of $\mathrm{ad}(a)$.

It is clear that if a is in an integral form of an algebra V, then the matrix of $\mathrm{ad}(a)$ has integer coefficients, and therefore $\chi(a;\, t)$ will be in $\mathbb{Z}[t]$. Thinking of a as a variable, each coefficient of $\chi(a;\, t)$ is then a function $V \to \mathbb{Q}$ which takes integer values on elements in an integral form. This motivates the following definition:

Definition 2.1.2. Let W be a subspace of a $\mathbb{Q}$-algebra V. An *integral form detector function (IFDF)* on W in m variables is a function $f : W^m \to \mathbb{Q}$ such that if $w_1, w_2, \ldots, w_m$ are in an integral form of V, then $f(w_1, w_2, \ldots, w_m)$ is an integer.

For a fixed subspace W and a fixed m, the set of integral form detector functions on W in m variables form a ring. They are also closed under some more subtle operations: an IFDF in m variables can be made into one of $m + 1$ variables by multiplication: if $f : W^m \to \mathbb{Q}$ is an

IFDF, then so is the following function:

$$(w_1, w_2, \ldots, w_m, w_{m+1}) \mapsto f(w_1, w_2, \ldots, w_{m-1},\ w_m \cdot w_{m+1}).$$

The proof is immediate: if $w_1, \ldots, w_{m+1}$ are in an integral form, then $w_m \cdot w_{m+1}$ is also in this integral form and hence $f(w_1, \ldots, w_m \cdot w_{m+1}) \in \mathbb{Z}$. This could be formally described as precomposition of f with multiplication.

An IFDF in m variables can also be made into an IFDF on $m - 1$ variables by 'precomposition with the diagonal map' ($\triangle(x) \stackrel{\text{def}}{=} (x, x)$). More concretely, if $f : W^m \to \mathbb{Q}$ is an IFDF, then so is the following function:

$$(w_1, w_2, \ldots, w_{m-1}) \mapsto f(w_1, w_1, w_2, \ldots, w_{m-1}).$$

The proof again is immediate from the definitions.

There are numerous permutations of how one can perform these multiplications or precompositions with the diagonal map, and stating these formally will not shed any new insight on these operations. We will exclusively use these operations on small degree (e.g. linear or quadratic) functions and on just one or two variables. For example, we will often use the fact that $v \mapsto \operatorname{trace}(v \cdot v)$ is an IFDF. This is fairly easy to see (if v is in an integral form, then so is $v \cdot v$), which makes calling this function "precomposition of trace with multiplication followed by precomposition with the diagonal map" somewhat unnecessarily verbose, and we will often avoid the excessive jargon if it is not illuminating.

Integral forms are also closed under a property which we can call "taking the kth root of the perfect k-power part," which we formalize with a basic lemma and then explain below.

Lemma 2.1.3. *Let k be positive integer, y a rational number, and m an integer such that no factor of m is a kth power. Then $m\, y^k$ is an integer if and only if y is an integer.*

Proof. Suppose $m \cdot y^k \in \mathbb{Z}$. In reduced form, the denominator of y^k has all prime factors with multiplicity a multiple of k. The prime factors of m all divide m with multiplicity strictly less than k. So the denominator of y^k must be 1 in order for my^k to be an integer. Thus y is an integer. $\square$

This will be used to reduce down integral form detector functions to smaller degrees. For example, suppose $g : W \to \mathbb{Q}$ is any function, and $f(w) = 24g(w)^2$ is an integral form detector function. Then write $f(w) = 6 \cdot [2g(w)]^2$. By the lemma, $f(w)$ is an integer if and only if $2g(w)$ is an integer. Thus $w \mapsto 2g(w)$ is an integral form detector function. In summary, we factored f as a square-free integer times a perfect square, and took the square-root of the perfect-square part. We will use this lemma freely and without citation when it is obvious – e.g. "If $x \in \mathbb{Q}$ and $5x^2 \in \mathbb{Z}$ then $x \in \mathbb{Z}$."

Producing integral form detector functions will be key to classifying maximal invariant integral forms. In a certain sense, the IFDFs are dual to integral forms. The more IFDFs we have, the more constricted the possibilities for integral forms are, which allows us to classify them.

As a key example, if one can produce $n = \dim(A)$ linearly-independent *linear* functions $f_1, \ldots, f_n : A \to \mathbb{Q}$ which are integral form detectors, then we can form the dual basis $f_1^*, \ldots, f_n^*$ of A defined by $f_i(f_j^*) = \delta_{ij}$. Then any integral form must be contained in $\mathrm{span}_{\mathbb{Z}}(f_1^*, \ldots, f_n^*)$ since this is the largest subset of A on which all of the functions $f_1, \ldots, f_n$ take integer values. If $\mathrm{span}_{\mathbb{Z}}(f_1^*, \ldots, f_n^*)$ happened to be closed under the algebra products, then this would be the unique maximal integral form in the algebra.

This sets the goal as constructing small degree (especially linear) integral form detector functions. As was mentioned, $\mathrm{trace}(a)$ is an integral form detector function, as are the other coefficients of $\chi(a; t)$. We next show that for any $\mathrm{ad}(a)$-invariant subspace W, $\chi(\mathrm{ad}(a)\big|_W; t)$ will be in $\mathbb{Z}[t]$. First an elementary lemma:

Lemma 2.1.4. *Let $0 \subsetneq W_1 \subsetneq W_2 \subsetneq \cdots \subsetneq W_n = W$ be a full flag for an n-dimensional $\mathbb{Q}$-vector space W (i.e. each W_i is a subspace, and $\dim W_i = i$), and let L be a discrete subgroup of W of rank n. Then L has a $\mathbb{Z}$-basis $b_1, \ldots, b_n$ such that $b_i \in W_i$.*

Proof. Proceed by induction on $\dim W$, with the $\dim W = 1$ case being trivial.

Let w_1 be a nonzero element of W_1. When expressed as a linear combination of a basis of L, the coefficients of w_i will be rational. So some integer times w_i will lie in L. In particular, $W_1 \cap L$ is a subgroup of L with rank at least 1. The rank can be no more than 1 because two $\mathbb{Z}$-linearly independent vectors in $W_1 \cap L$ would be two $\mathbb{Q}$-linearly independent vectors in W_1.

So $L \cap W_1$ equals $\mathbb{Z}b_1$ for some b_1. Then $(L + W_1)/W_1 \cong L/(W_1 \cap L) = L/\mathbb{Z}b_1$, and the latter is torsion free by the definition of b_1. (If $\frac{1}{k}b_1$ were in L for some positive integer k, then $\frac{1}{k}b_1$ would be in $L \cap W_1$.) Hence $(L + W_1)/W_1$ is a free subgroup of rank $n - 1$ inside W/W_1, and W_i/W_1 $(i = 2, \ldots, n)$ is a full flag of W/W_1. By induction hypothesis, take a $\mathbb{Z}$-basis of $\overline{b_2}, \ldots, \overline{b_n}$ of $(L + W_1)/W_1$ with $\overline{b_i} \in W_i/W_1$ for $i = 2, \ldots n$. Let $b_2, \ldots, b_n \in L$ be elements such that $\pi(b_i) = \overline{b_i}$ where $\pi : L \to W/W_1$ is the inclusion of L into W followed by the canonical quotient map.

Note that $b_i \in W_i$ for $i = 2, \ldots n$. The images of $b_2, \ldots, b_n$ are a $\mathbb{Z}$-basis of $L/\ker(\pi)$, and b_1 is a $\mathbb{Z}$-basis of $\ker(\pi)$, so $b_1, \ldots, b_n$ is a $\mathbb{Z}$-basis of L. □

Proposition 2.1.5. *Let A be a finite dimensional algebra over $\mathbb{Q}$. If x is in an integral form L of A, and $ad(x)$ leaves invariant a rational subspace W of A, then $\chi\left(ad(x)\big|_W; t\right)$ is in $\mathbb{Z}[t]$.*

Proof. Choose any full flag $A_1, \ldots, A_n$ of A such that $A_k = W$, where $k = \dim_{\mathbb{Q}} W$. Let $\ell_1, \ldots, \ell_n$ be a $\mathbb{Z}$-basis of L subordinate to this flag guaranteed by Lemma 2.1.4. Then $\ell_1, \ldots, \ell_k$ are k vectors that are $\mathbb{Z}$-linearly independent (hence $\mathbb{Q}$-linearly independent) in W, and therefore are a $\mathbb{Q}$-basis of W.

Since both L and W are invariant under $\mathrm{ad}(x)$, their intersection is also invariant. Note that $W \cap L = \mathrm{span}_{\mathbb{Z}}(\ell_1, \ldots, \ell_k)$. Therefore, with respect to the basis $\ell_1, \ldots, \ell_k$ of W, the matrix of $\mathrm{ad}(x)\big|_W$ has integer entries, and so the characteristic polynomial of $\mathrm{ad}(x)\big|_W$ has integer coefficients. □

The existence of $\mathrm{ad}(x)$ invariant subspaces, for certain choices of x, are guaranteed by the following lemma, which is a slight restatement of [FG92, Lemma 2.2]:

Lemma 2.1.6. *Let σ be an automorphism of a rng R, with C equal to the fixed-point subrng, and $\phi(t) \in \mathbb{Z}[t]$. Then $N = Im(\phi(\sigma))$ is stable under multiplication by C.*

Proof. Fix $c \in C$ and $r \in R$. Note that $\mathrm{ad}(c)$ commutes with all powers of σ, so $c \cdot \phi(\sigma)r = \phi(\sigma)(c \cdot r)$. □

In particular, for a GIIF L of a Norton-Sakuma algebra V, suppose that t is a nontrivial τ-involution. Then the lemma says that elements in L^t act with integer trace on $\mathrm{Im}(t+1)$ and of $\mathrm{Im}(t-1)$, which are the fixed points of t and the -1-eigenspace of t, respectively. This puts a considerable rigidity on the elements in the algebra which can be in L^τ for some GIIF L.

We conclude this section with another method of producing integral form detector functions.This will be used to factor characteristic polynomials in order to get linear integral form detector functions. The result is a slight variant of Gauss' lemma.

Lemma 2.1.7. *Suppose $p_i(t)$ is a monic polynomial in $\mathbb{Q}[t]$ for $i = 1, \ldots n$ such that $\prod_{i=1}^n p_i(t) \in \mathbb{Z}[t]$. Then $p_i(t) \in \mathbb{Z}[t]$ for each i.*

Proof. For each i, let r_i be the smallest positive rational number such that $r_i p_i(t) \in \mathbb{Z}[t]$. Then $r_i p(t)$ must be primitive (in the sense that its coefficients must have no common prime factor) because if q divides each coefficient, then $r_i/q p_i(t)$ would be in $\mathbb{Z}[t]$. Because $p_i(t)$ is monic, r_i must be an integer.

Gauss' lemma implies that $\prod_{i=1}^n r_i\, p_i(t)$ is primitive. Since $\prod_{i=1}^n p_i(t) \in \mathbb{Z}[t]$, this implies that $\prod_{i=1}^n r_i$ must equal 1. Therefore each $r_i = 1$ so $p_i(t) \in \mathbb{Z}[t]$. □

2.2 The intrinsic forms and extending GIIFs

Definition 2.2.1. For a, b in any finite-dimensional algebra, define the two forms $\kappa(a,b) = \mathrm{Tr}(\mathrm{ad}(a)\,\mathrm{ad}(b))$ and $\eta(a,b) = \mathrm{Tr}(\mathrm{ad}(a \cdot b))$. The form κ is called the *Killing form*.

Both of these forms are bilinear, and if the algebra is commutative then both forms are also symmetric. Note that neither form is, in general, equal to or a multiple of the associative inner product on the Griess algebras that is usually considered, for example in [IPSS10]. Both of these forms are also integral form detector functions, which is a consequence of the following slightly more general statement.

The importance of these intrinsic bilinear forms to the study of integral forms is given by the following easy but important result.

Proposition 2.2.2. *If R and S are integral forms of an algebra A with $R \subseteq S$, then $S \subseteq R^{*,\kappa} \cap R^{*,\eta}$ where $R^{*,\alpha} = \{x \in A : \alpha(R, x) \subseteq \mathbb{Z}\}$ is the dual space to R with respect to the form α.*

Proof. Take $s \in S$ and $r \in R$. With respect to a $\mathbb{Z}$-basis of S, both $\mathrm{ad}(r)$ and $\mathrm{ad}(s)$ are matrices with integer entries. Hence $\kappa(r, s) \in \mathbb{Z}$.

Similarly $s \cdot r \in S$ so the matrix of $\mathrm{ad}(s \cdot r)$ in a $\mathbb{Z}$-basis of S is an integer matrix. Thus, $\eta(r, s) \in \mathbb{Z}$. □

Taking $R = S$ in this proposition shows that every integral form in a finite-dimensional commutative algebra is a lattice with respect to both of these two forms. So we record a few definitions and results about lattices and the containment of lattices.

Definition 2.2.3.

(i) A *lattice* is a finitely-generated free abelian group L together with a symmetric bilinear form $\alpha : L \times L \to \mathbb{Q}$.

(ii) A lattice is called integral if $\alpha(L, L) \subseteq \mathbb{Z}$.

(iii) Given a $\mathbb{Z}$-basis of a lattice $\{b_i : i = 1, \dots, n\}$, the *Gram matrix* with respect to this basis is the $n \times n$-matrix with (i, j)-entry equal to $\alpha(b_i, b_j)$.

(iv) A lattice is *nonsingular* if for every $\ell \in L$, the function $L \to \mathbb{Q}$ defined by $x \mapsto \alpha(\ell, x)$ is not identically zero.

(v) The *dual* of a nonsingular rational lattice is $L^{*,\alpha} = \{\ell \in \mathbb{Q} \otimes L \mid \alpha(\ell, y) \in \mathbb{Z} \text{ for all } y \in L\}$ where we make the identification $L \cong 1 \otimes L$ and extend the bilinear form to $\mathbb{Q} \otimes L$ by linearity.

(vi) The *determinant* $\det_\alpha(L)$ of an integral lattice L is the determinant of the Gram matrix of any $\mathbb{Z}$-basis of L, and this is independent of the choice of basis. The lattice is singular if and only if $\det_\alpha(L) = 0$. The absolute value of the determinant of a nonsingular integral lattice L equals $[L^{*,\alpha} : L]$ [Gri11, 2.3].

Note that often times the bilinear form is implicitly understood, so the α is omitted in these notation – e.g. in $\det L = \det_\alpha L$ and $L^* = L^{*,\alpha}$. Since integral forms are lattices with respect to both κ and η, it will be important for us to emphasize the form.

Proposition 2.2.4 ("Index-determinant formula")**.** *Let $R \subseteq S$ be two nonsingular integral lattices with respect to a form α and $[S : R] < \infty$. Then* $\det_\alpha(S)[S : R]^2 = \det_\alpha(R)$.

Proof. [Gri11, 2.3.3] □

As a corollary to Propositions 2.2.2, we have the following.

Corollary 2.2.5. *If R is an integral form in a finite-dimensional commutative algebra, then the set of integral forms containing R correspond to some collection of (additive) subgroups of $(R^{*,\kappa} \cap R^{*,\eta})/R$.*

Furthermore, $[R^{*,\kappa} \cap R^{*,\eta} : R] \leqslant \gcd(\det_\kappa(R), \det_\eta(R))$, *(where* $\gcd(0, 0) = \infty$*).*

Proof. The first claim is a restatement of 2.2.2 combined with the correspondence theorem for subgroups of quotient groups. To prove the inequality, first note that if $\det_\kappa(R) = \det_\eta(R) = 0$ then there is nothing to prove. So we may assume that one of these is nonzero. Therefore at least one of the groups $R^{*,\kappa}/R$ and $R^{*,\eta}/R$ is finite. Note that $(R^{*,\kappa} \cap R^{*,\eta})/R$ is a subgroup of both $R^{*,\kappa}/R$ and $R^{*,\eta}/R$. By the comment in Definition 2.2.3(iv), $[R^{*,\kappa} \cap R^{*,\eta} : R]$ divides both $\det_\kappa(R)$ and $\det_\eta(R)$. □

This gives a finite time algorithm to produce maximal (G-invariant) integral forms in any finite-dimensional rational algebra V with one of κ and η nonsingular. We start with a general integral form R of V, which one can find by taking any $\mathbb{Q}$-basis and multiplying the basis by a sufficiently large integer, as explained in the paragraph following Definition 1.2.4. Corollary

2.2.5 guarantees that every integral form containing R corresponds to some subgroup of the finite group $(R^{*,\kappa} \cap R^{*,\eta})/R$.

The following easy but important result proves that if we want to prove R is maximal, we do not need to search through all of these subgroups.

Proposition 2.2.6. *Let $R \subsetneq S$ be two integral forms in a finite-dimensional algebra V with p a prime a divisor of $[S : R]$. Then there exists an integral form S' such that $S' \subseteq \frac{1}{p}R$ but $S' \nsubseteq R$.*

Proof. Let m be the exponent of S/R. So p divides m, and note that an integer multiple of an integral form is still an integral form. Take $S' = (m/p)S$. Then $pS' = mS \subseteq R$ with $S \nsubseteq R$. $\square$

So to find an integral form not contained in R, one only needs to search through the subgroups of $\frac{1}{p}R/R \cap (R^{*,\kappa} \cap R^{*,\eta})/R$. And in fact if one is searching for GIIFs, then the corresponding subgroups of the quotient will actually be submodules of the $\mathbb{F}_p[G]$-module $\frac{1}{p}R/R \cap (R^{*,\kappa} \cap R^{*,\eta})/R$.

One should note here that the quotient $R^{*,\alpha}/R$ is called the *discriminant group* of the lattice (L, α), and that there are algorithms available for computing the dual of lattice, intersections of lattices, finding generators of the quotients of two lattices (which is related to finding a Smith basis for an inclusion of finitely generated $\mathbb{Z}$-modules, see for example Theorem 7.8 in [Lan02]). In the remaining sections, we begin with an integral form and prove that it is the unique maximal G_0-invariant integral form[1]. The preceding discussion indicates how we discovered these maximal G-invariant integral forms to begin with – namely by checking through the G-submodules of $(R^{*,\kappa} \cap R^{*,\eta})/R$ for some fixed R, using knowledge of $\mathbb{F}_p[G]$ representation theory.

Below we want to collect a few results about integral forms, the τ-involutions and integral representation theory that we will need in other sections. The following results in this section

[1]where G_0 is either G or in the 2A case, we must take $G_0 = \mathrm{Aut}(V)$

should not be considered original, but it will be convenient to collect them here. First we make the observation that I is in any maximal GIIF.

Lemma 2.2.7. *Let V be a rational vector space, and $S \subset V$ a finite set. Then $\mathrm{span}_{\mathbb{Z}}(S)$ is a discrete subgroup and has a $\mathbb{Z}$-basis consisting of at most $n = \dim_{\mathbb{Q}}(V)$ elements.*

Proof. Fix a basis $v_1, \ldots, v_n$ of V. There is an integer m such that, for all $s \in S$, the coefficients of ms in the basis $v_1, \ldots, v_n$ are integers. Therefore $\mathrm{span}_{\mathbb{Z}}(S) \subseteq \frac{1}{m}\mathrm{span}_{\mathbb{Z}}(v_1, \ldots, v_n)$. Submodules of free modules are free, so $\mathrm{span}_{\mathbb{Z}}(S)$ is also free over $\mathbb{Z}$ and its rank is no more than n [DF04, 12.1 Thm 4]. □

Proposition 2.2.8. *Let V be a $\mathbb{Q}$-algebra with a multiplicative identity I, and let H be any subgroup of $Aut(V)$. Then every maximal H-invariant integral form contains I.*

Proof. Let L be any H-invariant integral form of V. Then clearly $L + \mathbb{Z}I$ will also be an integral form. By the previous lemma (2.2.7), $L + \mathbb{Z}I$ is also discrete and its rank is at most $\dim V$ and at least $\mathrm{rank}\, L = \dim V$. So $L + \mathbb{Z}I$ is also an integral form, and it is clearly H-invariant, since $hI = I$ for all $h \in \mathrm{Aut}(V)$. □

Lemma 2.2.9. *For an axis a in a $\mathbb{Q}$-algebra V, $\tau(a)$ is a rational polynomial in $ad(a)$.*

Proof. Let $p(t)$ be a rational polynomial such that $p(0) = p(1) = p(1/4) = 1$ and $p(1/32) = -1$. For a μ-eigenvector v of $\mathrm{ad}(a)$, $p(\mathrm{ad}(a))v = p(\mu)v$. In particular, $p(\mathrm{ad}(a))$ acts as 1 on $V_0^{(a)} \oplus V_1^{(a)} \oplus V_{1/4}^{(a)}$ and it acts on $V_{1/32}^{(a)}$ as the scalar -1. So $p(\mathrm{ad}(a)) = \tau(a)$. □

This also shows that any subalgebra containing a will be closed under the action of $\tau(a)$.

Proposition 2.2.10. *Let V be an algebra with at least one axis and g an automorphism of V.*

(i) If a is an axis, then ga is an axis and $\tau(ga) = g\tau(a)g^{-1}$.

Let A be a set of axes in V and $T = \{\tau(a) : a \in A\}$ be the corresponding set of τ-involutions. Suppose that the function from A to T given by $a \mapsto \tau(a)$ is bijective. Let $t \mapsto a_t$ be its inverse.

(ii) If $t \in T$, then $ga_t = a_{gtg^{-1}}$.

Proof. (i) The function $a \mapsto \tau(a)$ is a polynomial in $\mathrm{ad}(a)$ by Lemma 2.2.9. Since $g\,\mathrm{ad}(a)g^{-1} = \mathrm{ad}(ga)$, it follows that $g\tau(a)g^{-1} = \tau(ga)$.

(ii) By definition, $t = \tau(a_t)$ and $a_{\tau(a')} = a'$. Then by part (i), $a_{gtg^{-1}} = a_{\tau(ga_t)} = ga_t$. □

Corollary 2.2.11. *Let V be an algebra. Then $G = \langle \tau(a) : \text{ a an axis} \rangle$ is a normal subgroup of $Aut(V)$. Therefore the set of all G-invariant integral forms (GIIFs) is closed under the action of $Aut(V)$. So if there is a unique maximal GIIF in V, then this is also the unique maximal $Aut(V)$-invariant integral form.*

Proof. By (i) of the previous result (2.2.10), the set of τ-involutions is invariant under conjugation by any element $\mathrm{Aut}(V)$, so the subgroup G generated by the τ-involutions is normal. Let h be an element in $\mathrm{Aut}(V)$ and L a GIIF. Then we claim that hL is also a GIIF. If $\{\ell_1, \ldots, \ell_n\}$ is a $\mathbb{Z}$-basis of L, then $\{h\ell_1, \ldots, h\ell_n\}$ is a $\mathbb{Z}$-basis of hL, and the structure coefficients of hL under this algebra are the same as the structure coefficients of L. So hL is also an integral form. Choose any $g \in G$. Then

$$g \cdot hL = hh^{-1}ghh^{-1} \cdot hL = h(h^{-1}gh)\,L = hL.$$

The final inequality follows since L is invariant under G and $h^{-1}gh \in G$ by normality. □

We conclude here with a proposition regarding the action of dihedral groups on lattices which will be relevant in the cases $3A, 3C, 5A$ and $6A$.

Proposition 2.2.12. *Let V be a finite-dimensional rational vector space with a symmetric bilinear form $\alpha : V \otimes V \to \mathbb{Q}$. Let L be a lattice inside V and let g be a lattice automorphism of L of order p a prime such that L/L^g has rank $(p-1)^k$. Then $[L : L^g + (L^g)^{\perp}]$ divides p^k.*

Proof. We may assume $L \neq L^g$, and so $(g-1)L \neq 0$. Observe that $(g-1)L \subseteq (L^g)^{\perp}$, because if $v, x \in L$ with $g \cdot v = v$, then:

$$((g-1)x, v) = (gx, v) - (x, v) = (x, gv) - (x, v) = 0. \tag{2.1}$$

We then have:

$$0 = (g^p - 1)L = (g^{p-1} + g^{p-2} + \cdots g + 1)(g-1)L.$$

The polynomial $\Phi_p(t) = t^{p-1} + t^{p-2} + \cdots + 1$, being irreducible in $\mathbb{Z}[t]$, is therefore the minimal polynomial of g on $(g-1)L$. Since $\operatorname{rank} L/L^g = (p-1)^k$, then g acts on $(g-1)L$ with characteristic polynomial $\pm\Phi_p(t)^k$. Therefore $g-1$ acts on $(g-1)L$ with characteristic polynomial $\pm\Phi_p(t+1)^k$ and in so in particular with determinant $\pm p^k$.

So there is an inclusion:

$$L^g + (g-1)L \subseteq L^g + (L^g)^{\perp} \subseteq L,$$

where the outer inclusion is of index p^k. The desired result follows. □

2.3 The general strategy

Throughout this section V is finite-dimensional algebra (with axes), and $G = \langle \tau(a) :$ a an axis of $V \rangle$ is the subgroup of $\operatorname{Aut}(V)$ generated by the τ-involutions. We will show the general strategy of classifying the maximal G-invariant integral forms.

Let $W_1, \ldots, W_k$ be a set of representatives of all irreducible $\mathbb{Q}[G]$-modules up to isomorphism, with W_1 the trivial 1-dimensional representation. Decompose $V = \bigoplus_{i=1}^k V_i$ into corresponding isotypic subspaces with respect to the action of G, meaning that each V_i is the sum of all submodules of V isomorphic to W_i. For each i we will first try to classify the elements in V_i which can be in an integral form.

The most important isotypic piece to consider will turn out to be the fixed point subalgebra $V^G = V_1$. The importance stems from the following fact: suppose $g \in G \subseteq \mathrm{Aut}(V)$, $f \in V^G$, and $v \in V$; then

$$g\,(f \cdot v) = (g\,f) \cdot (g\,v) = f \cdot (g\,v).$$

In other words, the map $\mathrm{ad}(f)$ from $V \to V$ is a G-module endomorphism. In particular $f \cdot V_i \subseteq V_i$ for each index i. If we concatenate bases of each V_i to produce a basis of V, then with respect to this basis, $\mathrm{ad}(f)$ is a block diagonal matrix with blocks of size $\dim V_i$. This implies that the characteristic polynomial of $\mathrm{ad}(f)$ necessarily factors nontrivially as long as there is more than one isotypic component. This allows us to apply the variant of Gauss' lemma (2.1.7) in order to produce many integral form detector functions, corresponding to every coefficient in every factor of the characteristic polynomial. In particular, the trace of $\mathrm{ad}(f)\big|_{V_i}$ is a linear integral form detector function on V^G for each i.

This is in fact a special case of a more general phenomenon. The tensor product of every pair of irreducible $\mathbb{Q}[G]$-modules will decompose as a direct sum of some subset (with multiplicities) of the set of irreducible modules, and not every irreducible will necessarily occur in this decomposition. The algebra product is a G-module map $V \otimes V \to V$ and this restricts to a G-module map $V_i \otimes V_j \to V$ for each pair i and j. The image of this map will be a G-submodule of V, and this image can only contain the irreducible submodules which occur in $V_i \otimes V_j$ and which also occur in V. And in practice the image of $V_i \otimes V_j$ will contain even fewer irreducible submodules.

Suppose we choose a basis of each of $V_1, \ldots V_k$ and concatenate this to a basis of V. So if $v_i \in V_i$ then $\mathrm{ad}(v_i)$ will be decomposable in terms of blocks, where there will be a block of 0s when there is an irreducible W_k that does not occur in both V and $V_i \otimes V_j$ for some j. Supposing there are sufficiently many zero blocks, this will cause a *tendency* for $\mathrm{ad}(v_i)$ to preserve some proper subspaces and also to have the characteristic polynomial of $\mathrm{ad}(v_i)$ factor, providing more IFDFs on V_i.

In particular, this is will always happen for the isotypic pieces corresponding to one-dimensional irreducibles, since if W_i and W_j are one-dimensional, then $W_i \otimes W_j \cong W_\ell$ for some other one-dimensional W_ℓ, and in this case $V_i \cdot V_j \subseteq V_\ell$. This is especially effective for the 4A and 4B algebras in which the group G is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$, meaning all the irreducible $\mathbb{Q}[G]$-modules are one-dimensional.

As mentioned in the previous section, in each of the algebras we will be able to find some maximal GIIF M of V. By constructing enough detector functions on each isotypic subspace, for each i we will try to prove that for every GIIF L, $L \cap V_i \subseteq M$. Now GIIFs are $\mathbb{Z}$-free $\mathbb{Z}[G]$-modules, and in particular they are cannot always be uniquely decomposed into irreducibles – meaning that in general for a GIIF L, $L \neq \sum_{i=1}^{k}(L \cap V_i)$. However, it is a fact that L cannot be too far off from this.

Lemma 2.3.1. *Let L be a discrete $\mathbb{Z}[G]$-submodule of the $\mathbb{Q}[G]$-module V and $V = \bigoplus_{i=1}^{k} V_i$ the decomposition of V into G-isotypic subspaces. Then $L \subseteq \frac{1}{|G|}\sum_{i=1}^{k}(L \cap V_i)$.*

Proof. Decompose $\mathbb{Q}[G]$ as $\bigoplus_{i=1}^{k} e_i\mathbb{Q}[G]$ where each e_i is a primitive central idempotent of $\mathbb{Q}[G]$, where we let e_i be ordered so that e_i acts on V_j as the scalar δ_{ij}. Then we first claim that $|G|e_i \in \mathbb{Z}[G]$.

To prove this, note that for an irreducible complex character χ of G, the idempotent corresponding to χ is given by $e(\chi) = \frac{\chi(1)}{|G|}\sum_{g\in G}\chi(g^{-1})g$. Then the primitive central idempotents in $\mathbb{Q}[G]$ are given by $\sum_{h\in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})} e(\chi^h)$ for some irreducible complex character χ [Yam74, Prop 1.1] . The coefficients of each $g \in G$ in this sum will all be $\frac{1}{|G|}$ times rational integers.

Write $1 = \sum_{i=1}^{k} e_i$ in $\mathbb{Q}[G]$. Since L is invariant under $\mathbb{Z}[G]$, oberve that $|G|e_iL \subseteq L \cap V_i$. Thus we have,

$$|G|L = |G|(e_1 + e_2 + \cdots e_k)L \subseteq |G|e_1L + \cdots |G|e_kL \subseteq \sum_{i=1}^{k}(L \cap V_i).$$

□

Therefore, if we have proven that, for every GIIF L and each $i = 1, \dots k$ that $L \cap V_i \subseteq M$, then the previous lemma implies that $L \subseteq \frac{1}{|G|}M$. Now if L is a GIIF not contained in M then $(|G|/p)L$ will be a GIIF not contained in M which is contained in $\frac{1}{p}M$ for some prime divisor of $|G|$. So it suffices to check if there are any integral forms in $\frac{1}{p}M$ for each prime p dividing the order of G. This turns out to often be a finite problem in arithmetic modulo p. When no such GIIFs are found, we will have proven that every GIIF is contained in M.

It should be noted here that the strategy explained here is not always followed exactly, step-by-step, in each algebra – there are occasional shortcuts and alternate routes. For the most part, however, you can view this strategy as a template attempted to be followed in each subsection, which hopefully will help motivate the ideas presented therein.

We note here that much of the work in classifying the maximal G-invariant integral forms will rely on calculation of traces, characteristic polynomials, and the intrinsic forms on elements in various isotypic subspaces. When a calculation is required, we will include a reference like '`[★2A.2]`'. This indicates that this calculation was performed with a computer algebra system. Code for these calculations as well as an explanations of the necessary structural code is given in Appendix B.

CHAPTER 3

GIIFs in the Norton-Sakuma Algebras

3.1 The 2A algebra

Notation 3.1.1. The 2A dihedral algebra V_{2A} has a basis of axes (therefore idempotents) $a_0,\ a_1,\ a_\rho$ such that for every choice of indices $\{i, j, k\} = \{0, 1, \rho\}$,

$$a_i \cdot a_j = 2^{-3}(a_i + a_j - a_k).$$

([IPSS10, Table 3])

The group of τ-involutions acts trivially on V_{2A} [IPSS10, Lemma 2.20]. Let I be the multiplicative identity. We set $a = a_0$ and $k = I - a$, so $k \cdot k = k$ and $k \cdot a = 0$. We set $q = 4(a_1 - a_\rho)$, and we compute that $q \cdot q = 7a + 15k$ and $a \cdot q = \frac{1}{4}q$ [**✶2A.1**].

It follows that $k \cdot q = (I - a) \cdot q = \frac{3}{4}q$. These notations were chosen because *a kills* k, and *a quarters* q. Idempotents a and k generate a subalgebra isomorphic to $\mathbb{Z}^2$.

Lemma 3.1.2. *The following gives the trace of each element a, k, and q*

$$trace(a) = \frac{5}{4}, \qquad trace(k) = \frac{7}{4}, \qquad trace(q) = 0.$$

Proof. Let $\mathcal{B}$ denote the ordered basis (a, k, q). With respect to $\mathcal{B}$, the matrix of $\mathrm{ad}(a)$ is diagonal with entries $1, 0, \frac{1}{4}$. The matrix $[\mathrm{ad}(k)]_{\mathcal{B}}$ of $\mathrm{ad}(k)$ with respect to $\mathcal{B}$ has diagonal components 0, 1, $\frac{3}{4}$, and the diagonal entries of $[\mathrm{ad}(q)]_{\mathcal{B}}$ are all 0. $\square$

Proposition 3.1.3. *If $4xa + yq$ is in an integral form of V_{2A}, with $x, y \in \mathbb{Q}$, then $x, y \in \mathbb{Z}$.*

Proof. Set $w = 4xa + yq$. We compute $\mathrm{trace}(w) = 5x$ and $\mathrm{trace}(w \cdot w) = 5(4x^2 + 7y^2)$ [$\bigstar$`2A.2`] which are both integers. We note that $100x^2 = 4(5x)^2$ is an integer, hence $5^2 7y^2 = 5^2(4x^2 + 7y^2) - 100x^2$ is also an integer. Since y is rational, we conclude that $5y$ is an integer.

Set $X = 5x$ and $Y = 5y$, so that $X, Y \in \mathbb{Z}$, we have:

$$\mathrm{trace}(w \cdot w) = 20x^2 + 35y^2 = \frac{1}{5}(4X^2 + 7Y^2).$$

The equation $4X^2 + 7Y^2 \equiv 0, \pmod 5$ is equivalent to $X^2 \equiv 2Y^2 \pmod 5$. Since 2 is not a square mod 5, this equation has only the trivial solution $X \equiv Y \equiv 0, \pmod 5$. Hence $X, Y \in 5\mathbb{Z}$ and so $x, y \in \mathbb{Z}$. □

Lemma 3.1.4. *For any positive integer k, every discrete subrng of $\mathbb{Q}^k$ is contained in $\mathbb{Z}^k$.*

Proof. Let A be a discrete subrng of $\mathbb{Q}^n$. Then A is additively generated by at most n elements [Bou98, Ch VII §1.1-1.2]. So there is some $N > 0$ such that $A \subseteq \frac{1}{N}\mathbb{Z}^n$. Let e_i be the ith standard basis vector of $\mathbb{Q}^n$. Let $a = \sum_{i=1}^n a_i e_i$ be an element of A. Then $a^k = \sum_{i=1}^n a_i^n e_i$.

Write $a_i = p_i/q_i$ for relatively prime integers $q_i > 0$ and p_i. Suppose $q_j > 1$ for some j. Choose k so that $q_j^k > N$. Then $a^k = \sum_{i=1}^n a_i^k e_i$ is not in $\frac{1}{N}\mathbb{Z}^n$, since $a_j^k = \frac{p_i^k}{q_i^k}$ is a reduced fraction with denominator larger than N. Therefore $q_i = 1$ and $A \subseteq \mathbb{Z}^n$. □

Corollary 3.1.5. *Suppose $x, y \in \mathbb{Q}$. If $xa + yk$ or $xa + yI$ is in an integral form of V_{2A}, then $x, y \in \mathbb{Z}$.*

Proof. The rational span of a and k is isomorphic to $\mathbb{Z}^2$. The intersection of $\mathrm{span}_{\mathbb{Q}}(a, k)$ with any integral form is a discrete subrng of $\mathrm{span}_{\mathbb{Q}}(a, k) \cong \mathbb{Q}^2$ and therefore is contained in $\mathrm{span}_{\mathbb{Z}}(a, k)$, by 3.1.4.

