$L_2(q)$ and the Rank Two Lie Groups: Their Construction, Geometry, and Character Formulas

by

Mark R. Sepanski

B.S., Mathematics, Purdue University, West Lafayette, IN (1990)

Submitted to the Department of Mathematics
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

May 1994

Signature of Author ....
Department of Mathematics
29th April, 1994

Certified by ....
Bertram Kostant
Professor of Mathematics
Thesis Supervisor

Accepted by ....
David Vogan
Chairman, Departmental Graduate Committee
Department of Mathematics

$L_2(q)$ and the Rank Two Lie Groups: Their Construction, Geometry, and Character Formulas

by

Mark R. Sepanski

Submitted to the Department of Mathematics
on 29th April, 1994, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

Abstract

This paper deals with certain aspects of a conjecture made by B. Kostant in 1983 relating the Coxeter number to the occurrence of the simple finite groups $L(2,q)$ in simple complex Lie groups. The first chapter of my thesis presents a unified approach to Kostant's conjecture that yields very general results for the rank two case. The second chapter examines when the conjecture gives rise to certain presentations of the Lie algebra as a sum of Cartan subalgebras for the rank two and exceptional cases. The third chapter looks at restricting representations of the the Lie group to the finite subgroup $L(2,q)$ and some resulting invariant theory.

Thesis Supervisor: Bertram Kostant
Title: Professor of Mathematics

To Laura

Acknowledgments

I am very grateful to my advisor, Bertram Kostant, for his enthusiasm and his powerful insights into mathematics. He has spent a great deal of time with me and I have grown enormously by the association. He will always represent the standard of mathematical excellence to which I will strive.

I would also like to thank David Vogan for all the conversations we have had. He has always made time to talk, has always explained things in a simple manner, and has always seemed to know the answer to my questions or at least a place for me to look.

I would also like to thank Richard Penney. It is from him at Purdue University that I first truly learned mathematics. Me feet were firmly set on this path by his marvelous classes.

Most of all, I would like to thank my family. My wife, Laura, my parents, Roger and Mary Sepanski, and my brothers and sister, Peter, Sheila, and Andy, all have been a constant source of encouragement, love, and faith. I cannot thank them enough. To be able to share this milestone with them is a great source of joy.

Contents

Introduction

This work centers around a conjecture made by B. Kostant in 1983 in *A Tale of Two Conjugacy Classes* ([17]). He proposed a link between a certain intrinsic number of a simple Lie group, called the Coxeter number, and the occurrence of certain finite simple groups. The conjecture has fueled quite a bit of research and turns out to have many connections to other areas of mathematics. Although a complete statement of Kostant's conjecture may be found in Theorem 2.1.1, let us outline the conjecture broadly in the following paragraphs.

The finite simple groups in question are the families alternately known as $PSL(2,q)$ or $L_2(q)$, where q is a prime power. To recall the definition of these groups, first write F_q for the field of q elements and write $SL(2,q)$ for the set of two by two matrices of determinant one with entries in F_q. Then $L_2(q)$ is defined as $SL(2,q)$ modulo its center (which consists of $\pm I$). These groups are of fundamental importance in group and representation theory since they often play the role of building blocks.

Now if we have some complex simple Lie group G, let us write h for the Coxeter number (see Table 2.1 for a list or [14] for a definition). Then, roughly, Kostant's conjecture states that when $2h+1$ is an odd prime power, then $L_2(2h+1)$ sits inside the Lie group. Moreover, it sits inside the Lie group in a special way. The conjecture states that the Lie algebra breaks up into certain "principal series" representations and subrepresentations of $L_2(2h+1)$ depending on the exponents of G (see Table 2.1 or [14] again). These principal series representations will be dealt with explicitly in Section 1.1.

Now considerable work has been done on finite subgroups of Lie groups (e.g. Cohen and Wales in [4] and [3]) and, in particular, on Kostant's conjecture ([3], [4], [6], [13], [23], and [13] of Cohen, Griess, Kleidman, Lisser, Meurman, Ryba, and Wales). The conjecture is verified easily in the non-exceptional cases by using a character table and Schur indicators (see [13] or [5]). However, the exceptional cases are much more difficult. The following table indicates the papers responsible for checking the conjecture in each case (note: a computer is relied upon in many of the papers below).

G_2	[23] and [3]
F_4	[4]
E_6	[4]
E_7	[13]
E_8	[6]

My research works with Kostant's conjecture in three broad ways. The first way examines a unified approach to the conjecture that yields very general results in the rank two case. The second way explores some geometry of certain Cartan subalgebras associated with the conjecture (primarily in the rank two and exceptional cases). The third way looks at restricting representations of G to $L_2(2h+1)$ and some invariant theory that arises from these finite groups. In the following paragraphs, I will go into more detail.

The first avenue my thesis explores is an attempt to prove Kostant's conjecture. The conjecture has been checked in all cases as noted above. However, most proofs have relied on a computer and this was the case for E_8 in particular ([6]). In fact, it was mainly this one result of $L_2(61)$ sitting inside E_8 that remained outstanding in the classification of all finite simple subgroups occurring in complex simple Lie groups (only $L_2(2,29)$ for E_7 and only $L_2(31)$, $L_2(32)$, and $Sz(8)$ for E_8 are still in doubt–see [5], Table 1). Of course, it is desirable to have a proof that does not need a computer.

One of the aims of my research is to provide such a proof. In fact, I propose to do something even stronger: I hope to start with $L_2(q)$ and construct the corresponding Lie group out of knowledge of this finite group and its representations. In my thesis, this construction is completely carried out in the rank two case.

To explain in more detail, I begin with three pieces of data: a principal series representation of $L_2(q)$ on a vector space V, a $L_2(q)$ invariant symmetric non-degenerate two-form $(,)$ on V, and a $L_2(q)$ invariant alternating three-form $(,,)$ on V. With these, I define a $L_2(q)$ invariant algebra structure $[,]$ on V according to the rule:

$$(v_1, v_2, v_3) \quad = \quad ([v_1, v_2], v_3) \tag{0.1}$$

for $v_1, v_2, v_3 \in V$. Then the idea is to see when it is possible to get a Lie algebra by this method, i.e, when does $[,]$ satisfy the Jacobi identity. If this can be done, then automatically $L_2(q)$ injects into the automorphism group of the Lie algebra. For instance, if this were done in the case of E_8, it would prove Kostant's conjecture. A central result of my thesis is the following theorem (Theorem 1.11.2, Corollary 1.12.1, and Theorem 1.9.1):

Theorem 0.0.1 *For V an irreducible principal series representation of $L_2(q)$ with q an odd prime power subject to Restriction 1.1.1, the above construction can make V into a non-trivial Lie algebra if and only if q = 7, 9, or 13. Moreover, in these cases, the resulting Lie algebra is A_2, B_2, and G_2, respectively.*

The above theorem proves Kostant's conjecture in the rank two case. In the course of the proof, certain interesting facts appear. Chief among them is the connection between the Jacobi identity in the rank two case and the problem of tiling the plane. It turns out that in most cases, the Jacobi identity forces certain integrality conditions (see Theorem 1.11.2) that are equivalent to the condition of being able to tile the plane with triangles, squares, or hexagons.

In the second part of my thesis, I study some geometry. In the setting of Kostant's conjecture, $L_2(q)$ injects into a simple Lie group G with Lie algebra $\mathfrak{g}$. Thus $L_2(q)$ acts on $\mathfrak{g}$ by the Adjoint action. It turns out that a Borel subalgebra of $L_2(q)$ fixes a Cartan subalgebra of $\mathfrak{g}$. Hence it is easy to see that there are $q+1$ Cartans, $\mathfrak{h}_p$ indexed by $p \in \mathsf{P}^1(\mathsf{F}_q)$ (the projective line), such that $L_2(q)$ permutes the Cartans $\mathfrak{h}_p$ in the same way that $L_2(q)$ acts on $p \in \mathsf{P}^1(\mathsf{F}_q)$ by linear fractional transformations.

What can be hoped is that there is some good way to decompose $\mathfrak{g}$ as a direct sum of a subset of the $\mathfrak{h}_p$. Questions of this sort have been much studied, e.g. by Alekseevskiǐ, A. Kostrikin, I. Kostrikin, and Ufnarovskiǐ in [20], [21], [22], and [1]. Such situations lead to many interesting theorems. For instance, one may consider groups that preserve some aspect of such a decomposition (see [19] or [32] for E_8 and the finite simple sporadic Thompson group).

My work on the subject centers on decompositions with respect to two special conjugacy classes, namely Kostant and Kac elements ([17]). It is hard to overestimate the importance of these elements, especially the Kostant element. Let us write h for the Coxeter number. Then one has a standard theorem saying:

Theorem 0.0.2 *For G a complex simple Lie group with trivial center, a* **Kostant** *element is a element $g \in G$ satisfying either of the two following equivalent conditions:*
(1) g is regular and the order of g is h, or
(2) there exists a Cartan subalgebra, $\mathfrak{h}$, normalized by g such that $Ad(g) \mid_{\mathfrak{h}}$ is a Coxeter *element.*

An element $g \in G$ is said to be a **Kac** *element if it satisfies the following condition:*
(1′) g is regular and the order of g is $h+1$.

Moreover, the set of Kostant elements form a single conjugacy class and the set of Kac elements form a single conjugacy class in G. Finally, if χ is the character of any irreducible representation of G, then the value of χ on either a Kostant or a Kac element lies in the set $\{-1, 0, 1\}$.

For additional properties of these elements (including characterizations by their eigenvalues on a Cartan), see [17],[12], and [14]. For some applications, see e.g. [16] for relations to the Macdonald formulas, [18] for relations to the McKay correspondence, and [12] for relations to the Legendre symbol. Also see [17] for a result of Bomshik Chang that states that (except in the case of B_2) one can always choose a Kostant element and a Kac element which will together generate a $\mathbb{Z}$-form of G.

Since these two classes are so important and, moreover, will manifest themselves as members of $L_2(q)$, the question that I attempt to answer is whether it is possible to write $\mathfrak{g}$ as a sum of certain $\mathfrak{h}_p$ lying in orbits of either a Kostant or Kac element. In my thesis, this question is answered in the case of the rank two and exceptional Lie algebras in a surprising way. The theorem says (see Corollary 2.6.1) that a decomposition is always possible—but either the Kostant element works and the Kac element fails or vice versa:

Theorem 0.0.3 *Let G be one of the following: $A_2, A_4, B_2, G_2, F_4, E_6, E_7$, or E_8. With respect to Kostant's embedding of $L_2(q) \hookrightarrow G$, $\mathfrak{g}$ admits an invariant decomposition as vector spaces*

$$\mathfrak{g} = \bigoplus_{u \in \mathcal{P}_A} \mathfrak{h}_u$$

by a Kostant element, $A \in L_2(q)$, if and only if h is odd (i.e., A_2 or A_4).

Similarly, $\mathfrak{g}$ admits an invariant decomposition as vector spaces

$$\mathfrak{g} = \bigoplus_{u \in \mathcal{P}_K} \mathfrak{h}_u$$

by a Kac element, $K \in L_2(q)$, if and only if $h+1$ is odd (i.e., B_2, G_2, F_4, E_6, E_7, or E_8).

In proving this result, the main tools come from number theory. Gamma, Jacobi, and Bessel functions and their generalizations are used with the Stickelbeger Relation providing the key lemma. For instance, in Theorem 2.2.3 proving the existence of a Kostant element invariant decomposition reduces to knowing that two Jacobi sums (related by the Legendre symbol) are not equal.

The last part of my thesis centers on characters of the finite group and some applications to invariant theory. I calculate formulas for determining how an irreducible representation of G (in terms of its highest weight) breaks up into representations of $L_2(q)$ in the rank two cases (see Theorem 3.3.1, Theorem 3.3.2, and Theorem 3.3.3). Using these formulas, one may look at one-parameter families of representations and construct generating functions. Work such as this has been much studied (e.g. [24] and [25]). While the theory of Poincaré series is very old, my results seek to generalize Kostant's elegant results in [18].

In the case of A_2 with $L_2(7)$ (Theorem 3.6.1), the best generalization I found turns out to include a formula already known to Springer in [30]. However, for B_2 with $L_2(9)$ (Theorem 3.7.1), the results seem to be new. Unfortunately, for G_2 with $L_2(13)$ (Section 3.8), the answers completely lose their simplicity. Nevertheless, in Section 3.5, I have written formulas by which such results may be effectively computed even in complicated cases such as G_2.

Chapter 1

The Construction in the Rank Two Case

In this first chapter, we take a principal series representation of $L_2(q)$ and determine when it can be made into a Lie algebra according to the recipe given in the introduction relating to Equation 0.1. To do this, we will first need some information about these principal series representations.

1.1 The e-basis

Throughout this paper, let $q = p^f$ be an odd prime power. The main group under consideration will be $L_2(q) = PSL(2, q) =$ the group of 2×2 matrices of determinant 1 over the field F_q of q elements modulo its center. Since q is odd, we may write

$$q = 2h + 1 \tag{1.1}$$

with h an integer. This number, h, will end up playing the role of the Coxeter number in Lie theory.

It is well known that

$$\begin{aligned} \mid L_2(q) \mid &= \frac{q(q^2 - 1)}{2} \\ &= 2(h + 1)h(2h + 1) \end{aligned} \tag{1.2}$$

where $\mid L_2(q) \mid$ is the order of the group.

The product decomposition exhibited in Equation 1.2 corresponds to three special subgroups of $L_2(q)$. The first, denoted by $\mathcal{A}$, consists of diagonal matrices. It is cyclic of order h. The second, denoted by $\mathcal{N}$, consists of the upper triangular matrices with ones on the diagonals. Its order is $q = 2h+1$ and it is cyclic only if $p = q$. Together, these two subgroups generate $\mathcal{B}$, a *Borel* subgroup of $L_2(q)$ consisting of upper triangular matrices. The third special subgroup, denoted $\mathcal{K}$, is cyclic of order $h+1$. It is more complicated than $\mathcal{A}$ and $\mathcal{N}$ and will be discussed in detail in Section 2.5.

For the present, the study of $\mathcal{B}$ will be the most important task. Of course one has

$$| L_2(q)/\mathcal{B} | \;=\; q+1.$$

Basically, all this says is that $L_2(q)/\mathcal{B}$ may be viewed as the projective line, $\mathsf{P}^1(\mathsf{F}_q) = \mathsf{F}_q \bigcup \{\infty\}$, over the field F_q. Thus if we take a complex character π of $\mathcal{B}$ and induce the representation up to $L_2(q)$, we get a $q+1$ dimensional representation. It is precisely these *principal series* representations that play a central role in Kostant's conjecture. Even though they are well understood, it will be useful for us to write them out explicitly.

Notation: To begin with, we *fix a generator* λ for the multiplicative group $\mathsf{F}_q^* = \mathsf{F}_q \backslash \{0\}$. This generator will be fixed throughout the paper. Next fix π to be a complex *multiplicative character* of F_q^* such that $\pi(-1) = 1$. Thus, for each integer m where $1 \leq m \leq h$, there exists such a character uniquely determined by $\pi_m(\lambda) = e^{2\pi i m/h}$. The reason for choosing π to be trivial on -1 is that by using the obvious homomorphism from F_q^* onto $\mathcal{A}$ (with kernel $\{\pm 1\}$), we may view π as a character of $\mathcal{A}$. Next, by extending π to be trivial on $\mathcal{N}$, we may view π as a character of $\mathcal{B}$. We will view π interchangeably as a character either of F_q^* or of $\mathcal{B}$ as context dictates.

Now let V_π be $Ind_{\mathcal{B}}^{L_2(q)}(\pi)$, the induced representation of π from $\mathcal{B}$ to $L_2(q)$. The notation will be simplified to just V whenever π is understood. As in [26], we may consider V to be the set of all complex valued functions f on $L_2(q)$ satisfying

$$f(bg) \;=\; \pi(b)f(g)$$

for all $b \in \mathcal{B}$ and $g \in L_2(q)$. With this, we have the action $gf(x) = f(xg)$. The appropriate theorem regarding the nature of V is standard. For instance, it may be found in [26] §5.4:

Theorem 1.1.1 *V_{π_m} is an irreducible representation of $L_2(q)$ if and only if $\pi_m^2 \neq 1$. Moreover, V_{π_m} and V_{π_n} are equivalent if and only if $\pi_m = \pi_n$ or $\pi_m = {\pi_n}^{-1}$.*

It will be useful to write out a "delta" basis for V ,i.e. each basal element is supported on one right coset of $\mathcal{B} \backslash L_2(q)$. To this end, we choose the following representatives for $\mathcal{B} \backslash L_2(q)$:

$$g_u \;=\; \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix}$$

$$g_\infty = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

for $u \in \mathsf{F}_q$. Now let us define the *e-basis* by requiring that $e_v \in V$ and

$$e_v(g_w) = \delta_{v,w}$$

for all $v, w \in \mathsf{P}^1(\mathsf{F}_q)$ where $\delta_{v,w}$ is 1 if $v = w$ and 0 otherwise. It is obvious that these functions form a basis for V. It is also well known and easily checked that $L_2(q)$ acts on this basis as an (inverse transpose) linear fractional transformation on $\mathsf{P}^1(\mathsf{F}_q)$ with certain non-zero coefficients. This is detailed in the next theorem.

Theorem 1.1.2 *Let $u \in \mathsf{P}^1(\mathsf{F}_q)$ and $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in L_2(q)$. Then $L_2(q)$ acts on V in the e-basis by*

$$ge_u = ke_v$$

where $v \in \mathsf{P}^1(\mathsf{F}_q)$ is determined by

$$v = \frac{du - c}{-bu + a}$$

and $k \in \mathsf{C}^*$ is determined by

$$k = \begin{cases} \pi(-bu + a) & \text{if } u, v \neq \infty \\ \pi(1/b) & \text{if } u \neq \infty \text{ but } v = \infty \\ \pi(1/a) & \text{if } u, v = \infty \\ \pi(-b) & \text{if } u = \infty \text{ but } v \neq \infty. \end{cases}$$

Proof. Since this result is well known and just a matter of checking definitions, we omit the details. Part of it may be found in [26] . □

It will be useful for us to write out this action for a few elements in $L_2(q)$ that will be particularly important to us. Namely, define

$$A = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \tag{1.3}$$

$$N_x = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \tag{1.4}$$

$$M_x = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \tag{1.5}$$

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tag{1.6}$$

where $x \in \mathsf{F}_q^*$ and we recall that λ was the fixed generator for F_q^*. For simplicity, we will refer to N_1 as N and to M_1 as M. The action on these elements is given by:

Corollary 1.1.1 *Let $u \in \mathsf{F}_q$. Then with the preceding notation, $L_2(q)$ acts on V by*
(1) $Ae_u = \pi(\lambda)e_{\frac{u}{\lambda^2}}$ and $Ae_\infty = \pi(\lambda^{-1})e_\infty$
(2) $N_x e_u = \pi(-xu+1)e_{\frac{u}{-xu+1}}$ if $u \neq 1/x$, $N_x e_{\frac{1}{x}} = \pi(x^{-1})e_\infty$, and $N_x e_\infty = \pi(-x)e_{\frac{-1}{x}}$
(3) $M_x e_u = e_{u-x}$ and $M_x e_\infty = e_\infty$
(4) $Se_u = \pi(u)e_{\frac{-1}{u}}$ and $Se_\infty = e_0$.

Our goal in Chapter 1 will be to determine when a principal series representation can be made into a non-trivial Lie algebra by the recipe given in Equation 0.1. To get our desired results, throughout Chapter 1 we will need to place a restriction on the type of principal series we consider or require more of Kostant's conjecture to hold (Theorem 2.1.1). Specifically, we will always assume that:

Restriction 1.1.1 *We will only consider in Chapter 1 those principal series representations V_{π_m} where we assume that if h is even and m is odd, then $\pi_m(\lambda)$ is a primitive h'th root of unity, i.e., that m and h are relatively prime. Alternately, if we change our goal from determining when V_{π_m} is a non-trivial Lie algebra to determining when it is a Lie algebra satisfying all Kostant's conjecture (namely, Theorem 2.1.1 part(4)), we could drop this hypothesis.*

1.2 The f-basis

For reasons that will become apparent later, it is convenient to introduce a "fourier transform" of our earlier e-basis. For now, we can view it as a way of diagonalizing the operators M_x. To this end, fix a non-trivial *additive character* χ of F_q. This character will also be fixed throughout the remainder of the paper. The next definition gives the *f-basis.*

Definition 1.2.1 *For $u \in \mathsf{F}_q$, define*

$$f_u = \sum_{a \in \mathsf{F}_q} \chi(au)e_a$$

and let $f_\infty = e_\infty$.

We will also need the following "Bessel" and "Gamma" functions since they will come up often:

Definition 1.2.2 *For $i, j \in \mathsf{F}_q$, let*

$$\Gamma_{i,j} = \frac{1}{q} \sum_{a \in \mathsf{F}_q^*} \chi\left(\frac{i}{a} + ja\right)\pi(a).$$

Note that $\Gamma_{0,0} = 0$.