If $xa + yI = (x + y)a + yk$ is in an integral form, then the previous paragraph shows $x + y \in \mathbb{Z}$ and $y \in \mathbb{Z}$ and hence $x \in \mathbb{Z}$. □

Corollary 3.1.6. *Let L be an integral form of V_{2A} with $I \in L$. Then there exists a positive integer t and a $w \in V_{2A}$ such that I,$4ta$,w is a $\mathbb{Z}$-basis of L. Furthermore, we may write $w = xa + yq + zI$ where $x, y, z \in \mathbb{Q}$ with $0 \leqslant x \leqslant 2t$ and $0 \leqslant z < 1$.*

Proof. Note that if $xa \in L$ for some rational x, then $x \in 4\mathbb{Z}$ by Proposition 3.1.3. Let $t \in \mathbb{Z}$ be such that $4ta$ is the smallest integer multiple of a in L. If we can show that $L/\mathrm{span}_{\mathbb{Z}}(I, 4ta)$ is torsion-free, then $\{I,\ 4ta\}$ can be extended to a $\mathbb{Z}$-basis of L. Let $n, m, \ell \in \mathbb{Z}$ (with $\ell \neq 0$) be such that $\varphi = \frac{nI+m4ta}{\ell}$ is in L. By Corollary 3.1.5, n/ℓ and $4tm/\ell$ are integers. But then $z - \frac{n}{\ell}I = \frac{4tm}{\ell}a$ is in L. By minimality of t, $(4tm/\ell)a$ is an integer multiple of $4ta$. In other words, m/ℓ is an integer. Therefore, $z \in \mathrm{span}_{\mathbb{Z}}(I, 4ta)$.

If w is the preimage in L of a generator of $L/\mathrm{span}_{\mathbb{Z}}(I, 4ta)$, then $L = \mathrm{span}_{\mathbb{Z}}(I, 4ta, w)$. Writing $w = xa + yq + zI$ we may add or subtract integer multiples of $4ta$ and I from w to ensure that $0 \leqslant x < 4t$ and that $0 \leqslant z < 1$. Then we may replace w by $-w + I + 4ta$ if necessary to ensure that $0 \leqslant x \leqslant 2t$. □

Definition 3.1.7. For subsets $S_1, \ldots, S_k$ of an algebra A, define $\mathrm{rng}(S_1, \ldots, S_n)$ to be the rng generated by $\bigcup_{i=1}^{k} S_i$, i.e. the smallest (additive) subgroup of A containing $\bigcup_{i=1}^{k} S_i$ that is closed under the algebra multiplication.

We omit brackets on singleton subsets: for example if $S \subset A$ and $v \in A$ then $\mathrm{rng}(S, v) = \mathrm{rng}(S, \{v\})$.

Definition 3.1.8. Set $P = \mathrm{span}_{\mathbb{Z}}(4a, I, q)$

Proposition 3.1.9. *P is an integral form of V_{2A}.*

Proof. Showing that P is a ring is an easy verification: $(4a)^2 = 16a$, $4a \cdot q = q$ and $q^2 = -8a + 15I$ are all in P.

Then since $a,\ k = a - I$, and q form a basis of V_{2A}, it follows that P has rank 3. □

Lemma 3.1.10. *Let $L(m) = \mathrm{span}_{\mathbb{Z}}(I, 8a, \frac{1}{2}a + \frac{2m+1}{2}q + \frac{1}{2}I)$. Then $L(m)$ is an integral form for V_{2A} for every $m \in \mathbb{Z}$. If L is maximal integral form of V_{2A} then either $L = P$ or $L = L(m)$ for some integer m.*

Proof. With our mind on the conclusion of 3.1.6, suppose $L = \mathrm{span}_{\mathbb{Z}}(I, 4ta, w)$, where t is an integer and where $w = xa + \frac{y}{4}q + \frac{z}{4}I$ with $x, y, z \in \mathbb{Q}$ and where $0 \leqslant x < 2t$ and $0 \leqslant z < 4$. (The factors of 4 are included here and not in 3.1.6 because this will simplify the computations to come.)

The set L is clearly closed under multiplication by I. It also contains $(4ta)^2 = 16t^2a$. Therefore, L will be an integral form if and only if L contains $(4ta) \cdot w$ and $w \cdot w$.

We compute the coefficients of $(4ta) \cdot w$ and $w \cdot w$ in the $\mathbb{Z}$-basis $I, 4ta, w$ of L: [★2A.4]

$$\begin{aligned}(4ta) \cdot w &= -\frac{tz}{4} I + \frac{1}{4}(3x+z)\ (4ta) + t\, w \\ w \cdot w &= \frac{1}{16}\left(15y^2 - z(2x+z)\right)\ I + \frac{(x^2 - y^2)}{8t}\ (4ta) + \frac{1}{2}(x+z)\, w\end{aligned}$$

Thus we conclude that L is an integral form if and only if the following six terms are integers:

$$-\frac{tz}{4}, \quad \frac{1}{4}(3x+z), \quad t, \quad \frac{1}{16}(15y^2 - z(2x+z)), \quad \frac{x^2-y^2}{8t}, \quad \frac{x+z}{2}. \tag{3.1}$$

Now suppose that L is a maximal integral form of V_{2A}, not equal to P. By Corollary 3.1.6, we may indeed write $L = \mathrm{span}_{\mathbb{Z}}(I, 4ta, w)$, where t is an integer and where $w = xa + \frac{y}{4}q + \frac{z}{4}I$ with $x, y, z \in \mathbb{Q}$ and where $0 \leqslant x < 2t$ and $0 \leqslant z < 4$. As we showed above, the six expressions given in (3.1) are integers.

We observe that x and z are integer linear combinations of these:

$$\begin{aligned}x &= -\left(\frac{x+z}{2}\right) + 2\left(\frac{1}{4}(3x+z)\right) \\ z &= 3\left(\frac{x+z}{2}\right) - 2\left(\frac{1}{4}(3x+z)\right).\end{aligned}$$

Therefore both x and z are integers. Then $t \in \mathbb{Z}$ and $(x^2 - y^2)/(8t) \in \mathbb{Z}$ imply $x^2 - y^2 \in \mathbb{Z}$ which implies that $y^2 \in \mathbb{Z}$. Since y is rational, $y \in \mathbb{Z}$.

Note that $(3x + z)/4 \in \mathbb{Z}$ implies that $x \equiv z \pmod 4$ and so $2x \equiv 2z, \pmod 8$. Then $(15y^2 - z(2x + z))/16 \in \mathbb{Z}$ implies $15y^2 \equiv z(2x + z) \equiv 3z^2 \pmod 8$, which implies $y^2 \equiv 5z^2$, (mod 8). Since 5 is not a perfect square modulo 8, it must be that z is not invertible modulo 8. So z is even.

Supposing $z = 0$, then $w \in (\mathbb{Q}a + \mathbb{Q}q) \cap L \subseteq P$, where the last inclusion follows from 3.1.3. It follows that $L \subseteq P$. Maximality of L implies $L = P$. So we may assume z is not zero. Then z is even and $0 < z < 4$, so $z = 2$.

Observe that t occurs only in three terms of the six expressions in (3.1) above: $-tz/4$, t, and $(x^2 - y^2)/(8t)$. It must be then that $\gcd(tz/4, t) = 1$ for if there were a prime p such that $tz/(4p)$ and t/p are integers, then $\mathrm{span}_{\mathbb{Z}}(I, 4ta/p, w)$ would be an integral form (because the 6 expressions given in (3.1) would still be integers with t/p substituted in place of t), and this integral form would be strictly larger than L. Now $1 = \gcd(tz/4, t) = \gcd(t/2, t)$ implies $t = 2$. Then we have $0 \leqslant x < 2t = 4$ and $x \equiv z \equiv 2 \pmod 4$ so $x = 2$.

Then $(x^2 - y^2)/(8t) = (4 - y^2)/16$ being an integer implies that $y^2 \equiv 4 \pmod{16}$, and:

$$y^2 \equiv 4 \pmod{16} \Leftrightarrow 16 \text{ divides } (y-2)(y+2) \Leftrightarrow y \equiv 2 \pmod 4.$$

To summarize, if L is a maximal integral form and $L \neq P$, then $L = \mathrm{span}_{\mathbb{Z}}(I, 8ta, 2a + \frac{y}{4}q + \frac{1}{2}I)$ where $y = 4m + 2$ for some integer m.

It is an easy verification that if $t = x = z = 2$ and $y = 4m + 2$ for an integer m, then the six expressions in (3.1) are integers. Therefore $L(m) = \mathrm{span}_{\mathbb{Z}}(I, 8a, 2a + (m + \frac{1}{2})q + \frac{1}{2}I)$ is an integral form for any integer m. □

Theorem 3.1.11. *There are three maximal integral forms in V_{2A}: P, $L(0)$, and $L(-1)$. If $\sigma(x)$ denotes the σ-involution associated to the axis x, then $L(0) = \sigma(a_1)P$ and $L(-1) = \sigma(a_\rho)P$.*

Proof. By the previous theorem, any maximal integral form equals P or $L(m)$ for some integer m. We will show that $L(0)$ and $L(-1)$ are the only maximal integral forms among the set of $\{L(m) : m \in \mathbb{Z}\}$. Set $w_m = 2a + (m + \frac{1}{2})q + \frac{1}{2}I$ so that $L(m) = \mathrm{span}_{\mathbb{Z}}(I, 8a, w_m)$. We in fact will show that $L(m) \subseteq L(0)$ if m is even, and $L(m) \subseteq L(-1)$ if m is odd. Compute the coefficients of w_m in the bases $\{I, 8a, w_0\}$ and $\{I, 8a, w_{-1}\}$: [★2A.5]

$$\begin{aligned} w_m &= -mI - \frac{m}{2}(8a) + (1+2m)w_0, \\ &= (1+m)I + \frac{m+1}{2}(8a) - (1+2m)w_{-1}. \end{aligned}$$

Therefore, if m is even, $w_m \in L(0)$ and if m is odd, then $w_m \in L(-1)$. Note that $w_m \in L(n)$ implies $L(m) \subseteq L(n)$. So $L(m)$ can only be maximal for $m = 0$ and $m = -1$.

If $p(t) = \frac{32}{3}t^2 - \frac{32}{3}t + 1$, then $p(0) = p(1) = 1$ and $p(1/4) = -1$. So the σ-involution associated to an axis a_x is given by $\sigma(a_x) = p(\mathrm{ad}(a_x))$. We verify computationally that $\sigma(a_1)P = L(0)$ and that $\sigma(a_\rho)P = L(-1)$ [★2A.6].

So by Lemma 3.1.10, any integral form of V_{2A} is contained in P, $L(0)$, or $L(-1)$, so at least one of these integral forms must be maximal. However, they are all conjugate under automorphisms of the algebra, so they are all maximal. $\square$

3.2 The 2B algebra

The 2B algebra has a basis of idempotents a_0, a_1 such that $a_0 \cdot a_1 = 0$. So V_{2B} is isomorphic to the algebra $\mathbb{Q}^2$. Since $\mathrm{ad}(a_0)$ and $\mathrm{ad}(a_1)$ do not have $1/32$ as an eigenvalue, the τ-involutions are trivial. Therefore every integral form will be G-invariant. The following result gives a list of all integral forms of $V_{2B} \cong \mathbb{Q}^2$.

Proposition 3.2.1. *For every rank 2 free-abelian subgroup A of $\mathbb{Q}^2$, there are unique rational numbers k, a, b with $0 \leqslant a < \min(k, b)$ such that $A = \mathbb{Z}(k, k) + \mathbb{Z}(a, b)$. Such a subgroup is a subring if and only if $k, a, b \in \mathbb{Z}$ and $k|ab$.*

Proof. There is a unique $k > 0$ such that $\mathbb{Z}(k, k) = \mathbb{Q}(1, 1) \cap A$. There are two cosets which generate the infinite cyclic group $A/\mathbb{Z}(k, k)$; let $(x, y) + \mathbb{Z}(k, k)$ be one generator and so the other is $(-x, -y) + \mathbb{Z}(k, k)$. If (k, k) and Z additively generate A, then $Z \in (x, y) + \mathbb{Z}(k, k) \cup (-x, -y) + \mathbb{Z}(k, k)$. There is a unique element (a, b) in $(x, y) + \mathbb{Z}(k, k) \cup (-x, -y) + \mathbb{Z}(k, k)$

such that $0 \leqslant a < k$ and $a < b$.

Let $A = \mathbb{Z}(k, k) + \mathbb{Z}(a, b)$ for some $a, b, k \in \mathbb{Q}$ with $0 \leqslant a < \min(b, k)$. If A is a ring then $k, a, b \in \mathbb{Z}$. Under the conditions that $a, b, k \in \mathbb{Z}$, A will be a ring if it contains (a^2, b^2) (since A is clearly closed under multiplication by (k, k)). Observe that $(a^2, b^2) = [a+b](a, b) - (ab, ab)$. Therefore, (a^2, b^2) is in A if and only if $(ab, ab) \in A$ which happens if and only if $k|ab$. $\square$

Note that this implies there is a unique maximal integral form in $V_{2B} \cong \mathbb{Q}^2$, namely $\mathrm{span}_{\mathbb{Z}}(a_0, a_1) \cong \mathbb{Z}^2$.

3.3 The 3A algebra

Notation 3.3.1. The 3A Norton-Sakuma algebra V_{3A} has a basis of idempotents a_{-1}, a_0, a_1 and u_ρ, with:

$$a_0 \cdot a_1 = 2^{-5}(2a_0 + 2a_1 - a_{-1}) - 2^{-11}3^3 5u_\rho,$$
$$a_0 \cdot u_\rho = 3^{-2}(2a_0 - a_1 - a_{-1}) + 2^{-5}5u_\rho.$$

([IPSS10, Table 3]) The subgroup G generated by τ-involutions fixes u_ρ and induces the dihedral group of order 6 on the set $\{a_{-1}, a_0, a_1\}$ of axes. This uniquely determines the remaining products [IPSS10, Lemma 2.20].

Since $\tau(a)a = a$ for any axis, this also implies that for any permutation p, q, r of $\{-1, 0, 1\}$, we have that $\tau(a_p)$ induces the involution in $\mathrm{Sym}(\{a_p, a_q, a_r\})$ that fixes a_p and interchanges a_q with a_r. Let $g = \tau(a_{-1})\tau(a_0)$. Then g cyclicly permutes the list (a_{-1}, a_0, a_1) one element to the right. Let I be the multiplicative identity in the algebra.

Lemma 3.3.2. *For $i = -1, 0, 1$, trace$(a_i) = \frac{41}{32}$. Also, trace$(u_\rho) = \frac{5}{3}$.*

Proof. With respect to the basis a_{-1}, a_0, a_1, u_ρ, the matrix of $\mathrm{ad}(a_{-1})$ has diagonal components $1, \frac{1}{16}, \frac{1}{16}, \frac{5}{32}$ and the matrix of $\mathrm{ad}(u_\rho)$ has diagonal components $\frac{2}{9}, \frac{2}{9}, \frac{2}{9}, 1$. Since each a_i is conjugate under the group of automorphism of V_{3A}, it follows that $\mathrm{trace}(a_i) = \mathrm{trace}(a_{-1}) = \frac{41}{32}$. $\square$

Definition 3.3.3. $L^G = \{l \in L : \; hl = l, \; \forall h \in G\}$ and $L^{G,\perp} = (L^G)^\perp$, where $\perp$ is defined with respect to the Killing form.

Proposition 3.3.4. *For a GIIF L of V_{3A}, $[L : L^G + L^{G,\perp}]$ is either 1 or 3.*

Proof. We first observe that $L^G = L^g$. For if $w = \alpha u_\rho + \sum_i \alpha_i a_i$, with $\alpha, \alpha_{-1}, \alpha_0, \alpha_1 \in \mathbb{Q}$, is g-invariant, then $\alpha_{-1} = \alpha_0 = \alpha_1$ and therefore w is G-invariant. This also shows that L/L^g has rank $4 - 2 = 2$. The result follows from 2.2.12. $\square$

Proposition 3.3.5. *For a GIIF L of V_{3A}, L^G is contained in* $\mathrm{span}_{\mathbb{Z}}(3u_\rho, I)$.

Proof. Thinking of V_{3A} as a module of $G \cong \mathrm{Sym}(3)$, V_{3A} decomposes as the permutation representation of $\mathrm{Sym}(3)$ $\mathrm{span}_{\mathbb{Q}}(a_{-1}, a_0, a_1)$ plus a one-dimensional trivial representation $\mathrm{span}_{\mathbb{Q}}(u_\rho)$. So the G-fixed points of V_{3A} are 2-dimension, spanned by I and u_ρ. The elements u_ρ and $I - u_\rho$ are idempotents which multiply to zero, so their rational span is an algebra isomorphic to $\mathbb{Q}^2$. The maximal rank 2 subring of $\mathbb{Q}^2$ is $\mathbb{Z}^2$, which corresponds to $\mathrm{span}_{\mathbb{Z}}(u_\rho, I - u_\rho) = \mathrm{span}_{\mathbb{Z}}(u_\rho, I)$.

So if $w = xu_\rho + yI$ is in a GIIF. Then $x, y \in \mathbb{Z}$. Using Lemma 3.3.2, we compute that $\mathrm{trace}(xu_\rho + yI) = \frac{5x}{3} + 4y$. (We can also verify this computationally [`★3A.1`].) This must be an integer, hence $x \in 3\mathbb{Z}$. So L^G is contained in $\mathrm{span}_{\mathbb{Z}}(3u_\rho, I)$. $\square$

Lemma 3.3.6. *Suppose W is a two dimensional $\mathbb{Q}[G]$-module (where $G = \langle g, t\rangle$ is the dihedral group of order 6, with $g^3 = t^2 = tgtg = 1$), such that g acts with minimal polynomial $x^2 + x + 1$. Let N be a G-invariant rank two free-abelian subgroup of W. Then every G-invariant rank two free-abelian subgroup of W is either sN or $s(g-1)N$ for some rational number s.*

Proof. Let M be a rank two G-invariant subgroup of W such that $M \neq sN$ for any $s \in \mathbb{Q}$. Choose $s \in \mathbb{Q}_{>0}$ such that $sN \subseteq M$ and $[M : sN]$ is minimal. Then M/sN is cyclic, since otherwise there would be elements $m_0, m_1 \in M$ and a prime p such that pm_0, pm_1 is a $\mathbb{Z}$-basis of sN, which would imply that $(s/p)N \subseteq M$, and this contradicting the minimality of $[M : sN]$.

Since the automorphism group of a cyclic group is abelian, the commutator subgroup $G' = \langle g \rangle$ acts trivially on M/sN. In other words, $(g-1)M \subseteq sN$.

Note that $(g-1)^2 = -3g + (1 + g + g^2)$ so $(g-1)^2 M = 3M$, and therefore $M = \frac{(g-1)^2}{3} M \subseteq \frac{s}{3}(g-1)N$.

The characteristic polynomial of g on W being $x^2 + x + 1$ implies that the characteristic polynomial of $g - 1$ on W is $(x+1)^2 + (x+1) + 1$ and therefore $g - 1$ acts with determinant 3 on W. We therefore have:

$$sN \subsetneq M \subseteq \frac{s}{3}(g-1)N \subsetneq \frac{s}{3}N.$$

Now $\left[\frac{s}{3}N : sN\right] = 9$, and the right-most containment has index 3. It follows that $M = \frac{s}{3}(g-1)N$. □

Definition 3.3.7. Define $n_0 = 2^6(a_1 - a_{-1})$ and $n_1 = 2^6(a_{-1} - a_0) = gn_0$. Let $N = \mathrm{span}_{\mathbb{Z}}(n_0, n_1)$.

These notations were chosen because n_i is negated by $\tau(a_i)$.

Proposition 3.3.8. *N is a G-submodule of V. For any GIIF L of V_{3A}, $L^{G,\perp}$ is either $\frac{k}{3}(g-1)N$ or kN for some $k \in \mathbb{Z}$.*

Proof. N is the intersection of two G-invariant subgroups: $2^6\mathrm{span}_{\mathbb{Z}}(a_{-1}, a_0, a_1)$ and the kernel of the trace map trace : $V_{3A} \to \mathbb{C}$. Therefore N is G-invariant. Note that N contains no elements fixed by G, so g acts on N with minimal polynomial $x^2 + x + 1$. The previous lemma applies to ensure that $L^{G,\perp}$ is either sN or $\frac{s}{3}(g-1)N$ a rational number s. We need only show that s must be an integer in these two cases.

Suppose sN is contained in GIIF of V_{3A} for some $s \in \mathbb{Q}$. We compute that trace$((sn_0) \cdot$

$(sn_1)) = -2^1 3^2 271^1 s^2$ and $\kappa(sn_0, sn_1) = -2^2 3^1 313^1 s^2$, both of which must be integers [$\bigstar$3A.2].

$2^1 3^2 271^1 s^2 \in \mathbb{Z}$ implies $3s \in \mathbb{Z}$, and $2^2 3^1 313^1 s^2 \in \mathbb{Z}$ implies $2s \in \mathbb{Z}$. Therefore $s \in \mathbb{Z}$.

Next, suppose that $L^{G,\perp} = \frac{s}{3}(g-1)N$ for some $s \in \mathbb{Q}$. Recall that $(g-1)^2 N = [-3g + (g^2+g+1)]N = 3N$, so $(g-1)L^{G,\perp} = sN$. By the previous paragraph, $s \in \mathbb{Z}$. □

Definition 3.3.9. For $i = 0, 1$, set $m_i = \frac{1}{3}(g-1)n_i$, and let $M = \operatorname{span}_{\mathbb{Z}}(m_0, m_1) = \frac{1}{3}(g-1)N$. So the previous proposition says that for any GIIF L, $L^{G,\perp}$ is either kM or kN for some integer k.

Proposition 3.3.10. *$P = M + 3\mathbb{Z}u_\rho + \mathbb{Z}I$ is a GIIF of V_{3A}.*

Proof. To show G-invariance, it is enough to show that M is G-invariant, since G acts trivially on I and u_ρ. Proposition 3.3.8 says that N is G-invariant. By definition $M = \frac{1}{3}(g-1)N$, so M is clearly invariant under g. Let $t \in G$ be an element of order 2 in G such that $tgt = g^{-1}$ and $G = \langle g, t\rangle$. Then we have:

$$tM = t \cdot \frac{1}{3}(g-1)N = \frac{1}{3}(g^{-1}-1)(tN) = -\frac{1}{3}(g-1)(-g^{-1}tN) = M.$$

We compute the matrix of $\operatorname{ad}(3u_\rho)$ and $\operatorname{ad}(m_0)$ with respect to the ordered basis $\mathcal{B} = (m_0, m_1, 3u_\rho, I)$ [$\bigstar$3A.3]:

$$[\operatorname{ad}(3u_\rho)]_{\mathcal{B}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad [\operatorname{ad}(m_0)]_{\mathcal{B}} = \begin{bmatrix} 20 & -20 & 1 & 1 \\ 0 & -20 & 0 & 0 \\ -156 & 78 & 0 & 0 \\ 1008 & -504 & 0 & 0 \end{bmatrix}.$$

Therefore $P = \operatorname{span}_{\mathbb{Z}}(\mathcal{B})$ is closed under multiplication by $3u_\rho$ and m_0. Since $gm_0 = m_1$ and P is invariant under the action of g, it follows that P is also closed under multiplication by m_1. So P is a ring. □

Lemma 3.3.11. *Suppose L is a maximal GIIF of V_{3A} with $[L : L^G + L^{G,\perp}] = 3$. Then there is some $\ell \in L^{G,\perp}$ and $k \in \mathbb{Z}$ such that the coset of $\frac{1}{3}\ell + 3ku_\rho$ generates $L/(L^G + L^{G,\perp})$.*

Proof. There is an element z in $L^G + L^{G,\perp}$ such that the coset of $\frac{1}{3}z$ generates $L/(L^G + L^G)$. Since $L^{G,\perp} \subseteq M$ and $L^G \subseteq \mathrm{span}_{\mathbb{Z}}(3u_\rho, I)$, we may write $z = am_0 + bm_1 + 3cu_\rho + dI$ for some integers a, b, c, d.

We compute $\mathrm{trace}(z) = 5c+4d$ and $\eta(z,z) = 3252a^2-3252ab+3252b^2+15c^2+10cd+4d^2$ [$\bigstar$`3A.4`]. Since $z/3 \in L$, $\mathrm{trace}(z) \in 3\mathbb{Z}$ and $\eta(z,z) = \mathrm{trace}(z \cdot z) \in 9\mathbb{Z}$.

$5c + 4d \in 3\mathbb{Z}$ implies $c \equiv d \pmod 3$. Then $\eta(z,z) \in 3\mathbb{Z}$ implies $cd + d^2 \in 3\mathbb{Z}$. Therefore $0 \equiv cd + d^2 \equiv 2d^2, \pmod 3$. So $c \equiv d \equiv 0, \pmod 3$.

Let $\ell = am_0 + bm_1 = z - dI - 3cu_\rho$. Since $d/3 \in \mathbb{Z}$ it follows that $\frac{d}{3}I \in L^G$. Therefore $z/3-d/3I = \frac{\ell}{3}+cu_\rho$ is equivalent to $z/3 \pmod{(L^G+L^{G,\perp})}$ and in particular, it also generates $L/(L^G + L^{G,\perp})$. Since $3|c$, it follows that $\frac{\ell}{3} + cu_\rho$ is the desired generator. □

Lemma 3.3.12. *$9u_\rho$ is in every maximal GIIF of V_{3A}.*

Proof. Let L be a maximal integral form of V_{3A}. If $L = L^G + L^{G,\perp}$, then $L^{G,\perp} \subseteq M$ (by 3.3.8) and $L^G \subseteq \mathbb{Z}I + \mathbb{Z}3u_\rho$ (by 3.3.5) so by maximality $L = \mathbb{Z}I + \mathbb{Z}3u_\rho + M$, since this is GIIF by 3.3.10. So we may suppose that $L \neq L^G + L^{G,\perp}$. By the previous lemma (3.3.11), let $z = \frac{\ell}{3} + 3ku_\rho$ be in L with $\ell \in L^{G,\perp}$ and $k \in \mathbb{Z}$ and such that $L = L^G + L^{G,\perp} + \mathbb{Z}z$. Note that $I \in L$ so by 3.2.1 and 3.3.5, $L^G = \mathbb{Z}I + \mathbb{Z}3tu_\rho$ for some $t \in \mathbb{Z}$.

We claim that $L' = \mathbb{Z}9u_\rho + L$ is still an integral form. Since L is a ring, it suffices to show that L' is closed under the action of $\mathrm{ad}(9u_\rho)$.

From Notation 6.1, one can check that $3u_\rho$ acts as the identity on $V^{G,\perp} = \mathrm{span}_{\mathbb{Z}}(a_0 - a_1, a_1 - a_{-1})$ (or we can check this computationally [$\bigstar$`3A.5`]). So $9u_\rho \cdot L^{G,\perp} = 3L^{G,\perp} \subset L'$, and $9u_\rho \cdot z = \ell + 27ku_\rho \in L'$. Clearly, L' contains $I \cdot 9u_\rho$. And L' contains $9u_\rho \cdot (3tu_\rho) = t(9u_\rho)$.

Therefore $9u_\rho \cdot L \subseteq L'$. And $(9u_\rho)^2 = 9(9u_\rho)$ finishes the proof that L' is a ring. By maximality, $L' = L$. □

Theorem 3.3.13. *$M + \mathbb{Z}I + \mathbb{Z}3u_\rho$ is the unique maximal GIIF in V_{3A}.*

Proof. $M + \mathbb{Z}I + \mathbb{Z}3u_\rho$ is a GIIF by 3.3.10, and by 3.3.5 and 3.3.8, it is the unique maximal GIIF L such that $L = L^G + L^{G,\perp}$.

Let L be a maximal GIIF such that $L \neq L^G + L^{G,\perp}$. By 3.3.4, the index of $L^G + L^{G,\perp}$ in L equals 3. By 3.3.11, there is an element $z = \frac{1}{3}(am_0 + bm_1) + 3cu_\rho$ with $a, b, c \in \mathbb{Z}$ such that $L = \mathbb{Z}z + L^G + L^{G,\perp}$. By the previous lemma, $9u_\rho \in L$, so we may replace z with a linear combination of z and $9u_\rho$ to ensure that $c = 1$, and still have that $L = \mathbb{Z}z + L^G + L^{G,\perp}$.

By 3.2.1 and 3.3.5, $L^G = \mathbb{Z}I + \mathbb{Z}3tu_\rho$ for some positive integer t. Since L^G contains $9u_\rho$ we must have that t divides 3. If $t = 1$, then $z \in L^G + L^{G,\perp}$, a contradiction. Therefore $t = 3$. Since $L^{G,\perp} \subseteq M$ (by 3.3.8 and Definition 3.3.9), we have $L^G + L^{G,\perp} \subseteq \mathrm{span}_{\mathbb{Z}}(m_0, m_1, 9u_\rho, I)$.

The quotient $L/(L^G + L^{G,\perp})$ is additively generated by the coset of z. So we may let k be such that $z \cdot z \equiv kz \pmod{L^G + L^{G,\perp}}$ with $0 \leqslant k < 3$. Then $z \cdot z - kz \in \mathrm{span}_{\mathbb{Z}}(m_0, m_1, 9u_\rho, I)$. We compute the coefficients of $z \cdot z - kz$ with respect to the basis $\{m_0, m_1, 9u_\rho, I\}$: `[★3A.6]`

$$
\begin{aligned}
z \cdot z - kz = & \frac{1}{9}\left(20a^2 - 40ab - 3ak + 6a\right)\, m_0 \\
& + \frac{1}{9}\left(6b - 40ab + 20b^2 - 3bk\right)\, m_1 \\
& + \frac{1}{9}(9 - 52a^2 + 52ab - 52b^2 - 3k)\,(9u_\rho) \\
& + 112(a^2 - ab + b^2)I.
\end{aligned}
$$

All of these coefficients are integers; in particular, the numerators of the first three must be integers divisible by 9. We want to analyze all integers a, b, k such that these three equivalences are satisfied:

$$
\begin{aligned}
20a^2 - 40ab - 3ak + 6a &\equiv 0, \quad \pmod 9, \\
6b - 40ab + 20b^2 - 3bk &\equiv 0, \quad \pmod 9, \\
9 - 52a^2 + 52ab - 52b^2 - 3k &\equiv 0, \quad \pmod 9.
\end{aligned}
$$

Computer verification shows that the solution is all a, b, k such that $a, b, k \in 3\mathbb{Z}$ `[★3A.7]`.

Therefore $z = (a/3)m_0 + (b/3)m_1 + 3u_3 \in M + \mathbb{Z}I + \mathbb{Z}3u_\rho$, and therefore $L \subseteq M + \mathbb{Z}I +$

$\mathbb{Z}3u_\rho$. $\square$

3.4 The 3C algebra

Notation 3.4.1. The 3C Norton-Sakuma algebra V_{3C} has a basis of axes (which are necessarily idempotents) a_{-1}, a_0, a_1 where for any choice of indices $\{i, j, k\} = \{-1, 0, 1\}$,

$$a_i \cdot a_j = 2^{-6}(a_i + a_j - a_k).$$

([IPSS10, Table 3])

The dihedral group G generated by the τ-involutions has order 6 by [IPSS10, 2.20], and so $\tau(a)$ cannot be trivial for any axis a, since there is an automorphism of the algebra acting transitively on the 3 axes. For any axis a, $\tau(a)a = a$. It follows then that $\tau(a_i)$ interchanges a_j with a_k. We define $g = \tau(a_{-1})\tau(a_0)$, so that $|g| = 3$ and g permutes cyclicly the list (a_{-1}, a_0, a_1) one space to the right.

Definition 3.4.2. Define $n_0 = 2^6(a_1 - a_{-1})$ and $n_1 = 2^6(a_{-1} - a_0) = gn_0$, and $N = \mathrm{span}_{\mathbb{Z}}(n_0, n_1)$. Again these notations were chosen because n_i is negated by $\tau(a_i)$.

For $i = 0, 1$ define $m_i = \frac{(g-1)}{3}n_i$ and $M = \mathrm{span}_{\mathbb{Z}}(m_0, m_1) = \frac{(g-1)}{3}N$.

Recall Definition 3.3.3, that $L^G = \{l \in L : \ hl = l, \ \forall h \in G\}$ is the set of elements in L fixed by G, and $L^{G,\perp} = (L^G)^\perp$ where the $\perp$ is with respect to the Killing form κ.

Lemma 3.4.3. *For a GIIF L of V_{3C}, $L^{G,\perp}$ is either sN or sM for some integer s.*

Proof. Note that N is G-invariant, since it is the intersection of $2^6\mathrm{span}_{\mathbb{Z}}(a_{-1}, a_0, a_1)$ with $\mathrm{trace}^{-1}(0)$.Also, elements in $(V_{3C})^G$ must be of the form $\lambda(a_{-1} + a_0 + a_1)$, and therefore $L^G \cap N = 0$. It follows that g (an element in G of order 3) acts with minimal polynomial $x^2 + x + 1$ on N.

The situation is analogous to the 3A case. In particular, Lemma 3.3.6 applies, proving that $L^{G,\perp}$ equals sN or $\frac{s}{3}(g-1)N = sM$ for some rational number s. It suffices to verify that s must be an integer in either of these two cases.

Suppose sN is contained in an integral form of V_{3C}. We compute $\eta(n_0, n_1) = -2^1 3^3 7^1 11^1$ and $\kappa(n_0, n_1) = -12^2 3^1 331^1$ [$\bigstar$`3C.1`].

Then $\eta(sn_0), sn_1) = -2^1 3^3 7^1 11^1 s^2 \in \mathbb{Z}$ implies $3s \in \mathbb{Z}$, and $\kappa(sn_0, sn_1) = -2^2 3^1 331^1 s^2 \in \mathbb{Z}$ implies $2s \in \mathbb{Z}$. Hence $s \in \mathbb{Z}$.

Next, suppose $sM = L^{G,\perp}$ for some rational s. Since $(g-1)^2 N = [-3g + (g^2 + g + 1)]N = 3N$, we have:

$$(g-1)L^{G,\perp} = (g-1)sM = \frac{s}{3}(g-1)^2 N = sN.$$

By the previous paragraph, $s \in \mathbb{Z}$. $\square$

Theorem 3.4.4. *$M + \mathbb{Z}I$ is the unique maximal GIIF of V_{3C}.*

Proof. Observe that to show $M + \mathbb{Z}I$ is G-invariant it suffices to prove that M is. In fact, for any G-invariant set S, $(g-1)S$ will also be G-invariant. To see this write $G = \langle g, t \rangle$ with t an element of order 2 such that $tgt = g^{-1}$. Then $t(g-1) = (g^{-1}-1)t = -(g-1)g^2 t$ and similarly $g(g-1) = (g-1)g$. This proves that $(g-1)S$ will be G-invariant, and in particular proves that $M = \frac{(g-1)}{3}N$ is G-invariant.

We will verify that $M + \mathbb{Z}I$ is an integral form by computing the matrix of $\mathrm{ad}(m_0)$ with respect to the basis $\mathcal{B} = (m_0, m_1, I)$ [$\bigstar$`3C.2`].

$$[\mathrm{ad}(m_0)]_{\mathcal{B}} = \begin{bmatrix} 20 & -20 & 1 \\ 0 & -20 & 0 \\ 924 & -462 & 0 \end{bmatrix}.$$

So $M + \mathbb{Z}I = \mathrm{span}_{\mathbb{Z}}(\mathcal{B})$ is closed under the multiplication by m_0. Since $M + \mathbb{Z}I$ is G-invariant and $gm_0 = \frac{1}{3}(g-1)(gn_0) = m_1$, it follows that $M + \mathbb{Z}I$ is closed under multiplication by m_1 as well. So $M + \mathbb{Z}I$ is a ring.