Though we will not need any properties of the $\Gamma_{i,j}$ at this moment, we will eventually need a few of their elementary properties. Thus we prove:

Lemma 1.2.1 *The $\Gamma_{i,j}$ satisfy the following relations:*
(1) $\Gamma_{i,j} = \Gamma_{-i,-j}$
(2) $\overline{\Gamma_{i,j}} = \Gamma_{j,i}$
(3) $\Gamma_{i,j} = \pi(1/j)\Gamma_{ij,1}$ for $i \in \mathsf{F}_q$ and $j \in \mathsf{F}_q^*$
(4) $\Gamma_{i,j} = \pi(i)\Gamma_{1,ij}$ for $i \in \mathsf{F}_q^*$ and $j \in \mathsf{F}_q$
(5) $\Gamma_{1,0}\Gamma_{0,1} = 1/q$. In particular, $\Gamma_{0,1}$ is non-zero.

Proof. Part (1) follows by the substitution of $a \to -a$ and the fact that $\pi(-1) = 1$. Part (2) uses the behavior of the characters under conjugation and the substitution $a \to 1/a$. Parts (3) and (4) simply use the substitutions $a \to a/j$ and $a \to ia$, respectively. Part (5) is merely the fact that in this case, our definitions reduce to Gauss sums. One checks this below using the substitutions $c = ab$ and $d = 1/b$:

$$\begin{aligned} \Gamma_{1,0}\Gamma_{0,1} &= 1/q^2 \sum_{a,b \in \mathsf{F}_q^*} \chi(1/b + a)\pi(ab) \\ &= 1/q^2 \sum_{c \in \mathsf{F}_q^*} \pi(c) \sum_{d \in \mathsf{F}_q^*} \chi(d(c+1)) \\ &= 1/q^2 \sum_{c \in \mathsf{F}_q^*} \pi(c)[-\delta_{c+1 \neq 0} + (q-1)\delta_{c+1=0}] \\ &= 1/q^2[\pi(-1) + (q-1)\pi(-1)] \\ &= 1/q \end{aligned}$$

where $\delta_{condition}$ is 1 if the condition is satisfied and 0 otherwise. □

It is now easy to check how the f-basis behaves under the operators M, A, and S from Equations 1.5, 1.3, and 1.6. In the following, recall that λ was the fixed generator of F_q^*, π is the fixed multiplicative character of F_q^*, χ is the fixed additive character of F_q, and the Γ's are as defined above.

Theorem 1.2.1 *For $u \in \mathbf{F}_q$,*
(1) $M_x f_u = \chi(xu) f_u$ and $M_x f_\infty = f_\infty$
(2) $Af_u = \pi(\lambda) f_{\lambda^2 u}$ and $Af_\infty = \pi(\lambda^{-1}) f_\infty$
(3) $Sf_u = \sum_{i \in \mathbf{F}_q} (\Gamma_{i,u} f_i) + f_\infty$ and $Sf_\infty = 1/q \sum_{i \in \mathbf{F}_q^*} f_i$.

Proof. Using Theorem 1.1.2 for part (1) we have:

$$\begin{aligned} Mf_u = \sum_{a \in \mathbf{F}_q} \chi(au) Me_a = \sum_{a \in \mathbf{F}_q} \chi(au) e_{a-1} \\ = \sum_{a \in \mathbf{F}_q} \chi((a+1)u) e_a = \chi(u) f_u. \end{aligned}$$

In a similar fashion, $M_k f_u = \chi(ku) f_u$. For part (2) we have:

$$\begin{aligned} Af_u &= \sum_{a \in \mathbf{F}_q} \chi(au) \pi(\lambda) e_{a/\lambda^2} \\ &= \sum_{a \in \mathbf{F}_q} \chi(a \lambda^2 u) e_a \\ &= \pi(\lambda) f_{\lambda^2 u}. \end{aligned}$$

For part (3), we use the trivial observation that $e_u = 1/q \sum_{a \in \mathbf{F}_q} \chi(-au) f_a$, i.e., the "inverse fourier transform:"

$$\begin{aligned} Sf_u &= \sum_{a \in \mathbf{F}_q^*} \chi(au) \pi(a) e_{-1/a} + e_\infty \\ &= 1/q \sum_{b \in \mathbf{F}_q} \sum_{a \in \mathbf{F}_q^*} \chi(au) \pi(a) \chi(b/a) f_b + e_\infty \\ &= 1/q \sum_{b \in \mathbf{F}_q} \Gamma_{b,u} f_b + e_\infty \end{aligned}$$

The computations for f_∞ are similar. □

1.3 $PGL(2, q)$

Since we have noted earlier that the action of $L_2(q)$ on the e-basis is basically a linear fractional transformation action on $\mathbf{P}^1(\mathbf{F}_q)$, it will be useful to bring the group $PGL(2, q)$ into the picture. The definition of $PGL(2, q)$ is the set of all 2×2 non-singular matrices with entries in F_q modulo its center. The order of this group is

$$| PGL(2,q) | \ = \ q(q^2-1).$$

One observes that the $PGL(2,q)$ has twice the order of $L_2(q)$. This is because $L_2(q)$ sits inside of $PGL(2,q)$ as a normal subgroup of index two. This can be seen using the determinant. Now the determinant function on $PGL(2,q)$ is only well defined up to multiples by squares in F_q^*, but this is enough to pick out $L_2(q)$ inside of $PGL(2,q)$. It is trivial to verify that $L_2(q)$ is precisely those elements of $PGL(2,q)$ whose determinant is of the form u^2, $u \in \mathsf{F}_q^*$.

The usefulness of $PGL(2,q)$ will arise from the fact that it acts on $\mathsf{P}^1(\mathsf{F}_q)$ by linear fractional transformations in a very nice way. Specifically, the Fundamental Theorem of Projective Geometry says that any three distinct point of the projective line may always be sent to any other three distinct points by a unique element of $PGL(2,q)$, i.e., it is strictly 3-transitive. For future use, we give the determinant of the following specific maps (determined up to a square in F_q^*):

Theorem 1.3.1 *Let s,t,v be distinct elements in F_q. The determinant of the unique element in $PGL(2,q)$ that maps the triple $(1,0,\infty)$ to the triple (s,t,v), (∞,t,v), (s,∞,t), and (s,t,∞) is, respectively, the following : $(s-t)(s-v)(t-v)$, $(t-v)$, $-(s-v)$, and $(s-t)$.*

Proof. One has only to examine the following matrices, bearing in mind that the determinant is only defined up to a square: $\begin{pmatrix} -v(s-t) & -(s-t) \\ t(s-v) & s-v \end{pmatrix}$, $\begin{pmatrix} -v & -1 \\ t & 1 \end{pmatrix}$, $\begin{pmatrix} -v & -1 \\ -(s-v) & 0 \end{pmatrix}$, and $\begin{pmatrix} s-t & 0 \\ t & 1 \end{pmatrix}$. □

1.4 The Invariant Two-form

In this section we wish to examine the nature and existence of $L_2(q)$ invariant two-forms on the induced representation V. Of course, if V is irreducible then there is at most one (depending on whether it is self-dual or not). One way to see abstractly there is only one invariant symmetric two-form is by using the Fundamental Theorem of Projective Geometry and the "linear fractional" action of the e-basis. While this is easy, we will need an explicit description. The f-basis provides a very nice formulation of our invariant two-form.

Theorem 1.4.1 *For π^2 non-trivial, up to a constant multiple, there exists a unique $L_2(q)$ invariant symmetric non-degenerate two form (,) on V characterized uniquely by*

(1) $(f_u, f_{-u}) = 1/\pi(u)$ *for* $u \in \mathsf{F}_q^*$
(2) $(f_0, f_\infty) = (f_\infty, f_0) = \frac{1}{q\Gamma_{0,1}} = \Gamma_{1,0}$
(3) All other pairings between the f-basis are zero.

Proof. We first comment on the requirement that $\pi^2 \neq 1$. This will actually be useful in the proof. However, the real reason for it lies in Theorem 1.1.1 which makes it the requirement for V to be irreducible. If π^2 were trivial, one could easily check that there would be *two* different invariant two-forms on V. Namely, the one above and a second one defined only on the diagonal parts (e_x, e_x). However, this will not be needed.

As already noted, there are many ways to check the existence of a non-zero $L_2(q)$ invariant two-form. Since this is easy, we merely record that in any character table for $L_2(q)$ (say in [26]) one may check that the characters for V are all real valued so that V is self dual and there exists such a form (as noted earlier, it is possible to see this directly by using the FT of Projective Geometry). Let us write $(,)$ for a non-zero choice of an invariant two form.

First note that by A invariance (see Corollary 1.1.1) and the fact that $\pi^2 \neq 1$, it is easy to see that $(e_x, e_x) = 0$ for $x \in \mathsf{P}^1(\mathsf{F}_q)$. Next, since the Fundamental Theorem of Projective Geometry says that $PGL(2,q)$ is strictly three transitive on $\mathsf{P}^1(\mathsf{F}_q)$, it is easy to see that $L_2(q)$ will be two transitive. In particular, if (e_0, e_1) were zero, then by invariance we would have (e_x, e_y) zero for all x, y distinct in $\mathsf{P}^1(\mathsf{F}_q)$. However, by definition $(,)$ is non-zero which forces $(e_0, e_1) \neq 0$. One may also see that $(,)$ is symmetric using the $L_2(q)$ action, but we will let it follow from the calculations done below. All we will need is that (e_0, e_1) is non-zero so that we will be able to re-normalize it.

Now let $(,)$ be the unique non-zero invariant two-form on V that we have from the proceeding paragraph. Then for $x, y \in \mathsf{F}_q$, we have (using M_a invariance–see Corollary 1.1.1):

$$\begin{aligned}(f_x, f_y) &= 1/q^2 \sum_{a,b \in \mathsf{F}_q} \chi(ax+by)(e_a, e_b) \\ &= 1/q^2 \sum_{a,b \in \mathsf{F}_q} \chi(ax+by)(e_0, e_{b-a}).\end{aligned}$$

Setting $c = b - a$ yields

$$\begin{aligned}(f_x, f_y) &= \sum_{a,c \in \mathsf{F}_q} \chi(ax+ay+cy)(e_0, e_c) \\ &= \sum_{c \in \mathsf{F}_q} \chi(cy)(e_0, e_c) \sum_{a \in \mathsf{F}_q} \chi(a(x+y)) \\ &= q\delta_{x+y=0} \sum_{c \in \mathsf{F}_q} \chi(cy)(e_0, e_c)\end{aligned}$$

$$= \quad q\delta_{x+y=0} \sum_{c\in \mathbf{F}_q^*} \chi(cy)(e_0, e_c) \qquad (1.7)$$

where again $\delta_{condition}$ is 1 or 0 depending on whether the condition is satisfied or not. Now we make use of the invariance again. For $b \in \mathbf{F}_q^*$, we know that $N_b e_0 = e_0$ and if $b \neq 1$, then $N_b e_1 = \pi(1-b)e_{\frac{1}{-b+1}}$ by Corollary 1.1.1. Observe now that the images of $1 \to \frac{1}{-b+1}$ in $\mathbf{P}^1(\mathbf{F}_q)$ as b varies over $\{b \in \mathbf{F}_q | b \neq 1\}$ is precisely $\mathbf{F}_q^*$. Therefore $\{c \in \mathbf{F}_q^*\} = \{\frac{1}{-b+1} \mid b \neq 1\}$. Thus we may continue Equation 1.7 to write:

$$\begin{aligned}
(f_x, f_y) &= q\delta_{-x=y} \sum_{b\in \mathbf{F}_q, b\neq 1} \chi(\frac{y}{-b+1})(e_0, e_{\frac{1}{-b+1}}) \\
&= q\delta_{-x=y} \sum_{b\neq 1} \chi(\frac{y}{-b+1})(N_b e_0, N_b e_1)\pi(-b+1)^{-1} \\
&= q\delta_{-x=y}(e_0, e_1) \sum_{b\neq 1} \chi(\frac{y}{1-b})\pi(\frac{1}{1-b}).
\end{aligned}$$

By setting $a = \frac{1}{1-b}$ and using Definition 1.2.2 and Lemma 1.2.1 part (3), we get

$$\begin{aligned}
(f_x, f_y) &= q\delta_{-x=y}(e_0, e_1) \sum_{a\in \mathbf{F}_q^*} \chi(ya)\pi(a) \\
&= q^2\delta_{-x=y}(e_0, e_1)\Gamma_{0,y} \\
&= q^2\delta_{-x=y}\pi(1/y)\Gamma_{0,1}(e_0, e_1).
\end{aligned}$$

This gives us the desired formula for (f_x, f_y) when $x, y \in \mathbf{F}_q$. Let us compute the formulas for the remaining cases, namely when x or y are ∞. Again by A invariance, we know that $(f_\infty, f_\infty) = 0$. Thus it only remains to evaluate (f_∞, f_x) (the calculation for (f_x, f_∞) is similar). We shall use techniques similar to the ones above, however, let us now use

$$g_d = \begin{pmatrix} 0 & -1 \\ 1 & -d \end{pmatrix}$$

instead of N_b. This element (using Theorem 1.1.2) satisfies $g_d e_0 = e_\infty$ and $g_d e_1 = e_{d+1}$. This will allow us to write:

$$\begin{aligned}
(f_\infty, f_x) &= \sum_{a\in \mathbf{F}_q} \chi(ax)(e_\infty, e_a) \\
&= \sum_{d\in \mathbf{F}_q} \chi((d+1)x)(g_d e_0, g_d e_1) \\
&= (e_0, e_1)\chi(x) \sum_{d\in \mathbf{F}_q} \chi(dx)
\end{aligned}$$

$$= \quad q\delta_{x=0}(e_0, e_1).$$

By re-normalizing (e_0, e_1) properly (which, as seen earlier can be arbitrary), we have finished the proof. Merely recall that $\Gamma_{1,0}\Gamma_{0,1} = 1/q$ by Lemma 1.2.1 part (5). □

As a result of this theorem, we get a formula for the e-basis as well.

Theorem 1.4.2 *Suppose $\pi^2 \neq 1$. Extend π to F_q by setting $\pi(0) = 0$. Then for $u, v \in \mathsf{F}_q$, the invariant symmetric two-form on V satisfies*
(1) $(e_u, e_v) = \Gamma_{1,0}/q\ \pi(u-v)$
(2) $(e_u, e_\infty) = \Gamma_{1,0}/q$
(3) $(e_\infty, e_\infty) = 0$.

Proof. By A invariance, we have already noted that $(e_u, e_u) = 0$ for all $u \in \mathsf{P}^1(\mathsf{F}_q)$. For $x, y \in \mathsf{F}_q$, take the "inverse fourier transform" of the e-basis to get the f-basis and use the above theorem:

$$\begin{aligned}
(e_x, e_y) &= 1/q^2 \sum_{a,b \in \mathsf{F}_q} \chi(-ax - by)(f_a, f_b) \\
&= 1/q^2 \sum_{a,b \in \mathsf{F}_q^*} \chi(-ax - by)\delta_{a+b=0}\pi(a)^{-1} \\
&= 1/q^2 \sum_{a \in \mathsf{F}_q^*} \chi(a(y-x))\pi(1/a) \\
&= 1/q\Gamma_{y-x,0} \\
&= \pi(x-y)\Gamma_{1,0}/q.
\end{aligned}$$

Next

$$\begin{aligned}
(e_x, e_\infty) &= 1/q \sum_{a \in \mathsf{F}_q} \chi(-ax)(f_a, f_\infty) \\
&= 1/q(f_0, f_\infty) \\
&= 1/q\frac{1}{q\Gamma_{0,1}} \\
&= \Gamma_{1,0}/q.
\end{aligned}$$

□

1.5 The Invariant Three-forms

We would like to examine the nature of $L_2(q)$ invariant alternating three forms on V and get an explicit description of them. In other words, using our $L_2(q)$ invariant symmetric non-degenerate two-form to get V isomorphic to V^*, we are interested in $\bigwedge^3 V$, the third exterior power of V, and its orbit structure under $L_2(q)$. As a first step, let us look at the action on $\bigotimes^3 V$, the third tensor power of V, which may be regarded as the space of *all* 3-forms.

If we work in the e-basis, it will be sufficient to look at the action of $L_2(q)$ on elements of the form $e_x \otimes e_y \otimes e_z$ where $x, y, z \in \mathsf{P}^1(\mathsf{F}_q)$ since this basis is preserved by $L_2(q)$ up to non-zero scalars (Theorem 1.1.2). As a second refinement, it is enough to look at the action of $L_2(q)$ on the $L_2(q)$ invariant subspace of $\bigotimes^3 V$ spanned by $\{e_x \otimes e_y \otimes e_z \mid x, y, z \text{ are distinct in } \mathsf{P}^1(\mathsf{F}_q)\}$. Let us call this subspace $D \bigotimes^3 V$. The reason we may restrict our attention to $D \bigotimes^3 V$ is because we will eventually want to look at alternating forms ($\bigwedge^3 V$) and the fact that elements in the natural complement to $D \bigotimes^3 V$ will project to zero under anti-symmetrization.

As a next step, let us "projectivize" the action. That is, for the moment let us ignore the (non-zero) constants of Theorem 1.1.2 and concentrate on the "linear fractional" aspect of the action. Thus we look at the action of $L_2(q)$ on $D \bigotimes^3 \mathsf{P}^1(\mathsf{F}_q) = \{x \bigotimes y \bigotimes z \mid x, y, z \text{ are distinct in } \mathsf{P}^1(\mathsf{F}_q)\}$. Now the previous discussion in Section 1.3 on $PGL(2, q)$ basically amounts to the fact that whereas $PGL(2, q)$ breaks this set into a single orbit, the action of $L_2(q)$ yields two orbits depending on whether the cross-ratio of x, y, z is a square or not in F_q^* (Theorem 1.3.1). Thus there cannot possibly be more than two $L_2(q)$ invariant forms that have a hope of being alternating. Using Theorem 1.3.1, we see that the determinant of the element in $PGL(2, q)$ taking $1 \otimes 0 \otimes -1$ to $\lambda \otimes 0 \otimes -\lambda$ (via $1 \otimes 0 \otimes \infty$) is λ^3, a non-square. Thus, these are representatives of the two $L_2(q)$ orbits in $D \bigotimes^3 \mathsf{P}^1(\mathsf{F}_q)$.

Now let us put the constants back in and look again at $D \bigotimes^3 V$. First we show that the stabilizer of $1 \otimes 0 \otimes -1$ and the stabilizer of $\lambda \otimes 0 \otimes -\lambda$ also fixes $e_1 \otimes e_0 \otimes e_{-1}$ and $e_\lambda \otimes e_0 \otimes e_{-\lambda}$, respectively. However, both stabilizers are trivial by the Fundamental Theorem of Projective Geometry. Thus the orbit of each defines an invariant 3-form. Hence we are allowed to make the following definition.

Definition 1.5.1 *Let $(,,)_+$ and $(,,)_-$ be the two $L_2(q)$ invariant three-forms on V defined by*
(1) $(e_1, e_0, e_{-1})_+ = 1$ *and* $(e_\lambda, e_0, e_{-\lambda})_+ = 0$
(2) $(e_1, e_0, e_{-1})_- = 0$ *and* $(e_\lambda, e_0, e_{-\lambda})_- = 1$.

As a result of the above discussion, we see that any non-zero invariant 3-form on V, for V irreducible, that has a possibility of being an *alternating* form must be a linear combination of $(,,)_+$ and $(,,)_-$. Since each of these forms will be so important to us, we will give explicit descriptions of their structure. First we make the following notational definition:

Definition 1.5.2 *Let $u \in \mathsf{F}_q$. Then define the symbol $\sqrt{u}^{\delta} \in \mathsf{F}_q$ to be*

$$\sqrt{u}^{\delta} = \begin{cases} v & \text{if } u = v^2 \text{ for some } v \in \mathsf{F}_q \\ 0 & \text{if } u \text{ is not a square in } \mathsf{F}_q. \end{cases}$$

Note that if $u \neq 0$, then $\sqrt{u}^{\delta}$ is only well defined up to ± 1. However, this will be sufficient for our purposes.

Theorem 1.5.1 *Let $x, y, z \in \mathsf{F}_q$. Recalling that π is extended to all of F_q by $\pi(0) = 0$, one has:*
(1)

$$(e_x, e_y, e_z)_+ = \pi(\sqrt{2(x-y)(x-z)(y-z)}^{\delta}),$$

and

$$(e_x, e_y, e_z)_- = \pi(\sqrt{2\lambda^3(x-y)(x-z)(y-z)}^{\delta}).$$

(2) $(e_\infty, e_y, e_z)_+ = \pi(\sqrt{2(y-z)}^{\delta})$ *and* $(e_\infty, e_y, e_z)_- = \pi(\sqrt{2\lambda(y-z)}^{\delta})$,
(3) $(e_x, e_\infty, e_z)_+ = \pi(\sqrt{-2(x-z)}^{\delta})$ *and* $(e_x, e_\infty, e_z)_- = \pi(\sqrt{-2\lambda(x-z)}^{\delta})$,
(4) $(e_x, e_y, e_\infty)_+ = \pi(\sqrt{2(x-y)}^{\delta})$ *and* $(e_x, e_y, e_\infty)_- = \pi(\sqrt{2\lambda(x-y)}^{\delta})$.
In particular, if u, v, w are not distinct, then $(e_u, e_v, e_w)_+ = (e_u, e_v, e_w)_- = 0$.