Let L be any maximal integral form, and fix any $w \in L$. Write $w = \alpha m_0 + \beta m_1 + \gamma I$ where $\alpha, \beta, \gamma \in \mathbb{Q}$. Then $\mathrm{trace}(w) = 3\gamma$ is an integer. Since $I \in L$ (Lemma 2.2.8), it follows that

$3w - 3\gamma I = 3\alpha m_0 + 3\beta m_1 \in L \cap \mathrm{span}_{\mathbb{Q}}(M) = L^{G,\perp}$.

By the previous lemma (Lemma 3.4.3), $L^{G,\perp} \subseteq M$. So 3α and 3β are integers. We compute $\mathrm{trace}(w \cdot w) = 2772\alpha^2 - 2772\alpha\beta + 2772\beta^2 + 3\gamma^2$, which must be an integer [✶`3C.3`].

Observe that 2772 is divisible by 9, so $2772\alpha^2$, $2772\alpha\beta$, and $2772\beta^2$ are integers. So $\mathrm{trace}(w \cdot w) \in \mathbb{Z}$ implies $3\gamma^2 \in \mathbb{Z}$ which in turn implies $\gamma \in \mathbb{Z}$.

Now $w - \gamma I = \alpha m_0 + \beta m_1 \in L \cap \mathrm{span}_{\mathbb{Q}}(M) = L^{G,\perp} \subseteq M$. Therefore $w \in M + \mathbb{Z}I$. Therefore $M + \mathbb{Z}I$ is the unique maximal GIIF. □

For the 3C case, we can say more about the GIIFs. The following is a classification all GIIFs in V_{3C}, partitioned into three 2-parameter families.

Proposition 3.4.5. *The set of GIIFs of V_{3C} is given by the following list, consisting of three types:*

$$
\begin{array}{lll}
sM + \mathbb{Z}tI & (s, t \in \mathbb{Z}_{>0}, & t | 462s^2), \\
sN + \mathbb{Z}tI & (s, t \in \mathbb{Z}_{>0}, & t | 1386s^2), \\
sN + \mathbb{Z}\left(\frac{sn_0 - sn_1}{3} + tI\right) & (s, t \in \mathbb{Z}_{>0}, & t | 462s^2 \quad \textit{and} \quad \left(\frac{462s^2}{t}\right) + s + t \equiv 0 \pmod{3})).
\end{array}
$$

Furthermore, no two distinct GIIFs on this list are equal.

Proof. Suppose L is a GIIF of V_{3C} with $L = L^G + L^{G,\perp}$. Then $L^G = \mathbb{Z}tI$ for some integer $t > 0$ and $L^{G,\perp}$ is either sN or sM (by 3.4.3) for a unique positive integer s. We need to verify that $sM + \mathbb{Z}tI$ and $sN + \mathbb{Z}tI$ are integral forms exactly under the conditions described.

The additive group $sM + \mathbb{Z}tI$ is an integral form if and only if it is closed under the action of $\mathrm{ad}(sm_0)$ and $\mathrm{ad}(sm_1)$. We compute the matrix of these endomorphisms with respect to the basis $\mathcal{M}(s,t)$ defined to be $\mathcal{M}(s,t) = \{sm_0, sm_1, tI\}$ [✶`3C.4`]:

$$
[\mathrm{ad}(sm_0)]_{\mathcal{M}(s,t)} = \begin{bmatrix} 20s & -20s & t \\ 0 & -20s & 0 \\ \frac{924s^2}{t} & -\frac{462s^2}{t} & 0 \end{bmatrix} \qquad \text{and} \qquad [\mathrm{ad}(sm_1)]_{\mathcal{M}(s,t)} = \begin{bmatrix} -20s & 0 & 0 \\ -20s & 20s & t \\ -\frac{462s^2}{t} & \frac{924s^2}{t} & 0 \end{bmatrix}
$$

With $s, t \in \mathbb{Z}_{>0}$, these entries are all integers if and only if t divides $462s^2$.

Similarly, $sN + \mathbb{Z}tI$ is a GIIF if and only if it is closed under the action of $\mathrm{ad}(sn_0)$ and $\mathrm{ad}(sn_1)$, and so we compute the matrices of these endomorphisms with respect to the basis $\mathcal{N}(s,t)$ defined to be $\{sn_0, sn_1, tI\}$ [$\bigstar$3C.5]:

$$[\mathrm{ad}(sn_0)]_{\mathcal{N}(s,t)} = \begin{bmatrix} 20s & 20s & t \\ 40s & -20s & 0 \\ \frac{2772s^2}{t} & -\frac{1386s^2}{t} & 0 \end{bmatrix} \quad \text{and} \quad [\mathrm{ad}(sn_1)]_{\mathcal{N}(s,t)} = \begin{bmatrix} 20s & 20s & t \\ 40s & -20s & 0 \\ \frac{2772s^2}{t} & -\frac{1386s^2}{t} & 0 \end{bmatrix}.$$

Since $s,t \in \mathbb{Z}_{>0}$, all of these coefficients are integers if and only if t divides $1386s^2$.

So every GIIF L with $L = L^G + L^{G,\perp}$ is one of the first two types, and each subgroup of the first two types is a GIIF.

So it remains to enumerate the GIIFs L of V_{3C} such that $L \supsetneq L^G + L^{G,\perp}$. Let L be a such a GIIF. First I claim that $[L : L^G + L^{G,\perp}]$ divides 3. To see this, note that $V_{3C}^g = \mathbb{Q}I = V_{3C}^G$. Therefore g acts without fixed points on L/L^G. Since $|g| = 3$ and g acts nontrivially, g acts with charactersistic polynomial $x^2 + x + 1$ on L/L^G. Hence $g - 1$ acts with determinant 3 on L/L^G. So $(g-1)L + L^G$ has index 3 in L. This completes the claim, since $(g-1)L$ is orthogonal to L^G and so equals $L^{G,\perp}$.

Clearly, $L/L^{G,\perp}$ is torsion free (for if $x \in L$ and $nx \in L^{G,\perp}$ then $x \perp L^G$ hence $x \in L^{G,\perp}$) so any $\mathbb{Z}$-basis of $L^{G,\perp}$ can be extended to a basis of L.

Consider the case that $L^{G,\perp} = sM$. Let sm_0, sm_1, w be a $\mathbb{Z}$-basis of L (extended from the $\mathbb{Z}$-basis of $L^{G,\perp}$). We may write $w = \frac{\alpha}{3} sm_0 + \frac{\beta}{3} sm_1 + tI$ for some $t \in \mathbb{Q}$ and some integers α, β (because $3w \in L^G + L^{G,\perp}$). Furthermore, we may add elements in sM to w to ensure that $\alpha, \beta \in \{0,1,2\}$ (and not both zero, since then $L = sM + \mathbb{Z}tI$). We now compute the matrices of $\tau(a_{-1})$ and $\tau(a_0)$ with respect to the basis sm_0, sm_1, w [$\bigstar$3C.6]:

$$[\tau(a_0)]_{(sm_0,sm_1,w)} = \begin{bmatrix} 1 & -1 & -\frac{\beta}{3} \\ 0 & -1 & -\frac{2\beta}{3} \\ 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad [\tau(a_{-1})]_{(sm_0,sm_1,w)} = \begin{bmatrix} -1 & 0 & -\frac{1}{3}(2\alpha) \\ -1 & 1 & -\frac{\alpha}{3} \\ 0 & 0 & 1 \end{bmatrix}$$

For these entries to all be integers clearly 3 divides both α and β. So $\alpha = \beta = 0$, which would imply $L = sM + \mathbb{Z}tI = L^G + L^{G,\perp}$, a contradiction. Therefore, there is no such GIIF L with $L \neq L^G + L^{G,\perp}$ and $L^{G,\perp} = sM$.

Finally, we consider the case that $L \neq L^G + L^{G,\perp}$ and $L^{G,\perp} = sN$. As before, we may extend the basis sn_0, sn_1 of $L^{G,\perp}$ to a $\mathbb{Z}$-basis sn_0, sn_1, w of L. In fact, by adding multiples of sn_0 or sn_1 if necessary, we may assume that there exists such a w with $w = \frac{\alpha}{3} sn_0 + \frac{\beta}{3} sn_1 + tI$, for some $\alpha, \beta \in \{-1, 0, 1\}$ and $t \in \mathbb{Q}$. We compute the matrix of $\tau(a_{-1})$ and $\tau(a_0)$ with respect to the basis sn_0, sn_1, w [✶`3C.7`]:

$$[\tau(a_0)]_{(sn_0, sn_1, w)} = \begin{bmatrix} -1 & 1 & \frac{1}{3}(\beta - 2\alpha) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad [\tau(a_{-1})]_{(sn_0, sn_1, w)} = \begin{bmatrix} 0 & -1 & \frac{1}{3}(-\alpha - \beta) \\ -1 & 0 & \frac{1}{3}(-\alpha - \beta) \\ 0 & 0 & 1 \end{bmatrix}$$

We see that $\mathrm{span}_{\mathbb{Z}}(sn_0, sn_1, w)$ is invariant under $\langle \tau(a_{-1}), \tau(a_0) \rangle = G$ if and only if $\alpha \equiv -\beta \pmod 3$, which implies $\alpha = -\beta$. So $\alpha = -\beta \neq 0$ or else $w = tI$ and $L = L^G + L^{G,\perp}$. Without loss of generality, we may take $\alpha = -\beta = 1$, for if not, then replace w by $-w$.

Define the ordered basis $\mathcal{B}(s,t) = (sn_0, sn_1, \frac{sn_0 - sn_1}{3} + tI)$ and set $B(s,t) = \mathrm{span}_{\mathbb{Z}}(\mathcal{B}(s,t))$. The computation done above shows that $B(s,t)$ is G-invariant. We have shown that any GIIF L with $L \neq L^G + L^{G,\perp}$ equals $B(s,t)$ for some integers $s, t > 0$. It suffices now to show that $B(s,t)$ is an integral form exactly under the conditions described in the statement of the proposition.

The element $\tau(a_1) \in G$ acts on $B(s,t)$ by interchanging $n_0 = 64(a_{-1} - a_1)$ with $-n_1 = 64(a_{-1} - a_0)$ and by fixing I. So $B(s,t)$ will be closed under $\mathrm{ad}(sn_0)$ if and only if it is closed under $\mathrm{ad}(sn_1)$.

So $B(s,t)$ will be an integral form if and only if the matrices of $\mathrm{ad}(sn_0)$ and $\mathrm{ad}(w)$ [where $w = \frac{1}{3}(sn_0 - sn_1) + tI$] with respect to the basis $\mathcal{B}(s,t) = (sn_0, sn_1, w)$ have integer components. We compute these matrices here:

$$[\mathrm{ad}(sn_0)]_{\mathcal{B}(s,t)} = \begin{bmatrix} 20s - \frac{924s^2}{t} & \frac{462s^2}{t} + 20s & t - \frac{462s^2}{t} \\ \frac{924s^2}{t} + 40s & -\frac{462s^2}{t} - 20s & \frac{462s^2}{t} + 20s \\ \frac{2772s^2}{t} & -\frac{1386s^2}{t} & \frac{1386s^2}{t} \end{bmatrix}$$

and

$$[\mathrm{ad}(w)]_{\mathcal{B}(s,t)} = \begin{bmatrix} t - \frac{462s^2}{t} & \frac{462s^2}{t} + 20s & -\frac{308s^2}{t} - \frac{20s}{3} + \frac{t}{3} \\ \frac{462s^2}{t} + 20s & t - \frac{462s^2}{t} & \frac{308s^2}{t} + \frac{20s}{3} - \frac{t}{3} \\ \frac{1386s^2}{t} & -\frac{1386s^2}{t} & \frac{924s^2}{t} + t \end{bmatrix}$$

These 18 expressions being integers is equivalent to the following two expressions being integers: $462s^2/t$ and $-((20s)/3) - (308s^2)/t + t/3$. These two are sufficient because in the 16 expressions that do not equal $-(20s)/3 - (308s^2)/t + t/3$, the only possibly non-integer terms are integer multiples of $462s^2/t$: namely $924s^2/t$, $1386s^2/t$, and $2772s^2/t$.

If $462s^2/t$ is an integer, then $-((20s)/3) - (308s^2)/t + t/3 \in \mathbb{Z}$ if and only if $(s+t)/3 + 152s^2/t \in \mathbb{Z}$; this is because the difference of these two is $7s + 462s^2/t$. The condition $(s+t)/3 + 152s^2/t \in \mathbb{Z}$ is equivalent to $\frac{s+t+462s^2/t}{3} \in \mathbb{Z}$, i.e. $s + t + (462s^2/t) \equiv 0 \pmod 3$.

So $B(s,t)$ ($s, t \in \mathbb{Z}_{>0}$) is a GIIF if and only if $t|462s^2$ and $s + t + (462s^2/t) \equiv 0 \pmod 3$.

It remains to prove that no two of the three types of GIIF in the list are equal. Let L be a GIIF. If $L^{G,\perp} = sM$ for a positive integer s, then it is of the first type, s is uniquely determined by L, and t is equal to $1/3$ times the unique positive additive generator of the image of trace : $L \to \mathbb{Z}$.

If $L^{G,\perp} = sN$ for a positive integer s and $L = L^G + L^{G,\perp}$, then L is of the second type, s is uniquely determined by L, and t again equals $1/3$ the unique positive generator of the image of trace : $L \to \mathbb{Z}$.

If $L^{G,\perp} = sN$ for a positive integer s and $L \neq L^G + L^{G,\perp}$, then L is of the third type, s is uniquely determined by L, and t again is $1/3$ the unique positive generator of the image of trace : $L \to \mathbb{Z}$. □

3.5 The 4A algebra

Notation 3.5.1. The Norton-Sakuma algebra V_{4A} of type 4A has a basis consisting of four axes a_{-1}, a_0, a_1, a_2 and another (non-axis) idempotent v_ρ, satisfying:

$$\begin{aligned}
a_0 \cdot a_1 &= 2^{-6}(3a_0 + 3a_1 + a_2 + a_{-1} - 3v_\rho) \\
a_0 \cdot a_2 &= 0. \\
a_0 \cdot v_\rho &= 2^{-4}(5a_0 - 2a_1 - a_2 - 2a_{-1} + 3v_\rho).
\end{aligned}$$

([IPSS10, Table 3]). There is an automorphism σ of the algebra that fixes v_ρ and cyclicly permutes the list (a_{-1}, a_0, a_1, a_2) one space to the right. This uniquely determines the remaining products. [IPSS10, 2.20].

Compute the matrix of $\tau(a_0)$ with respect to this given basis $\mathcal{B}$ of V_{4A}, and this verifies that $\tau(a_0)$ fixes a_0, a_2, and v_ρ and it interchanges a_{-1} with a_1 [★`4A.1`]:

$$[\tau(a_0)]_{\mathcal{B}} = \begin{bmatrix} 0&0&1&0&0 \\ 0&1&0&0&0 \\ 1&0&0&0&0 \\ 0&0&0&1&0 \\ 0&0&0&0&1 \end{bmatrix}$$

Define a_i for any $i \in \mathbb{Z}$ by defining $a_i = a_{i+4}$ for all $i \in \mathbb{Z}$; in other words, we only consider the subscripts of a_i modulo 4. If $\sigma \in \mathrm{Aut}(V)$ then $\tau(a_0)$ is a polynomial in $\mathrm{ad}(a_0)$ (B.2.2), and therefore $\sigma(\tau(a_0)v) = \tau(\sigma a_0)(\sigma v)$. Take σ to be the automorphism of V such that $a_i \mapsto a_{i+1}$ $(i = -1, 0, 1, 2)$ and which fixes v_ρ. Repeatedly applying σ shows that $\tau(a_i)$ fixes a_i, a_{i+2} and v_ρ and interchanges a_{i-1} with a_{i+1}.

In particular then, $\tau(a_0) = \tau(a_2)$ and $\tau(a_1) = \tau(a_{-1})$. Define $\tau_0 = \tau(a_0) = \tau(a_2)$ and set $\tau_1 = \tau(a_{-1}) = \tau(a_1)$. Note that $\tau_1\tau_0 = \tau_0\tau_1$. So $G = \langle \tau_0, \tau_1 \rangle \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Definition 3.5.2. For any finite abelian group A and any $\mathbb{Z}[A]$-module L, define the *total eigenlattice* $\textsc{tel}(L, A) = \sum_{\chi \in \mathrm{Hom}(A, \mathbb{C}^*)} L^\chi$, where $L^\chi = \{x \in L : \ a \cdot x = \chi(a)x \,\forall a \in A\}$. This makes $\textsc{tel}(L, A)$ into an $\mathrm{Hom}(A, \mathbb{C}^*)$-graded algebra.

Definition 3.5.3. For $i = 0, 1$ define $n_i = 4(a_{i-1} - a_{i+1})$ and $f_i = n_i^2 = 16(a_{i-1} + a_{i+1})$.

For brevity, for any selection of symbols $\epsilon_i \in \{+, -\}$ we let $L^{\epsilon_0,\epsilon_1}$ denote L^χ where χ is the linear character of G defined by $\chi(\tau_i) = \epsilon_i 1$ for $i = 0, 1$. So $n_0 \in (V_{4A})^{-,+}$ because $\tau_0(n_0) = -n_0$ and $\tau_1(n_0) = n_0$. Similarly, $n_1 \in (V_{3A})^{+,-}$. Using the $\mathrm{Hom}(G, \mathbb{C}^*)$-grading, we have $f_i \in (V_{3A})^{+,+}$. These notations were chosen because the n terms are *negated* and the f terms are *fixed*.

Proposition 3.5.4. *For either permutation of indices $\{i, j\} = \{0, 1\}$, the following products hold in V_{4A}:*

$$\begin{aligned} n_i \cdot n_i &= f_i & \qquad n_j \cdot n_i &= 0 \\ f_i \cdot n_i &= 16n_i & \qquad f_j \cdot n_i &= n_i \\ f_i \cdot f_i &= 16f_i & \qquad f_j \cdot f_i &= 8f_i + 8f_j - 120I. \end{aligned}$$

and

$$\tau_i(n_i) = -n_i \qquad\qquad \tau_i(n_j) = n_j.$$

Each of f_0 and f_1 is fixed by G.

Proof. Recall that σ is the automorphism of V sending $a_i \mapsto a_{i+1}$ (with the indices considered modulo 4) and which fixes v_ρ. Then $\sigma(n_0) = n_1$, $\sigma(n_1) = -n_0$ and σ interchanges f_0 with f_1. It follows that $\tau_0 \circ \sigma$ interchanges n_0 with n_1 and interchanges f_0 with f_1. Therefore it suffices to prove the desired products for $i = 0$ and $j = 1$.

Note that $n_0^2 = f_0$ by definition. We verify the remaining five products by computer calculation [`★4A.2`]. □

Corollary 3.5.5. *The list (I, f_0, f_1, n_0, n_1) is a $\mathbb{Q}$-basis of V_{4A}. For $i = 0$ or 1, trace$(f_i) = 41$ and trace$(n_i) = 0$.*

Proof. When expressed in the basis $a_{-1}, a_0, a_1, a_2, v_\rho$, it is evident that the list of 5 elements are linearly independent:

$$\begin{aligned} I &= \frac{4}{5}(a_{-1} + a_0 + a_1 + a_2) + \frac{2}{5}v_\rho, \\ f_0 &= 16(a_{-1} + a_1), \\ f_1 &= 16(a_0 + a_2), \\ n_0 &= 4(a_{-1} - a_1), \\ n_1 &= 4(a_0 - a_2). \end{aligned}$$

With respect to this ordered basis, the trace of f_i can be computed from the computations previous result: the components along the diagonal of the matrix of $\mathrm{ad}(f_i)$ are 0,16,8,16,1 which sum to 41. We can see directly that $n_i = 4(a_{i-1} - a_{i+1})$ has trace 0, since each a_j is conjugate under the automorphism group of V_{4A}. □

Proposition 3.5.6. *Define $F = \mathrm{span}_{\mathbb{Z}}(f_0, f_1, I)$. For a GIIF L of V_{4A}, $L^{+,+} \subseteq F$.*

Proof. $(V_{4A})^{+,+}$ is three dimensional, with $\mathbb{Q}$-basis f_0, f_1, I (by Corollary 3.5.5).

The adjoint action of any $v \in (V_{4A})^{+,+}$ fixes the one-dimensional subspaces $(V_{4A})^{-,+} = \mathbb{Q}n_0$ and $(V_{4A})^{+,-} = \mathbb{Q}n_1$. For $i = 0, 1$, we define the linear functional $\lambda_i : V^{+,+} \to \mathbb{R}$ by the formula $v \cdot n_i = \lambda_i(v)n_i$. And for clarity of notation in what follows, define $\lambda_t : V^{+,+} \to \mathbb{Q}$ by $\lambda_t(v) = \mathrm{Tr}(\mathrm{ad}(v))$. Using the products in 3.5.4, we compute:

$$\lambda_0(f_0) = 16 \qquad \lambda_0(f_1) = 1 \qquad \lambda_0(I) = 1 \tag{3.2}$$

$$\lambda_1(f_0) = 1 \qquad \lambda_1(f_1) = 16 \qquad \lambda_1(I) = 1 \tag{3.3}$$

$$\lambda_t(f_0) = 41 \qquad \lambda_t(f_1) = 41 \qquad \lambda_t(I) = 5. \tag{3.4}$$

But then:

$$\det\begin{pmatrix}16 & 1 & 1\\ 1 & 16 & 1\\ 41 & 41 & 5\end{pmatrix} = 45. \tag{3.5}$$

This being nonzero gives another proof that that f_0, f_1, and I are linearly independent in $(V_{4A})^{+,+}$ and also that λ_0, λ_1, λ_t is linearly independent in the dual space $[(V_{4A})^{+,+}]^*$. Let v_0, v_1, v_t be a basis of $(V_{4A})^{+,+}$ dual to the basis $\lambda_0, \lambda_1, \lambda_t$ of $[(V_{4A})^{+,+}]^*$.

Let L be a G-invariant integral form. Define $W = \operatorname{span}_{\mathbb{Z}}(v_0, v_1, v_t)$. We aim to show that $L^{+,+} \subseteq W$. Suppose $w \in L^{+,+}$. Write $w = av_0 + bv_1 + cv_t$ for some $a, b, c \in \mathbb{Q}$. Then:

$$w \cdot f_0 = af_0 \qquad w \cdot f_1 = bf_1 \qquad \operatorname{trace}(w) = c.$$

Since w is in a integral form, a, b, and c are integers (by Proposition 2.1.5). Thus $w \in W$, as desired.

Note that $L^{+,+}$ is a subalgebra of L. So w^2 is also in W. We compute the coefficients of w^2 in this basis v_0, v_1, v_t. (To do this in Mathematica, we first define $v = \alpha_0 f_0 + \alpha_1 f_1 + \alpha_3 I$, and then solve for the scalars α_i needed for v to equal v_j for $(j = 0, 1, t)$. [★4A.3])

$$\begin{aligned} w \cdot w =& \frac{1}{15}\left(159a^2 + 24a(13b - 5c) + (13b - 5c)^2\right)\ v_0 \\ &+ \frac{1}{15}\left(169a^2 + 26a(12b - 5c) + 159b^2 - 120bc + 25c^2\right)\ v_1 \\ &+ \left[\frac{1}{3}(169a^2 + 322ab + 169b^2) - 44(a + b)c + 9c^2\right]\ v_t \end{aligned}$$

These three coefficients must be integers. In particular, the first value being an integer implies that 3 must divide $(13b - 5c)^2$, or equivalently $b \equiv -c, \pmod 3$.

The second value being an integer implies that 5 divides $169a^2 + 159b^2 + 26a(12b)$, which can be simplified to:

$$0 \equiv 169a^2 + 159b^2 + 26a(12b) \equiv -a^2 - b^2 + 2ab \equiv -(a-b)^2 \pmod 5$$

So $a \equiv b \pmod 5$.

The third value being an integer implies that 3 divides $169a^2 + 322ab + 169b^2$, which gives

$$0 \equiv 169a^2 + 322ab + 169b^2 \equiv a^2 + ab + b^2 \equiv (a-b)^2 \pmod 3.$$

So $a \equiv b, \pmod 3$.

Let $F' = \{av_0 + bv_1 + cv_t : \ a, b, c \in \mathbb{Z} \text{ with } a \equiv b \pmod{15} \text{ and } b \equiv -c \pmod 3\}$. We have shown that for any GIIF L, $L^{+,+} \subseteq F'$.

It suffices to show that $F' = F$. Note that $F \subseteq F'$, since $F + \mathbb{Z}n_0 + \mathbb{Z}n_1$ is an integral form (by 3.5.4), and F is its G-fixed point subalgebra.

Define a $\mathbb{Z}$-linear map $W \to \mathbb{Z}/15\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ by $av_0 + bv_1 + cv_t \mapsto (a - b \pmod{15},\ b + c \pmod 3)$. This is surjective, with kernel F'. So $[W : F'] = 45$.

The computation done in (3.2) shows that:

$$f_0 = 16v_0 + v_1 + 41v_t,$$

$$f_1 = v_0 + 16v_1 + 41v_t,$$

$$I = v_0 + v_1 + 5v_t,$$

and the determinant computed in (3.5) shows that $[W : F] = 45$. So $W \subseteq F \subseteq F'$, and $[F : W] = [F' : W]$. Therefore $F = F'$, which completes the proof. □

The following is essentially a restatement of Lemma A.2 in [GL11] (This article was originally announced in [GL08]) with a twist by an automorphism. The proof is a modified version of the proof found there. First some notation:

Notation 3.5.7. For an additive group A and some $r \in \operatorname{End}(A)$, define $A^r = \{a \in A : ra = a\}$. This can be iterated: for example, $A^{r,-s} = \{a \in A : ra = a \text{ and } sa = -a\}$.

Lemma 3.5.8. *Suppose that a four group $D = \langle r, s \rangle \cong (\mathbb{Z}/2\mathbb{Z})^2$ acts on the abelian group A. If If $A^{-r,-s} = 0$ then $A/\operatorname{TEL}(A, D)$ is an elementary abelian 2-group.*

Proof. For $a \in A$, $(s-1)(r-1)a \in A^{-r,-s} = 0$.

From this we can conclude several things. First, $(r-1)a \in A^{-r,s}$ and similarly $(s-1)a \in A^{r,-s}$. We can also conclude that:

$$(r-1)(r+s)a = (1 + rs - r - s)a = (r-1)(s-1)a = 0.$$

Similarly, $(s-1)(r+s)a = 0$. Therefore $(r+s)a \in A^{r,s}$.

The proof is complete by noting that $2a = -(r-1)a - (s-1)a + (r+s)a \in \operatorname{TEL}(A, D)$. □

Corollary 3.5.9. *For any rank 5 G-invariant discrete subgroup L of the V_{4A}, the quotient $L/\operatorname{TEL}(L, G)$ is isomorphic to a subgroup of the Klein four group.*

Proof. Note that $L^{-,-} = 0$ as can be seen by noting that V_{4A} is five dimensional and $\dim V_{4A}^{+,+} + \dim V_{4A}^{-,+} + \dim V_{4A}^{+,-} = 3 + 1 + 1 = 5$ by Proposition 3.5.4. So we can apply the previous lemma to conclude that $L/\operatorname{TEL}(L, G)$ is an elementary abelian 2-group.

The $\mathbb{Q}$-basis f_0, f_1, I, n_0, n_1 of V_{4A} gives rise to a full flag of V_{4A}. By Lemma 2.1.4, there is a $\mathbb{Z}$-basis of L compatible with this flag. The first three elements in this basis are in L^G, hence the rank of $L/\operatorname{TEL}(L, G)$ is at most two. □

Theorem 3.5.10. $\mathbb{Z}n_0 + \mathbb{Z}n_1 + F$ *is the unique maximal GIIF in* V_{4A}.

Proof. Let L be a maximal GIIF of V_{4A}. Write $\operatorname{TEL}(L, G) = \mathbb{Z}s_0n_0 + \mathbb{Z}s_1n_1 + L^{+,+}$ for some $s_0, s_1 \in \mathbb{Q}$. By 3.5.6, $L^{+,+} \subseteq F$. The products in 3.5.4 show that (for $i = 0, 1$) $(s_in_i)^2 = s_i^2 f_i$, which is an element in $L^{+,+} \subseteq F$. Since f_0 and f_1 are primitive elements of the free abelian group F, we have $s_0^2, s_1^2 \in \mathbb{Z}$ which implies $s_0, s_1 \in \mathbb{Z}$. Therefore $\operatorname{TEL}(L, G) \subseteq \mathbb{Z}n_0 + \mathbb{Z}n_1 + F$.

So if $L = \textsc{tel}(L, G)$ we are done. If not, let $w \in L$ with $w \notin \textsc{tel}(L, G)$. By 3.5.9, $2w \in \textsc{tel}(L, G) \subseteq \mathbb{Z}n_0 + \mathbb{Z}n_1 + F$, so we may write $w = \frac{1}{2}(an_0 + bn_1 + cf_0 + df_1 + eI)$ where $a, b, c, d, e \in \mathbb{Z}$. By maximality, $I \in L$ (Lemma 2.2.8). Adding an integer multiple of I to w if necessary, we may assume that $e \in \{0, 1\}$.

Note that $w \cdot w \in L$ so $2w \cdot w \in \textsc{tel}(L, G) \subseteq \mathbb{Z}n_0 + \mathbb{Z}n_1 + F$. We compute the coefficients of $2w \cdot w$ with respect to the basis n_0, n_1, f_0, f_1, I [✶`4A.4`]:

$$\begin{aligned}2w \cdot w =& (16ac + ad + ae)\ n_0 + (bc + 16bd + be)\ n_1 \\ &+ \left(\frac{a^2}{2} + 8c^2 + 8cd + ce\right)\ f_0 + \left(\frac{b^2}{2} + 8cd + 8d^2 + de\right)\ f_1 + \left(\frac{e^2}{2} - 120cd\right)\ I\end{aligned}$$

All 5 of these coefficients must be integers. Therefore $a, b, e \in 2\mathbb{Z}$. Thus $e = 0$. Under the condition that $e = 0$, we compute $\kappa(w, w)$ [✶`4A.5`]:

$$\kappa(w, w) = 8a^2 + 8b^2 + \frac{577c^2}{4} + 56cd + \frac{577d^2}{4}$$

This is an integer if and only if $c^2 + d^2 \equiv 0 \pmod 4$ which happens if and only if $c, d \in 2\mathbb{Z}$. This completes the proof that $w \in \mathbb{Z}n_0 + \mathbb{Z}n_1 + F$. □

‘

3.6 The 4B algebra

Notation 3.6.1. The 4B Norton-Sakuma algebra V_{4B} has a basis of axes a_{-1}, a_0, a_1, a_2 and a_{ρ^2}, with:

$$\begin{aligned}a_0 \cdot a_1 &= 2^{-6}(a_0 + a_1 - a_{-1} - a_2 + a_{\rho^2}), \\ a_0 \cdot a_2 &= 2^{-3}(a_0 + a_2 - a_{\rho^2}), \\ a_0 \cdot a_{\rho^2} &= 2^{-3}(a_0 + a_{\rho^2} - a_2).\end{aligned}$$

([IPSS10, Table 3]) There is an algebra automorphism ϕ of V_{4B} fixing a_{ρ^2} and cyclicly permuting the list (a_{-1}, a_0, a_1, a_2) one space to the right; this determines the remaining products [IPSS10, 2.20].

Define $\tau_i = \tau(a_i)$. We compute the matrix of τ_0 with respect to the given basis $\mathcal{B}$ of V_{4B}, and this verifies that τ_0 fixes $a_0,\ a_2,$ and a_{ρ^2} and it interchanges a_{-1} with a_1 [$\bigstar$`4B.1`].

$$[\tau(a_0)]_{\mathcal{B}} = \begin{bmatrix} 0&0&1&0&0 \\ 0&1&0&0&0 \\ 1&0&0&0&0 \\ 0&0&0&1&0 \\ 0&0&0&0&1 \end{bmatrix}$$

Since $\tau(a)$ is a polynomial in $\mathrm{ad}(a)$ (Lemma 2.2.9), we have that $\phi \circ \tau(a) = \tau(\phi(a)) \circ \phi$. Applying ϕ repeatedly shows that $\tau(\phi^k a_0)$ fixes $\phi^k a_0,\ \phi^{k+2} a_0$, and a_{ρ^2} and it interchanges $\phi^{k-1} a_0$ with $\phi^{k+1} a_0$.

In particular, $\tau_0 = \tau_2$ fixes a_0 and a_2 and interchanges a_{-1} with a_1, and similarly $\tau_{-1} = \tau_1$ fixes a_{-1} and a_1 and interchanges a_0 with a_2. We use a computer to verify that $\tau(a_{\rho^2})$ acts trivially [$\bigstar$`4B.2`]. Therefore $G = \langle \tau_0, \tau_1 \rangle$ is isomorphic to the four group.

Recall Definition 3.5.2 which for finite abelian group A acting on a finite rank free group L, defines the total eigenlattice $\textsc{tel}(L, A) = \sum_{\chi \in \mathrm{Hom}(A, \mathbb{C}^*)} L^{\chi}$. For any GIIF L, $\textsc{tel}(L, G)$ is a $\mathrm{Hom}(G, \mathbb{C}^*)$-graded subrng of L.

Definition 3.6.2. For $i = 0, 1$ define $n_i = 8(a_{i-1} - a_{i+1})$ and $f_i = \frac{1}{60} n_i^2 - \frac{7}{15} a_{\rho^2}$.

For brevity, we denote by (ϵ_0, ϵ_1) with $\epsilon_i \in \{+, -\}$, the linear character χ of G defined by $\chi(\tau_i) = \epsilon_i 1$ for $i = 0, 1$. So $n_0 \in V^{-,+}$ and $n_1 \in V^{+,-}$. Using the $\mathrm{Hom}(G, \mathbb{C}^*)$-grading, we have $f_i \in V^{+,+}$ for $i = 0, 1$. These notations were chosen because the n terms are *negated* and the f terms are *fixed.*

Lemma 3.6.3. *For either permutation of indices* $\{i, j\} = \{0, 1\}$*, the following products hold* *in V_{4B}:*

$$
\begin{aligned}
n_i \cdot n_i &= 32f_i - 28f_j + 28I & \qquad n_j \cdot n_i &= 0 \\
f_i \cdot n_i &= \frac{3}{4}n_i & f_j \cdot n_i &= 0 \\
f_i \cdot f_i &= f_i & f_j \cdot f_i &= 0
\end{aligned}
$$

Proof. Let ϕ be the automorphism of V_{4B} that sends $a_i \mapsto a_{i+1}$ for $i = -1, 0, 1$, sends $a_2 \mapsto a_{-1}$ and which fixes a_{ρ^2}. Then $\phi(n_0) = n_1$, $\phi(n_1) = -n_0$ and ϕ interchanges f_0 with f_1. It follows that $\tau_0 \circ \phi$ interchanges n_0 with n_1 and interchanges f_0 with f_1. Therefore it suffices to prove the desired products for $i = 0$ and $j = 1$. We verify the six products by computer calculation [★`4B.3`]. □

Proposition 3.6.4. *f_0, f_1, and a_{ρ^2} are three idempotents whose pairwise products are zero. Therefore $V^{+,+}$ is associative and isomorphic to $\mathbb{Q}^3$ as a ring. And $I = f_0 + f_1 + a_{\rho^2}$.*

Proof. We verify that $I = f_0 + f_1 + a_{\rho^2}$ [★`4B.4`]. The previous result shows that f_0 and f_1 are idempotents whose product is zero, and a_{ρ^2} is an idempotent (since it is an axis). Finally, we compute $f_i \cdot a_{\rho^2} = f_i(I - f_0 - f_1) = f_i - f_i = 0$ for $i = 0, 1$.

This also shows that f_0, f_1, a_{ρ^2} are linearly independent, because if one idempotent were in the linear span of the other two, then it would square to zero. Hence $V^{+,+} = \mathrm{span}_{\mathbb{Q}}(f_0, f_1, a_{\rho^2}) \cong \mathbb{Q}^3$. □

Corollary 3.6.5. *The list (f_0, f_1, I, n_0, n_1) is a $\mathbb{Q}$-basis of V_{4B}. For either $i = 0$ or $i = 1$, $trace(n_i) = 0$ and $trace(f_i) = \frac{7}{4}$.*

Proof. It was shown that f_0, f_1, I are linearly independent (Proposition 3.6.4). Note that $\{f_0, f_1, I\} \subseteq V_{4B}^{+,+}$, $n_0 \in V_{4B}^{-,+}$, and $n_1 \in V_{4B}^{+,-}$. Therefore (f_0, f_1, I, n_0, n_1) is linearly independent and so a $\mathbb{Q}$-basis of V_{4B}.