Proof. First observe that since $\pi(\pm 1) = 1$, everything above is well defined with respect to the symbol $\sqrt{\cdot}^{\delta}$. Now all we need to use is Theorem 1.3.1. Consider (1a) first. The element $g' \in PGL(2,q)$ that takes the triple (x, y, z) to $(1, 0, -1)$ is

$$g' = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} z(x-y) & x-y \\ -y(x-z) & -(x-z) \end{pmatrix}$$

whose determinant is $d = 2(x-y)(x-z)(y-z)$. Now, if d is not a square in F_q^*, then g' is not in $L_2(q)$ and thus the triple (x, y, z) is not in the $L_2(q)$ orbit of $(1, 0, -1)$ but necessarily in the $(\lambda, 0, -\lambda)$ orbit. Hence by definition, if d is not a square, $(e_x, e_y, e_z)_+ = 0$. On the other hand, if d is a square, then we may consider $g = \frac{1}{\sqrt{d}} g'$ as element of $L_2(q)$. Then using Theorem 1.1.2, we check the equation using invariance of g:

$$(e_x, e_y, e_z) \;=\; (ge_x, ge_y, ge_z)$$

$$
\begin{aligned}
&= \pi(\frac{(x-y)(-x+z)}{\sqrt{d}})\pi(1-2)\pi(\frac{(x-y)(-y+z)}{\sqrt{d}}) \cdot \\
&\quad \pi(0-2)\pi(\frac{\sqrt{d}}{x-y})\pi(-1)(e_1, e_0, e_\infty)_+ \\
&= \pi(\frac{2(x-y)(x-z)(y-z)}{\sqrt{d}})(e_1, e_0, e_\infty)_+ \\
&= \pi(\sqrt{2(x-y)(x-z)(y-z)}^{\delta})(e_1, e_0, e_\infty)_+.
\end{aligned}
$$

Finally, we use use that $(e_1, e_0, e_\infty)_+ = 1$ to finish the proof.

For (1b), make use of

$$g'' = \begin{pmatrix} 2\lambda & \lambda \\ 0 & \lambda^2 \end{pmatrix} \begin{pmatrix} z(x-y) & x-y \\ -\lambda y(x-z) & -\lambda(x-z) \end{pmatrix}$$

which has determinant $d'' = 2\lambda^3(x-y)(x-z)(y-z)$. Since this and the remaining calculations are similar, we omit them. □

We note that had we used $(1, 0, \infty)$ and $(\lambda, 0, \infty)$ as our starting points in Definition 1.5.1 instead of $(1, 0, -1)$ and $(\lambda, 0, -\lambda)$, the "2's" and "3" would have not appeared in the formulas in Theorem 1.5.1 above. However, we chose $(1, 0, -1)$ and $(\lambda, 0, -\lambda)$ since it will make the formulas a bit more symmetrical for the f-basis (below) which will be much more important to us. A more fundamental problem with the above formulas for the e-basis is the presence of the $\sqrt{x}^{\delta}$. It is very difficult to proceed when one is constantly being concerned with whether or not an object is a square in the field or not. The formulas we present next for the f-basis, while not as pretty as those for the e-basis, nevertheless avoid talking about things such as $\sqrt{x}^{\delta}$.

Theorem 1.5.2 *Let $x, y \in \mathsf{F}_q$. Then*
(1)

$$(f_x, f_{-x-y}, f_y)_+ = q/2 \sum_{a,b \in \mathsf{F}_q, a \neq 0, \pm b} \chi(\frac{x}{a(a-b)} - \frac{y}{a(a+b)})\pi(a(a-b)(a+b))^{-1}$$

(2)

$$(f_x, f_{-x-y}, f_y)_- = q/2 \sum_{a,b \in \mathsf{F}_q, a \neq 0, \pm\lambda b} \chi(\frac{\lambda x}{a(a-\lambda b)} - \frac{\lambda y}{a(a+\lambda b)})\pi(a(a-\lambda b)(a+\lambda b))^{-1}$$

(3) $(f_\infty, f_{-x}, f_x)_+ = q/2 \sum_{a \in \mathsf{F}_q^*} \chi(\frac{-x}{2a^2})\pi(2a)^{-1}$

(4) $(f_\infty, f_{-x}, f_x)_- = q/2\sum_{a\in \mathsf{F}_q^*}\chi(\frac{-x}{2\lambda a^2})\pi(2\lambda^2 a)^{-1}$
(5) $(f_\infty, f_{-x}, f_x)_\pm = (f_x, f_\infty, f_{-x})_\pm = (f_{-x}, f_x, f_\infty)_\pm$
(6) All other pairings in the f-basis are zero.

Proof. We shall make use of the matrices M_u (Equation 1.5) and the matrices

$$g_{a,b} = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}.$$

Using M_u invariance in the second line, we calculate:

$$\begin{aligned} (f_x, f_z, f_y)_+ &= \sum_{a,b,c\in\mathsf{F}_q} \chi(ax+cz+by)(e_a, e_c, e_b)_+ \\ &= \sum_{a,b,c\in\mathsf{F}_q} \chi(ax+cz+by)(e_{a-c}, e_0, e_{b-c})_+ \\ &= \sum_{a',b',c\in\mathsf{F}_q} \chi(a'x+b'y+c(x+y+z))(e_{a'}, e_0, e'_b)_+ \\ &= q\delta_{x+y+z=0}\sum_{a,b\in\mathsf{F}_q} \chi(ax+by)(e_a, e_0, e_b)_+ \qquad (1.8) \end{aligned}$$

Now it is clear that $(1,0,-1)$ and $(a,0,b)$ are in the same $L_2(q)$ orbit if and only if $(a,0,b)$ is of the form $g(1,0,-1)$ for some $g \in L_2(q)$. Since $(e_a, e_0, e_b)_+$ vanishes unless $(a,0,b)$ is in the $(1,0,-1)$ orbit, we may ignore the terms not of the form $g(e_1, 0, e_{-1})\mathbf{C}^*$ in Equation 1.8. Now note that by Theorem 1.1.2, the only $g \in L_2(q)$ that preserve the element $0 \in \mathsf{P}^1(\mathsf{F}_q)$ are of the form $g_{a,b}$ for $a, b \in \mathsf{F}_q, a \neq 0$. Explicitly, the action is given by

$$g_{a,b}(e_1, e_0, e_{-1}) \;=\; \pi(a-b)\pi(a)\pi(a+b)(e_{\frac{a-1}{a-b}}, e_0, e_{\frac{-a-1}{a+b}}).$$

For this to be of the form $(e_c, 0, e_d)\mathbf{C}^*$ for $c, d \in \mathsf{F}_q$, we only need that $a(a^2-b^2) \neq 0$. Using this formula and the FT of Projective Geometry, it is clear that $\{g_{a,b}(1,0,-1)|a, b \in \mathsf{F}_q, a(a^2-b^2) \neq 0\}$ is equal to $\{(a,0,b)|a,b \in \mathsf{F}_q,\ (a,0,b) \in L_2(q)(1,0,-1)\}$. It is also clear that the map $(a,b) \to g_{a,b}(1,0,-1)$ is 2-to-1 since $g_{a,b} = g_{-a,-b}$ in $L_2(q)$. Putting this together in Equation 1.8, dropping terms that are zero, and using invariance, we continue:

$$\begin{aligned} (f_x, f_z, f_y)_+ &= \frac{q}{2}\delta_{x+y+z=0}\sum_{a,b\in\mathsf{F}_q, a(a^2-b^2)\neq 0} \chi(\frac{xa^{-1}}{a-b} - \frac{ya^{-1}}{a+b})\cdot \\ &\quad g_{a,b}(e_1, e_0, e_{-1})_+\pi(a(a^2-b^2))^{-1}. \end{aligned}$$

Then Definition 1.5.1 finishes (1).

For (2), we have similar arguments, however, things will be non-zero if and only if they are in the $(\lambda, 0, -\lambda)$ orbit. Since these and the remaining calculations are contain nothing new, they are omitted. □

To make a simple observation that will be useful later, let us introduce the following notation.

Definition 1.5.3 *Let $x \in \mathsf{P}^1(\mathsf{F}_q)$. Define the symbol $|x|$ by*

$$|x| = \begin{cases} x & \textit{if } x \neq \infty \\ 0 & \textit{if } x = \infty. \end{cases}$$

Then we may note that Theorem 1.5.2 now tells us that

$$(f_x, f_y, f_z)_\pm = 0 \text{ if } |x| + |y| + |z| \neq 0. \tag{1.9}$$

The following theorem gives some useful elementary properties of our invariant 3-forms.

Theorem 1.5.3 *Let $x, y, c \in \mathsf{F}_q, c \neq 0$. Then*
(1) $(f_x, f_{-x-y}, f_y)_- = (f_{\lambda x}, f_{\lambda(-x-y)}, f_{\lambda y})_+$
(2) $(f_\infty, f_{-x}, f_x)_- = (f_\infty, f_{-\lambda^3 x}, f_{\lambda^3 x})_+$
(3) $(f_x, f_{-x-y}, f_y)_\pm = (f_{-y}, f_{x+y}, f_{-x})_\pm$
(4) $(f_{c^2 x}, f_{c^2(-x-y)}, f_{c^2 y})_\pm = (f_x, f_{-x-y}, f_y)_\pm \pi(c)^{-3}$
(5) $(f_\infty, f_{-c^2 x}, f_{c^2 x})_\pm = (f_\infty, f_{-x}, f_x)_\pm \pi(c)^{-1}$.

Proof. To get (1), use the substitution $b \rightarrow b'/\lambda$ in Theorem 1.5.2 part (2) above. (2) follows from the above theorem part (4) by $b \rightarrow b'/\lambda^2$. (3) follows from the above theorem part (1) and (2) by $b \rightarrow -b'$. (4) and (5) follow by A invariance and Theorem 1.2.1. □

Next we wish to see when these forms can be fit together to make alternating forms. To do this, we first consider $a, b, c \in \mathsf{P}^1(\mathsf{F}_q)$, distinct, and σ a permutation of a, b, c. Then observe that by Theorem 1.3.1, the element in $PGL(2, q)$ mapping (a, b, c) (via $(1, 0, \infty)$) to $(\sigma a, \sigma b, \sigma c)$ has a -1 entering into the determinant for each transposition. This tells us that the map $g_{\sigma,a,b,c} \in PGL(2, q)$ taking the triple (a, b, c) to $\sigma(a, b, c) = (\sigma a, \sigma b, \sigma c)$ has determinant $sgn(\sigma)$.

Let us now work in the e-basis for V. By definition and by the discussion so far, we know that if $(e_a, e_b, e_c)_\pm$ is non-zero, then $\sigma(e_a, e_b, e_c)_\pm = (e_{\sigma a}, e_{\sigma b}, e_{\sigma c})_\pm$ is non-zero if and only if (a, b, c) and $\sigma(a, b, c)$ are in the same $L_2(q)$ orbit, that is, if and only if $sgn(\sigma)$ is a square in F_q^*.

Say that $sgn(\sigma)$ *is* a square. Then we claim that actually, $\sigma(e_a, e_b, e_c)_\pm = \pi(\sqrt{sgn(\sigma)})(e_a, e_b, e_c)_\pm$. First we note that it is sufficient to check this statement for any particular (a_0, b_0, c_0) in the $L_2(q)$ orbit. To see that this is enough, let $g \in L_2(q)$ such that $g(a,b,c) = (a_0, b_0, c_0)$. The FT of Projective Geometry says that $g_{\sigma,a,b,c} = g^{-1} g_{\sigma,a_0,b_0,c_0} g$. Hence, checking the statement for (a_0, b_0, c_0) will check it for $g(a,b,c)$. It will be easiest if we choose $(a_0, b_0, c_0) = (1, 0, \infty)$ and use Theorem 1.5.3 to extend the results from $(,,)_+$ to $(,,)_-$ (or vice versa depending what orbit $(1,0,\infty)$ is in). However, this case is easily checked using Theorem 1.3.1 and Theorem 1.1.2. This allows us to prove (recalling h from Equation 1.1 and that λ is the fixed generator for F_q^*):

Theorem 1.5.4 *Using the symbol* F_q^{*2} *to denote the set of squares in* F_q^* *and recalling the notation from Section 1.1 so that* $\pi(\lambda) = e^{2\pi i m/h}$, *then the alternating invariant 3-forms on V are described explicitly as follows:*

(1) If $-1 \in \mathsf{F}_q^{*2}$ *(i.e., h is even) and m is odd, then there are precisely two linearly independent invariant alternating 3-forms. They are of the form*

$$c_+(,,)_+ + c_-(,,)_-$$

for any $c_+, c_- \in \mathsf{C}$. *If m is even, there are no invariant alternating 3-forms.*

(2) If $-1 \notin \mathsf{F}_q^{*2}$ *(i.e., h is odd), then, there is only one invariant alternating 3-form up to scalar multiplication. It is of the form*

$$c_+(,,)_+ + c_-(,,)_-$$

for any $c_+ \in \mathsf{C}$ *with* $c_- = -c_+\pi(\sqrt{-1/\lambda})^{-3}$.

Proof. Let us recall the result of our above discussion. With the same notation as above so that a permutation σ acts by $\sigma(e_a, e_b, e_c) = (e_{\sigma a}, e_{\sigma b}, e_{\sigma c})$, we derived:

$$\sigma(e_a, e_b, e_c)_\pm = \begin{cases} 0 & \text{if } sgn(\sigma) \notin \mathsf{F}_q^{*2} \\ \pi(\sqrt{sgn(\sigma)})(e_a, e_b, e_c)_\pm & \text{else.} \end{cases} \tag{1.10}$$

With our old notation, this may be more compactly written as $\sigma(e_a, e_b, e_c)_\pm = \pi(\sqrt{sgn(\sigma)}^{\,\delta})(e_a, e_b, e_c)_\pm$.

In case (1), we see that Equation 1.10 says that both the "+" form and the "–" form are already alternating if m is odd since then $\pi(\sqrt{-1}) = -1$. If m is even, they are never alternating since $\pi(\sqrt{-1}) = 1$. By our discussion at the beginning of this section, we are done.

Let us consider case (2). By Equation 1.10, we see that if $sgn(\sigma) = 1$, we already have $\sigma(e_a, e_b, e_c)_\pm = sgn(\sigma)(e_a, e_b, e_c)_\pm$. Thus to see how to combine things in order to get alternating forms, it is sufficient to consider the case where $sgn(\sigma) = -1$. Therefore it is enough to consider σ to be a transposition. Moreover, since we will see that all the calculations are similar, let us just do the calculations for the fixed permutation σ where $\sigma(a,b,c) = (b,a,c)$. Also let $x \in \mathsf{F}_q^*$ so that $x^2\lambda = -1$, that is, $x^2 = -1/\lambda$ (since $-1 \notin \mathsf{F}_q^{*2}$).

For $a,b,c \in \mathsf{F}_q$ and $c_+, c_- \in \mathsf{C}$, consider the form $(,,) = c_+(,,) + c_-(,,)_-$. It will be convenient to work now in the f-basis to find out what restrictions on c_+ and c_- are needed to make the form alternating Making much use of Theorem 1.5.3 part (1), (3), and (4) and Equation 1.10, we calculate:

$$\begin{aligned}
\sigma(f_a, f_b, f_c) &= (f_{\sigma a}, f_{\sigma b}, f_{\sigma c}) \\
&= (f_b, f_a, f_c) \\
&= c_+(f_b, f_a, f_c)_+ + c_-(f_b, f_a, f_c)_- \\
&= c_+(f_{-c}, f_{-a}, f_{-b})_+ + c_-(f_{-c}, f_{-a}, f_{-b})_- \\
&= c_+(f_{x^2\lambda c}, f_{x^2\lambda a}, f_{x^2\lambda b})_+ + c_-(f_{x^2\lambda c}, f_{x^2\lambda a}, f_{x^2\lambda b})_- \\
&= c_+(f_{x^2c}, f_{x^2a}, f_{x^2b})_- + c_-(f_{x^2\lambda^2c}, f_{x^2\lambda^2a}, f_{x^2\lambda^2b})_+ \\
&= c_+(f_c, f_a, f_b)_-\pi(x)^{-3} + c_-(f_c, f_a, f_b)_+\pi(\lambda x)^{-3} \\
&= c_+(f_a, f_b, f_c)_-\pi(x)^{-3} + c_-(f_a, f_b, f_c)_+\pi(\lambda x)^{-3}.
\end{aligned}$$

Now for $(,,)$ to be alternating, we need $\sigma(f_a, f_b, f_c) = -(f_a, f_b, f_c)$. By the above calculations, this is true if and only if $c_+/\pi(x)^3 = -c_-$ and $c_-/\pi(\lambda x)^3 = -c_+$. In fact, these two conditions are equivalent. To see this, observe that the second equation gives $c_- = -c_+\pi(\lambda x)^3$. But since $x^2 = -1/\lambda$, we have $(\lambda x)^3 = \lambda^3 x^6/x^3 = x^{-3}\lambda^3(x^2)^3 = x^{-3}$. Thus the two requirements are the same. One may similarly check that if one of the a, b, c are ∞, the same result appears. Thus we have the stated result. □

We record for future use an immediate consequences of this theorem in three cases:

Corollary 1.5.1 *Up to scalar multiplication, there is precisely one 3-form on V for $q = 7$ and two 3-forms on V for $q = 9$ or 13 that are $L_2(q)$ invariant and alternating.*

□

1.6 The Algebra Structure

Now that we have non-zero $L_2(q)$ invariant alternating 3-forms and a non-degenerate symmetric 2-form, we are in a position to define an invariant skew-symmetric algebra structure, $[,]$, on V. To do this, first fix $(,)$, the unique 2-form from Theorem 1.4.1, and $(,,)$, any non-zero invariant alternating 3-form. We then may make the following definition.

Definition 1.6.1 *Given the fixed 2-form and 3-form above, let $[,] : V \times V \to V$ be the non-zero $L_2(q)$ invariant skew-symmetric algebra structure on V defined by*

$$(v_1, v_2, v_3) = ([v_1, v_2], v_3)$$

for all $v_1, v_2, v_3 \in V$. Note that $[,]$ depends on our choice of the 3-form $(,,)$.

It is very useful to compute explicitly what this algebra structure looks like. It is particularly nice in the f-basis as the next theorem demonstrates.

Theorem 1.6.1 *Let $(,,)$ be a non-zero $L_2(q)$ invariant alternating 3-form and write $[,]$ for the corresponding algebra structure on V. Then for $p, q \in \mathsf{F}_q^*$,*
(1) $[f_p, f_q] = (f_q, f_{-q-p}, f_p)\, \pi(p+q)\, f_{p+q}$ if $p + q \neq 0$
(2) $[f_0, f_q] = (f_q, f_{-q}, f_0)\, \pi(q)\, f_q$
(3) $[f_\infty, f_q] = (f_q, f_{-q}, f_\infty)\, \pi(q)\, f_q$
(4) $[f_0, f_\infty] = 0$
(5) $[f_p, f_{-p}] = (f_{-p}, f_\infty, f_p)/\Gamma_{1,0}\, f_0 + (f_{-p}, f_0, f_p)/\Gamma_{1,0}\, f_\infty$.

Proof. This follows easily by Definition 1.6.1, Theorem 1.4.1, and Equation 1.9. For instance, let us check (1). First of all we may write $[f_p, f_q] = \sum_{r \in \mathsf{P}^1(\mathsf{F}_q)} c_r f_r$ for some constants $c_r \in \mathsf{C}$. Then applying $(\cdot, f_s)$, $s \in \mathsf{F}_q$, to both sides gives

$$(f_p, f_q, f_s) = c_{-s} \frac{1}{\pi(s)}.$$

Thus $c_{-s} = \pi(s)(f_q, f_s, f_p)$ (by Equation 1.10). In particular, we have $c_{-s} = 0$ unless $s = -p - q$ which gives the stated result. The other cases are similar. □

Now of course this algebra structure on V will be a Lie algebra if and only if it satisfies the Jacobi identity

$$[[v_1, v_2], v_3] + [[v_3, v_1], v_2] + [[v_2, v_3], v_1] = 0 \qquad (1.11)$$

for all $v_1, v_2, v_3 \in V$. As a corollary of the above work, we get an expression for the Jacobi identity in terms of the 3-form. Part (3) below will be very useful later in the paper.