Based on the products in Lemma 3.6.3, the diagonal components of $\mathrm{ad}(f_i)$ with respect to this basis are $1, 0, 0, \frac{3}{4}, 0$ which sum to $\frac{7}{4}$. Since $n_i = 8(a_{i-1} - a_{i+1})$, we can see that

$\operatorname{trace}(n_i) = 0$. $\square$

Corollary 3.6.6. *For any GIIF L of the 4B algebra,* $\textsc{tel}(L, G) \subseteq \operatorname{span}_{\mathbb{Z}}(n_0, n_1, 4f_0, 4f_1, I)$.

Proof. By Lemma 3.1.4, $L^{+,+}$ is contained in $\operatorname{span}_{\mathbb{Z}}(f_0, f_1, a_{\rho^2})$, which equals $\operatorname{span}_{\mathbb{Z}}(f_0, f_1, I)$ since $I = f_0 + f_1 + a_{\rho^2}$ (by 3.6.4).

Suppose $w = af_0 + bf_1 + cI$ ($a, b, c \in \mathbb{Z}$) is in $L^{+,+}$. The products in Lemma 3.6.3 imply that $w \cdot n_0 = (3a/4 + c)n_0$ and $w \cdot n_1 = (3b/4 + c)n_1$. Both of these eigenvalues must be integers (by 2.1.5), therefore 4 divides a and 4 divides b.

Recall that $V_{4B}^{-,+} = \operatorname{span}_{\mathbb{Q}}(n_0)$ and so $L^{-,+}$ equals $\mathbb{Z}pn_0$ for some $p \in \mathbb{Q}$. We compute $\kappa(pn_0, pn_0) = 104p^2$ and $\eta(pn_0, pn_0) = 147p^2$ [$\bigstar$`4B.5`]. So both $104p^2$ and $147p^2$ are integers. Since $\gcd(104, 147) = 1$ this implies that $p^2 \in \mathbb{Z}$ and therefore $p \in \mathbb{Z}$. So if pn_0 is in an integral form, then $p \in \mathbb{Z}$.

Recall (as in the proof of 3.6.3) that the automorphism $\tau_1 \circ \phi$ interchanges n_0 and n_1. Therefore, the arguments just given for n_0 also applies to n_1, and so $L^{+,-} \subseteq \mathbb{Z}n_1$. $\square$

The 4B algebra and the 4A algebra are isomorphic as $\mathbb{Q}[G]$-modules (both $\dim V^{+,+} = 3$, $\dim V^{-,+} = \dim V^{+,-} = 1$ and $V^{-,-} = 0$). This isomorphism and Corollary 3.5.9 gives the following:

Proposition 3.6.7. *For any rank 5 G-invariant discrete subgroup L of the 4B algebra, $L/\,\textsc{tel}(L, G)$ is isomorphic to a subgroup of the four group.*

Theorem 3.6.8. $\operatorname{span}_{\mathbb{Z}}(n_0, n_1, 4f_0, 4f_1, I)$ *is the unique maximal GIIF of V_{4B}.*

Proof. The computations done in 3.6.3 show that $Q \overset{\text{def}}{=} \operatorname{span}_{\mathbb{Z}}(n_0, n_1, 4f_0, 4f_1, I)$ is an integral form, and it is clearly closed under the action of τ_0 and τ_1 since in fact $Q = \textsc{tel}(Q, G)$. Let L be a maximal GIIF of V_{4B}. We aim to show that $L \subseteq Q$. If $L = \textsc{tel}(L, G)$, then we are done, by Corollary 3.6.6. Otherwise, there is some $w \in L \setminus \textsc{tel}(L, G)$. Proposition 3.6.7 and Corollary 3.6.6 ensure that $w = \frac{1}{2}(an_0 + bn_1 + 4cf_0 + 4df_1 + eI)$, for some integers a, b, c, d, e. By maximality, $I \in L$ (Lemma 2.2.8). Therefore we may add an integer multiple of I to w to ensure that $e \in \{0, 1\}$, and we still have that $w \in L \setminus \textsc{tel}(L, G)$.

Now $w \cdot w \in L$ and therefore $2w \cdot w \in \textsc{tel}(L, G) \subseteq \operatorname{span}_{\mathbb{Z}}(n_0, n_1, 4f_0, 4f_1, I)$. We compute the coefficients of $2w \cdot w$ in the basis $n_0, n_1, 4f_0, 4f_1, I$ [★`4B.6`]:

$$\begin{aligned} 2w \cdot w = {} & (3ac + ae)\, n_0 + (3bd + be)\, n_1 \\ & + \left(4a^2 - \frac{7b^2}{2} + 2c^2 + ce\right)(4f_0) + \left(-\frac{7a^2}{2} + 4b^2 + 2d^2 + de\right)(4f_1) \\ & + \left(14a^2 + 14b^2 + \frac{e^2}{2}\right) I \end{aligned}$$

All of these coefficients must be integers. Therefore $a, b, e \in 2\mathbb{Z}$. So $e = 0$.

Next compute $\kappa(w, w) = 26a^2 + 26b^2 + \frac{25c^2}{4} + \frac{25d^2}{4}$ [★`4B.7`]. This is an integer if and only if $c^2 + d^2 \equiv 0 \pmod 4$ which is equivalent to $c, d \in 2\mathbb{Z}$. This completes the proof that $w \in \operatorname{span}_{\mathbb{Z}}(n_0, n_1, 4f_0, 4f_1, I)$. □

3.7 The 5A algebra

Notation 3.7.1. The Norton-Sakuma algebra V_{5A} of type 5A has a basis consisting of five axes (which are therefore idempotents) $a_{-2}, a_{-1}, a_0, a_1, a_2$ together with a non-idempotent w_ρ which satisfy the following products:

$$\begin{aligned} a_0 \cdot a_1 &= 2^{-7}(3a_0 + 3a_1 - a_2 - a_{-1} - a_{-2}) + w_\rho, \\ a_0 \cdot a_2 &= 2^{-7}(3a_0 + 3a_2 - a_1 - a_{-1} - a_{-2}) - w_\rho, \\ a_0 \cdot w_\rho &= 7 \cdot 2^{-12}(a_1 + a_{-1} - a_2 - a_{-2}) + 2^{-5} \cdot 7 w_\rho, \\ w_\rho \cdot w_\rho &= 2^{-19} \cdot 5^2 \cdot 7\,(a_{-2} + a_{-1} + a_0 + a_1 + a_2). \end{aligned}$$

([IPSS10, Table 3].) There is an automorphism g of this algebra which fixes w_ρ and permutes cyclicly the list $(a_{-2}, a_{-1}, a_0, a_1, a_2)$ one space to the right. This uniquely determines the remaining products [IPSS10, Lemma 2.20].

We compute the matrix of $\tau(a_0)$ with respect to the ordered basis $\mathcal{A} = (a_{-2}, a_{-1}, \ldots, a_2, w_\rho)$

[★5A.1]:

$$[\tau(a_0)]_{\mathcal{A}} = \begin{bmatrix} 0&0&0&0&1&0 \\ 0&0&0&1&0&0 \\ 0&0&1&0&0&0 \\ 0&1&0&0&0&0 \\ 1&0&0&0&0&0 \\ 0&0&0&0&0&1 \end{bmatrix}$$

So $\tau(a_0)$ fixes w_ρ and a_0 and it interchanges a_{-1} with a_1 and also interchanges a_{-2} with a_2.

Since $\tau(a_0)$ is a polynomial in $\mathrm{ad}(a_0)$ (Lemma 2.2.9), we have that $g^k(\tau(a_0)y) = \tau(g^k a_0)(g^k y)$. Define a_i for $i \in \mathbb{Z}$ by $a_i = a_{i+5}$ for all $i \in \mathbb{Z}$ (or equivalently: consider the indices modulo 5). Then for all i, $\tau(a_i)$ interchanges a_{i-1} with a_{i+1}, interchanges a_{i-2} with a_{i+2}, and fixes w_ρ and a_i.

Therefore the subgroup G of $\mathrm{Aut}(V_{5A})$ generated by $\{\tau(a) : \ a \text{ an axis}\}$ is isomorphic to the dihedral group of order 10, and $g = \tau(a_{-2})\tau(a_0)$ is the element of order 5 in $\mathrm{Aut}(V_{5A})$ which fixes w_ρ and sends $a_i \mapsto a_{i+1}$ (where the indices are considered modulo 5).

Definition 3.7.2. Define $z = \frac{1}{2}I + \frac{2048}{7}w_\rho$, and for $-2 \leqslant i \leqslant 2$ define $m_i = 14I - 64a_i$. Let $\mathcal{Q}$ be the ordered list $(I, z, m_{-1}, m_0, m_1, m_2)$. Note that w_ρ and each a_i $(-2 \leqslant i \leqslant 2)$ are contained in $\mathrm{span}_{\mathbb{Q}}(\mathcal{Q})$ which implies $\mathcal{Q}$ is a basis of V_{5A}. Define $Q = \mathrm{span}_{\mathbb{Z}}(\mathcal{Q})$.

Proposition 3.7.3. *The additive group Q is in fact a GIIF of V_{5A}.*

Proof. Note that $I = \sum_{i=-2}^{2} \frac{35}{32} a_i$ which implies $\sum_{i=-2}^{2} m_i = 0$. Therefore Q also contains m_{-2}. Since G acts transitively on the set of axes, G also acts transitively on the set $\{m_{-2}, m_{-1}, \ldots, m_2\}$. So we can describe Q as $\mathrm{span}_{\mathbb{Z}}(I, z) + \mathrm{span}_{\mathbb{Z}}(G \cdot m_0)$. This shows that Q is G-invariant, since G acts trivially on z and I.

We compute the matrices of $\mathrm{ad}(z)$ and $\mathrm{ad}(m_0)$ with respect to the $\mathbb{Z}$-basis $\mathcal{B}$ of Q given in Definition 3.7.2 [★5A.2]:

$$[\mathrm{ad}(z)]_{\mathcal{B}} = \begin{bmatrix} 0&31&0&0&0&0 \\ 1&1&0&0&0&0 \\ 0&0&0&1&0&-1 \\ 0&0&0&1&1&-1 \\ 0&0&-1&1&1&0 \\ 0&0&-1&0&1&0 \end{bmatrix} \qquad [\mathrm{ad}(m_0)]_{\mathcal{B}} = \begin{bmatrix} 0&0&-182&700&-182&-168 \\ 0&0&14&0&14&-14 \\ 0&1&12&0&0&0 \\ 1&1&12&-36&12&12 \\ 0&1&0&0&12&0 \\ 0&0&0&0&0&12 \end{bmatrix}$$

These being integer matrix shows that Q is closed under multiplication by z and by m_0. Since

Q is G-invariant, it is therefore also closed under multiplication by hm_0 for all $h \in G$ and therefore Q is closed under multiplication by each of the m_i. So Q is a ring. $\square$

Lemma 3.7.4. *$z^2 = 31I + z$. Also for $a, b \in \mathbb{Q}$, $\mathrm{span}_{\mathbb{Z}}(I, aI + bz)$ is a ring if and only if $a, b \in \frac{1}{5}\mathbb{Z}$ and $2a + b \in \mathbb{Z}$.*

Proof. The fact that $z^2 = 31I + z$ is an easy verification, or it follows from computing the matrix of $\mathrm{ad}(z)$ in the the proof of Proposition 3.7.3. For the second result, write $x = aI + bz$ for some $a, b \in \mathbb{Q}$ and suppose that $\mathrm{span}_{\mathbb{Z}}(I, x)$ is a ring. Then we have:

$$x \cdot x = (-a^2 - ab + 31b^2)I + (2a + b)x \tag{3.6}$$

Therefore both $-a^2 - ab + 31b^2$ and $2a + b$ are integers. Hence so is $4(-a^2 - ab + 31b^2) + (2a + b)^2 = 125b^2$. This implies that $5b \in \mathbb{Z}$. So $2a = (2a + b) - b \in \frac{1}{5}\mathbb{Z}$ which implies that $a \in \frac{1}{10}\mathbb{Z}$.

The following is also an integer:

$$\left(-a^2 - ab + 31b^2\right) - 31(2a + b)^2 = -125a(a + b) = 5(5a)(5a + 5b).$$

If $5a \in \frac{1}{2}\mathbb{Z}\backslash\mathbb{Z}$ then $5(5a)(5a + 5b)$ would not be an integer. Thus $5a \in \mathbb{Z}$.

Conversely, suppose that $a, b \in \frac{1}{5}\mathbb{Z}$ and $2a + b \in \mathbb{Z}$. Again set $x = aI + bz$. We aim to show that $\mathrm{span}_{\mathbb{Z}}(I, x)$ is a ring. According to equation (3.6) expressing $x \cdot x$ in terms of I and x, we just need to verify that $-a^2 - ab + 31b^2$ is an integer. Multiplying it by four gives $4(-a^2 - ab + 31b^2) = 125b^2 - (2a + b)^2$, which is an integer. On the other hand, the assumptions imply $25(-a^2 - ab + 31b^2) \in \mathbb{Z}$. Since $\gcd(25, 4) = 1$, this proves that $-a^2 - ab + 31b^2 \in \mathbb{Z}$. $\square$

Lemma 3.7.5. *For any GIIF L of V_{5A}, $L^G \subseteq \mathrm{span}_{\mathbb{Z}}(I, z)$.*

Proof. Recall that V_{5A} decomposes as a G-module as $\mathrm{span}_{\mathbb{Q}}(I, z) \oplus \mathrm{span}_{\mathbb{Q}}(G \cdot m_0)$ where $G \cdot m_0 = \{m_{-2}, m_{-1}, m_0, m_1, m_2\}$ and $\sum_{i=-2}^{2} m_i = 0$. It follows that $\mathrm{span}_{\mathbb{Q}}(G \cdot m_0)$ contains no

G-fixed points, and therefore $V_{5A}^G = \mathrm{span}_{\mathbb{Q}}(I, z)$.

To prove the result, we may assume that L is a maximal GIIF, and in particular $I \in L$ (Lemma 2.2.8). Since I is primitive in L^G (meaning I/k is not in L^G for any integer k), we may write $L^G = \mathrm{span}_{\mathbb{Z}}(I, x)$ for some $x = aI + bz$ where the previous result (Lemma 3.7.4) implies that $a, b \in \frac{1}{5}\mathbb{Z}$ and $2a + b \in \mathbb{Z}$. We need to show that $a, b \in \mathbb{Z}$.

The characteristic polynomial of the action of $\mathrm{ad}(x)$ on $\mathrm{span}_{\mathbb{Z}}(m_i : -2 \leqslant i \leqslant 2)$ is given by [`★5A.3`]: $(t^2 - (2a+b)t + a^2 + ab - b^2)^2$.

By the variant of Gauss' Lemma (2.1.7), $a^2 + ab - b^2 \in \mathbb{Z}$. Write $A = 5a$ and $B = 5b$, so that $A, B \in \mathbb{Z}$. Then $A^2 + AB - B^2 \equiv 0 \pmod{25}$. This will imply that $A \equiv B \equiv 0, \pmod 5$. For if A were invertible modulo 25, then BA^{-1} would be a root of the polynomial $x^2 - x - 1$ modulo 25. This polynomial has no roots in $\mathbb{Z}/25\mathbb{Z}$ (since its discriminant is 5, which is not a square modulo 25). Similarly, if B were invertible modulo, then AB^{-1} would be a root of $x^2 + x - 1$ modulo 25, but this also has discriminant 5 and therefore has no roots modulo 25. So $A, B \equiv 0 \pmod 5$, which implies $a, b \in \mathbb{Z}$. □

Corollary 3.7.6. *If L is a maximal GIIF of V_{5A}, then $L^G = \mathrm{span}_{\mathbb{Z}}(I, z)$.*

Proof. We first need to establish the decomposition of V_{5A} with respect to the Killing form. Because G acts transitively on the set $\{m_{-2}, m_{-1}, \ldots, m_2\}$ it follows that $\kappa(m_i, f) = \kappa(m_0, f)$ for all $-2 \leqslant i \leqslant 2$ and all $f \in V_{5A}^G$. Since $\sum_{i=-2}^{2} m_i = 0$ it follows that $0 = \sum_{i=-2}^{2} \kappa(m_i, f) = 5\kappa(m_0, f)$. So m_0 is perpendicular to V_{5A}^G. Since κ is nondegenerate [`★5A.4`] and since $\dim \mathrm{span}_{\mathbb{Q}}(G \cdot m_0) = 4 = \dim V_{5A} - 2$, it follows that $\mathrm{span}_{\mathbb{Q}}(G \cdot m_0) = {V_{5A}}^{G,\perp}$.

In fact, $\mathrm{ad}(z)\Big|_{\mathrm{span}_{\mathbb{Q}}(G \cdot m_0)} = (-g^2 - g^3)\Big|_{\mathrm{span}_{\mathbb{Q}}(G \cdot m_0)}$ [`★5A.5`]. (This is verified by taking the basis $m_{-1}, \ldots, m_2$ of $\mathrm{span}_{\mathbb{Q}}(G \cdot m_0)$ and computing the matrix of $\mathrm{ad}(z) + g^2 + g^3$ to be the zero matrix.) So since $L^{G,\perp}$ is closed under the action of $-g^2 - g^3$ it is also closed under the action of $\mathrm{ad}(z)$.

By 3.7.5, $L^G \subseteq \mathrm{span}_{\mathbb{Z}}(I, z)$. By maximality, $I \in L$ (Lemma 2.2.8). Thus $L^G + \mathbb{Z}z = \mathrm{span}_{\mathbb{Z}}(I, z)$ is a ring. Since $L^{G,\perp}$ is closed under the action of $\mathrm{ad}(z)$, it follows that $L^G + L^{G,\perp} + \mathbb{Z}z$ is an integral form and is clearly G-invariant (since G acts trivially on z). If $L = L^G + L^{G,\perp}$

then $L + \mathbb{Z}z$ being a GIIF and maximality would imply $z \in L$, so $L^G = \mathrm{span}_{\mathbb{Z}}(I, z)$.

So we may assume that there is some element in $L \backslash (L^G + L^{G,\perp})$. Let $\varphi + n$ be such an element, with $\varphi \in {V_{5A}}^G$ and $n \in {V_{5A}}^{G,\perp}$.

Note that $\mathrm{ad}(z) + g^2 + g^3$ acts invertibly on ${V_{5A}}^G$. (This is just saying that $\mathrm{ad}(z)$ does not act as the scalar -2 on ${V_{5A}}^G$.) Let $x, y \in \mathbb{Q}$ be such that $(ad(z) + g^2 + g^3)\varphi = xI + yz$.

Applying the inverse of $(ad(z) + g^2 + g^3)\Big|_{{V_{5A}}^G}$ this gives [`✱5A.6`]:

$$\varphi = \left(-\frac{3x}{25} + \frac{6y}{25} + y\right) I + \left(\frac{x}{25} - \frac{2y}{25}\right) z, \tag{3.7}$$

Note that I is primitive in L so we may find a $\mathbb{Z}$-basis of L^G of the form $\{I, mI + kz\}$, where Lemma 3.7.5 implies $m, k \in \mathbb{Z}$. Then $L^G = \mathrm{span}_{\mathbb{Z}}(I, kz)$. Since $kz \in L$, L is closed under the action of $k(\mathrm{ad}(z) + g^2 + g^3)$. We compute:

$$k(\mathrm{ad}(z) + g^2 + g^3)(\varphi + n) = kx\, I + kyz.$$

This being in L and therefore L^G implies that $y \in \mathbb{Z}$.

Let $\Phi_5(g) = 1 + g + g^2 + g^3 + g^4$. This annihilates ${V_{5A}}^{G,\perp}$ since $g^5 - 1$ acts as zero and since $g - 1$ acts invertibly. So $\Phi_5(g)(\varphi + n) = 5\varphi$ is in L which implies that it is in $\mathrm{span}_{\mathbb{Z}}(I, kz)$. Using equation 3.7, this implies that $\frac{x-2y}{5} \in k\mathbb{Z}$ so that $x \in 2y + 5k\mathbb{Z} \subset \mathbb{Z}$.

The coefficients x and y being integers implies that $(\mathrm{ad}(z) + g^2 + g^3)(\varphi + n) \in L + \mathbb{Z}z$. Since $L + \mathbb{Z}z$ is closed under the action of $\mathbb{Z}[G]$, this implies that $\mathrm{ad}(z)(\varphi + n)$ is in $L + \mathbb{Z}z$. This is true for all $\varphi + n \in L \backslash (L^G + L^{G,\perp})$. As was established in the third paragraph of this proof, $\mathrm{ad}(z)(L^G + L^{G,\perp}) \subseteq L + \mathbb{Z}z$.

So $L + \mathbb{Z}z$ is closed under the action of $\mathrm{ad}(z)$ and is therefore a ring. It is clearly discrete and G-invariant and so is a GIIF. Maximality implies $z \in L$. $\square$

Lemma 3.7.7. *Suppose $x, y \in \mathbb{Q}$ are such that $x(m_{-1} + m_1) + ym_0$ is in an 5A GIIF. Then $x, y \in \mathbb{Z}$.*

Proof. Set $w = x(m_{-1} + m_1) + ym_0$. Then the characteristic polynomial of $\mathrm{ad}(w)$ is given by [$\bigstar$`5A.7`]:

$$\Big[\left(t^4 + 12t^3(x - 2y) - 20t^2\left(69x^2 - 58xy + 58y^2\right) - 336t(x - 2y)\left(76x^2 + 11xy - 11y^2\right)\right.$$
$$\left. + 19600\left(x^2 + xy - y^2\right)^2\Big]\,(t - 36x + 12y))\,(t + 24x + 12y)).$$

By the variant of Gauss' Lemma (2.1.7), the coefficients $-36x + 12y$ and $24x + 12y$ are integers. The polynomials $60x$ and $60y$ are both $\mathbb{Z}$-linear combinations of these:

$$60x = -(-36x + 12y) + 24x + 12y, \quad \text{and}$$
$$60y = 2(-36x + 12y) + 3(24x + 12y).$$

So if we define $X = 60x$ and $Y = 60y$, then both are both integers.

Compute the following [$\bigstar$`5A.8`], all of which must be integers:

$$\begin{aligned} \operatorname{trace}\left(w \cdot \left(\tau\left(a_0\right) w\right)\right) &= \frac{7}{24}\left(X^2 - 4XY - Y^2\right), \\ \operatorname{trace}\left(w \cdot \left(\tau\left(a_{-1}\right) w\right)\right) &= -\frac{7}{24}\left(4X^2 - 6XY + Y^2\right), \\ \kappa(w, w) &= \frac{199}{450}\left(3X^2 - 2XY + 2Y^2\right). \end{aligned} \tag{3.8}$$

These three expressions being integers will imply that the integers X and Y are divisible by 60, which can be shown prime by prime. For example, $3X^2 - 2XY + 2Y^2 \equiv 0, \pmod{25}$ because $\kappa(w, w) \in \mathbb{Z}$. Note:

$$3X^2 - 2XY + 2Y^2 = 3(X + 3Y)^2 - 20XY - 25Y^2. \tag{3.9}$$

This expression being equivalent to zero modulo 25 implies that $3^{-1}20XY$ is a square mod 25, which implies at least one of X and Y are divisible by 5. But now (3.9) being equivalent to 0 mod 25 simplifies to $3(X + 3Y)^2 \equiv 0 \pmod{25}$ and hence $X + 3Y \equiv 0, \pmod{5}$, which proves that both of X and Y are 0 mod 5.

One can analyze the numerators of the first two polynomials mod 8 and mod 3 in a similar way as was just done mod 5; the only solutions are $X \equiv Y \equiv 0 \pmod{12}$ [✶5A.9]. Therefore 60 divides both X and Y, and so $x, y \in \mathbb{Z}$. □

Lemma 3.7.8. *For a maximal 5A GIIF L, $L^{G,\perp} \subseteq Q^{G,\perp}$.*

Proof. Fix an arbitrary $w \in L^{G,\perp}$ and write $w = \sum_{i=-1}^{2} x_i m_i$ for some rational $x_{-1}, \ldots, x_2$. The image of $L^{G,\perp}$ under the endomorphism $\tau(a_0) + \mathrm{ad}(I)$ will lie in the $\tau(a_0)$ fixed-point subspace: $(L^{G,\perp})^{\tau(a_0)} \subseteq \mathrm{span}_{\mathbb{Q}}(m_{-1} + m_1, m_0)$. The previous lemma says that $L \cap \mathrm{span}_{\mathbb{Q}}(m_{-1} + m_1, m_0) \subseteq \mathrm{span}_{\mathbb{Z}}(m_{-1} + m_1, m_0)$. We compute the coefficients of $(\tau(a_0) + \mathrm{ad}(I))w$ and of $(\tau(a_0) + \mathrm{ad}(I))g\, w$ with respect to $m_{-1} + m_1$ and m_0 [✶5A.10]:

$$(\tau(a_0) + I)\, w = (x_{-1} + x_1 - x_2)\, [m_{-1} + m_1] + (2x_0 - x_2)\, m_0,$$
$$(\tau(a_0) + I)\, g\, w = (x_0 - x_1 - x_2)\, [m_{-1} + m_1] + (2x_{-1} - x_1 - x_2)\, m_0.$$

Since w is in L, both of the expressions above lie in L, and hence the four coefficients must be integers:

$$x_{-1} + x_1 - x_2, \quad 2x_0 - x_2, \quad x_0 - x_1 - x_2, \quad 2x_{-1} - x_1 - x_2. \tag{3.10}$$

Having fixed a basis $m_{-1}, \ldots, m_2$ of ${V_{5A}}^{G,\perp}$, we may identify the ring of regular functions on ${V_{5A}}^{G,\perp}$ with $\mathbb{Q}[x_{-1}, \ldots, x_2]$. If $p(x_{-1}, \ldots, x_2)$ is a linear polynomial with rational coefficients, then we identify this with a linear functions ${V_{5A}}^{G,\perp} \to \mathbb{Q}$ defined by $w = \sum_{i=-1}^{2} x_i m_i \mapsto p(x_{-1}, \ldots, x_2)$. Let $p_1, \ldots, p_4$ denote the linear functions ${V_{5A}}^{G,\perp} \to \mathbb{Q}$ given by the four polynomials given in (3.10). Then these functions evaluated at w give integer outputs if w is in a GIIF. Equivalently, w is contained in the $\mathbb{Z}$-span of the basis $d_1, \ldots, d_4$ of

${V_{5A}}^{G,\perp}$ dual to $p_1, \dots p_4$ (meaning $p_i(d_j) = \delta_{ij}$). This dual basis is given by[$\bigstar$`5A.11`]:

$$
\begin{aligned}
d_1 &= \frac{1}{5}\left(-m_{-1} - 2m_0 + 2m_1 - 4m_2\right),\\
d_2 &= \frac{1}{5}\left(2m_{-1} + 4m_0 + m_1 + 3m_2\right),\\
d_3 &= \frac{1}{5}\left(-4m_{-1} - 3m_0 - 2m_1 - 6m_2\right),\\
d_4 &= \frac{1}{5}\left(3m_{-1} + m_0 - m_1 + 2m_2\right).
\end{aligned}
$$

Set $D = \mathrm{span}_{\mathbb{Z}}(d_1, d_2, d_3, d_4)$. Then $L^{G,\perp}$ is contained in D.

Suppose $v = \sum_{i=1}^{4} \lambda_i d_i$ is in $L^{G,\perp}$, with $\lambda_i \in \mathbb{Z}$. Then the coefficient of t^2 in the characteristic polynomial $\chi(\mathrm{ad}(v), t)$ is equivalent to $\frac{1}{5}\left(3\lambda_1 + 4\lambda_2 + 2\lambda_3 + \lambda_4\right)^4$ modulo $\mathbb{Z}[\lambda_1, \lambda_2, \lambda_3, \lambda_4]$ [$\bigstar$`5A.12`]. Therefore $3\lambda_1 + 4\lambda_2 + 2\lambda_3 + \lambda_4 \equiv 0, \pmod 5$. The proof will be completed by showing that

$$
\left\{\sum_{i=1}^{4} \lambda_i d_i :\ \lambda_i \in \mathbb{Z} \text{ and } 3\lambda_1 + 4\lambda_2 + 2\lambda_3 + \lambda_4 \equiv 0, \pmod 5\right\} = Q^{G,\perp}. \tag{3.11}
$$

Since we have shown $L^{G,\perp}$ is contained in the left hand side.

This is a fairly routine calculation. We expand each m_i in the basis of D to verify that the right hand side of (3.11) is contained in the left side [$\bigstar$`5A.13`]:

$$
\begin{aligned}
m_{-1} &= d_1 + 2d_4,\\
m_0 &= 2d_2 + d_3,\\
m_1 &= d_1 - d_3 - d_4,\\
m_2 &= -d_1 - d_2 - d_3 - d_4.
\end{aligned}
$$

Writing each of these as $\sum_{i=1}^{4} \lambda_i d_i$, we can verify that $3\lambda_1 + 4\lambda_2 + 2\lambda_3 + \lambda_4, \pmod 5$, for each.

Furthermore we can compute the determinant of the following matrix [`★5A.14`]:

$$\det\begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 2 & 1 & 0 \\ 1 & 0 & -1 & -1 \\ -1 & -1 & -1 & -1 \end{pmatrix} = -5$$

This shows that $Q^{G,\perp} = \mathrm{span}_{\mathbb{Z}}(m_{-1}, m_0, m_1, m_2)$ is contained in $D = \mathrm{span}_{\mathbb{Z}}(d_1, d_2, d_3, d_4)$ with index 5. Therefore the right side of (3.11) is contained in the left side and both have index 5 in D, so the two sides are equal. $\square$

Theorem 3.7.9. *The GIIF Q is the unique maximal 5A GIIF.*

Proof. Let L be a maximal 5A GIIF, and suppose $L \neq Q$. By 3.7.6 and 3.7.8, $L^G = Q^G$ and $L^{G,\perp} \subseteq Q^{G,\perp}$. So if $L = L^G + L^{G,\perp}$, we are done since $Q = Q^G + Q^{G,\perp}$.

Since g cyclicly permutes the axes, the g-fixed points of V_{5A} are spanned by $\sum_{i=-2}^{2} a_i$ and w_ρ. This means $L^G = L^g$. Then $L/L^g = L/L^G$ has rank $6 - 2 = 4$, and so 2.2.12 gives that $[L : L^G + L^{G,\perp}] = 5$. This index being prime and the inclusion $L^G + L^{G,\perp} \subseteq L \cap Q \subsetneq L$ together imply that $L^G + L^{G,\perp} = L \cap Q$. Thus $[L : L \cap Q] = 5$.

Suppose v is an element in $L \setminus Q$. For $\ell \in L^G$,

$$\kappa((g-1)v, \ell) = \kappa(gv, \ell) - \kappa(v, \ell) = \kappa(v, \ell) - \kappa(v, \ell) = 0.$$

So $(g-1)v \in L^{G,\perp}$. Since κ is nondegenerate, g acts without fixed points on ${V_{5A}}^{G,\perp}$. In particular, $g - 1\big|_{L^{G,\perp}}$ is invertible, and the matrix of its inverse with respect to the basis m_{-1}, m_0, m_1, m_2 is given by [`★5A.15`]:

$$\frac{1}{5}\begin{pmatrix} -4 & 1 & 1 & 1 \\ -3 & -3 & 2 & 2 \\ -2 & -2 & -2 & 3 \\ -1 & -1 & -1 & -1 \end{pmatrix}$$

Set $\hat{m}_i = \left(g - 1\big|_{L^{G,\perp}}\right)^{-1} m_i$. The computation of the matrix above gives the following:

$$\begin{aligned}
\hat{m}_{-1} &= \frac{1}{5}\left(-4m_{-1} - 3m_0 - 2m_1 - m_2\right), \\
\hat{m}_0 &= \frac{1}{5}\left(m_{-1} - 3m_0 - 2m_1 - m_2\right), \\
\hat{m}_1 &= \frac{1}{5}\left(m_{-1} + 2m_0 - 2m_1 - m_2\right), \\
\hat{m}_2 &= \frac{1}{5}\left(m_{-1} + 2m_0 + 3m_1 - m_2\right).
\end{aligned}$$

Write $v = aI + bz + \sum_{i=-1}^{2} x_i \hat{m}_i$ with $a, b \in \mathbb{Q}$ and $x_i \in \mathbb{Q}$ $(-1 \leqslant i \leqslant 2)$. Then $(g-1)v = \sum_{i=-1}^{2} x_i m_i$ so $(g-1)v \in L^{G,\perp} \subseteq Q^{G,\perp}$ implies $x_{-1}, x_0, x_1, x_2 \in \mathbb{Z}$.

Also, since g has order 5, and $g - 1$ is invertible on ${V_{5A}}^{G,\perp}$ it follows that $\Phi_5(g) = g^4 + g^3 + g^2 + g + 1$ annihilates ${V_{5A}}^{G,\perp}$. So $\Phi_5(g)v = 5aI + 5bz$. This is in $L^G = Q^G$ so if we define $A = 5a$ and $B = 5b$ then both A and B are integers.

Compute $\kappa(v, v)$ [`✶5A.16`]:

$$\begin{aligned}
\frac{6A^2 + 6AB + 69B^2}{25} &+ 1592x_{-1}^2 + 1592x_0^2 + 1592x_1^2 + 1592x_2^2 \\
&- 1592x_{-1}x_1 - 1592x_{-1}x_2 - 1592x_0x_2
\end{aligned}$$

This must be an integer, and the the x_i are integers, therefore $\frac{1}{25}(6A^2 + 6AB + 69B^2)$ is an integer. But $6A^2 + 6AB + 69B^2 \equiv 6(A^2 + AB - B^2), \pmod{25}$. It has been shown in the proof of 3.7.5 that this only has solutions if $A, B \equiv 0 \pmod 5$. Therefore $a, b \in \mathbb{Z}$.

But then this implies that $aI + bz \in Q^G = L^G$, with the equality coming from Corollary 3.7.6. So $v - aI - bz = \sum_{i=-1}^{2} x_i \hat{m}_i \in L^{G,\perp}$. Therefore $v \in L^G + L^{G,\perp} \subseteq Q$, as desired. $\square$

3.8 The 6A algebra

The 6A algebra V_{6A} over $\mathbb{Q}$ has a $\mathbb{Q}$-basis consisting of seven axes $a_{-2}, a_1, a_0, a_1, a_2, a_3, a_{\rho^3}$ along with a non-axis idempotent u_{ρ^2}. Some of the algebra products are given below:

$$
\begin{aligned}
a_0 \cdot a_1 &= 2^{-6}\,(a_{\rho^3} - a_{-2} - a_{-1} + a_0 + a_1 - a_2 - a_3) + 2^{-11} \cdot 5 \cdot 3^2\, u_{\rho^2} \\
a_0 \cdot a_2 &= 2^{-5}\,(a_{-2} + 2a_0 + 2a_2) - 2^{-6} \cdot 3^3 \cdot 5\, u_{\rho^2}, \\
a_0 \cdot a_3 &= 2^{-3}\,(a_0 + a_3 - a_{\rho^3}), \\
a_0 \cdot a_{\rho^3} &= 2^{-3}(a_0 - a_3 + a_{\rho^3}), \\
a_0 \cdot u_{\rho^2} &= 3^{-2}\,(-a_{-2} + 2a_0 - a_2) + 2^{-5} \cdot 5\, u_{\rho^2}, \\
a_{\rho^3} \cdot u_{\rho^2} &= 0.
\end{aligned}
$$

[IPSS10, Table 3 and Lemma 2.20]. There is an automorphism f of V which fixes a_{ρ^3} and u_{ρ^2} and which permutes cyclically the list $(a_{-2}, a_{-1}, a_0, a_1, a_2, a_3)$ one space to the right. This determines the remaining algebra products.