Corollary 1.6.1 *Let $p, q, r \in \mathsf{F}_q^*$ and $s = -(p + q + r)$. Then the 3-form $(,,)$ makes V into a Lie algebra if and only if the following three conditions hold:*

(1) When none of the subscripts are zero, one must have:

$$\frac{(f_p, f_{-p-q}, f_q)(f_r, f_{p+q}, f_s)}{(f_{p+q}, f_{-p-q})} + \frac{(f_r, f_{-r-p}, f_p)(f_q, f_{r+p}, f_s)}{(f_{r+p}, f_{-r-p})} + \frac{(f_q, f_{-q-r}, f_r)(f_p, f_{q+r}, f_s)}{(f_{q+r}, f_{-q-r})} = 0.$$

(2) When none of the subscripts are zero, one must have:

$$\frac{(f_p, f_{-p}, f_0)(f_q, f_{-q}, f_\infty) + (f_p, f_{-p}, f_\infty)(f_q, f_{-q}, f_0)}{(f_0, f_\infty)} + \frac{(f_q, f_{-p-q}, f_p)^2}{(f_{p+q}, f_{-p-q})} - \frac{(f_q, f_{p-q}, f_{-p})^2}{(f_{p-q}, f_{-p+q})} = 0.$$

(3) Let $\Box \in \{0, \infty\}$. When none on the subscripts are zero, one must have:

$$(f_p, f_{-p-q}, f_q)(-\frac{(f_{p+q}, f_{-p-q}, f_\Box)}{(f_{p+q}, f_{-p-q})} + \frac{(f_q, f_{-q}, f_\Box)}{(f_q, f_{-q})} + \frac{(f_p, f_{-p}, f_\Box)}{(f_p, f_{-p})}) = 0.$$

Proof. The proof of this is just a straightforward application of the various cases of Theorem 1.6.1 applied to Equation 1.11. We omit the details as they are trivial and not very enlightening. □

1.7 The Four-form

We have seen that any $L_2(q)$ invariant alternating 3-form gives rise to an algebra structure. Since we will be concerned with the veracity of the Jacobi identity, let us make the following definition.

Definition 1.7.1 *Let $x, y, z, w \in V$. Given a non-zero $L_2(q)$ invariant alternating 3-form and the corresponding algebra structure $[,]$, define a 4-form $(,,,)$ on V by*

$$(x, y, z, w) = ([[x, y], z] + [[y, z], x] + [[z, x], y], w)$$

where $(,)$ is the fixed 2-form. Note that $(,,,)$ depends on $[,]$ which in turn depends on the 3-form.

Theorem 1.7.1 *The above 4-form is a $L_2(q)$ invariant alternating form on V. Moreover, it is identically zero if and only if V is a Lie algebra under $[,]$.*

Proof. That the 4-form is invariant is obvious from the invariance of $(,)$ and $[,]$. The fact that it is alternating follows from:

$$\begin{aligned} (x, y, z, w) &= ([[x, y], z] + [[y, z], x] + [[z, x], y], w) \\ &= ([x, y], z, w) + ([y, z], x, w) + ([z, x], y, w) \end{aligned}$$

$$\begin{aligned} &= (z,w,[x,y]) + (x,w,[y,z]) + (y,w,[z,x]) \\ &= ([z,w],[x,y]) + ([x,w],[y,z]) + ([y,w],[z,x]). \end{aligned}$$

The statement about being a Lie algebra is clear since $(,)$ is non-degenerate and it is precisely the Jacobi identity that appears in the definition of the 4-form. □

We now record a simple calculation for future use.

Theorem 1.7.2 *Up to scalar multiplication, there are precisely no 4-forms on V for $q = 7$ and one 4-form on V for $q = 9$ or 13 that are $L_2(q)$ invariant and alternating.*

Proof. It is possible to give explicit expression for these 4-forms just as we did for the 3-forms earlier. However, since we will only need results for $q = 7, 9$, and 13 and then only of a quantitative nature, we simply calculate the number of times the trivial representation of $L_2(q)$ occurs in $\bigwedge^4 V$. Here we recall that if μ is a character of a finite group, then the character of the fourth exterior power of μ evaluated on some $g \in L_2(q)$ is given by

$$\bigwedge^4 \mu(g) = \frac{\mu(g)^4 - 6\mu(g)^2\mu(g^2) + 8\mu(g^3)\mu(g) + 3\mu(g^2)^2 - 6\mu(g^4)}{24}.$$

Using a character table for $L_2(q)$ (see Theorem 3.2.1), the calculations needed to apply the Schur orthogonality relations to the theorem are easy and omitted. □

1.8 The Clifford Algebra

It turns out that the 4-form has a nice connection to Clifford algebras which we develop in this section. First recall some notation from Exterior algebras. Let W is a finite dimensional vector space over C equipped with a non-degenerate symmetric two-form $(,)$. Then one may extend $(,)$ to all of $\bigwedge W$ by requiring $(\bigwedge^k W, \bigwedge^l W) = 0$ if $k \neq l$ and letting

$$(w_1 \wedge \ldots w_k, w_1' \wedge \ldots w_k') = det[(w_i, w_j')]$$

for all $w_i, w_j' \in W$.

There are also two standard maps of $\bigwedge W$ that will be useful. Fix $w \in W$. The first map is $\epsilon(w) : \bigwedge^i W \to \bigwedge^{i+1} W$ defined by

$$\epsilon(w)u = w \wedge u$$

for all $u \in \bigwedge W$. Clearly $\epsilon(w)^2 = 0$. The second map is $\iota(w) : \bigwedge^i W \to \bigwedge^{i-1}$ by setting $\iota(w) = \epsilon(w)^t$, the transpose. Thus it is clear that $\iota(w)^2 = 0$ also. Moreover, it is well known that there is an explicit formula for $\iota(w)$ given by

$$\iota(w)(w_1 \wedge \ldots w_k) = \sum_{i=1}^{k}(-1)^{i+1}(w, w_i)w_1 \wedge \ldots \widehat{w_i} \wedge \ldots w_k$$

where the $\widehat{w_i}$ means to omit the w_i term.

Now to prepare our coming connection with Clifford algebras, we define the operator $L_w : \bigwedge W \to \bigwedge W$ by

$$L_w = \epsilon(w) + \iota(w).$$

It is classical that

$$L_w^2 = (w, w)1. \tag{1.12}$$

(This follows from the easily checked equation $\iota(w)\epsilon(w) + \epsilon(w)\iota(w) = (w, w)1$).

Let $\bigotimes W$ be the tensor algebra of W. Then we recall that the Clifford algebra, $C(W)$, is just

$$C(W) = \bigotimes W/(< w \otimes w - (w, w) >).$$

Now there is an interesting bijective map of $C(W)$ onto $\bigwedge W$. To see this, first observe that we have a map $\Phi : W \to End(\bigwedge W)$ by $w \to L_w$. This naturally extends to a map of the same name $\Phi : \bigotimes W \to End(\bigwedge W)$ in the obvious way. Next, Equation 1.12 tells us that the map Φ descends to the quotient $\Phi : C(W) \to End(\bigwedge W)$. At last, let us define $\Psi : C(W) \to \bigwedge W$ by

$$\Psi(x) = \Phi(x)(1).$$

Explicitly, let $w_i \in W$ and consider elements of the form $w_1, \ldots w_k \in W \subset C(W)$. One easily checks that,

$$\Psi(w_1) = (\epsilon(w_1) + \iota(w_1))1 = w_1$$

and

$$\Psi(w_1 w_2) = (\epsilon(w_1) + \iota(w_1))w_2 = w_1 \wedge w_2 + (w_1, w_2)1 \tag{1.13}$$

and in general,

$$\Psi(w_1 \ldots w_k) = w_1 \wedge \ldots w_k + \sum_{i>0} \text{ terms in } \textstyle\bigwedge^{k-2i} W \ . \tag{1.14}$$

With this, we may now state the well known bijection of $C(W)$ and $\bigwedge W$. This material may be found in many places, e.g., [2] Chapter 1 §6.

Theorem 1.8.1 *With the above definitions,*

$$\Psi : C(W) \to \bigwedge W$$

is a $\mathbb{C}$*-linear one-to-one onto map. Thus, Clifford multiplication induces a second algebra structure on* $\bigwedge W$*. This new multiplication will be denoted by placing two elements of* $\bigwedge W$ *next to each other (i.e. with no* $\wedge$ *in between).*

We observe that by Equation 1.13 that for $w_i \in \bigwedge^1 W$, the new "Clifford" multiplication in $\bigwedge W$ is:

$$w_1 w_2 = w_1 \wedge w_2 + (w_1, w_2)1.$$

We also observe by the same sources that if $w_1, \dots w_k$ are mutually orthogonal with respect to the two-form $(,)$, then

$$w_1 \dots w_k = w_1 \wedge \dots w_k.$$

It will be useful to have a more general formula for this new multiplication. For our purposes, this will be provided by

Theorem 1.8.2 *Let* x_i *be a basis for* $\bigwedge W$ *and let* y_i *be its dual basis, that is,* $(x_i, y_j) = \delta_{i,j}$*. Then for any* $u, v \in \bigwedge W$*, the Clifford multiplication is given by:*

$$uv = \sum_{i=1}^{2^{dim(W)}} \iota(x_i)u \wedge \iota(y_i)v.$$

Proof. This is a simple matter of checking the result in one particularly nice basis and then using the universality of the tensor product space trick to show independence of basis. The proof, due to Kostant, may be found in [27]. □

Corollary 1.8.1 *With the above notation,*

$$u^2 = \sum_i \iota(x_i)u \wedge \iota(y_i)u.$$

Now let us return to our original concern where V is our induced $L_2(q)$ module, $(,)$ is our invariant symmetric non-degenerate 2-form, $(,,)$ is a fixed non-zero invariant alternating 3-form, and $(,,,)$ is the corresponding invariant alternating 4-form measuring the failure of the Jacobi identity. Now we may view $(,,)$ and $(,,,)$ to be elements of $\bigwedge^3 V$ and $\bigwedge^4 V$, respectively, by our 2-form. The remarkable observation of Kostant is that the relation of the 4-form to the 3-form is encapsulated by Clifford multiplication in $\bigwedge V$.

Theorem 1.8.3 *(Kostant) Viewing $(,,)$ and $(,,,)$ as elements in $\bigwedge^3 V$ and $\bigwedge^4 V$, respectively, and using Clifford multiplication,*

$$(,,)^2 = 2(,,,) + \text{ a degree zero term.}$$

Proof. A priori, the Clifford product of two elements in $\bigwedge^3 V$ would have components in degrees 6, 4, 2, and 0 by Equation 1.14. Let us first check that Clifford squaring of an element $x \in \bigwedge^3 V$ results in only degree 4 and 0 terms. To do this, let us recall the algebra anti-automorphism of $\bigotimes V$ defined by $(v_1 \otimes \ldots v_k)^* = v_k \otimes \ldots v_1$. This anti-automorphism descends compatibly with Ψ to both $C(V)$ and $\bigwedge V$. We observe that "*" reduces to $+1$ in degrees 0 and 4 of $\bigwedge V$ while it reduces to -1 in degrees 2,3, and 6. However, this implies that on the Clifford square of a degree 3 object, "*" acts by $(-1)(-1) = +1$. Hence, "*" must act by $+1$ on each of the components. Thus there are no 2 or 6 degree terms.