We first verify that $\tau(a_{\rho^3})$ is trivial and compute the matrix of $\tau(a_0)$ with respect to the basis $\mathcal{B}$ given above [★6A.1]:

$$
[\tau(a_0)]_{\mathcal{B}} = \begin{bmatrix}
0&0&0&0&1&0&0&0\\
0&0&0&1&0&0&0&0\\
0&0&1&0&0&0&0&0\\
0&1&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&1
\end{bmatrix}
$$

So $\tau(a_0)$ fixes $a_0, a_3,\ a_{\rho^2}$, and u_ρ^3 and it interchanges a_{-2} with a_2 and a_{-1} with a_1.

Define a_i for all $i \in \mathbb{Z}$ by $a_i = a_{i+6}$, so the a_i is determined by the residue of i modulo 6. Since $\tau(a_0)$ is a polynomial in $\mathrm{ad}(a_0)$ (Lemma B.2.2), we have that $\sigma^k(\tau(a_0)y) = \tau(\sigma^k a_0)(\sigma^k y)$ which implies that for any $i \in \mathbb{Z}$, $\tau(a_i)$ fixes a_i, a_{i+3}, a_{ρ^3} and u_{ρ^2} and it interchanges a_{i-1} with a_{i+1} and interchanges a_{i-2} with a_{i+2}.

It follows that $\tau(a_i) = \tau(a_{i+3})$ for all i. One can check directly, or reference [IPSS10] that $G = \langle \tau(a) :\ a \text{ and axis} \rangle \cong \mathrm{Sym}(3)$.

Definition 3.8.1. Define the following 8 elements in V_{6A}.

$$
\begin{aligned}
q_1 &= I,\\
q_2 &= 3u_{\rho^2},\\
q_3 &= 4a_{\rho^3} - I,\\
q_4 &= \frac{16}{3}\big[(a_{-2} + a_0 + a_2) - (a_{-1} + a_1 + a_3)\big],\\
q_5 &= 16(a_0 - a_3) - q_4,\\
q_6 &= 16(a_2 - a_{-1}) - q_4,\\
q_7 &= 32(a_0 + a_3) - 16I + 8a_{\rho^3} + 6u_{\rho^2},\\
q_8 &= 32(a_{-1} + a_2) - 16I + 8a_{\rho^3} + 6u_{\rho^2}.
\end{aligned}
$$

Let $\boldsymbol{Q}$ denote the ordered list $q_1, \dots, q_8$ and set $Q = \operatorname{span}_{\mathbb{Z}}(\boldsymbol{Q})$.

Proposition 3.8.2. *Q is a GIIF of V_{6A} with $Q^G = \operatorname{span}_{\mathbb{Z}}(q_1, q_2, q_3, q_4)$ and $Q^{G,\perp} = \operatorname{span}_{\mathbb{Z}}(q_5, q_6, q_7, q_8)$.*

Proof. To check that Q is an integral form is a straightforward computation: we just need to check that the matrix of $\operatorname{ad}(q_i)$ with respect to the basis $\boldsymbol{Q}$ has integer entries, for each $i = 1, \dots, 8$. (This is automized with the Mathematica function `IntegralFormQ`.) We also compute the matrices of $\tau(a_0)$ and $\tau(a_1)$ (which generate G) with respect to the basis $\boldsymbol{Q}$ [★`6A.2`]:

$$
[\tau(a_0)]_{\boldsymbol{Q}} = \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&-1&0&0\\ 0&0&0&0&0&-1&0&0\\ 0&0&0&0&0&0&1&-1\\ 0&0&0&0&0&0&0&-1 \end{bmatrix} \quad \text{and} \quad [\tau(a_1)]_{\boldsymbol{Q}} = \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{bmatrix}.
$$

These both being integer matrices means that Q is invariant under $\langle \tau(a_0), \tau(a_1) \rangle = G$ and therefore Q is a GIIF. Also the block decompositions of these two matrices show that $Q = \operatorname{span}_{\mathbb{Z}}(q_1, q_2, q_3, q_4) + \operatorname{span}_{\mathbb{Z}}(q_5, q_6) + \operatorname{span}_{\mathbb{Z}}(q_7, q_8)$ is the decomposition of Q as a G-module, with the latter two summands having no fixed points of G. So $Q^G = \operatorname{span}(q_1, q_2, q_3, q_4)$.

The κ-Gram matrix for the basis $\boldsymbol{Q}$ is given by [★`6A.3`]:

$$\begin{bmatrix} 8 & 7 & -1 & 0 & 0 & 0 & 0 & 0 \\ 7 & 13 & -5 & 0 & 0 & 0 & 0 & 0 \\ -1 & -5 & 13 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 172 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 268 & -134 & 0 & 0 \\ 0 & 0 & 0 & 0 & -134 & 268 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1560 & -780 \\ 0 & 0 & 0 & 0 & 0 & 0 & -780 & 1560 \end{bmatrix}$$

This shows that $Q^{G,\perp} = \operatorname{span}_{\mathbb{Z}}(q_5, q_6, q_7, q_8)$. □

Proposition 3.8.3. *For any GIIF L of the 6A algebra, $L^G \subseteq Q^G$.*

Proof. Let v be an arbitrary element in V^G. Write $v = \sum_{i=1}^4 x_i q_i$ with $x_i \in \mathbb{Q}$. If v is in a GIIF, then the characteristic polynomial of $\mathrm{ad}(v)$ has integer coefficients. We can compute this characteristic polynomial and factor it, to show that it has the form [`★6A.4`]:

$$\chi(\mathrm{ad}(v), t) =$$
$$\big(t - (x_1 + 3x_2 - x_3)\big) \cdot \big(t^2 + t\,(-2x_1 - 2x_2 + x_3) + \gamma_1\big)^2 \cdot \big(t^3 - t^2\,(3x_1 + 2x_3) + \gamma_2 t + \gamma_3\big),$$

where $\gamma_1, \gamma_2, \gamma_3 \in \mathbb{Z}[x_1, x_2, x_3, x_4] \subseteq \mathbb{Q}$. In particular, the variant of Gauss' Lemma (2.1.7) applies ensuring that if we define $k_1 = x_1 + 3x_2 - x_3$, $k_2 = -2x_1 - 2x_2 + x_3$ and $k_3 = 3x_1 + 2x_3$ are integers.

We can solve this set of linear equations to write each x_i in terms of the k_1, k_2, k_3. This produces [`★6A.5`]:

$$\begin{aligned} x_1 &= -\frac{4k_1}{11} - \frac{6k_2}{11} + \frac{k_3}{11}, \\ x_2 &= \frac{7k_1}{11} + \frac{5k_2}{11} + \frac{k_3}{11}, \\ x_3 &= \frac{6k_1}{11} + \frac{9k_2}{11} + \frac{4k_3}{11}. \end{aligned}$$

If we define $X_i = 11x_i$, then X_i is an integer for each index $i = 1, 2, 3$. Also, we can compute that

$$X_1 - X_2 = -11(k_1 + k_2) \equiv 0 \pmod{11}, \qquad \text{and}$$
$$3X_3 - X_1 = 11(2k_1 + 3k_2 + k_3) \equiv 0 \pmod{11}.$$

To finish the proof, we analyze the value of $\kappa(v,v) - \eta(v,v)$. Compute [$\bigstar$`6A.6`]:

$$\kappa(v,v) - \eta(v,v) = \frac{1}{121}\big(-8X_2^2 + 4X_2X_3 - 9X_3^2\big) - 86x_4^2 \tag{3.12}$$

Since $121[\kappa(v,v) - \eta(v,v)] \in \mathbb{Z}$ and $X_1, X_2, X_3 \in \mathbb{Z}$, this implies that $121 \cdot 86x_4^2 \in \mathbb{Z}$. This factors as $2^1 11^2 43^1 x_4^2$. Therefore $X_4 = 11x_4$ is an integer. Use this to rewrite the computation of $\kappa(v,v) - \eta(v,v)$ in equation (3.12): put everything over the denominator 121:

$$\kappa(v,v) - \eta(v,v) = \frac{1}{121}\big(-8X_2^2 + 4X_2X_3 - 9X_3^2 - 86X_4^2\big)$$

This numerator is an integer which must be divisible by 121, so in particular:

$$-8X_2^2 + 4X_2X_3 - 9X_3^2 - 86X_4^2 \equiv 0, \pmod{11}.$$

We can simplify this equivalence, using $X_1 \equiv X_2 \equiv 3X_3$ to:

$$-69X_3^2 - 86X_4^2 \equiv 8X_3^2 + 2X_4^2 \equiv 0, \pmod{11}.$$

If $X_3 \not\equiv 0$, then $7 \equiv (-8) \cdot 2^{-1} \equiv (X_4/X_3)^2$, (mod 11), which is impossible as 7 is not a square mod 11. Therefore $X_3 \equiv X_4 \equiv 0$, (mod 11). And therefore $X_1 \equiv X_2 \equiv 3X_3 \equiv 0$, (mod 11).

This means that $x_1, x_2, x_3, x_4 \in \mathbb{Z}$, so $v \in Q^G$. $\square$

Lemma 3.8.4. *Suppose $x, y \in \mathbb{Q}$ and $x(q_5 + q_6) + y(q_7 + q_8)$ is in a GIIF of V_{6A}. Then $x, y \in \mathbb{Z}$.*

Proof. Suppose $w = x(q_5 + q_6) + y(q_7 + q_8)$ is in a GIIF. Compute the characteristic polynomial of $ad(w)$, and after factoring and simplifying we can verify that it equals the following [$\bigstar$`6A.7`]:

$$t^2 \cdot \left(t^2 - 22ty - 20\left(x^2 - 6y^2\right)\right) \cdot$$
$$\left(t^4 + 22t^3y - 2t^2\left(57x^2 + 208y^2\right) + 88t\left(8x^2y - 65y^3\right) + 72\left(29x^4 - 161x^2y^2 + 890y^4\right)\right).$$

By the variant of Gauss' Lemma (2.1.7), all of the coefficients of t in the factors of this polynomial are integers. In particular, $22y$, $-20\left(x^2 - 6y^2\right)$ and $2\left(57x^2 + 208y^2\right) = 114x^2 + 416y^2$ are all integers. Compute $\mathrm{trace}(w \cdot (\tau(a_0)w)) = -227x^2 - 1102y^2$ [$\bigstar$`6A.8`]. This also must be an integer. Then we can find the smallest multiple of x^2 in the $\mathbb{Z}$-span of the three quadratic polynomials in x and y that have been produced. This search yields the following equation [$\bigstar$`6A.9`]:

$$22x^2 = 442(-20x^2 + 120y^2) + 699(114x^2 + 416y^2) + 312(-227x^2 - 1102y^2).$$

Therefore $22x^2$ is an integer. Since 22 is square-free, this implies $x \in \mathbb{Z}$. Then $-227x^2 - 1102y^2 \in \mathbb{Z}$ implies $1102y^2 \in \mathbb{Z}$ and $1102 = 2^1 19^1 29^1$ is square-free, so $y \in \mathbb{Z}$. $\square$

Proposition 3.8.5. *For any GIIF L of V_{6A}, $L^{G,\perp} \subseteq Q^{G,\perp}$.*

Proof. Choose any $v \in L^{G,\perp}$. Note that $V^{G,\perp}$ is 4 dimensional, based on the computation of the Gram matrix for Q in the proof of Proposition 3.8.2. So $\mathrm{span}_{\mathbb{Q}}(Q^{G,\perp}) = V^{G,\perp}$. Write $v = \sum_{i=5}^{8} x_i q_i$ for rational numbers x_5, x_6, x_7, x_8. We need to show that each x_i is an integer. Compute [$\bigstar$`6A.10`]:

$$\left(\tau\left(a_0\right)\tau\left(a_1\right) + 2\tau\left(a_1\right) + \tau\left(a_2\right) + 2I\right) v = 3x_6\left(q_5 + q_6\right) + 3x_8\left(q_7 + q_8\right),$$
$$\left(-\tau\left(a_0\right)\tau\left(a_1\right) + \tau\left(a_1\right) - \tau\left(a_2\right) + I\right) v = 3x_5\left(q_5 + q_6\right) + 3x_7\left(q_7 + q_8\right)$$

Since v is in a GIIF, both of these elements also are, and therefore Lemma 3.8.4 implies

$3x_5, 3x_6, 3x_7, 3x_8 \in \mathbb{Z}$. Define $X_i = 3x_i$ for $i = 5, 6, 7, 8$.

Compute [$\bigstar$`6A.11`]:

$$\eta(v, v) = \frac{1}{9}\left(454\left(X_5^2 + X_6X_5 + X_6^2\right) + 2204\left(X_7^2 - X_8X_7 + X_8^2\right)\right)$$
$$\kappa(v, v) = \frac{1}{9}\left(268\left(X_5^2 + X_6X_5 + X_6^2\right) + 1560\left(X_7^2 - X_8X_7 + X_8^2\right)\right)$$

These are both integers, therefore the numerators of are both integers divisible by 9. Write $P(x, y) = x^2 - xy + y^2$. Then we have:

$$454P(X_5, X_6) + 2204P(X_7, X_8) \equiv 0, \pmod 9,$$
$$268P(X_5, X_6) + 1560P(X_7, X_8) \equiv 0, \pmod 9.$$

Or equivalently:

$$4P(X_5, X_6) + 8P(X_7, X_8) \equiv 0, \pmod 9,$$
$$7P(X_5, X_6) + 3P(X_7, X_8) \equiv 0, \pmod 9.$$

Since $\det\left[\begin{smallmatrix} 4 & 8 \\ 7 & 3 \end{smallmatrix}\right] = -44 \equiv 1 \pmod 9$, this matrix is invertible in $\mathrm{Mat}_{2\times 2}(\mathbb{Z}/9\mathbb{Z})$. So $P(X_5, X_6) \equiv P(X_7, X_8) \equiv 0 \pmod 9$.

The proof will be completed after proving the following fact: if $x, y \in \mathbb{Z}$ are such that $P(x, y) \equiv 0 \pmod 9$, then $x \equiv y \equiv 0 \pmod 3$. To see this, write $P(x, y) = (x + y)^2 - 3xy$. If this is 0 mod 9, then it is 0 mod 3, which implies $x \equiv -y, \pmod 3$. Thus $P(x, y) \equiv 3xy, \pmod 9$ which means $xy \equiv 0, \pmod 3$ and this forces $x \equiv -y \equiv 0, \pmod 3$.

Thus each X_i ($i = 5, 6, 7, 8$) is divisible by 3, which implies $v \in Q$. $\square$

Theorem 3.8.6. *The GIIF Q is the unique maximal GIIF of V_{6A}.*

Proof. Let L be a maximal GIIF of the 6A algebra. It has been shown that $L^G \subseteq Q^G$ and $L^{G,\perp} \subseteq Q^{G,\perp}$ (Propositions 3.8.3 and 3.8.5).

First, we need to show that $V_{6A}^G = V_{6A}^g$ where g is an element of order 3 in $G \cong \mathrm{Sym}(3)$. This is straightforward: because g cyclicly permutes the lists (a_{-2}, a_0, a_2) and (a_{-1}, a_1, a_3) and g fixes a_{ρ^3} and u_{ρ^2} we can see that V_{6A}^g is spanned by the four vectors $a_{-2} + a_0 + a_2$, $a_{-1} + a_1 + a_3$, a_{ρ^3}, and u_ρ^2. These vectors are all invariant under every element in G and so $V_{6A}^G = V_{6A}^g$. It follows that $L^G = V_{6A}^G \cap L = V_{6A}^g \cap L = L^g$.

Next, we claim that $3L$ is contained in $L^G + L^{G,\perp}$. To that end, note that the index is finite because κ is nondegenerate. (For a sublattice S inside L, $\operatorname{rank} S + \operatorname{rank} S^\perp$ will always equal $\operatorname{rank} L$ if the form is nondegenerate.) Choose any $v \in L$. Then notice that we can write $(g^2 + g + 1) - (g - 1)^2 = 3g$. Applying both sides of this to $g^2\ell$ yields:

$$(g^2 + g + 1)g^2\ell - (g - 1)^2 g^2 \ell = 3\ell.$$

Then we just observe that $(g^2 + g + 1)g^2\ell$ is in L and is annihilated by $g - 1$ so is in $L^g = L^G$. And the other term $(g - 1)^2 g^2\ell$ is in $(g - 1)L$ and therefore in $(L^g)^\perp = L^{G,\perp}$. It follows that

$$3L \subseteq L^G + L^{G,\perp} \subseteq Q^G + Q^{G,\perp} = Q.$$

For any $v \in L$ we may therefore write $v = \sum_{i=1}^{8} \frac{X_i}{3} q_i$ for some integers X_i $(i = 1, \dots 8)$. We can compute the following [$\bigstar$`6A.12`]:

$$\begin{aligned}
\tau(a_0)v - v &= -\frac{X_6}{3} q_5 - \frac{1}{3}(2X_6)\, q_6 - \frac{X_8}{3} q_7 - \frac{1}{3}(2X_8)\, q_8, \\
\tau(a_1)v - v &= \frac{1}{3}(X_6 - X_5)\, q_5 + \frac{1}{3}(X_5 - X_6)\, q_6 + \frac{1}{3}(X_8 - X_7)\, q_7 + \frac{1}{3}(X_7 - X_8)\, q_8.
\end{aligned}$$

Both of these elements are in $L \cap V^{G,\perp} = L^{G,\perp} \subseteq Q^{G,\perp}$. So the coefficients of q_i $(i = 5, \dots 8)$ that occur here are integers. The first equation then implies that $X_6 \in 3\mathbb{Z}$ and $X_8 \in 3\mathbb{Z}$ and then using this fact in the second equation implies $X_5 \in 3\mathbb{Z}$ and $X_7 \in 3\mathbb{Z}$.

Write $x_i = X_i/3$ for $i = 5, 6, 7, 8$, so that $x_i \in \mathbb{Z}$ and $v = \sum_{i=1}^{4} \frac{X_i}{3} q_i + \sum_{i=5}^{8} x_i q_i$. Note that

$v \cdot v \in L$ therefore $3v \cdot v \in Q$. If we write $3v \cdot v = \sum_{i=1}^{8} \gamma_i q_i$ then we compute [$\bigstar$`6A.13`]:

$$\begin{aligned}\gamma_1 &= 2x_1X_1 + 6x_3X_3 + 92x_4X_4 + 3x_1^2 + 9x_3^2 + 138x_4^2 + 162x_5^2 + 162x_6^2 + 864x_7^2 + 864x_8^2 \\ &\qquad + 162x_5x_6 - 864x_7x_8 + \frac{X_1^2}{3} + X_3^2 + \frac{46X_4^2}{3}, \\ \gamma_2 &= 2x_2X_1 + 6x_2X_2 - 2x_2X_3 + 2x_1X_2 - 2x_3X_2 - 32x_4X_4 + 9x_2^2 + 6x_1x_2 - 6x_3x_2 \\ &\qquad - 48x_4^2 + 12x_5^2 + 12x_6^2 - 84x_7^2 - 84x_8^2 + 12x_5x_6 + 84x_7x_8 + X_2^2 \\ &\qquad + \frac{2X_1X_2}{3} - \frac{16X_4^2}{3} - \frac{2X_2X_3}{3}.\end{aligned}$$

These are both integers.

Since the x_i $(i = 5, \ldots, 8)$ and X_i $(i = 1, \ldots 8)$ are integers, γ_1 being an integer implies that ${X_1}^2 + 46{X_4}^2 \equiv 0, \pmod 3$. This has only the trivial solution $X_1 \equiv X_4 \equiv 0, \pmod 3$.

Now this implies that $X_1X_2/3$ and $16X_4^2/3$ are both integers, so $\gamma_2 \in \mathbb{Z}$ implies $X_2X_3 \equiv 0, \pmod 3$. And $\mathrm{trace}(v) = 8X_1/3 + 2X_2 + \frac{1}{3}(X_2 - X_3)$ [$\bigstar$`6A.14`] being an integer implies $X_2 \equiv X_3, \pmod 3$ so $X_2 \equiv X_3 \equiv 0, \pmod 3$, which completes the proof that $v \in Q$. $\square$

CHAPTER 4

GIIFs in some larger Griess algebras

4.1 The algebra with group Sym(4) of shape (2B,3C)

Notation 4.1.1. Let T_1 be the set of transpositions in Sym(4). Throughout this section, let V denote the rational subalgebra generated by the axes of the algebra of shape $(2B, 3C)$ as described in [IPSS10, §4.3]. Explicitly, V has a $\mathbb{Q}$-basis $\{a_t : t \in T_1\}$ where each a_t is an axis. For simplicity of notation, we will omit the parenthesis around transpositions in this context; e.g. $a_{12} = a_{(12)}$. We read the product cycles right to left, as in function composition, so for example $(12)(23) = (123)$.

Each axis is an idempotent, so $a_t^2 = a_t$ for all $t \in T_1$. For a pair of commuting transpositions $s, t \in T_1$, the pair a_s, a_t generate a $2B$-subalgebra [IPSS10, Lemma 3.1], meaning that $a_s \cdot a_t = 0$. For two transposition $s, t \in T_1$ that do not commute, then $sts = tst$ and the triple $a_s,\ a_t,\ a_{sts}$ generate a $3C$-subalgebra [IPSS, §4.3], meaning $a_s \cdot a_t = 2^{-6}(a_s + a_t - a_{sts})$.

We can summarize this with the following formulas [IPSS,§4.3] (this is for any permuation $\{i, j, k, \ell\} = \{1, 2, 3, 4\}$):

$$a_{ij} \cdot a_{ij} = a_{ij}, \qquad a_{ij} \cdot a_{k\ell} = 0, \qquad a_{ij} \cdot a_{ik} = \frac{1}{2^6}(a_{ij} + a_{ik} - a_{jk}).$$

The group $G = \langle \tau(a) :\ a \text{ an axis of } V \rangle$ is isomorphic to Sym(4). The action of Sym(4) on V can be summarized by the following: for $t, s \in T_1$, $t \cdot a_s = \tau(a_t)\, a_s = a_{tst}$ (Lemma 2.2.10).

Definition 4.1.2. Define the following elements of V:

$$\begin{aligned} q_1 &= I = \frac{16}{17}\left(a_{12} + a_{13} + a_{14} + a_{23} + a_{24} + a_{34}\right), \\ q_2 &= 32\left(a_{14} + a_{23}\right), \\ q_3 &= 32\left(a_{13} + a_{24}\right), \\ q_4 &= 32\left(a_{13} - a_{24}\right), \\ q_5 &= 32\left(a_{12} - a_{34}\right), \\ q_6 &= 32\left(a_{14} - a_{23}\right) \end{aligned}$$

Define $\mathcal{Q}$ to be the ordered basis $(q_1, q_2, \ldots, q_6)$, and set $Q = \operatorname{span}_{\mathbb{Z}}(\mathcal{Q})$. The fact that Q is a G-invariant integral form is a straightforward calculation [✶`2B3C.1`].

We will show that the integral form Q is the unique maximal GIIF in V.

Definition 4.1.3. Define $K = O_2(\mathrm{Sym}(4)) = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$. This is a normal subgroup of $G = \mathrm{Sym}(4)$ isomorphic $(\mathbb{Z}/2\mathbb{Z})^2$. Define $k_1 = (12)(34)$ and $k_2 = (13)(24)$.

Lemma 4.1.4. *We have the following decomposition of Q into isotypic subspaces with respect to the action of K:*

$$\begin{aligned} Q^K = Q^{k_1,k_2} &= \operatorname{span}_{\mathbb{Z}}(q_1, q_2, q_3), \\ Q^{-k_1,k_2} &= \operatorname{span}_{\mathbb{Z}}(q_4), \\ Q^{k_1,-k_2} &= \operatorname{span}_{\mathbb{Z}}(q_5) \\ Q^{-k_1,-k_2} &= \operatorname{span}_{\mathbb{Z}}(q_6). \end{aligned}$$

Therefore $Q = \textsc{tel}(Q, K)$ (see Definition 3.5.2).

Proof. It suffices to show that the matrix of the action of k_1 on V with respect to the basis $\mathcal{Q}$ is $\operatorname{diag}(1, 1, 1, -1, 1, -1)$ and that the matrix of k_2 in the basis $\mathcal{Q}$ is $\operatorname{diag}(1, 1, 1, 1, -1, -1)$. This is a straightforward calculation [✶`2B3C.2`]. □

Lemma 4.1.5. *If L is a GIIF of V, then $\textsc{tel}(L, K) \subseteq Q$.*

Proof. Suppose $w \in L^K$. By Lemma 4.1.4, V^K is three-dimensional, and we may write $w = xq_1 + yq_2 + zq_3$ for some $x, y, z \in \mathbb{Q}$.

Compute the following [$\bigstar$`2B3C.3`]:

$$\begin{aligned}\chi(\,\mathrm{ad}[(123)w - w];\; t) = \;& (t + 31y) \cdot (t - 31z) \cdot (t - 31y + 31z) \\ & \cdot [t^3 + t\left(-964y^2 + 964yz - 964z^2\right) + 29512y^2z - 29512yz^2],\end{aligned}$$

Define $Y = 31y$ and $Z = 31z$. By the variant of Gauss' lemma (2.1.7), both Y and Z are integers. The following coefficients are also integers:

$$\begin{aligned}-964y^2 + 964yz - 964z^2 &= -\frac{964}{31^2}\left(Y^2 - YZ + Z^2\right) \quad \text{and} \\ 29512y^2z - 29512yz^2 &= \frac{952}{31^2}(Y - Z)YZ.\end{aligned}$$

The first expression being an integer implies that $Y^2 - YZ + Z^2 \equiv 0, \pmod{31}$. The second expression being an integer implies that one of the following holds: $Y \equiv 0$, $Z \equiv 0$, or $Y \equiv Z \pmod{31}$. Together with the first equivalence, each of these three cases leads to the conclusion $Y \equiv Z \equiv 0, \pmod{31}$. Thus, $y, z \in \mathbb{Z}$.

We compute also that $w \cdot q_5 = (x + y + z)q_5$ [$\bigstar$`2B3C.4`]. This eigenvalue must be an integer, hence $x \in \mathbb{Z}$. This proves that $L^K \subseteq Q$.

Next, one can see from the definition of q_i ($i = 4, 5, 6$) and Lemma 2.2.10 that the action of the transposition (23) fixes q_6 and it interchanges q_4 with q_5. Similarly, (24) fixes q_4 and interchanges q_5 with q_6. So $\langle(23), (24)\rangle \cong \mathrm{Sym}(3)$ acts faithfully on the three element set $\{q_4, q_5, q_6\}$. We also compute that $q_4 \cdot q_5 = q_6$ [$\bigstar$`2B3C.5`] and therefore $q_i \cdot q_j = q_k$ for any permutation $\{i, j, k\} = \{4, 5, 6\}$.

Next, suppose that $v \in L^{\epsilon_1 k_1, \epsilon_2 k_2}$ for some choice of $\epsilon_1, \epsilon_2 \in \{\pm 1\}$, not both equal to 1. By Lemma 4.1.4, $v = rq_i$ for some $i \in \{4, 5, 6\}$ and some rational r. So by the previous paragraph, L contains all three rq_4, rq_5, and rq_6. Then L also contains $(rq_5) \cdot (rq_6) = r^2 q_4$. By the same reasoning, L contains $r^n q_4$ for all natural numbers n. This is a discrete set only if $r \in \mathbb{Z}$. Therefore $v \in Q$. $\square$

Corollary 4.1.6. *For any GIIF L of V, $L \subseteq \frac{1}{4}Q$.*

Proof. The four subspaces $V^{\pm k_1,\pm k_2}$ are the four isotypic subspaces of V with respect to the action of K. For each of the four irreducible $\mathbb{Q}[K]$-module M_i $(i = 1,2,3,4)$, the group algebra $\mathbb{Z}[K]$ (and therefore also $\mathbb{Z}[G]$) contains $|K|e_i = 4e_i$ where e_i is the idempotent in $\mathbb{Q}[K]$ that acts as the identity of M_i and annihilates M_j for $i \neq j$.

Therefore $4L = 4e_1L + 4e_2L + 4e_3L + 4e_4L \subseteq \text{TEL}(L,K) \subseteq Q$. □

Theorem 4.1.7. *The GIIF Q is the unique maximal GIIF in the algebra V of shape $(2B,3C)$.*

Proof. Suppose there is another GIIF L not contained in Q. By Corollary 4.1.6, $L \subseteq \frac{1}{4}Q$, and therefore there exists an element $w \in L \cap \left(\frac{1}{2}Q\backslash Q\right)$. Write $w = \frac{1}{2}\sum_{i=1}^{6} X_i q_i$ for some integers $X_1,\dots X_6$. Define $x_i = X_i/2$. So we aim to show that for each i, $1 \leqslant i \leqslant 6$, X_i is even or equivalently $x_i \in \mathbb{Z}$.

We compute [✶`2B3C.6`]: $\eta(w,w) \equiv \frac{3X_1^2}{2}, \pmod{\mathbb{Z}}$, and therefore X_1 is even and hence $x_1 \in \mathbb{Z}$.

Next we compute [✶`2B3C.7`]

$$\kappa\Big(w,\ (123)\cdot w\Big) = 68x_1X_2 + 68x_1X_3 + 6x_1^2 + \frac{1025}{2}\left(X_4X_5 - X_6X_5 - X_4X_6\right) + \frac{1}{4}\left(129X_2^2 + 2183X_3X_2 + 129X_3^2\right).$$

For this to be an integer, it must be that $129X_2^2 + 2183X_3X_2 + 129X_3^2$ is even. This implies $X_2 \equiv X_3 \equiv 0, \pmod 2$. This then implies that $129X_2^2 + 2183X_3X_2 + 129X_3^2$ is divisible by 4. So now $\kappa\big(w,\ (123)\cdot w\big)$ being an integer implies $X_4X_5 + X_5X_6 + X_4X_6 \equiv 0, \pmod 2$.

Finally, we compute [✶`2B3C.8`]:

$$\kappa\Big((12)\cdot w - w, w\Big) = -1925x_2^2 + 3850x_3x_2 - 1925x_3^2 - 1025X_4X_6 - \frac{1025}{2}\left(X_4^2 + X_6^2\right),$$
$$\kappa\Big((13)\cdot w - w, w\Big) = -1925x_2^2 - 1025X_5X_6 - \frac{1025}{2}\left(X_5^2 + X_6^2\right).$$

Therefore $X_4^2 + X_6^2 \equiv X_5^2 + X_6^2 \equiv 0, \pmod 2$ which forces $X_4 \equiv X_5 \equiv X_6, \pmod 2$. Together with $X_4X_5 + X_5X_6 + X_4X_6 \equiv 0, \pmod 2$, this yields $X_4 \equiv X_5 \equiv X_6 \equiv 0, \pmod 2$. This completes the proof that $w \in Q$. □

4.2 The algebra with group Sym(4) of shape (2A,3C)

Notation 4.2.1. Let T be the set of involutions in Sym(4). Let V denote the rational subalgebra generated by the axes of the algebra of shape $(2A, 3C)$ as described in [IPSS10, §4.4]. Explicitly, V has a $\mathbb{Q}$-basis $\{a_t : t \in T\}$ where each a_t is an axis. For simplicity of notation, we omit the parenthesis on transpositions in this context, e.g. $a_{12} = a_{(12)}$. For an involution equal to a product of two transpositions, we separate the transpositions by a comma, e.g. $a_{12,34} = a_{(12)(34)}$.

Each axis is an idempotent, so $a_t^2 = a_t$ for all $t \in T$. For any pair of commuting involutions $s, t \in T$, the triplet a_s, a_t, a_{st} generate a $2A$-subalgebra [Lemma 3.1, IPSS10], meaning that $a_s \cdot a_t = \frac{1}{8}(a_s + a_t - a_{st})$. The remaining products in the algebra are given by the following formulas [IPSS,§4.4] (this is for any permuation $\{i, j, k, \ell\} = \{1, 2, 3, 4\}$):

$$
\begin{aligned}
a_{ij} \cdot a_{ik} &= \frac{1}{2^6}(a_{ij} + a_{ik} - a_{jk}),\\
a_{ij} \cdot a_{ik,j\ell} &= \frac{1}{2^6}(a_{ij} + a_{ik,j\ell} - a_{k\ell} - a_{i\ell,jk} + a_{ij,k\ell}).
\end{aligned}
$$

Definition 4.2.2. Define the following elements of V:

$$
\begin{aligned}
m_1 &= I = \frac{16}{105}\left(4a_{12,34} + 4a_{13,24} + 4a_{14,23} + 5a_{12} + 5a_{13} + 5a_{14} + 5a_{23} + 5a_{24} + 5a_{34}\right),\\
m_2 &= \frac{16}{5}\left(a_{12,34} + a_{13,24} + a_{14,23}\right),\\
m_3 &= 32a_{13,24},\\
m_4 &= 32a_{14,23},\\
m_5 &= 32\left(a_{13} + a_{24}\right),\\
m_6 &= 32\left(a_{14} + a_{23}\right),\\
m_7 &= 32\left(a_{23} - a_{14}\right),\\
m_8 &= 32\left(a_{24} - a_{13}\right),\\
m_9 &= 32\left(a_{34} - a_{12}\right).
\end{aligned}
$$

Define $M = \mathrm{span}_{\mathbb{Z}}(m_i : 1 \leqslant i \leqslant 9)$. The fact that M is a G-invariant integral form is a straightforward calculation [★2A3C.1].

Lemma 4.2.3. *Define the following subspaces of V:*

$$
\begin{aligned}
V(1) &= \operatorname{span}_{\mathbb{Q}}\left(\textstyle\sum_{t\in T\setminus Alt(4)} a_t,\ \sum_{t\in T\cap Alt(4)} a_t\right),\\
V(2) &= \operatorname{span}_{\mathbb{Q}}(a_{13,34}-a_{14,23},\ a_{12,34}-a_{14,23},\ a_{13}+a_{34}-a_{14}-a_{23},\ a_{12}+a_{34}-a_{14}-a_{23}),\\
V(3) &= \operatorname{span}_{\mathbb{Q}}(m_7,\ m_8,\ m_9).
\end{aligned}
$$

Then $V = V(1)+V(2)+V(3)$ is the decomposition of V into isotypic subspaces with respect to the action of G.

Proof. All of the irreducible complex representations of $\mathrm{Sym}(4)$ are rational, so the representation V will decompose into these familiar complex representations. Let N denote the normal subgroup $\{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ of $G = \mathrm{Sym}(4)$. There is a unique irreducible $\mathbb{Q}[G]$-module for which N acts nontrivially. It is three dimensional. The remaining 4 irreducible representations come from inflating the irreducible representations of $G/N \cong \mathrm{Sym}(3)$ to G. Note that G acts transitively on the set $\{m_7, m_8, m_9\}$ and also N acts nontrivially on this space. Hence $V(3)$ is isomorphic to the unique 3-dimensional irreducible $\mathbb{Q}[G]$-module.

The two spaces $\operatorname{span}_{\mathbb{Q}}(a_{ij,kl} : \ \{i,j,k,l\} = \{1,2,3,4\})$ and $\operatorname{span}_{\mathbb{Q}}(a_{ij}+a_{kl} : \ \{i,j,k,l\} = \{1,2,3,4\})$ are both submodules and they are isomorphic as G-modules under the map defined by $a_{ij,kl} \mapsto a_{ij}+a_{kl}$. The former decomposes as a one-dimensional trivial module plus a nontrivial two dimensional module:

$$
\begin{aligned}
&\operatorname{span}_{\mathbb{Q}}(a_{ij,kl} : \{i,j,k,l\} = \{1,2,3,4\}) = \\
&\qquad\qquad \operatorname{span}_{\mathbb{Q}}\left(\textstyle\sum_{t\in T\cap \mathrm{Alt}(4)} a_t\right) \oplus \operatorname{span}_{\mathbb{Q}}(a_{13,24}-a_{14,23}, a_{12,34}-a_{14,23})
\end{aligned}
$$

□

Lemma 4.2.4. *If $v \in V(1)$ is in a GIIF then $v \in M$.*

Proof. From the definitions of $m_1 = I$ and m_2, we can see that $V(1) = \operatorname{span}_{\mathbb{Q}}(I, m_2)$. Suppose $v = xI + ym_2$ is in a GIIF for some $x, y \in \mathbb{Q}$.

We compute [★`2A3C.2`] that $ad(m_2)$ has eigenvalues 0, 1, and 4. Thus x and $x+y$ and $x+4y$ are (rational) eigenvalues of $xI+ym_2$. By the variant of Gauss' lemma (2.1.7), both x and $x+y$ are integers. Hence y is also an integer. □

Lemma 4.2.5. *If $v = 16x(a_{13,24} - a_{14,23}) + 16y(a_{13} + a_{24} - a_{14} - a_{23})$ is in a GIIF for some $x, y \in \mathbb{Q}$, then $x, y \in \mathbb{Z}$.*

Proof. We can compute the characteristic polynomial of $\mathrm{ad}(v)$ in factored form to be [★`2A3C.3`]:

$$-t^3\left(t^2 - 381y^2\right)\left(t - \frac{1}{2}(7x+31y)\right)\left(t + \frac{1}{2}(7x+31y)\right)\left(t^2 - 13(4x+y)^2\right)$$

By the variant of Gauss' lemma (2.1.7), all of the coefficients ($381y^2$, $\frac{7x+31y}{2}$, and $13(4x+y)^2$) are integers. Since $381y^2 = 3\cdot 127y^2$ it follows that $y\in\mathbb{Z}$. Similarly, $13(4x+y)^2$ being an integer implies $4x+y$ is an integer, which then implies $4x\in\mathbb{Z}$.

Then $(7x+31y)\in 2\mathbb{Z}$ implies $7x\in\mathbb{Z}$ and therefore $x\in\mathbb{Z}$. □

Lemma 4.2.6. *If $v\in V(2)$ is in a GIIF, then $12v\in M$.*

Proof. First observe that M contains the following four elements:

$$\begin{aligned}
32(a_{13,24} - a_{14,23}) &= m_3 - m_4,\\
32(a_{12,34} - a_{14,23}) &= \tau(a_{14})(m_3 - m_4),\\
32(a_{13} + a_{24} - a_{14} - a_{23}) &= m_5 - m_6,\\
32(a_{12} + a_{34} - a_{14} - a_{23}) &= \tau(a_{14})(m_5 - m_6).
\end{aligned}$$

Write $v = 32x_1(a_{13,24} - a_{14,23}) + 32x_2(a_{12,34} - a_{14,23}) + 32x_3(a_{13} + a_{24} - a_{14} - a_{23}) + 32x_4(a_{12} + a_{34} - a_{14} - a_{23})$ for some scalars $x_1, x_2, x_3, x_4 \in \mathbb{Q}$. To show that $12v \in M$ we need to show that $12x_i$ is an integer for each $i = 1, 2, 3, 4$.

We compute the following actions of certain elements in $\mathbb{Z}[G]$ on v [★2A3C.4]:

$$[(12) - \mathrm{id}][(34) - \mathrm{id}]\, v = \\ [4x_1 + 2x_2]\, 32(a_{13,24} - a_{14,23}) + [4x_3 + 2x_4]\, 32(a_{13} + a_{24} - a_{14} - a_{23}),$$

$$[(12) - \mathrm{id}][(34) - \mathrm{id}](13)\, v = \\ [2x_1 - 2x_2]\, 32(a_{13,24} - a_{14,23}) + [2x_3 - 2x_4]\, 32(a_{13} + a_{24} - a_{14} - a_{23}).$$

Both of these elements are in the GIIF containing v, and by Lemma 4.2.5, the coefficients $4x_1 + 2x_2, 4x_3 + 2x_4,\ 2x_1 - 2x_2,$ and $2x_3 - 2x_4$ are in $\frac{1}{2}\mathbb{Z}$. Therefore the following are also in $\frac{1}{2}\mathbb{Z}$:

$$\begin{aligned} 6x_1 &= (4x_1 + 2x_2) + (2x_1 - 2x_2), \\ 6x_2 &= (4x_1 + 2x_2) - 2(2x_1 - 2x_2), \\ 6x_3 &= (4x_3 + 2x_4) + (2x_3 - 2x_4), \\ 6x_4 &= (4x_3 + 2x_4) - 2(2x_3 - 2x_4). \end{aligned}$$

So $12x_i \in \mathbb{Z}$ for $i = 1, 2, 3, 4$. Therefore, $12v \in M$. □

Lemma 4.2.7. *If $v \in V(3)$ is in a GIIF, then $4v \in M$.*

Proof. We compute that $m_i \cdot m_j = m_k$ for any permutation $\{i, j, k\} = \{7, 8, 9\}$ [★2A3C.5]. Fix $i \in \{7, 8, 9\}$. The the orbit of m_i under G contains $\{m_7, m_8, m_9\}$. So if sm_i were in a GIIF for some rational s, then this GIIF would contain $\mathrm{rng}(G \cdot sm_i) = \mathrm{rng}(\{sm_7, sm_8, sm_9\})$ which contains $s^n m_i$ for every positive integer n. So s must be an integer.

Write $v = x_7 m_7 + x_8 m_8 + x_9 m_9$ for some $x_7, x_8, x_9 \in \mathbb{Q}$. It is easy to verify that

$$\begin{aligned} &m_7 \in V^{-(12)(34),-(13)(24)}, \\ &m_8 \in V^{-(12)(34),(13)(24)}, \quad \text{and} \\ &m_9 \in V^{(12)(34),-(13)(24)}. \end{aligned}$$

So

$$[\mathrm{id} - (12)(34)][\mathrm{id} - (13)(24)]\, v = 4x_7 m_7,$$
$$[\mathrm{id} - (12)(34)][\mathrm{id} + (13)(24)]\, v = 4x_8 m_8,$$
$$[\mathrm{id} + (12)(34)][\mathrm{id} - (13)(24)]\, v = 4x_9 m_9.$$

All three of these elements are in the GIIF containing v. By the previous paragraph, $4x_7, 4x_8, 4x_9 \in \mathbb{Z}$. Therefore $4v \in \mathrm{span}_{\mathbb{Z}}(m_7, m_8, m_9) \subseteq M$. □

Lemma 4.2.8. *There is no GIIF L such that 2 divides $[L + M : M]$.*

Proof. If there were such a GIIF then Proposition 2.2.6 guarantees existence of a GIIF L not contained in M with $2L \subseteq M$.

Let v be an element of L. Write $v = \frac{1}{2}\sum_{i=1}^{9} X_i m_i$ for some integers $X_1, \ldots, X_9$. Then set $x_i = X_i/2$ for all $i = 1, \ldots, 9$. The goal then is to show that each x_i is an integer, which will prove that $v \in M$ and thus contradict the fact that L is not contained in M.

For $i = 1, \ldots, 9$, define $\mu_1, \ldots, \mu_9$ to be the basis of V^* dual to the basis $m_1, \ldots m_9$ of V. Explicitly, for $y_1, \ldots, y_9 \in \mathbb{Q}$ we have $\mu_i : \sum_{j=1}^{9} y_j m_j \mapsto y_i$. If $\ell \in L$ then since $2\ell \in M$, we have that $2\mu_i(\ell) \in \mathbb{Z}$ for all $i = 1, \ldots, 9$.

We compute [$\bigstar$`2A3C.6`]:

$$2\mu_1(v \cdot v) = \frac{X_1^2}{2} + 504X_9^2 - 42X_5X_6$$

This being an integer implies X_1 is even, so $x_1 \in \mathbb{Z}$. Since this is true for an arbitrary v, this implies $\mu_1(\ell) \in \mathbb{Z}$ for all $\ell \in L$.

We compute $\mathrm{trace}(v) = 9x_1 + \frac{15X_2}{2} + 25X_3 + 25X_4 + 43X_5 + 43X_6$. Therefore x_2 is an integer. We then compute [$\bigstar$`2A3C.8`]:

$$\mu_1(v \cdot (\tau(a_{13})v)) = 21x_1X_6 + x_1^2 + \frac{21X_6^2}{2} - 252X_7X_9,$$
$$\mu_1(v \cdot (\tau(a_{23})v)) = 21x_1X_5 + x_1^2 + \frac{21X_5^2}{2} + 252X_8X_9.$$

Hence x_5 and x_6 are integers.

We compute the following [$\bigstar$`2A3C.9`]:

$$2\kappa\left(v,\tau\left(a_{24}\right)\tau\left(a_{12}\right)v\right)\equiv\frac{273X_3^2}{2}+\frac{273X_4^2}{2}+\frac{1427X_3X_4}{2},\quad(\text{mod }\mathbb{Z}[x_1,x_2,X_3,X_4,x_5,x_6,X_7,X_8,X_9]).$$

Therefore $X_3^2+X_3X_4+X_4^2\equiv 0,\ (\text{mod }2)$, which has only the trivial solution $X_3\equiv X_4\equiv 0$, $(\text{mod }2)$. So x_3 and x_4 are integers.

Then we compute [$\bigstar$`2A3C.10`]:

$$\begin{aligned}
\kappa\left(v,\tau\left(a_{12}\right).v\right)&\equiv\frac{833X_9^2}{2},\quad(\text{mod }\mathbb{Z}[x_1,x_2,x_3,x_4,x_5,x_6,X_7,X_8,X_9]),\\
\kappa\left(v,\tau\left(a_{13}\right).v\right)&\equiv\frac{833X_8^2}{2},\quad(\text{mod }\mathbb{Z}[x_1,x_2,x_3,x_4,x_5,x_6,X_7,X_8,X_9]),\\
\kappa\left(v,\tau\left(a_{14}\right).v\right)&\equiv\frac{833X_7^2}{2},\quad(\text{mod }\mathbb{Z}[x_1,x_2,x_3,x_4,x_5,x_6,X_7,X_8,X_9]).
\end{aligned}$$

These being integers imply that x_9,x_8,x_7 are integers. This completes the proof that $v\in M$. Therefore there is no element in $(L+M)/M$ of order 2. $\square$

Lemma 4.2.9. *There is no GIIF L of V with $[L+M:M]$ divisible by 3.*

Proof. If there were such a GIIF, then Proposition 2.2.6 guarantees existence of a GIIF L not contained in M with $3L\subseteq M$.

Let v be an element of L. Write $v=\frac{1}{3}\sum_{i=1}^{9}X_im_i$ for some integers $X_1,\ldots,X_9$. Define $x_i=X_i/3$ for $i=1,\ldots,9$. Our goal is to show that each x_i is an integer, because this will imply $v\in M$ which will contradict the fact that $L\nsubseteq M$.

For $i=1,\ldots,9$, recall the definition of the component functions $\mu_i:V\to\mathbb{Q}$ defined by $\mu_i:\sum_{j=1}^{9}y_jm_i\mapsto y_i$. If $\ell\in L$ then since $3\ell\in M$, we have that $3\mu_i(\ell)\in\mathbb{Z}$ for all $i=1,\ldots,9$.

Compute the following [$\bigstar$`2A3C.11`]:

$$3\mu_1(v\cdot v)=\frac{X_1^2}{3}+336X_9^2-28X_5X_6,$$

Therefore 3 divides X_1. Since this is true for an arbitrary $v\in L$, it follow that $\mu_1(\ell)\in\mathbb{Z}$ for all $\ell\in L$. Write $X_1=3x_1$ for an integer x_1.

We compute [★2A3C.12]:

$$\mu_1\big(v \cdot [\tau(a_{34})\,\tau(a_{13,24})\,v]\big) = x_1^2 - 112X_9^2 - \frac{14X_5^2}{3} - \frac{14X_6^2}{3}.$$

Therefore $X_5^2 + X_6^2 \equiv 0, \pmod 3$, which has only the trivial solution $X_5 \equiv X_6 \equiv 0, \pmod 3$. So write $X_5 = 3x_5$ and $X_6 = 3x_6$ for integers x_5 and x_6. Since this is true for an arbitrary $v \in L$, it follows that for any $\ell \in L$ both $\mu_5(\ell)$ and $\mu_6(\ell)$ are integers. We compute [★2A3C.13]:

$$\mu_5\big(v \cdot [\tau(a_{13,24})\,v]\big) = 40x_5^2 + 2x_1x_5 + 4x_6x_5 + \frac{8X_8^2}{3} + \frac{8X_9^2}{3},$$
$$\mu_6\big(v \cdot [\tau(a_{13,24})\,v]\big) = 40x_6^2 + 2x_1x_6 + 4x_5x_6 + \frac{8X_9^2}{3} - \frac{8X_7^2}{3}.$$

Again, since $x^2 + y^2 \equiv 0, \pmod 3$ has only the trivial solution, it follows that $X_8 \equiv X_9 \equiv 0,$ $\pmod 3$. Then the second equation implies $X_7 \equiv 0 \pmod 3$. For for $i = 7, 8, 9$, write $X_i = 3x_i$ with $x_i \in \mathbb{Z}$.

We next compute [★2A3C.14]:

$$3\kappa(v,\, v) - 3\kappa\,(v,\, \tau(a_{13})\,v) = 850x_6X_4 + 7611x_6^2 + 4998x_7^2 + 4998x_9^2 + 9996x_7x_9 + \frac{881X_4^2}{3}.$$

So $X_4 \in 3\mathbb{Z}$. And $\mathrm{trace}(v) = 9x_1 + 86x_5 + 86x_6 + 5X_2 + \frac{50X_3}{3} + \frac{50X_4}{3}$ ([★2A3C.15]) then implies that $X_3 \in 3\mathbb{Z}$. So write $X_3 = 3x_3$ and $X_4 = 3x_4$ for integers x_3 and x_4.

Finally, we compute [★2A3C.16]:

$$3\mu_2(v \cdot v) = 2x_1X_2 - 336x_9^2 - 240x_3x_4 - 60x_4x_5 - 60x_3x_6 + 48x_5x_6 + \frac{4X_2^2}{3},$$

This being an integer implies $X_2 \in 3\mathbb{Z}$ which completes the proof that $v \in M$. So there is no element of order 3 in $(L + M)/M$. □

Theorem 4.2.10. *The GIIF M is the unique maximal GIIF in the algebra V of shape* $(2A, 3C)$

Proof. Let χ be a character of an irreducible $\mathbb{Q}$-representation of G. Then the element $e_\chi = \frac{\chi(1)}{|G|}\sum_{g\in G}\chi(g^{-1})g \in \mathbb{Q}[G]$ acts on any $\mathbb{Q}[G]$-module as the identity on any irreducible subrepresentation affording χ and acts as 0 on any irreducible representation affording a different character. In other words, e_χ acts as the projection on the isotypical submodule corresponding to χ, in any rational representation of G.

Let v be an element in a GIIF L. Write $v = v_1 + v_2 + v_3$ where $v_i \in V(i)$ for $i = 1, 2, 3$. Then L is closed under the action of $|G|e_\chi = 24e_\chi \in \mathbb{Z}[G]$. Therefore $24v_i \in L$ for $i = 1, 2, 3$. Then Lemmas 4.2.4, 4.2.6, and 4.2.7 imply that $12 \cdot 24v_i \in M$ for $i = 1, 2, 3$. Therefore $12 \cdot 24v \in M$. However $12 \cdot 24 = 2^5 3^2$ is coprime to the order of $(L + M)/M$ by Lemmas 4.2.8 and 4.2.9. Thus $v + M = M$ and so $v \in M$. $\square$

4.3 The Lam-Chen algebra with group $3^2 : 2$.

Notation 4.3.1. Throughout this section, V will be the nine dimensional Griess algebra described in Lemma 3.2 of [CL14], defined over $\mathbb{Q}$. So V is a nine-dimensional rational vector space, with basis $\{e_u : u \in \mathbb{F}_3^2\}$ where each $\frac{1}{2}e_u$ is an axis. The algebra product is given by:

$$e_u \cdot e_v = \begin{cases} \frac{1}{32}(e_u + e_v - e_{-u-v}) & \text{if } u \neq v \\ 2e_u & \text{if } u = v. \end{cases}$$

Define $\tau_u = \tau(\frac{e_u}{2})$ for all $u \in \mathbb{F}_3^2$.

Lemma 4.3.2. *For any $u \in \mathbb{F}_3^2$, the trace of $ad(e_u)$ is $\frac{9}{4}$. The mutliplicative identity I of V is $\frac{4}{9}\sum_{u\in\mathbb{F}_3^2} e_u$.*

Proof. The products in Notation 4.3.1 show that $\mathrm{trace}(e_u) = 8 \cdot (1/32) + 2 = 9/4$.

If we define $v = \sum_{s\in\mathbb{F}_3^2} e_s$, then $v \cdot e_u = 2e_u + \sum_{s\neq u,\ s\in\mathbb{F}_3^2} e_s \cdot e_u$ will be a multiple of e_u since each term $\frac{1}{32}(e_u + e_s - e_{-u-s})$ in the sum will have a corresponding term $\frac{1}{32}(e_u + e_{-s-u} - e_s)$. Besides the term $2e_u$ there are 8 other terms which sum to $8 \cdot \frac{1}{32}e_u = \frac{1}{4}e_u$. Therefore v acts as the scalar $2 + \frac{1}{4} = \frac{9}{4}$ on each basis element, and therefore $\frac{4}{9}v$ is the multiplicative identity. □

Lemma 4.3.3. *The automorphism group of the algebra V is isomorphic to $AGL(2,3) = 3^2 : GL(2,3)$.*

Proof. One can show by direct calculation that $\{\frac{1}{2}e_u : u \in \mathbb{F}_3^2\}$ is exactly the set of idempotents in V whose trace equals 9/8 [$\bigstar$`LC.1`]. Therefore $\mathrm{Aut}(V)$ must preserve this set. So $\mathrm{Aut}(V)$ has a faithful permutation representation on the set $\mathbb{F}_3^2$.

Let f be an automorphism of V, which we also think of as an element in $\mathrm{Sym}(\mathbb{F}_3^2)$. Given any $x \neq y \in \mathbb{F}_2^3$ we claim that $f(-x-y) = -f(x) - f(y)$. To see this, we expand out $f(e_x \cdot e_y)$ in two ways:

$$\begin{aligned} f(e_x \cdot e_y) = f\left(\frac{1}{24}(e_x + e_y - e_{-x-y})\right) &= \frac{1}{32}[e_{f(x)} + e_{f(y)} - e_{f(-x-y)})] \\ f(e_x) \cdot f(e_y) = e_{f(x)} \cdot e_{f(y)} &= \frac{1}{32}[e_{f(x)} + e_{f(y)} - e_{-f(x)-f(y)}]. \end{aligned} \tag{4.1}$$

Since these expressions are equal, $f(-x-y) = -f(x) - f(y)$.

The set of all three element subsets in $\{\{x, y, -x-y\} : x, y \in \mathbb{F}_3^2, x \neq y\}$ is equal to the set of affine lines in $\mathbb{F}_3^2$. To see this, note that $\{x, y, -x-y\} = x + \{0, y-x, 2y-2x\} = x + \mathbb{F}_3(y-x)$. Since $f(-x-y) = -f(x) - f(y)$ it follows that f sends affine lines to affine lines. Therefore, for any k-dimensional affine subset U of $\mathbb{F}_3^2$ $(0 \leqslant k \leqslant 2)$, $f(U)$ is also an affine subset of dimension k. It follows that f acts on $\mathbb{F}_3^2$ as an invertible affine transformation, hence $f \in AGL(2, 3)$.

Conversely, let f be any element in $AGL(2, 3)$ which acts linearly on V by permuting the basis elements: $f(e_u) = e_{f(u)}$. We first observe:

$$f(e_x \cdot e_x) = f(2e_x) = 2e_{f(x)} = e_{f(x)} \cdot e_{f(x)} = f(e_x) \cdot f(e_x).$$

For any two distinct elements $x, y \in \mathbb{F}_3^2$, the map f transforms the affine line $\{x, y, -x-y\}$ into $\{f(x), f(y), f(-x-y)\}$ which must also be an affine line, and hence $f(-x-y) = -f(x) - f(y)$. Then this shows that the two lines in (4.1) are equal, which proves that f acts on V as an automorphism. $\square$

This shows in particular that $G \cong 3^2 : 2$ can be views as a subset of $AGL(2, 3)$. In particular, $O_3(G)$ must be identified with $(\mathbb{F}_3^2, +)$, which is the unique subgroup of order 9 in $AGL(2, 3)$. An element $u \in \mathbb{F}_3^2$ acts on V by the rule $u \cdot e_v = e_{v+u}$. Also, observe that for any $u \in \mathbb{F}_3^2$, e_u, e_0, e_{-x} span a subgroup isomorphic to the 3C-algebra. So τ_0 interchanges e_x with e_{-x}. So with respect to the identification of $\mathrm{Aut}(V)$ with $AGL(2, 3)$, the subgroup G is identified with $(\mathbb{F}_3^2, +) \rtimes \{\pm I\}$.

Definition 4.3.4. For any affine line L of $\mathbb{F}_3^2$, define $v_L = \dfrac{32}{3} \sum_{u \in L} e_u$.

Notation 4.3.5. For a subset S of $\mathbb{F}_3^2$, $\langle S \rangle$ is the additive subgroup generated by S. If $s, r \in \mathbb{F}_3^2$ with $s \neq 0$, $r + \langle s \rangle$ is the affine line parallel to $\langle s \rangle$ containing r.

Lemma 4.3.6.

(i) For each nontrivial proper subgroup H of $O_3(G)$, there is a two dimensional rational irreducible representation of G with kernel H.

(ii) *G has six rational irreducible representations: four of which are two-dimensional, and two of which are one-dimensional.*

(iii) *The $\mathbb{Q}[G]$-module V decomposes as the direct sum of all four two-dimensional irreducibles plus the one-dimensional trivial representation.*

(iv) *If $\langle s, r\rangle = \mathbb{F}_3^2$, then $V^s = \operatorname{span}_{\mathbb{Q}}(v_{\langle s\rangle}, v_{r+\langle s\rangle}, v_{2r+\langle s\rangle})$.*

Proof. The quotient $G/H \cong \mathrm{Sym}(3)$ has a faithful two-dimensional rational irreducible which inflates to a representation of G. Note that $G/O_3(G) \cong \mathbb{Z}/2\mathbb{Z}$ has two one-dimensional complex irreducible representations, both of which are rational. Then $|G| = 18 = 4(2^2) + 1^2 + 1^2$ so these 6 are all of the complex irreducible representations of G and all of these are rational.

We identify G with $\mathbb{F}_3^2 \rtimes \{\pm I\}$. Suppose $\{r, s\}$ is a basis of $\mathbb{F}_3^2$. Because $\{0, s, 2s\}$ is a normal subgroup in G, this implies that V^s is a G-submodule of V. Also V^s contains $\{v_{0+\langle s\rangle}, v_{r+\langle s\rangle}, v_{2r+\langle s\rangle}\}$ which are linearly independent since they are defined by taking sums of elements $\frac{32}{3}e_u$ for u in disjoint (in fact, parallel) affine lines in $\mathbb{F}_3^2$. So V^s is at least three-dimensional. And since $r \cdot v_{r+\langle s\rangle} = v_{2r+\langle s\rangle}$, we have that r acts nontrivially on V^s. So V^s contains the two-dimensional irreducible on which s acts trivially but not all of $O_3(G)$ acts trivially. Since s was arbitrary, V contains all four such irreducibles. Then V also contains the trivial representation $\operatorname{span}_{\mathbb{Q}}(I)$. Since $\dim V = 9$, this accounts for the complete decomposition of V.

We have shown that r acts nontrivially on V^s, and by symmetry, s acts nontrivially on each of the three two-dimensional irreducibles whose kernel is not $\langle s\rangle$. So V^s is a G-submodule with dimension at least three, but the only irreducible representations of G it can contain are the trivial one and the two-dimensional irreducible with kernel $\langle s\rangle$. Thus $\dim(V^s) = 3$ and the three elements $v_{\langle s\rangle}, v_{r+\langle s\rangle}, v_{2r+\langle s\rangle}$ are a basis. $\square$

Lemma 4.3.7. *Suppose $\mathbb{F}_3^2 = \langle r, s\rangle$. If L is a GIIF of V, then $L \cap V^s \subseteq \operatorname{span}_{\mathbb{Z}}(I, v_{r+\langle s\rangle}, v_{2r+\langle s\rangle})$.*

Proof. We have shown that $v_{\langle s\rangle}, v_{r+\langle s\rangle}, v_{2r+\langle s\rangle}$ is a basis of V^s (Lemma 4.3.6(iv)). We have $I = \frac{1}{24}\left(v_{\langle s\rangle} + v_{r+\langle s\rangle} + v_{2r+\langle s\rangle}\right)$, and so $I, v_{r+\langle s\rangle}, v_{2r+\langle s\rangle}$ is also a basis of V^s.

For computational purposes, we will first prove this result for the specific case $r' = (0,1)$ and $s' = (1,0)$. Write $w = xI + yv_{r'+\langle s'\rangle} + zv_{2r'+\langle s'\rangle}$. Then we compute the following [$\bigstar$`LC.2`]:

$$\kappa(w, \tau_0(w) - w) = 1326(y-z)^2,$$
$$\kappa(w, \tau_{r'}(w) - w) = 1326z^2.$$

Since $1326 = 2 \cdot 3 \cdot 13 \cdot 17$ is square-free, this implies that both $y - z$ and z are integers and so y is also an integer. We also compute that [$\bigstar$`LC.3`]

$$w \cdot (e_0 - e_{-s'}) = (x+y+z)(e_0 - e_{-s'}).$$

So $\mathrm{ad}(w)$ has $x + y + z$ as an eigenvalue, and the variant of Gauss' lemma (2.1.7) implies that $x + y + z \in \mathbb{Z}$. Therefore $x \in \mathbb{Z}$.

Now we let r, s be an arbitrary basis of $\mathbb{F}_3^2$. There is some $\phi \in GL(2,3)$ such that $\phi(r) = r' = (0,1)$ and $\phi(s) = s' = (1,0)$. Under the identification $\mathrm{Aut}(V) \cong AGL(2,3)$, we may view ϕ as an automorphism of V by the rule $\phi(e_u) = e_{\phi(u)}$, for all $u \in \mathbb{F}_3^2$, and therefore $\phi(v_U) = v_{\phi(U)}$ for any affine line $U \subseteq \mathbb{F}_3^2$.

So now suppose that $w' = x'I + y'v_{r+\langle s\rangle} + z'v_{2r+\langle s\rangle}$ is in a GIIF L for some $x', y', z' \in \mathbb{Q}$. Then $\phi(L)$ is also an integral form, and this will also be G-invariant since G is normal in $\mathrm{Aut}(V)$. Explicitly: for $g \in G$ we have $g\phi(L) = \phi\phi^{-1}g\phi(L) \subseteq \phi(L)$. So $\phi(w) = x'I + y'v_{r+\langle s'\rangle} + z'v_{2r'+\langle s'\rangle}$ is in the GIIF $\phi(L)$. By the previous calculation, $x', y', z' \in \mathbb{Z}$. $\square$

Definition 4.3.8. Define $\mathcal{Q}$ to be the set containing I and v_U for every affine line U of $\mathbb{F}_3^2$ that does not pass through the origin. Set $Q = \mathrm{span}_{\mathbb{Z}}(\mathcal{Q})$.

Lemma 4.3.9. *The set $\mathcal{Q}$ is a $\mathbb{Q}$-basis of V, and Q is an $\mathrm{Aut}(V)$-invariant integral form.*

Proof. There are four linear one-dimensional subspaces in $\mathbb{F}_3^2$, and each one has two nontrivial affine translations that do not contain the origin. So $\mathcal{Q}$ contains 9 elements. So we aim to show that $\mathcal{Q}$ spans V. Suppose $\mathbb{F}_3^2 = \langle r, s\rangle$. Recall that $I = \frac{1}{24}(v_{\langle s\rangle} + v_{r+\langle s\rangle} + v_{2r+\langle s\rangle})$ and so $v_{\langle s\rangle}$ is also in $\mathrm{span}_{\mathbb{Q}}(\mathcal{Q})$, and in particular $\mathrm{span}_{\mathbb{Q}}(\mathcal{Q})$ contains v_U for every affine line $U \subseteq \mathbb{F}_3^2$.

Then $\mathrm{span}_{\mathbb{Q}}(\mathcal{Q})$ contains $V^s = \mathrm{span}_{\mathbb{Q}}(v_{\langle s\rangle}, v_{r+\langle s\rangle}, v_{2r+\langle s\rangle})$ (Lemma 4.3.6(iv)). Contained in V^s is the 2-dimensional irreducible $\mathbb{Q}[G]$-module with kernel $\langle s\rangle$. The decomposition of V as a G-module (Lemma 4.3.6(iii)) shows that $\mathrm{span}_{\mathbb{Q}}(Q)$ contains all of V.

For any $f \in AGL(2,3)$ and any $u \in \mathbb{F}_3^2$, recall that $f(e_u) := e_{f(u)}$ defines an identification of $AGL(2,3)$ with $\mathrm{Aut}(V)$. For any affine line $U \subseteq \mathbb{F}_3^2$ we have $f(v_U) = v_{f(U)}$ and hence $\mathrm{span}_{\mathbb{Z}}(Q)$ is invariant under $\mathrm{Aut}(V)$.

The proof that Q is closed under the algebra products is a straightforward calculation [`✶LC.4`]. $\square$

Lemma 4.3.10. *If L is a GIIF of the Lam-Chen algebra, then $9L \subseteq Q$.*

Proof. We may assume L is a maximal GIIF, and in particular $I \in L$. Let $V = \mathrm{span}_{\mathbb{Q}}(I) + V_1 + V_2 + V_3 + V_4$ be the decomposition of V into irreducible representations of G, where each V_i is two-dimensional. Let $\langle s_i \rangle \subset G$ be the kernel of the representation V_i. Suppose $v = xI + v_1 + v_2 + v_3 + v_4$ is in a GIIF, with $x \in \mathbb{Q}$ and $v_i \in V_i$ for $i = 1, 2, 3, 4$.

Because $\mathrm{trace}(I) = 9 \neq 0$, it follows that the kernel K of the trace function $V \to \mathbb{Q}$ is a codimension one subspace, which is also G-invariant. Based on the decomposition given in Lemma 4.3.6, the only possibility is $K = V_1 + V_2 + V_3 + V_4$. Therefore $\mathrm{trace}(w) = 9x$ is an integer.

Note that s_i acts on V_j without fixed points, if $i \neq j$. So $2s_i + s_i + 1$ annihilates V_j if $i \neq j$. For any $i \in \{1, 2, 3, 4\}$, the following is in L: $3(2s_i + s_i + 1)v = 9xI + 9v_i$. This element is in V^{s_i} and Lemma 4.3.7 implies it is in Q. Since $9xI \in \mathbb{Z}I \subset Q$ this implies $9v_i \in Q$. Since this is true for an arbitrary i, and since $9xI \in Q$, the lemma is established. $\square$

Notation 4.3.11. The element $-I$ in $AGL(2,3)$ induces the automorphism of V which sends v_U to v_{-U} for any affine line U not passing through the origin. Thus the elements $v_U + v_{-U}$ and $v_U - v_{-U}$ will be the $+1$ and -1 eigenvectors of this automorphism.

To perform calculations with respect to this eigenspace decomposition, we need to make an explicit choice of half of the eight affine lines that do not pass through the origin. We define the following four affine lines:

$$U_1 = (1,0) + \langle (0,1) \rangle, \qquad U_3 = (1,0) + \langle (1,2) \rangle,$$
$$U_2 = (1,0) + \langle (1,1) \rangle, \qquad U_4 = (0,1) + \langle (1,0) \rangle.$$

For $i = 1,2,3,4$, we define $f_i = v_{U_i} + v_{-U_i}$ and $n_i = v_{U_i} - v_{-U_i}$.

Then set $\mathcal{B}_+ = \{I, f_1, f_2, f_3, f_4\}$ and $\mathcal{B}_- = \{n_1, n_2, n_3, n_4\}$.

Lemma 4.3.12.

(i) $\mathcal{B}_+$ *is a* $\mathbb{Q}$*-basis for* V^{τ_0}

(ii) $\mathcal{B}_-$ *is a* $\mathbb{Q}$*-basis for* $V^{-\tau_0}$.

Furthermore, Let L be a GIIF such that $3L \subseteq Q$*. Then,*

(iii) $L \cap V^{\tau_0} \subseteq \operatorname{span}_{\mathbb{Z}}(\mathcal{B}_+)$.

(iv) $L \cap V^{-\tau_0} \subseteq \operatorname{span}_{\mathbb{Z}}(\mathcal{B}_-)$.

Proof. First, we note that $\tau_0 = \tau\left(\frac{1}{2}e_0\right)$ fixes e_0. Hence in the identification of G with $\mathbb{F}_3^2 \rtimes \{\pm I\}$, the element τ_0 corresponds to $-I$.

It is clear that τ_0 fixes each element of $\mathcal{B}_+$ and it negates each element of $\mathcal{B}_-$. To prove (i) and (ii), it suffices to show that $\mathcal{B}_+ \cup \mathcal{B}_-$ is a basis of V.

Observe that $\{U_i : i = 1,2,3,4\} \cup \{-U_i : i = 1,2,3,4\}$ is the set of all 8 affine lines in $\mathbb{F}_3^2$ which do not pass through the origin. For any $i = 1,2,3,4$, we have $2v_{U_i} = f_i + n_i$ and $2v_{-U_i} = f_i - n_i$. Thus $\operatorname{span}_{\mathbb{Q}}(\mathcal{B}_+ \cup \mathcal{B}_-)$ contains v_U for every affine line U not passing through the origin and it also contains I. So $\mathcal{B}_+ \cup \mathcal{B}_-$ is a basis of V, which proves (i) and (ii).

Let w be an arbitrary element in $L \cap V^{\tau_0}$. By hypothesis, we may write $w = \frac{1}{3}yI + \frac{1}{3}\sum_{i=1}^{4} X_i f_i$ with y and each X_i an integer.

We compute the following, which all must be integers integers [★`LC.5`]:

$$
\begin{aligned}
\kappa(w, \tau_{0,1}w) - \kappa(w,w) &= -\frac{442}{3}\left(X_2^2 + X_3^2 + X_4^2\right) \\
\kappa(w, \tau_{1,0}w) - \kappa(w,w) &= -\frac{442}{3}\left(X_1^2 + X_2^2 + X_3^2\right) \\
\kappa(w,w) - \eta(w,w) &= -\frac{124}{9}\left(X_1^2 + X_2^2 + X_3^2 + X_4^2\right)
\end{aligned}
$$

Since $a^2 + b^2 + c^2 \equiv 0, \pmod 3$ implies $a \equiv b \equiv c, \pmod 3$, the first two equations above imply $X_1 \equiv X_2 \equiv X_3 \equiv X_4, \pmod 3$, and the last equation implies all of these must be 0 $\pmod 3$.

So we may write $w = \frac{y}{3}I + q$, where $q = \sum_{i=1}^{4} \frac{X_i}{3} f_i$ is contained in Q. It follows that $3w^2 = \frac{y^2}{3}I + 2y\,q + 3q^2$. Since $3w^2 \in 3L \subseteq Q$ we must have $\frac{y^2}{3}I \in Q$, which implies $y/3 \in \mathbb{Z}$. This completes the proof that $w \in Q$, and (ii) follows.

Finally, let $w = \frac{1}{3}\sum_{i=1}^{4} X_i n_i$ be an element in $L \cap V^{-\tau_{0,0}}$, with $X_i \in \mathbb{Z}$ for each u.

Then $w \cdot w$ is is in $L \cap V^{\tau_{0,0}}$ and therefore is in $\mathrm{span}_{\mathbb{Z}}(\mathcal{B}_+\}$ by part (ii). We define the coefficients of $w \cdot w = z_I I + \sum_{i=1}^{4} z_i f_i$, then we compute the following [★`LC.6`]:

$$
\begin{aligned}
z_I &= \frac{16}{3}\left(X_1^2 + X_2^2 + X_3^2 + X_4^2\right),\\
z_1 &= 2X_1^2 + \frac{14}{3}\left(X_2X_3 + X_2X_4 - X_3X_4\right),\\
z_2 &= 2X_2^2 + \frac{14}{3}\left(X_1X_3 - X_1X_4 + X_3X_4\right),\\
z_3 &= 2X_3^2 + \frac{14}{3}\left(X_1X_2 + X_1X_4 - X_2X_4\right),\\
z_4 &= 2X_4^2 - \frac{14}{3}\left(X_1X_2 + X_1X_3 + X_2X_3\right).
\end{aligned}
$$

For z_I to be an integer, there are two possibilities: $X_i \equiv 0, \pmod 3$ for either a single $i \in \{1,2,3,4\}$ or for all four $i \in \{1,2,3,4\}$. So we may choose i such that $X_i \equiv 0, \pmod 3$. Suppose $\{i, j, k, \ell\} = \{1,2,3,4\}$. Then the condition that z_j is an integer reduces down to $X_kX_\ell \equiv 0, \pmod 3$, so one of these is also zero modulo 3. Then z_I being an integer implies that all four coefficients are zero modulo 3. Thus, $w \in \mathrm{span}_{\mathbb{Z}}(\mathcal{B}_{-1})$. □

Theorem 4.3.13. *The integral form Q is the unique maximal GIIF in the Lam-Chen algebra.*

Proof. Let L be a GIIF of the Lam-Chen algebra such that $3L \subseteq Q$. Note that $L^{\tau_0} + L^{-\tau_0}$ is the total eigenlattice in L with respect to the group of order 2 generated by τ_0. If $\ell \in L$, then $2\ell = (\tau_0 + 1)\ell + (\tau_0 - 1)\ell \in L^{\tau_0} + L^{-\tau_0}$.

Therefore $2L \subseteq L^{\tau_0} + L^{-\tau_0}$, and Lemma 4.3.12 shows that $L^{\tau_0} + L^{-\tau_0} \subseteq Q$. Therefore (for some $k > 0$) $2L \subseteq L^{\tau_{0,0}} + L^{-\tau_{0,0}} \subseteq Q$. Then by Lemma 4.3.10, $9L \subseteq Q$. Combining these gives $L = 2L \cap 9L \subseteq Q$, as desired.

Now suppose L' is a GIIF such that $3L' \nsubseteq Q$. Then by 4.3.10, we have $3(3L') \subseteq Q$. So taking $L = 3L'$ in the previous paragraph implies that $3L' \subseteq Q$, which is a contradiction.

Therefore, every GIIF L is contained in Q. □

APPENDIX A

Glossary of terms and notations

ad() Def 2.1.1 page 8

For an element a in an algebra A, $\mathrm{ad}(a)$ is the endomorphism of A given by $x \mapsto ax$.

axes Def 1.2.1 page 4

In an algebra, axes are a distinguished set of idempotents which satisfy the Virasoro $\mathfrak{V}(4,3)$ fusion rules. In particular, if a is an axis then the adjoint action of a is semisimple with eigenvalues taken from the set $\{0, 1, \frac{1}{4}, \frac{1}{32}\}$ and the eigenspaces satisfy the Virasoro fusion rules: $V_\lambda^{(a)} \cdot V_\mu^{(a)} \subseteq \sum_{\nu \in \lambda \star \mu} V_\nu^{(a)}$ where $\star : \{0, 1, \frac{1}{4}, \frac{1}{32}\}^2 \to \mathscr{P}(\{0, 1, \frac{1}{4}, \frac{1}{32}\})$ is given by the table below.

$\star$	1	0	$\frac{1}{4}$	$\frac{1}{32}$
1	1	0	$\frac{1}{4}$	$\frac{1}{32}$
0	0	$1, 0$	$\frac{1}{4}$	$\frac{1}{32}$
$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$1, 0$	$\frac{1}{32}$
$\frac{1}{32}$	$\frac{1}{32}$	$\frac{1}{32}$	$\frac{1}{32}$	$1, 0, \frac{1}{4}$

$\chi(\mathbf{x}, \mathbf{t})$ Def 2.1.1 page 8

For an endomorphism x on a finite dimensional vector space V, $\chi(x,t) = \det(x - t\mathrm{Id}_V)$ is the characteristic polynomial of x.

$\mathbf{det}_\alpha(\mathbf{L})$ Def 2.2.3 page 13

For a lattice L with bilinear form α, let $e_1, \ldots, e_n$ be a $\mathbb{Z}$-basis of L. Then $\det_\alpha(L)$ is the determinant of the matrix $(\alpha(e_i, e_j))_{1\leqslant i,j\leqslant n}$. This is independent of the choice of $\mathbb{Z}$-basis.

η Def 2.2.1 page 12

For two elements x, y in a finite dimensional algebra, $\eta(x, y) = \mathrm{Tr}[\mathrm{ad}(x \cdot y)]$.

GIIF Def 1.2.4 page 6

Stands for G-invariant integral form; For a commutative algebra V with axes, a GIIF is an integral form which is invariant under the subgroup G of $\mathrm{Aut}(V)$ generated by the τ-involutions of V.

integral form Def 1.2.2 page 5

An integral form in a (not necessarily associative) algebra A over a field k of characteristic zero is a subrng of A which is the $\mathbb{Z}$-span of a k-basis of A.

integral form detector page 8

For an algebra A over a field $\mathbb{F}$ of characteristic zero, an integer k and a subspace W of A, an integral form detector on W is a function $f : W^k \to \mathbb{F}$ such that if $w \in W$ is in an integral form of A, then $f(w) \in \mathbb{Z}$.

κ Def 2.2.1 page 12

The Killing form; for two elements x, y in a finite dimensional algebra, $\kappa(x, y) = \mathrm{Tr}(\mathrm{ad}(x)\,\mathrm{ad}(y))$.

$\mathbf{L}^{\pm,\pm}$ page 42

This is defined when $A \cong (\mathbb{Z}/2\mathbb{Z})^2$ is generated by an ordered pair of generators $A = \langle \tau_0, \tau_1 \rangle$ and L is a $\mathbb{Z}[A]$-module. Then for $\epsilon_0, \epsilon_1 \in \{+, -\}$, we define $L^{\epsilon_0,\epsilon_1} = \{\ell \in L : \tau_0(\ell) = \epsilon_0 \ell \text{ and } \tau_1(\ell) = \epsilon_1 \ell\}$.

lattice Def 2.2.3 page 13

A finitely-generated free abelian group L with a symmetric bilinear form $L \times L \to \mathbb{Q}$.

Norton-Sakuma algebra page 2

One of 8 nonassociative algebras which, up to isomorphism, give every possible subalgebra in the monster Griess algebra generated by two 2A-axes.

$\mathbf{R}^{*,\alpha}$ Prop 2.2.2 page 13 and Def 2.2.3 page 13

The dual of R with respect to α; For an additive subgroup R of a vector space V over a field k of characteristic zero, and a symmetric bilinear form $\alpha : V \otimes V \to k$, $R^{*,\alpha} = \{r \in V : \alpha(r, v) \in \mathbb{Z} \text{ for all } v \in V\}$.

rng page 3 and Def 3.1.7 page 24

A rng is a set equipped with an abelian group structure and a (not necessarily associative) product satisfying the usual axioms of a ring other than associativity and the requirement of having a multiplicative unit. For a subset S of a rng, rng(S) is the smallest rng containing S.

σ**-involution /** $\sigma(\mathbf{a})$ page 5

For an axis a in a commutative algebra V, $\sigma(a)$ is the involutive automorphism of the subalgebra $V_1^{(a)} \oplus V_0^{(a)} \oplus V_{1/4}^{(a)}$ which is the identity on $V_1^{(a)} \oplus V_0^{(a)}$ and which acts as the scalar -1 on $V_{1/4}^{(a)}$.

τ**-involution /** $\tau(\mathbf{a})$ page 5

For an axis a in a commutative algebra V, $\tau(a)$ is the involutive automorphism of V which is the identity on $V_1^{(a)} \oplus V_0^{(a)} \oplus V_{1/4}^{(a)}$ and which acts as the scalar -1 on $V_{1/32}^{(a)}$.

$\textsc{tel}(\mathbf{L}, \mathbf{A})$ Def 3.5.2 page 41

The total eigenlattice in L with respect to A; When A is a finite abelian group, and L is a $\mathbb{Z}[A]$-module, then $\textsc{tel}(A) = \sum_{\chi \in \mathrm{Hom}(A,\mathbb{C}^*)} L^\chi$ where $L^\chi = \{\ell \in L : \text{ for all } a \in A,\ a \cdot \ell = \chi(a)\ell\}$.

Tr / trace Def 2.1.1 page 8

For an endomorphism x on a finite dimensional space, $\mathrm{Tr}(x)$ is the trace of x. If a is in a finite dimensional algebra, then $\mathrm{trace}(a)$ means $\mathrm{Tr}(\mathrm{ad}(a))$.

$\mathbf{V}_\lambda^{(a)}$ page 4

For a commutative algebra V and an axis a in V, this is the λ-eigenspace of $\mathrm{ad}(a)$: $V_\lambda^{(a)} = \{v \in V : a \cdot v = \lambda v\}$.

$[x]_{\mathcal{B}}$ page 31

The matrix of a linear endomorphism with respect to an ordered basis $\mathcal{B}$.

APPENDIX B

Mathematica chapter

In this appendix, we discuss the methods for performing calculations in the algebras in this document using the computer algebra system *Mathematica* [Wol]. The code described can be found in the document `GIIFs.nb`, available at both `https://umich.box.com/ggs` and `https://github.com/gregorygsimon/GIIFs/`.

Section B.1 describes the initialization needed to calculate algebra products for each algebra. Then Section B.2 covers other functions needed, for example to compute the trace or Killing form.

When computations are needed in the text, a citation of the form [$\bigstar$`2A.2`] is given. The accompanying code will be found in the 2A section of this Appendix, which is Section B.3. Code is also given for 3A in B.4, 3C in B.5, 4A in B.6, 4B in B.7, 5A in B.8, 6A in B.9, 2A3C in B.10, 2B3C in B.11, and the Lam-Chen algebra in B.12.

B.1 The initialization code for computing algebra products

In this section, we explain the code used to compute the products of two elements in the algebra. The specific case of the Norton-Sakuma algebra of type 2A will be used as an illustrative example; the code for the remaining algebras follows the same logic.

Let V be the rational 2A Norton-Sakuma algebras and set $n = \dim V$. Table 3 in [IPSS10] gives a basis and the associated algebra products for V. We take the ordering of the basis elements as they are printed in this table to give us an ordered basis for V, which yields a linear isomorphism of V with $\mathbb{Q}^n$. The Mathematica code will be based on this isomorphism.

The Initialization section begins with the user defining the `type`.

```
In[1]:= type = "2A";
```

There are currently 9 options for `type`: `"2A"`, `"3A"`, `"4A"`, `"4B"`, `"5A"`, `"6A"`, `"2A3C"`, `"2B3C"`, `"3^2:2"`, corresponding to 9 of the 10 algebras considered in this document. (There is no code for computations in 2B, since this algebra is isomorphic with $\mathbb{Q}^2$.) We explain the code for `type = "2A"`, and the remaining cases are analogous.

We define a `StructureCoefficientsForType["2A"]` to be the $n \times n$-matrix with (i, j)th entry equal to the product of the ith and jth basis elements.

```
In[2]:= StructureCoefficientsForType["2A"] =
   {{a0, 1/8(a0+a1-aρ), 1/8(a0+aρ-a1)},
   {1/8(a1+a0-aρ), a1, 1/8 (a1+aρ-a0)},
   {1/8(aρ+a0-a1), 1/8(a1+aρ-a0), aρ}};
```

(Caveat: when the product of two elements is zero, we do not write `0` here, which will be interpretted as a scalar. Instead we enter `zero`. Then we later define `zero` to be the appropriate zero vector.) We also define the number of axes (also called Ising vectors in VOA theory) with the following.

```
In[3]:= numIsing["2A"]=3;
```

Next we have a snippet of code that defines `dim` to be the dimension of the algebra, and then defines the ordered list of basis elements to equal to the identity matrix of size `dim` $\times$ `dim`:

```
In[4]:= If[type=="2A",
    dim=3;
    {a0,a1,aρ} = IdentityMatrix[dim];
   ];
```

The basis for 2A that we are using is a_0, a_1, a_ρ. The result of this code is that if we type in a_0 in Mathematica, then the result is the same as the first standard basis vector $\{1, 0, 0\}$ of $\mathbb{Q}^{\mathtt{dim}}$, and similarly for the 2nd and 3rd basis elements.

Next we have the following:

```
In[5]:= StructureCoefficients = StructureCoefficientsForType[type];
        zero = Table[0,{dim}];
        AlgebraProduct[W_,V_]:= Sum[
          W[[i]]V[[j]]StructureCoefficients[[i,j]],
        {i,1,dim},{j,1,dim}];
        W_·V_:=AlgebraProduct[W,V];
```

This defines `StructureCoefficients` to equal the matrix of the structure coefficients for the particular `type` that the user has selected. It defines `zero` to be the zero vector of $\mathbb{Q}^{\mathtt{dim}}$.

The algebra product is defined as `AlgebraProduct[V,W]`. For vectors `V` and `W` of length `dim`, the product of `V` and `W` is defined to be the sum (over $1 \leqslant i, j \leqslant \mathtt{dim}$) of the ith component of `W` times the jth component of `V` times the (i, j)th entry of `StructureCoefficients`.

Finally, the center dot `W·V` is defined to be the algebra product of `W` and `V` for brevity.

B.2 Mathematica functions for calculations in the Norton-Sakuma and related algebras

We proceed understanding that `type` is a string giving the type of the algebra, `dim` equals the dimension of the algebra, and for two vectors `u,v` of length `dim`, we have that `u·v` equals the vector of length `dim` corresponding to the algebra product of `u` and `v` under the identification of the algebra with $\mathbb{Q}^{\mathtt{dim}}$. Section B.1 gives a detailed account of these.

Notation B.2.1. For a in a commutative algebra V recall that $\mathrm{ad}(a)$ is the endomorphism $x \mapsto a \cdot x$ of V. Define $\mathrm{trace}(a)$ to be the trace of $\mathrm{ad}(a)$.

We define $\mathtt{e}_i$ to equal the ith row of the $\mathtt{dim}\times\mathtt{dim}$ identity matrix, i.e. the ith standard basis element of $\mathbb{Q}^{\mathtt{dim}}$. For a vector w in $\mathbb{Q}^{\mathtt{dim}}$ we first define `ad[w]` to be the matrix of size $\mathtt{dim}\times\mathtt{dim}$ where the (i, j) entry equals the ith component of $w \cdot \mathtt{e}_j$. We also define `trace[w]` to be the trace of `ad[w]`.

```
In[6]:= ad[w_]:=Table[(w·e_j)[[i]],{i,1,dim},{j,1,dim}];
        trace[w_]:=Tr[ad[w]] // Simplify;
```

For the next piece of code, we will need the following lemma.

Lemma B.2.2. *Let* $p(t) = -\frac{65536}{217}t^3 + \frac{81920}{217}t^2 - \frac{16384}{217}t + 1$. *Then for an axis a (see definition 1.2.1), the* τ*-involution in* $Aut(V)$ *associated to a equals* $p(ad(a))$.

Proof. The polynomial $p(t)$ was chosen so that $p(0) = p(1) = p(1/2^2) = 1$ and $p(1/2^5) = -1$.

Let a be an axis. Write $V = V_1^{(a)} \oplus V_0^{(a)} \oplus V_{\frac{1}{2^2}}^{(a)} \oplus V_{\frac{1}{2^5}}^{(a)}$, where $V_\lambda^{(a)} = \{v \in V : \ av = \lambda v\}$ the λ-eigenspace of $\mathrm{ad}(a)$. So $p(\mathrm{ad}(a))$ acts as the scalar $p(\lambda)$ on $V_\lambda^{(a)}$. In particular, $p(\mathrm{ad}(a))$ acts trivially on $V_1^{(a)} \oplus V_0^{(a)} \oplus V_{\frac{1}{2^2}}^{(a)}$, and $p(\mathrm{ad}(a))$ acts as the scalar -1 on $V_{\frac{1}{2^5}}^{(a)}$, as required. $\square$

For an axis a, we define the Mathematica function $\tau[a]$ to be $p(\mathrm{ad}(a))$, i.e. the τ-involution associated to a.

```
In[7]:= τ[a_]:=IdentityMatrix[dim]-16384/217 ad[a]
          +81920/217 MatrixPower[ad[a],2]-65536/217 MatrixPower[ad[a],3];
```

We next define the multiplicative identity in the algebra. We start by defining `Ι` to be a vector with undefined variable entries[1]. We then use Mathematica's `Solve` function to find the values of the variables which make `ad[Ι]` equal to the identity matrix. Since the multiplicative identity is unique, there will be a unique solution found by Mathematica. We redefine `Ι` with its undefined variable entries replaced by the values found by `Solve`.

[1] Capital iota is used instead of I (uppercase i) because the latter is reserved in Mathematica for $\sqrt{-1}$.

```
In[8]:= I = Table[idcomponent_i,{i,1,dim}];
        I = I /. Solve[ad[I]==IdentityMatrix[dim]][[1]];
```

Next we want to define the group G generated by the τ-involutions, as matrices with respect to the given ordered basis of V. We recall the function `numIsing` which takes the string `type` and outputs the number of axes in this type. Then `generators` is defined to be the list of the τ-involutions, i.e. the list containing $\tau(e_i)$ for $i = 1, 2, \ldots,$ `numIsing[type]`.

We next define G by iterating the function `Union[#,Dot@@@Tuples[#,2]]` on the initial input `generators`. On the first iteration, this gives the union of `generators` with the collection of the matrix product of all pairs of elements from `generators`, this would be the collection of all elements of G which have word length $\leqslant 2$ in the generating set consisting of τ-involutions. Iterating this function k times produces the subset of G consisting of all elements with word length $\leqslant k - 1$. The Mathematica function `FixedPoint` repeatedly does this procedure until the process stabilizes, i.e. it halts after all of the words of length k in the generators of G equals the set of all words of length $k + 1$ in the generators of G. This means the set contains all of the matrices generated by the τ-involutions, as desired.

```
In[9]:= generators = Table[τ[e_i],{i,1,numIsing[type]}];
        G = FixedPoint[Union[#,Dot @@@ Tuples[#,2]]&,generators];
```

The remaining Mathematica functions will rely on an identification of three distinct but highly related concepts: a basis of $\mathbb{Q}^n$, an invertible $n \times n$ rational matrix, and a $\mathbb{Z}$-basis of a rank n free additive subgroup of $\mathbb{Q}^n$. In Mathematica, a list of vectors in $\mathbb{Q}^n$ is indistinguishable from a matrix, where the first vector in the list is understood to be the first row, the second in the list is the second row, and so on. Therefore, for a vector `v` of length n and a basis `B` of $\mathbb{Q}^n$, the coefficients of `v` in the basis of `B` is given by `Inverse[Transpose[B]].v` . If `B` is a set of linearly independent vectors, but has less than n elements, and if `v` is in the span of these vectors, then we can find the coefficients of `v` with respect to the list of vectors `B` using the function `LinearSolve[Transpose[B],v]`. .

```
In[10]:= vec[x_,B_]:=LinearSolve[Transpose[B],x];
```

So given a list of linearly-independent vectors `B` and a vector `x`, the function `vec[x,B]` will give the coefficients of the vector `x` expressed in the basis `B` if possible – if not possible, this will result in an error.

Similarly, if `f` is an $n \times n$ matrix which preserves $\mathrm{span}_{\mathbb{Q}}(\mathtt{B})$, then the associated matrix with respect to a linearly independent list of vectors `B` will have its ith column equal to the product of `f` with ith element of `B`, expressed in the basis `B`.

```
In[11]:= mat[f_,B_]:=
           Transpose[Table[vec[f.B[[i]],B],{i,1,Length[B]}]];
```

So given a matrix `f` and a list of linearly independent vectors `B`, the function `mat[f,B]` will give the matrix of `f` in the basis `B` as long as $\mathrm{span}_{\mathbb{Q}}(\mathtt{B})$ is `f` invariant.

This can immediately be used to check if a basis `B` spans an integral form: we create a list consisting of the matrices $ad(b)$ with respect to the basis `B`, for all b in `B`. Then we check if every component produced is an integer. This furnishes the following code:

```
In[12]:= IntegralFormQ[B_]:=AllTrue[Flatten[
           Table[mat[ad[B[[i]]],B],{i,1,Length[B]}]
         ],IntegerQ]
```

So `IntegralFormQ[B]` will output `True` if and only if the $\mathbb{Z}$-span of the list of vectors `B` is an integral form.

The next result will be used to define a function to compute when one lattice is contained in another.

Lemma B.2.3. *Let α and β be two matrices in $GL_n(\mathbb{Q})$. Let A be the lattice in $\mathbb{Q}^n$ additively generated by the rows of α and let B be the lattice additively generated by the rows of β. Then $A \subseteq B$ if and only if the matrix $\alpha\beta^{-1}$ has integer entries.*

Proof. Let α_i and β_i denote the ith row of the matrix α and β, respectively, thought of as a row vectors. Let x_i be the unique column vector that satisfies $\beta^T x_i = \alpha_i^T$. The entries of x_i give the coefficients of α_i expressed in the basis $\{\beta_i\}_{i=1}^n$. So α_i is in B if and only if the vector x_i has integer entries. Therefore, $A \subseteq B$ if and only if x_i has integer entries, for all i with $1 \leqslant i \leqslant n$.

If X is the matrix whose ith column is x_i, then we can combine the n equations $\beta^T x_i = \alpha_i^T$ into the single matrix equation $\beta^T X = \alpha^T$. So we see that $A \subseteq B$ if and only if $X = (\beta^T)^{-1}\alpha^T$ has integer entries. Equivalently, $A \subseteq B$ if and only if $X^T = \alpha\beta^{-1}$ has integer entries. $\square$

This furnishes the following code for the function `LatticeContainQ`, which takes two invertible $n \times n$ matrices α and β as input, and which outputs `True` if and only the lattice spanned by the rows of α is contained in the lattice spanned by β. Then `LatticeEqualQ` is defined to check if the both `LatticeContainQ[α,β]` and `LatticeContainQ[β,α]` are both true.

```
In[13]:= LatticeContainQ[α_,β_]:=
           AllTrue[Flatten[α.Inverse[β]],IntegerQ]
         LatticeEqualQ[α_,β_]:=
           LatticeContainQ[α,β]&&LatticeContainQ[β,α]
```

We provide code to compute the Killing form (κ`[v,w]`) and the Gram matrix κ`Gram[B]` of a list of vectors `B`, i.e. the matrix whose (i, j)-entry is κ evaluated on the ith and jth elements of `B`.

```
In[14]:= κ[x_,y_]:= Simplify[Tr[ad[x].ad[y]]]
         κGram[B_]:=
           Table[κ[B[[i]],B[[j]]],{i,1,Length[B]},{j,1,Length[B]}]
```

The code for the form $\eta(v, w) = \mathrm{trace}(\mathrm{ad}(v \cdot w))$ is completely analogous.

```
In[15]:= η[x_,y_]:=trace[x·y]
         ηGram[L_]:=
           Table[η[L[[i]],L[[j]]],{i,1,Length[L]},{j,1,Length[L]}]
```

Finally, we define `IntegerFactor[x]` to be the prime factorization of an integer x expressed using dots and exponents (instead of as a difficult to read long list of prime factors and exponents). This is suggested in the help page for `FactorInteger` under "Applications" in Mathematica 9 & 10.

```
In[16]:= IntegerFactor[x_]:=Times@@(Superscript@@@ FactorInteger[x]);
```

B.3 2A Mathematica code

✶2A.1

```
In[17]:= k = I - a0;
         q =4 (a1-aρ);


         q·q  == 7a0+15k
         a0·q == 1/4 q

Out[17]= True

Out[18]= True
```

✶2A.2

```
In[19]:= w=4x a0 + y q;
         trace[w]
         trace[w·w]

Out[19]= 5 x

Out[20]= 5 (4 x^2+7 y^2)
```

✶2A.3

In[21]:=
```
B = {4a_0,k,q};
IntegerFactor[Det[κGram[B]]]
IntegerFactor[Det[ηGram[B]]]
```

Out[21]= $2^2\ 13^2$

Out[22]= $5^2\ 7^2$

✶2A.4

In[23]:= $w = x\ a_0 + \frac{y}{4}q + \frac{z}{4}I;$

$w\cdot w == \frac{1}{2}(x+z)w + \frac{1}{16}(15y^2 - z(2x+z))I + \frac{(x^2-y^2)(4ta_0)}{8t}$ //Reduce

$(4ta_0)\cdot w == tw - \frac{tzI}{4} + \frac{1}{4}(3x+z)(4ta_0)$ // Reduce

Out[23]= True

Out[24]= True

✶2A.5

In[25]:= $w_{m\_} := 2\ a_0 + (m + \frac{1}{2})q + \frac{1}{2}I;$

$w_m == -m\ I - \frac{m}{2}(8a_0) + (1+2m)w_0$ //Simplify

$w_m == (1+m)\ I + \frac{m+1}{2}(8a_0) - (1+2m)w_{-1}$ // Simplify

Out[25]= True

Out[26]= True

✶2A.6

In[27]:= $\sigma[x\_] := \frac{32}{3}ad[x].ad[x] - \frac{32}{3}ad[x] + ad[I];$

$P=\{I,4\ a_0,\ q\};$

```
w_m_:=2 a_0 +(m+1/2)q + 1/2 I;
L[m_]:={I,8a_0,w_m};
LatticeEqualQ[  Table[σ[a_1].P[[i]],{i,1,dim}],L[0]]
LatticeEqualQ[ Table[σ[a_ρ].P[[i]],{i,1,dim}],L[-1]]
```

Out[27]= True

Out[28]= True

B.4 3A Mathematica code

✶3A.1

```
In[29]:= trace[x u_ρ+y I]
```

Out[29]= $\frac{5\ x}{3}+4\ y$

✶3A.2

```
In[30]:= n_0= 2^6(a_1-a_-1);
         n_1=2^6(a_-1-a_0);
         η[n_0,n_1] // IntegerFactor
         κ[n_0, n_1] // IntegerFactor
```

Out[30]= $-1^1\ 2^1\ 3^2\ 271^1$

Out[31]= $-1^1\ 2^2\ 3^1\ 313^1$

✶3A.3

```
In[32]:= g = τ[a_-1].τ[a_0];
         m_0=1/3(g - ad[I]).n_0;
         m_1=1/3(g - ad[I]).n_1;
```

```
B =  {m0,m1,3uρ,I};
mat[ad[3uρ],B] // MatrixForm
mat[ad[m0],B] // MatrixForm
```

Out[32]= $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$

Out[33]= $\begin{pmatrix} 20 & -20 & 1 & 1 \\ 0 & -20 & 0 & 0 \\ -156 & 78 & 0 & 0 \\ 1008 & -504 & 0 & 0 \end{pmatrix}$

✶3A.4

```
In[34]:= z = a m0+b m1+  c 3uρ + d I;
trace[z]
η[z,z]
κ[z,z]
```

Out[34]= $5\ c+4\ d$

Out[35]= $3252\ a^2-3252\ a\ b+3252\ b^2+15\ c^2+10\ c\ d+4\ d^2$

Out[36]= $2504\ a^2-2504\ a\ b+2504\ b^2+11\ c^2+10\ c\ d+4\ d^2$

✶3A.5

```
In[37]:= mat[ad[3 uρ],{m0,m1}] // MatrixForm
```

Out[37]= $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

✶3A.6

```
In[38]:= z = 1/3(a m0+b m1)+ 3 uρ;
         vec[z·z - k z, {m0,m1,9uρ,I}]
```

Out[38]= $\{\frac{1}{9}$ (6 a+20 a^2-40 a b-3 a k), $\frac{1}{9}$ (6 b-40 a b+20 b^2-3 b k), $\frac{1}{9}$ (9-52 a^2+52 a b-52 b^2-3 k), 112 (a^2-a b+b^2)$\}$

✶3A.7

```
In[39]:= Reduce[6 a+20 a^2-40 a b-3 a k ==0 &&
         6 b-40 a b+20 b^2-3 b k ==0 &&
         9-52 a^2+52 a b-52 b^2-3 k ==0 &&
         (3a≠0 ∨ 3b≠0 ∨ 3k≠0), Modulus→9]
```

Out[39]= False

B.5 3C Mathematica Code

✶3C.1

```
In[40]:= n0= 2^6(a1-a-1);
         n1= 2^6(a-1-a0);
         trace[n0·n1] // IntegerFactor
         κ[n0,n1] // IntegerFactor
```

Out[40]= $-1^1\ 2^1\ 3^3\ 7^1\ \ 11^1$

Out[41]= $-1^1\ 2^2\ 3^1\ 331^1$

✶3C.2

In[42]:=
```
g=τ[a₋₁].τ[a₀];
n₀= 2^6(a₁-a₋₁);  n₁= 2^6(a₋₁-a₀);
m_i_:= 1/3 (g-ad[I]).n_i;
mat[ad[m₀],{m₀,m₁,I}] //  MatrixForm
```

Out[42]= $\begin{pmatrix} 20 & -20 & 1 \\ 0 & -20 & 0 \\ 924 & -462 & 0 \end{pmatrix}$

✶3C.3

In[43]:=
```
w = α m₀+β m₁+γ I;
trace[w·w] // Expand
```

Out[43]= $2772\ \alpha^2 - 2772\ \alpha\ \beta + 2772\ \beta^2 + 3\ \gamma^2$

✶3C.4

In[44]:=
```
mat[ad[s m₀],{s m₀,s m₁,t I}]  //MatrixForm
```

Out[44]= $\begin{pmatrix} 20s & -20s & t \\ 0 & -20s & 0 \\ \frac{924s^2}{t} & -\frac{462s^2}{t} & 0 \end{pmatrix}$

In[45]:=
```
mat[ad[s m₁],{s m₀,s m₁,t I}]  //MatrixForm
```

Out[45]= $\begin{pmatrix} -20s & 0 & 0 \\ -20s & 20s & t \\ -\frac{462s^2}{t} & \frac{924s^2}{t} & 0 \end{pmatrix}$

✶3C.5

In[46]:=
```
mat[ad[s n₀],{s n₀,s n₁,t I}]  //MatrixForm
```

Out[46]= $\begin{pmatrix} 20s & 20s & t \\ 40s & -20s & 0 \\ \frac{2772s^2}{t} & -\frac{1386s^2}{t} & 0 \end{pmatrix}$

In[47]:= `mat[ad[s n_0],{s n_0,s n_1,t I}] //MatrixForm`

Out[47]= $\begin{pmatrix} 20s & 20s & t \\ 40s & -20s & 0 \\ \frac{2772s^2}{t} & -\frac{1386s^2}{t} & 0 \end{pmatrix}$

✶3C.6

In[48]:= $w = \frac{\alpha}{3}s\ m_0 + \frac{\beta}{3}s\ m_1 + t\ I;$

`mat[τ[a_0],{s m_0,s m_1,w}] //MatrixForm`

`mat[τ[a_-1],{s m_0,s m_1,w}] //MatrixForm`

Out[48]= $\begin{pmatrix} -1 & 0 & -\frac{1}{3}(2\alpha) \\ -1 & 1 & -\frac{\alpha}{3} \\ 0 & 0 & 1 \end{pmatrix}$

Out[49]= $\begin{pmatrix} 1 & -1 & -\frac{\beta}{3} \\ 0 & -1 & -\frac{1}{3}(2\beta) \\ 0 & 0 & 1 \end{pmatrix}$

✶3C.7

In[50]:= $w = \frac{\alpha}{3}s\ n_0 + \frac{\beta}{3}s\ n_1 + t\ I;$

`mat[τ[a_0],{s n_0,s n_1,w}] //MatrixForm`

`mat[τ[a_-1],{s n_0,s n_1,w}] //MatrixForm`

Out[50]= $\begin{pmatrix} -1 & 1 & \frac{1}{3}(\beta-2\alpha) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

Out[51]= $\begin{pmatrix} -1 & 1 & \frac{1}{3}(\beta-2\alpha) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

✶3C.8

```
In[52]:= Clear[w]
         w[s_,t_]:= (s n₀-s n₁)/3 +t I;
         B[s_,t_]:={s n₀,s n₁,(s  n₀-s n₁)/3 +t I};
         mat[ad[s n₀],B[s,t]] //Expand  // MatrixForm
```

Out[52]=
$$\begin{pmatrix} 20s - \frac{924s^2}{t} & \frac{462s^2}{t} + 20s & t - \frac{462s^2}{t} \\ \frac{924s^2}{t} + 40s & -\frac{462s^2}{t} - 20s & \frac{462s^2}{t} + 20s \\ \frac{2772s^2}{t} & -\frac{1386s^2}{t} & \frac{1386s^2}{t} \end{pmatrix}$$

B.6 Mathematica for 4A

✶4A.1

```
In[53]:= τ[a₀] // MatrixForm
```

Out[53]=
$$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

✶4A.2

```
In[54]:= n₀=4 (a₋₁-a₁);
         n₁=4 (a₀-a₂);
         f₀=n₀·n₀;
         f₁=n₁·n₁;
         n₁·n₀== 0id &&
         f₀·n₀==16n₀ &&
         f₁·n₀==n₀&&
           f₀·f₀==16f₀ &&
          f₁·f₀==8f₀+8f₁- 120id
```

Out[54]= True

✶4A.3

```
In[55]:= v= α₀f₀+α₁f₁+α₃I;
        v₀=v/.Solve[{v·n₀,v· n₁,trace[v]} == {n₀,0n₁,0}][[1]];
        v₁=v/.Solve[{v·n₀,v· n₁,trace[v]} == {0n₀,1n₁,0}][[1]];
        vₜ=v/.Solve[{v·n₀,v· n₁,trace[v]} == {0n₀,0n₁,1}][[1]];

        w = a v₀+b v₁+c vₜ;
        vec[w·w,{v₀,v₁,vₜ}] //  FullSimplify
```

Out[55]= $\{\frac{1}{15}\ (159\ a^2+24\ a\ (13\ b-5\ c)+(13\ b-5\ c)^2),$
$15\ (169\ a^2+159\ b^2+26\ a\ (12\ b-5\ c)-120\ b\ c+25\ c^2),$
$3\ (169\ a^2+322\ a\ b+169\ b^2)-44\ (a+b)\ c+9\ c^2\}$

✶4A.4

In[56]:= $w\ =\ \frac{1}{2}(a\ n_0+\ b\ n_1+c\ \ f_0+d\ f_1+\ e\ id);$
$F\ =\ \{n_0,n_1,f_0,f_1,I\};$

```
vec[2w·w,F] // Expand
```

Out[56]= $\{16\ a\ c+a\ d+a\ e,\ b\ c+16\ b\ d+b\ e,\ \frac{a^2}{2}+8\ c^2+8\ c\ d+c\ e,$
$\frac{b^2}{2}+8\ c\ d+8\ d^2+d\ e,\ -120\ c\ d+\frac{e^2}{2}\}$

✶4A.5

In[57]:= $w\ =\ \frac{1}{2}(a\ n_0+\ b\ n_1+c\ f_0+d\ f_1);$
$\kappa[w,w]$ // Expand

Out[57]= $8\ a^2+8\ b^2+\frac{577\ c^2}{4}+56\ c\ d+\frac{577\ d^2}{4}$

B.7 Mathematica for 4B

✶4B.1

In[58]:= τ[a_0] // MatrixForm

Out[58]= $$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

✶4B.2

In[59]:= $\tau[a_{\rho^2}]$==ad[I]

Out[59]= True

✶4B.3

In[60]:= $n_0=8\ (a_{-1}-a_1);$

$n_1=8\ (a_0-a_2);$

$f_0=\frac{1}{60}n_0\cdot n_0\ -\frac{7}{15}a_{\rho^2};$

$f_1=\frac{1}{60}n_1\cdot n_1\ -\frac{7}{15}a_{\rho^2};$

$n_0\cdot n_0==32\ f_0-28\ f_1+28\ I$ &&

$n_1\cdot n_0==0I$ &&

$f_0\cdot n_0==\frac{3}{4}n_0$ &&

$f_1\cdot n_0==\ 0\ I$ &&

$f_0\cdot f_0==\ f_0$ &&

$f_1\cdot f_0==0\ I$

Out[60]= True

✶4B.4

In[61]:= $I == f_0+f_1+a_{\rho^2}$

Out[61]= True

✶4B.5

In[62]:= $\kappa[p\ n_0, p\ n_0]$

Out[62]= $104\ p^2$

In[63]:= $\eta[p\ n_0, p\ n_0]$

Out[63]= $147\ p^2$

✶4B.6

In[64]:= $w = \frac{1}{2}(a\ n_0+b\ n_1+4c\ f_0+4d\ f_1+\ e\ I);$

$F = \{n_0, n_1, 4f_0, 4f_1, I\};$

vec[2w·w,F] // Expand

Out[64]= $\{3ac+ae, 3bd+be, 4a^2-\frac{7b^2}{2}+2c^2+ce, -\frac{7a^2}{2}+4b^2+2d^2+de, 14a^2+14\ b^2+\frac{e^2}{2}\}$

✶4B.7

In[65]:= κ[w,w]/.e→0 // Expand

Out[65]= $26\ a^2+26\ b^2+\frac{25\ c^2}{4}+\frac{25\ d^2}{4}$

B.8 Mathematica for 5A

✶5A.1

In[66]:= $\tau[a_0]$ // MatrixForm

Out[66]=
$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

✶5A.2

In[67]:=
$$z = \frac{I}{2} + \frac{2048}{7} w_\rho;$$
$$m_{i\_} := 14I - 64a_i;$$
$$Q = \{I, z, m_{-1}, m_0, m_1, m_2\};$$

$\mathtt{mat[ad[z],Q]\ //\ MatrixForm}$

$\mathtt{mat[ad[m_0],Q]\ //\ MatrixForm}$

Out[67]=
$$\begin{pmatrix} 0 & 31 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 1 & 1 & -1 \\ 0 & 0 & -1 & 1 & 1 & 0 \\ 0 & 0 & -1 & 0 & 1 & 0 \end{pmatrix}$$

Out[68]=
$$\begin{pmatrix} 0 & 0 & -182 & 700 & -182 & -168 \\ 0 & 0 & 14 & 0 & 14 & -14 \\ 0 & 1 & 12 & 0 & 0 & 0 \\ 1 & 1 & 12 & -36 & 12 & 12 \\ 0 & 1 & 0 & 0 & 12 & 0 \\ 0 & 0 & 0 & 0 & 0 & 12 \end{pmatrix}$$

✶5A.3

In[69]:= $\kappa\mathtt{Gram[Q]//MatrixForm}$

Out[69]=
$$\begin{pmatrix} 6 & 3 & 0 & 0 & 0 & 0 \\ 3 & 69 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3184 & -796 & -796 & -796 \\ 0 & 0 & -796 & 3184 & -796 & -796 \\ 0 & 0 & -796 & -796 & 3184 & -796 \\ 0 & 0 & -796 & -796 & -796 & 3184 \end{pmatrix}$$

✶5A.4

```
In[70]:= x = a I+b z;
         FullSimplify[
           CharacteristicPolynomial[mat[ad[x],{m₋₁,m₀,m₁,m₂}],t]
         ]
```

Out[70]= $(a^2+a\ b-b^2-(2\ a+b)\ t+t^2)^2$

✶5A.5

```
In[71]:= N[Eigenvalues[κGram[Q]]]
```

```
Out[71]= {3980.,3980.,3980.,796.,69.1425,5.85747}
```

✶5A.6

```
In[72]:= g=τ[a₋₂].τ[a₀];
         mat[ad[z] + g.g + g.g.g,{m₋₁,m₀,m₁,m₂}] //MatrixForm
```

Out[72]= $\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$

✶5A.7

```
In[73]:= Clear[x,y]
         Inverse[mat[ad[z] + g.g + g.g.g,{I,z}]].{x,y}
```

Out[73]= $\{-\frac{3\ x}{25}+\frac{31\ y}{25},\frac{x}{25}-\frac{2y}{25}\}$

✶5A.8

```
In[74]:= w = x (m₀+m₂) + y m₁;
         CharacteristicPolynomial[ad[w],t] // FullSimplify
```

Out[74]= $(t+36x-12y)(t-12(2x+y))$
$(t^4-12t^3(x-2y)+336t(x-2y)(76x^2+11xy-11y^2)+19600(x^2+xy-y^2)^2$
$-20t^2(69x^2-58xy+58y^2))$

✶5A.9

In[75]:=
```
w = X/60 (m_0+m_2) + Y/60 m_1;
trace[w·(τ[a_0].w)]
trace[w·(τ[a_-1].w)]
κ[w,w]
```
$$w = \frac{X}{60}(m_0+m_2) + \frac{Y}{60} m_1;$$
$$\mathrm{trace}[w\cdot(\tau[a_0].w)]$$
$$\mathrm{trace}[w\cdot(\tau[a_{-1}].w)]$$
$$\kappa[w,w]$$

Out[75]= $\frac{7}{24}(X^2-4\,X\,Y-Y^2)$

Out[76]= $-\frac{7}{24}(4\,X^2-6\,X\,Y+Y^2)$

Out[77]= $\frac{199}{450}(3\,X^2-2\,X\,Y+2\,Y^2)$

✶5A.10

In[78]:= $\mathrm{Solve}[X^2-4\,X\,Y-Y^2==0\ \&\&\ 4\,X^2-6\,X\,Y+Y^2==0,\mathrm{Modulus}\to 24]$

Out[78]= $\{\{X\to 0,Y\to 0\},\{X\to 0,Y\to 12\},\{X\to 12,Y\to 0\},\{X\to 12,Y\to 12\}\}$

✶5A.11

In[79]:=
$$w = \sum_{i=-1}^{2} x_i m_i;$$
$$g=\tau[a_{-2}].\tau[a_0];$$

$$\mathrm{vec}[(\tau[a_0]+\mathrm{ad}[\mathrm{id}]).w,\{m_{-1}+m_1,m_0\}]$$
$$\mathrm{vec}[(\tau[a_0]+\mathrm{ad}[\mathrm{id}]).g.w,\{m_{-1}+m_1,m_0\}]$$

Out[79]= $\{x_{-1}+x_1-x_2,2x_0-x_2\}$

Out[80]= $\{x_0-x_1-x_2,2x_{-1}-x_1-x_2\}$

✶5A.12

In[81]:=
$$w = \sum_{i=-1}^{2} x_i m_i;$$
```
polys={x₋₁+x₁-x₂,2x₀-x₂,x₀-x₁-x₂,2x₋₁-x₁-x₂};
d_i_:=w/.Solve[polys == IdentityMatrix[4][[i]]][[1]];

vec[d1,Q]
vec[d2,Q]
vec[d3,Q]
vec[d4,Q]
```

Out[81]= $\{0,0,-\frac{1}{5},-\frac{2}{5},\frac{2}{5},-\frac{4}{5}\}$

Out[82]= $\{0,0,\frac{2}{5},\frac{4}{5},\frac{1}{5},\frac{3}{5}\}$

Out[83]= $\{0,0,-\frac{4}{5},-\frac{3}{5},-\frac{2}{5},-\frac{6}{5}\}$

Out[84]= $\{0,0,\frac{3}{5},\frac{1}{5},-\frac{1}{5},\frac{2}{5}\}$

✶5A.13

In[85]:=
$$D=\{\frac{1}{5}(-m_{-1}-2m_0+2m_1-4m_2),\frac{1}{5}(2m_{-1}+4m_0+m_1+3m_2),\frac{1}{5}(-4m_{-1}-3m_0-2(m_1+3m_2)),\frac{1}{5}(3m_{-1}+m_0-m_1+2m_2)\};$$
$$d_{i\_}:=D[[i]];$$
$$v=\sum_{i=1}^{4}\lambda_i d_i;$$
```
coeff=CoefficientList[
    CharacteristicPolynomial[ad[v],t],t][[3]];
```
$$\text{Simplify[coeff} - \frac{1}{5}(3\lambda_1+4\lambda_2+2\lambda_3+1\lambda_4)^4]$$

Out[85]=
$$239603\lambda_1^4+105936\lambda_2^4+239616\lambda_3^4-1043712\lambda_3^3\lambda_4+1510264\lambda_3^2\lambda_4^2-706184\lambda_3\lambda_4^3 +105987\lambda_4^4-4\lambda_1^3(260948\lambda_2-250262\lambda_3+119815\lambda_4) +\lambda_2^3(-565168\lambda_3+353040\lambda_4)+16\lambda_2^2(50288\lambda_3^2-76757\lambda_3\lambda_4+37511\lambda_4^2)$$

$$+2\lambda_1^2(755048\lambda_2^2+814444\lambda_3^2-16\lambda_2(96125\lambda_3-48921\lambda_4)$$
$$-1326260\lambda_3\lambda_4+402337\lambda_4^2)$$
$$-16\lambda_2(29954\lambda_3^3-97845\lambda_3^2\lambda_4+94393\lambda_3\lambda_4^2-22068\lambda_4^3)$$
$$-4\lambda_1(176584\lambda_2^3-250268\lambda_3^3+768964\lambda_3^2\lambda_4-642382\lambda_3\lambda_4^2+141267\lambda_4^3$$
$$+\lambda_2^2(-642328\lambda_3+377596\lambda_4)+4\lambda_2(165787\lambda_3^2-229239\lambda_3\lambda_4+76754\lambda_4^2))$$

✶5A.14

In[86]:=
```
vec[m-1,D]
vec[m0,D]
vec[m1,D]
vec[m2,D]
```

Out[86]= {1,0,0,2}

Out[87]= {0,2,1,0}

Out[88]= {1,0,-1,-1}

Out[89]= {-1,-1,-1,-1}

✶5A.15

In[90]:=
```
Table[vec[di,{m-1,m0,m1,m2}],{i,1,4}] // Det
```

Out[90]= $-\frac{1}{5}$

✶5A.16

In[91]:=
```
5(Inverse[mat[g-ad[I],{m-1,m0,m1,m2}]]  )// MatrixForm
```

Out[91]= $\begin{pmatrix} -4 & 1 & 1 & 1 \\ -3 & -3 & 2 & 2 \\ -2 & -2 & -2 & 3 \\ -1 & -1 & -1 & -1 \end{pmatrix}$

✶5A.17

In[92]:=
$$\hat{m}_{-1}=\frac{1}{5}\ (-4\ m_{-1}-3m_0-2\ m_1-m_2);$$
$$\hat{m}_0=\frac{1}{5}\ (m_{-1}-3m_0-2\ m_1-m_2);$$
$$\hat{m}_1=\ \frac{1}{5}\ (m_{-1}+2m_0-2\ m_1-m_2);$$
$$\hat{m}_2\ =\frac{1}{5}\ (m_{-1}+2m_0+3\ m_1-m_2);$$
$$v\ =\ A\ I/5\ +\ B\ z/5\ +\ \sum_{i=-1}^{2} x_i\ \hat{m}_i;$$
$$\kappa[v,v]//Expand$$

Out[92]=
$$\frac{6\ A^2}{25}+\frac{6\ A\ B}{25}+\frac{69B^2}{25}+1592\ x_{-1}^2+1592x_0^2-1592\ x_{-1}x_1+1592\ x_1^2$$
$$-1592\ x_{-1}x_2-1592\ x_0\ x_2+1592\ x_2^2$$

B.9 Mathematica for 6A

✶6A.1

In[93]:= $\tau[a_0]//MatrixForm$

Out[93]=
$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

✶6A.2

In[94]:=
$$q_1\ =\ I;$$
$$q_2\ =\ 3u_{\rho^2};$$
$$q_3=\ 4\ a_{\rho^3}\ -\ I;$$
$$q_4=\ \frac{16}{3}((a_{-2}+\ \ a_0+a_2)-(a_{-1}+a_1+a_3));$$
$$q_5=\ 16\ (a_0-a_3)\ -\ q_4;$$

```
q₆=16(a₂-a₋₁) - q₄;
q₇ = 32 (a₀+a₃)-16 I+8 a ρ³+6 uρ²;
q₈  = 32 (a₋₁+a₂)-16 I+8  aρ³+6 uρ²;
Q = Table[qᵢ,{i,1,8}];

IntegralFormQ[Q]

mat[τ[a₀],Q] // MatrixForm
mat[τ[a₁],Q] // MatrixForm
```

Out[94]= True

Out[95]=
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

Out[96]=
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

✶6A.3

In[97]:= κGram[Q] // MatrixForm

Out[97]=

$$\begin{pmatrix} 8 & 7 & -1 & 0 & 0 & 0 & 0 & 0 \\ 7 & 13 & -5 & 0 & 0 & 0 & 0 & 0 \\ -1 & -5 & 13 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 172 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 268 & -134 & 0 & 0 \\ 0 & 0 & 0 & 0 & -134 & 268 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1560 & -780 \\ 0 & 0 & 0 & 0 & 0 & 0 & -780 & 1560 \end{pmatrix}$$

✶6A.4

In[98]:= $\mathbf{v} = \sum_{i=1}^{4} x_i q_i;$

CharacteristicPolynomial[ad[v],t] == $(t-(x_1+3x_2-x_3))*$
$(t^2+t(-2x_1-2x_2+x_3)+x_1^2+2x_1x_2+x_2^2-x_1x_3-x_2x_3-20x_4^2)^2*$
$(t^3+t^2(-3x_1-2x_3)+t(3x_1^2+4x_1x_3-3x_3^2-46x_4^2)$
$-x_1(x_1-x_3)*(x_1+3x_3)+2(23x_1+49x_3)x_4^2)$ // Simplify

Out[98]= True

✶6A.5

```
In[99]:= Inverse[{{1,3,-1},{-2,-2,1},{3,0,2}}]//MatrixForm
```

Out[99]= $\begin{pmatrix} -\frac{4}{11} & -\frac{6}{11} & \frac{1}{11} \\ \frac{7}{11} & \frac{5}{11} & \frac{1}{11} \\ \frac{6}{11} & \frac{9}{11} & \frac{4}{11} \end{pmatrix}$

✶6A.6

In[100]:= $\mathbf{v} = \sum_{i=1}^{4} x_i q_i;$

κ[v,v] - η[v,v]

Out[100]= $-8x_2^2+4x_2x_3-9x_3^2-86x_4^2$

✶6A.7

```
In[101]:= CharacteristicPolynomial[ad[x(q5+q6)+y(q7+q8)],t] ==
            t^2*(t^2-22ty-20(x^2-6y^2))*( t^4+22t^3y-2t^2(57x^2+208y^2)
              +88t(8x^2y-65y^3)+72(29x^4-161x^2y^2+890y^4)) // Simplify

Out[101]= True
```

✶6A.8

```
In[102]:= w = x(q5+q6)+y(q7+q8);
          trace[w·(τ[a0].w)]

Out[102]= -227 x^2-1102 y^2
```

✶6A.9

```
In[103]:= 22x^2 ==
            442(-20x^2+120y^2)+699(114x^2+416y^2)+312(-227x^2-1102y^2)//Reduce

Out[103]= True
```

✶6A.10

```
In[104]:= v = Sum[x_i q_i, {i,5,8}];
          (τ[a0].τ[a1]+τ[a2]+2τ[a1]+2ad[id]).v==3x6(q5+q6)+3x8(q7+q8)&&
          (-τ[a0].τ[a1]-τ[a2]+τ[a1]+ad[id]).v==3x5(q5+q6)+3x7(q7+q8)
            // Reduce

Out[104]= True
```

✶6A.11

```
In[105]:= κ[v,v] // FullSimplify
          η[v,v] // FullSimplify
```

Out[105]= $4\ (67\ (x_5^2-x_5x_6+x_6^2)+390(x_7^2-x_7x_8+x_8^2))$

Out[106]= $454\ (x_5^2-x_5x_6+x_6^2)+2204(x_7^2-x_7x_8+x_8^2)$

✶6A.12

In[107]:= $\mathbf{v} = \sum_{i=1}^{8}\frac{\mathbf{X_i}}{\mathbf{3}}\mathbf{q_i};\quad \mathbf{vec[\tau[a_0].v-v\ ,Q]}$
$\mathbf{vec[\tau[a_1].v-v\ ,Q]}$

Out[107]= $\{0,0,0,0,-\frac{X_6}{3},-\frac{2X_6}{3},-\frac{X_8}{3},-\frac{2X_8}{3}\}$

Out[108]= $\{0,0,0,0,\frac{1}{3}(-X_5+X_6),\frac{1}{3}(X_5-X_6),\frac{1}{3}(-X_7+X_8),\frac{1}{3}(X_7-X_8)\}$

✶6A.13

In[109]:= $\mathbf{v} = \sum_{i=1}^{4}\frac{\mathbf{X_i}}{\mathbf{3}}\mathbf{q_i} + \sum_{i=5}^{8}\mathbf{x_i q_i};$
vec[3v·v,Q][[1]] // Expand
vec[3v·v,Q][[2]] // Expand

Out[109]= $162x_5^2-162x_5x_6+162x_6^2+864x_7^2-864x_7x_8+864x_8^2+\frac{X_1^2}{3}+X_3^2+\frac{46X_4^2}{3}$

Out[110]= $12x_5^2-12x_5x_6+12x_6^2-84x_7^2+84x_7x_8-84x_8^2+\frac{2X_1X_2}{3}+X_2^2-\frac{2X_2X_3}{3}-\frac{16X_4^2}{3}$

✶6A.14

In[111]:= **trace[v] // Expand**

Out[111]= $\frac{8X_1}{3}+\frac{7X_2}{3}-\frac{X_3}{3}$

B.10 Mathematica for (2A,3C)

✶2A3C.1

In[112]:=
```
m₁=I;
m₂=16/5 (a12,34+a13,24+ a14,23);
m₃=32 a13,24;
m₄=32 a14,23;
m₅=32 (a13+a24);
m₆=32 (a14+a23);
m₇=32 (a14-a23);
m₈=32 (a13-a24);
m₉=32 (a12-a34);
M=Table[mi,{i,1,9}];
IntegralFormQ[M]
AllTrue[
  Flatten[Table[mat[G[[i]],M],{i,1,Length[G]}]],
IntegerQ]
```

Out[112]= True

Out[113]= True

✶2A3C.2

In[114]:= `Eigenvalues[ad[m2]]`

Out[114]= {4,4,4,1,1,1,0,0,0}

✶2A3C.3

In[115]:=
```
v = 16 x (a13,24-a14,23) + 16 y  (a13+a24-a14-a23);
Factor[CharacteristicPolynomial[ad[v],t]]
```

Out[115]= $-\frac{1}{4}\, t^3\, (2\ t-7\ x-31\ y)\ (2\ t+7\ x+31\ y)\ (t^2-381\ y^2)\ (t^2-208\ x^2-104\ x\ y-13\ y^2)$

✶2A3C.4

```
In[116]:= v = 32 x1(a13,24-a14,23) + 32  x2(a12,34-a14,23) +
           32 x3(a13+a24-a14-a23) + 32  x4(a12+a34-a14-a23);

          vec[(τ[a12]-ad[I]).(τ[a34]-ad[I]).v,
            {32(a13,24-a14,23) , 32(a13+a24-a14-a23)}]

          vec[(τ[a12]-ad[I]).(τ[a34]-ad[I]).τ[a13].v,
            {32(a13,24-a14,23), 32(a13+a24-a14-a23)}]

Out[116]= {2 (2x1+x2),2 (2x3+x4)}

Out[117]= {2 (x1-x2),2 (x3-x4)}
```

$$v = 32\, x_1(a_{13,24}-a_{14,23}) + 32\, x_2(a_{12,34}-a_{14,23}) + 32\, x_3(a_{13}+a_{24}-a_{14}-a_{23}) + 32\, x_4(a_{12}+a_{34}-a_{14}-a_{23});$$

Out[116]= $\{2\ (2x_1+x_2),2\ (2x_3+x_4)\}$

Out[117]= $\{2\ (x_1-x_2),2\ (x_3-x_4)\}$

✶2A3C.5

In[118]:= $m_7 \cdot m_8 == m_9\ \&\&\ m_8 \cdot m_9 == m_7\ \&\&\ m_9 \cdot m_7 == m_8$

Out[118]= True

✶2A3C.6

In[119]:= $v = \frac{1}{2} \sum_{i=1}^{9} X_i\ m_i;$

```
2 vec[v·v,M][[1]] // Expand
```

Out[119]= $\frac{X_1^2}{2} - 42\ X_5\ X_6 + 504\ X_9^2$

✶2A3C.7

```
In[120]:= trace[v] // Expand
```

Out[120]= $\frac{9\ X_1}{2} + \frac{15\ X_2}{2} + 25\ X_3 + 25\ X_4 + 43\ X_5 + 43\ X_6$

✶2A3C.8

In[121]:= `vec[v·(τ[a13].v),M][[1]] // Expand`

`vec[v·(τ[a23].v),M][[1]] // Expand`

Out[121]= $\frac{X_1^2}{4}+\frac{21\ X_1\ X_6}{2}+\frac{21\ X_6^2}{2}-252\ X_7\ X_9$

Out[122]= $\frac{X_1^2}{4}+\frac{21\ X_1\ X_5}{2}+\frac{21\ X_5^2}{2}+252\ X_8\ X_9$

✶2A3C.9

In[123]:= $X_1=2x_1$;

$X_2=2x_2$;

$X_5=2x_5$;

$X_6=2x_6$;

`2 κ[v,τ[a24].τ[a12].v]  // Expand`

Out[123]= $18x_1^2+60x_1x_2+102x_2^2+344x_1x_5296x_2x_5+322x_5^2+344x_1x_6+296x_2x_6+5718x_5x_6$
$+322x_6^2+100x_1X_3+340x_2X_3+210x_5X_3+635x_6X_3+\frac{273X_3^2}{2}+100x_1X_4+340x_2X_4$
$+635x_5X_4+210x_6X_4+\frac{1427X_3X_4}{2}+\frac{273X_4^2}{2}-833X_7X_8+833X_7X_9-833X_8X_9$

✶2A3C.10

In[124]:= $X_3=2x_3$;

$X_4=2x_4$;

`κ[v,τ[a12].v]`

`κ[v,τ[a13].v]`

`κ[v,τ[a14].v]`

Out[124]= $9x_1^2+51x_2^2+273x_3^2+2308x_3x_4+273x_4^2+210x_3x_5+1060x_4x_5+161x_5^2+1060x_3x_6$
$+210x_4x_6+5396x_5x_6+161x_6^2+2x_1(15x_2+50x_3+50x_4+86x_5+86x_6)$
$+4x_2(85x_3+85x_4+37(x_5+x_6))-833X_7X_8+\frac{833X_9^2}{2}$

Out[125]= $9x_1^2+51x_2^2+1154x_3^2+546x_3x_4+273x_4^2+1060x_3x_5+210x_4x_5+2698x_5^2+210x_3x_6 +210x_4x_6+322x_5x_6+161x_6^2+2x_1(15x_2+50x_3+50x_4+86x_5+86x_6) +4x_2(85x_3+85x_4+37(x_5+x_6))+\frac{833X_8^2}{2}-833X_7X_9$

Out[126]= $9x_1^2+51x_2^2+273x_3^2+546x_3x_4+1154x_4^2+210x_3x_5+210x_4x_5+161x_5^2+210x_3x_6 +1060x_4x_6+322x_5x_6+2698x_6^2+2x_1(15x_2+50x_3+50x_4+86x_5+86x_6) +4x_2(85x_3+85x_4+37(x_5+x_6))+\frac{833X_7^2}{2}-833X_8X_9$

✶2A3C.11

In[127]:=
```
(* The following two lines ensure X_i is defined, and
 then erases that definition. The definition is required
 to prevent an error message by =.  . *)
{X1=0,X2=0,X3=0,X4=0,X5=0,X6=0,X7=0,X8=0,X9=0};
{X1=.,X2=.,X3=.,X4=.,X5=.,X6=.,X7=.,X8=.,X9=.};
```

$v = \frac{1}{3}\sum_{i=1}^{9} X_i m_i;$

```
3 vec[v·v,M][[1]] // Expand
```

Out[127]= $\frac{X_1^2}{3}-28X_5X_6+336X_9^2$

✶2A3C.12

In[128]:=
```
X1=3x1;
vec[v·(τ[a34].τ[a13,24].v),M][[1]] // Expand
```

Out[128]= $x_1^2-\frac{14X_5^2}{3}-\frac{14X_6^2}{3}-112X_9^2$

✶2A3C.13

In[129]:=
```
X5=3x5;X6=3x6;
vec[v·(τ[a13,24].v),M][[5]] // Expand
vec[v·(τ[a13,24].v),M][[6]] // Expand
```

Out[129]= $2x_1x_5+40x_5^2+4x_5x_6+\frac{8X_8^2}{3}+\frac{8X_9^2}{3}$

Out[130]= $2x_1x_6+4x_5x_6+40x_6^2-\frac{8X_7^2}{3}+\frac{8X_9^2}{3}$

✶2A3C.14

In[131]:= **X_7=3x_7; X_8=3x_8; X_9=3x_9;**

3 κ[v, (ad[I]-τ[a_{13}]).v] // Expand

Out[131]= $7611x_6^2+4998x_7^2+9996x_7x_9+4998x_9^2+850x_6X_4+\frac{881X_4^2}{3}$

✶2A3C.15

In[132]:= **trace[v]**

Out[132]= $9x_1+86x_5+86x_6+5X_2+\frac{50X_3}{3}+\frac{50X_4}{3}$

✶2A3C.16

In[133]:= **X_3=3x_3; X_4=3x_4;**

3 vec[v·v,M][[2]] // Expand

Out[133]= $-240x_3x_4-60x_4x_5-60x_3x_6+48x_5x_6-336x_9^2+2x_1X_2+\frac{4X_2^2}{3}$

B.11 Mathematica for (2B,3C)

✶2B3C.1

In[134]:= **Q={$\frac{16}{17}$(a_{12}+a_{13}+a_{14}+a_{23}+a_{24}+a_{34}),32(a_{14}+a_{23}),32(a_{13}+a_{24}),
32(a_{13}-a_{24}),32(a_{12}-a_{34}),32(a_{14}-a_{23})};**

{q_1,q_2,q_3,q_4,q_5,q_6}=Q;

IntegralFormQ[Q]

```
AllTrue[
  Flatten[Table[mat[G[[i]],Q],{i,1,Length[G]}]],IntegerQ
]
```

Out[134]= True

Out[135]= True

✶2B3C.2

In[136]:=
```
k₁=τ[a₁₂].τ[a₃₄];  k₂=τ[a₁₃].τ[a₂₄];
mat[k₁,Q] == DiagonalMatrix[{1,1,1,-1,1,-1}]
mat[k₂,Q] == DiagonalMatrix[{1,1,1,1,-1,-1}]
```

Out[136]= True

Out[137]= True

✶2B3C.3

In[138]:=
```
w = x q₁+y q₂+ z q₃;
Factor[
  CharacteristicPolynomial[ad[(τ[a₁₂].τ[a₂₃]-ad[I]).w],t]
]
```

Out[138]= $(t+31y)(t-31z)(t-31y+31z)(t^3-964ty^2+964tyz+29512y^2z-964tz^2-29512yz^2)$

✶2B3C.4

In[139]:=
```
w·q₅ == (x+y+z)q₅ // Simplify
```

Out[139]= True

✶2B3C.5

In[140]:= $q_4 \cdot q_5 == q_6$

Out[140]= True

✶2B3C.6

In[141]:= $w = \frac{1}{2}\sum_{i=1}^{6} X_i q_i$;

η[w,w] // Expand

Out[141]= $\frac{3\ X_1^2}{2}+34\ X_1 X_2+544\ X_2^2+34\ X_1 X_3+34\ X_2\ X_3+544 X_3^2+544\ X_4^2+544 X_5^2+544\ X_6^2$

✶2B3C.7

In[142]:= $X_1 = 2x_1$;

κ[w,(τ[a_{12}].τ[a_{23}].w)] // Expand

Out[142]= $6x_1^2+68x_1X_2+\frac{129X_2^2}{4}+68x_1X_3+\frac{2183X_2X_3}{4}+\frac{129X_3^2}{4}+\frac{1025X_4X_5}{2}-\frac{1025X_4X_6}{2}-\frac{1025X_5X_6}{2}$

✶2B3C.8

In[143]:= $X_2 = 2x_2$; $X_3 = 2x_3$;

κ[τ[a_{12}].w - w, w] // Expand

κ[τ[a_{13}].w - w, w] // Expand

Out[143]= $-1925x_2^2+3850x_2x_3-1925x_3^2-\frac{1025X_4^2}{2}-1025X_4X_6-\frac{1025X_6^2}{2}$

Out[144]= $-1925x_2^2-\frac{1025X_5^2}{2}-1025X_5X_6-\frac{1025X_6^2}{2}$

B.12 Mathematica for Lam-Chen algebra

✶LC.1

In[145]:=
```
w= Table[x_i,{i,1,9}];
Solve[w·w==w && trace[w]==9/8] // Length
```

Out[145]= 9

✶LC.2

In[146]:=
```
w= x I + y (64/3(a_{0,1}+a_{1,1}+a_{2,1})) + z(64/3(a_{0,2}+a_{1,2}+a_{2,2}));
κ[w,τ[a_{0,0}].w-w]
κ[w,τ[a_{0,1}].w-w]
```

Out[146]= $-1326\ (y-z)^2$

Out[147]= $-1326\ z^2$

✶LC.3

In[148]:=
```
w·(a_{0,0}-a_{2,0}) == (x+y+z)(a_{0,0}-a_{2,0}) // Simplify
```

Out[148]= True

✶LC.4

In[149]:=
```
(* note that v_{ab,cd} is short-hand for v_{(a,b)+<(c,d)>} *)
v_{10,01}=64/3(a_{1,0}+a_{1,1}+a_{1,2});
v_{20,01}=64/3(a_{2,0}+a_{2,1}+a_{2,2});
v_{10,11}=64/3(a_{1,0}+a_{2,1}+a_{0,2});
v_{20,11}=64/3(a_{0,1}+a_{1,2}+a_{2,0});
v_{10,12}=64/3(a_{1,0}+a_{2,2}+a_{0,1});
```

```
v20,12 = 64/3 (a2,0+a0,2+a1,1);
v01,10 = 64/3 (a0,1+a1,1+a2,1);
v02,10 = 64/3 (a0,2+a1,2+a2,2);
Q = {I,v10,01,v20,01,v10,11,v20,11,v10,12,v20,12,v01,10,v02,10};
IntegralFormQ[Q]
```

Out[149]= True

✶LC.5

```
In[150]:= B+ = {I,v10,01+v20,01,v10,11+v20,11,v10,12+v20,12,v01,10+v02,10};
w = 1/3 {y,X1,X2,X3,X4}.B+;
κ[w,τ[a0,1].w - w]
κ[w,τ[a1,0].w - w]
κ[w,w]-η[w,w] // Together
```

Out[150]= $-\frac{442}{3}(X_2^2+X_3^2+X_4^2)$

Out[151]= $-\frac{442}{3}(X_1^2+X_2^2+X_3^2)$

Out[152]= $-\frac{124}{9}(X_1^2+X_2^2+X_3^2+X_4^2)$

✶LC.6

```
In[153]:= B- = {v10,01-v20,01,v10,11-v20,11,v10,12-v20,12,v01,10-v02,10};
w = 1/3 {X1,X2,X3,X4}.B-;
vec[w·w,B+]
```

Out[153]= $\{\frac{16}{3}(X_1^2+X_2^2+X_3^2+X_4^2), \frac{2}{3}(3X_1^2+7X_2X_3+7X_2X_4-7X_3X_4), \frac{2}{3}(3X_2^2+7X_1X_3-7X_1X_4+7X_3X_4), \frac{2}{3}(7X_1X_2+3X_3^2+7X_1X_4-7X_2X_4), -\frac{2}{3}(7X_1X_2+7X_1X_3+7X_2X_3-3X_4^2)\}$

BIBLIOGRAPHY

[Bor86] Richard E. Borcherds, *Vertex algebras, Kac-Moody algebras, and the Monster*, Proc. Nat. Acad. Sci. U.S.A. **83** (1986), no. 10, 3068–3071.

[Bou98] Nicolas Bourbaki, *General topology. Chapters 5–10*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 1998, Translated from the French, Reprint of the 1989 English translation.

[CL14] Hsian-Yang Chen and Ching Hung Lam, *An explicit Majorana representation of the group* $3^2{:}2$ *of* $3C$*-pure type*, Pacific J. Math. **271** (2014), no. 1, 25–51.

[Con85] J. H. Conway, *A simple construction for the Fischer-Griess monster group*, Invent. Math. **79** (1985), no. 3, 513–540.

[DF04] David S. Dummit and Richard M. Foote, *Abstract algebra*, third ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004.

[DG12] Chongying Dong and Robert L. Griess, Jr., *Integral forms in vertex operator algebras which are invariant under finite groups*, J. Algebra **365** (2012), 184–198.

[FG92] Daniel E. Frohardt and Robert L. Griess, Jr., *Automorphisms of modular Lie algebras*, Nova J. Algebra Geom. **1** (1992), no. 4, 339–345.

[FLM88] Igor Frenkel, James Lepowsky, and Arne Meurman, *Vertex operator algebras and the Monster*, Pure and Applied Mathematics, vol. 134, Academic Press, Inc., Boston, MA, 1988.

[GL08] Robert L. Griess, Jr. and Ching Hung Lam, *Rootless pairs of* EE_8*-lattices*, Electron. Res. Announc. Math. Sci. **15** (2008), 52–61.

[GL11] ______, EE_8*-lattices and dihedral groups*, Pure Appl. Math. Q. **7** (2011), no. 3, Special Issue: In honor of Jacques Tits, 621–743.

[GL13] ______, *Applications of vertex algebra covering procedures to chevalley groups and modular moonshine*, `arXiv:1308.2270`, 2013.

[Gri82] Robert L. Griess, Jr., *The friendly giant*, Invent. Math. **69** (1982), no. 1, 1–102.

[Gri11] ______, *An introduction to groups and lattices: finite groups and positive definite rational lattices*, Advanced Lectures in Mathematics (ALM), vol. 15, International Press, Somerville, MA; Higher Education Press, Beijing, 2011.

[HRS15a] J. I. Hall, F. Rehren, and S. Shpectorov, *Primitive axial algebras of Jordan type*, J. Algebra **437** (2015), 79–115.

[HRS15b] ______, *Universal axial algebras and a theorem of Sakuma*, J. Algebra **421** (2015), 394–424.

[IPSS10] A. A. Ivanov, D. V. Pasechnik, Á. Seress, and S. Shpectorov, *Majorana representations of the symmetric group of degree 4*, J. Algebra **324** (2010), no. 9, 2432–2463.

[Iva09] A. A. Ivanov, *The Monster group and Majorana involutions*, Cambridge Tracts in Mathematics, vol. 176, Cambridge University Press, Cambridge, 2009.

[Kac98] Victor Kac, *Vertex algebras for beginners*, second ed., University Lecture Series, vol. 10, American Mathematical Society, Providence, RI, 1998.

[Lan02] Serge Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[McR14] Robert McRae, *On integral forms for vertex algebras associated with affine lie algebras and lattices*, `arXiv:1401.2505`, 2014.

[Miy96] Masahiko Miyamoto, *Griess algebras and conformal vectors in vertex operator algebras*, J. Algebra **179** (1996), no. 2, 523–548.

[Miy03] ______, *Vertex operator algebras generated by two conformal vectors whose τ-involutions generate S_3*, J. Algebra **268** (2003), no. 2, 653–671.

[Nor96] S. Norton, *The Monster algebra: some new formulae*, Moonshine, the Monster, and related topics (South Hadley, MA, 1994), Contemp. Math., vol. 193, Amer. Math. Soc., Providence, RI, 1996, pp. 297–306.

[Rud91] Walter Rudin, *Functional analysis*, second ed., International Series in Pure and Applied Mathematics, McGraw-Hill, Inc., New York, 1991.

[Sak07] Shinya Sakuma, *6-transposition property of τ-involutions of vertex operator algebras*, Int. Math. Res. Not. IMRN (2007), no. 9, Art. ID rnm 030, 19.

[Tit83a] Jacques Tits, *Remarks on Griess' construction of the Griess-Fischer sporadic group, i, ii, iii, iv*, Mimeographed letters (1982-1983), 89–102.

[Tit83b] ______, *Résumé de Cours*, Annuaire du Collège de France (1982-1983), 89–102.

[Tit84] ______, *On R. Griess' "friendly giant"*, Invent. Math. **78** (1984), no. 3, 491–499.

[Tit85] ______, *Le Monstre (d'après R. Griess, B. Fischer et al.)*, Astérisque (1985), no. 121-122, 105–122, Seminar Bourbaki, Vol. 1983/84.

[Wol] Wolfram Research, Inc., *Mathematica*, Version 10.4, Champaign, IL (2016).

[Yam74] Toshihiko Yamada, *The Schur subgroup of the Brauer group*, Lecture Notes in Mathematics, Vol. 397, Springer-Verlag, Berlin-New York, 1974.