We can now make use of Theorem 1.8.2. First recall that our 2-form $(,)$ on V extends to all of $\bigwedge V$ as described above. By viewing $(,,)$ and $(,,,)$ to be in $\bigwedge V$, we mean that we identify them with elements φ_3 and φ_4 in $\bigwedge^3 V$ and $\bigwedge^4 V$, respectively, such that for $v_i \in V$, $(v_1, v_2, v_3) = (\varphi_3, v_1 \wedge v_2 \wedge v_3)$ and $(v_1, v_2, v_3, v_4) = (\varphi_4, v_1 \wedge v_2 \wedge v_3 \wedge v_4)$. To show that the degree 4 component of φ_3^2 is φ_4, it suffices to show that $(\varphi_3^2, v_1 \wedge v_2 \wedge v_3 \wedge v_4) = (v_1, v_2, v_3, v_4)$. Now choose x_i to be a basis of homogeneous elements in $\bigwedge V$ and y_i to be the corresponding (homogeneous) dual basis so that $deg(x_i) = deg(y_i)$. We know by Corollary 1.8.1 that

$$\varphi_3^2 = \sum_i \iota(x_i)\varphi_3 \wedge \iota(y_i)\varphi_3.$$

By the fact that φ_3 is degree three and by the degree lowering nature of ι, x_i and y_i can contribute non-trivially to the fourth degree component of φ_3^2 only for x_i of degrees 0,1,or 2 and y_i of degrees 2, 1, or 0, respectively. But since x_i and y_i have the same degree, we only need to consider the above sum for $x_i, y_i \in \bigwedge^2 V$. Hence, we have

$$(\varphi_3^2, v_1 \wedge \ldots v_4) = \sum_{i, deg(x_i)=2} (\iota(x_i)\varphi_3 \wedge \iota(y_i)\varphi_3, v_1 \wedge \ldots v_4). \tag{1.15}$$

Of course $\iota(x_i)\varphi_3$ and $\iota(y_i)\varphi_3$ are in $\bigwedge^2 V$. We wish to "rewrite" the above determinant. Let $a_i \in V$. Then by definition one has $(a_1 \wedge \ldots a_4, v_1 \wedge \ldots v_4) = \sum_{\sigma \in S^4} sgn(\sigma)(a_1, v_{\sigma(1)}) \ldots (a_4, v_{\sigma(4)})$ and $(a_1 \wedge a_2, v_1 \wedge v_2) = \sum_{\sigma \in S^2} sgn(\sigma)(a_1, v_{\sigma(1)})(a_2, v_{\sigma(2)})$. Combining these, one can check that the following sum over $\begin{pmatrix} 4 \\ 2 \end{pmatrix} = 6$ permutations holds:

$$(a_1 \wedge \ldots a_4, v_1 \wedge \ldots v_4) = \sum_{\{i,j,k,l\}=\{1,2,3,4\}, i<j, k>l} (a_1 \wedge a_2, v_i \wedge v_j)(a_3 \wedge a_4, v_k \wedge v_l).$$

Applying this to Equation 1.15, we may now write

$$(\varphi_3^2, v_1 \wedge \ldots v_4) = \sum_{\{p,q,r,s\}=\{1,2,3,4\}, p<q, r>s} \sum_{i, deg(x_i)=2} (\iota(x_i)\varphi_3, v_p \wedge v_q)(\iota(y_i)\varphi_3, v_r \wedge v_s). \tag{1.16}$$

Now using $i(v)^t$ and $(\varphi_3, v_1 \wedge v_2 \wedge v_3) = (v_1, v_2, v_3) = ([v_1, v_2], v_3)$, we have

$$\begin{aligned} (\iota(v)\varphi_3, v_1 \wedge v_2) &= (\varphi_3, v \wedge v_1 \wedge v_2) \\ &= ([v, v_1], v_2). \end{aligned}$$

Putting this in Equation 1.16, we get (also using the nature of the dual basis)

$$\begin{aligned} (\varphi_3^2, v_1 \wedge \ldots v_4) &= \sum_{p,q,r,s} \sum_i ([x_i, v_p], v_q)([y_i, v_r], v_s) \\ &= \sum_{p,q,r,s} \sum_i ([v_p, v_q], x_i)([v_r, v_s], y_i) \\ &= \sum_{p,q,r,s} \sum_i ([v_p, v_q], ([v_r, v_s], y_i)x_i) \\ &= \sum_{p,q,r,s} ([v_p, v_q], [v_r, v_s]) \\ &= \sum_{p,q,r,s} ([[v_r, v_s], v_p], v_q). \end{aligned}$$

Writing out explicitly the 6 terms of $\{\{p, q, r, s\} = \{1, 2, 3, 4\}, p < q, r > s\}$ and rearranging terms, one checks that we get precisely the desired result. □

Corollary 1.8.2 *There exists a second degree homogeneous polynomial map from $L_2(q)$ invariant alternating 3-forms on V to invariant alternating 4-forms that takes any such 3-form to its corresponding 4-form.*

Proof. This is an immediate consequence of the above theorem and the nature of Clifford multiplication. □

1.9 Existence for Rank 2

Using the results from our Clifford structure, we can now show that for $q = 7, 9$, and 13, one may choose an appropriate 3-form on V so that the induced algebra structure yields a Lie algebra. Of course in these cases it is clear that $dim(V) = 8$, 10, and 13, respectively. We will later see that the Lie algebras obtained in this way are the simple rank two Lie algebras A_2, B_2, and G_2, respectively. Thus in these cases, knowledge of $L_2(q)$ determines the entire Lie algebra which in turn determines the Adjoint Lie groups in which $L_2(q)$ lies.

Theorem 1.9.1 *For $q = 7$, 9, and 13, there exits non-zero $L_2(q)$ invariant alternating 3-forms on V making V into a Lie algebra under the corresponding bracket structure.*

Proof. Since vanishing of the corresponding 4-form is equivalent to the Jacobi identity, it suffices to show that there always exist non-zero 3-forms whose 4-forms vanish. By Corollary 1.5.1 and Theorem 1.7.2, we already know that for $q = 7$, 9, and 13 there are always one more $L_2(q)$ invariant alternating 3-forms on V than there are invariant alternating 4-forms. In particular, for $q = 7$ we are done since there are no 4-forms. However, for $q = 9, 13$ there is a 4-form. But by Corollary 1.8.2, we have a homogeneous polynomial map taking 3-forms to 4-forms. Thus by choosing a basis for $q = 9, 13$, we have a map $\mathbf{C}^2 \to \mathbf{C}$ of the form $ax^2 + bxy + cy^2$. But by the quadratic formula this always has a non-trivial zero so we are done. □

Using a character table (Theorem 3.2.1), let us work backwards and make some general remarks about the groups in the cases of $q = 7, 9, 13, 5$:

$L_2(7)$ has exactly two 3 dimensional irreducible representations. This gives two non-isomorphic injections of $L_2(7)$ into $SL(3, \mathbf{C})$. One may arrange things so that the the outer automorphism of $L_2(7)$ corresponds to an outer automorphism of $SL(3, \mathbf{C})$ which interchanges the two non-isomorphic representations of $L_2(7)$. Of course, this outer automorphism is a Lie algebra automorphism of $SL(3, \mathbf{C})$ even though it is not an intertwining operator for $L_2(7)$. Next note that $L_2(7)$ has only one irreducible 8 dimensional representation. In fact, one may readily see that it is obtained by composing either of the two 3 dimensional representations with Ad and letting $L_2(7)$ act on $\mathfrak{sl}(3, \mathbf{C})$. The intertwining operator for these two equivalent representations may be obtained by conjugating by the outer automorphism of $SL(3, \mathbf{C})$. This is now simultaneously a Lie algebra automorphism and intertwining operator for $L_2(7)$. This must be the case since since there is only one invariant alternating three-form up to scalar multiplication (Corollary 1.5.1) so that there is only one invariant Lie algebra structure up to automorphisms. This will be reflected in Figures 1-1 and 1-2 in later sections which will show that the possible Lie algebras differ by an outer automorphism.

$L_2(9)$ has exactly two 5 dimensional irreducible representations. The Schur indicator of each is $+1$ so that we have $L_2(9)$ embedding into $SO(5, \mathbf{C})$. We note however, that $L_2(9)$ does not have any four dimensional representations so that it does not sit in the simply-connected covering of $SO(5, \mathbf{C})$, $Spin_5(\mathbf{C}) \cong Sp_4(\mathbf{C})$ (even though $SL(2, 9)$ does have four dimensional representations, these do not descend to $PSL(2, 9) = L_2(9)$). Regardless, we still have two embeddings of $L_2(9)$ into $SO(5, \mathbf{C})$. Unlike the above case for $q = 7$, these two embeddings cannot be related by an outer automorphism. Next note that $L_2(9)$ has only one irreducible 10 dimensional representation. It is easily checked that either of the 5 dimensional representations composed with Ad yields the 10 dimensional one. Thus there will be a $L_2(9)$ intertwining operator. However, there is no reason to suppose that this map will be a Lie algebra automorphism as was the case for $q = 7$. This makes perfect sense since we have seen in Corollary 1.5.1 that up to scalar multiplication, there are two invariant three forms. By the quadratic nature of Corollary 1.8.2, one would expect there to be two different ways of making V into a Lie algebra under $L_2(9)$. We will actually see that this is the case later on. It will be reflected in Figures 1-3 and 1-4.

$L_2(13)$ also has exactly two 7 dimensional irreducible representations. The Schur indicator of each is also $+1$ so that we have an embedding into $SO(7, \mathbf{C})$. In fact, we will later see that $L_2(13)$ actually lies inside of G_2 inside of $SO(7, \mathbf{C})$. These two inequivalent 7 dimensional representations also cannot be related by an outer automorphism of G_2 as they were for $q = 7$. Composition of either with Ad will yield a 14 dimensional representation. One may check that both 7 dimensional representations give the same 14 dimensional representation (in fact, in the notation of Theorem 3.2.1, χ_9 by either Theorem 1.5.4 part (1) or Theorem 3.3.3). Just as with $q = 9$ above, one expects that there are two ways of making V into a Lie algebra under G_2. Even though there is a $L_2(13)$ intertwining operator, it need not be a Lie algebra automorphism. This will be reflected in Figures 1-5 and 1-6 in later sections.

Let us also make a few comments about $q = 5$. For this value of q, Theorem 1.1.1 tells us that the only principal series representation of $L_2(5)$ is reducible. This 6 dimensional representation breaks up into two (non-isomorphic) 3 dimensional representations. In fact, it is easy to see that each of these 3 dimensional spaces becomes (by analogous techniques) the Lie algebra $\mathfrak{sl}(2, \mathbf{C})$. Thus one can check that we have $L_2(5)$ injecting to the Adjoint group $PSL(2, \mathbf{C})$. However, $L_2(5)$ has no two dimensional representations so it does not sit in $SL(2, \mathbf{C})$.

1.10 A Family of Subalgebras

A fundamental step in understanding the nature of semi-simple Lie algebras arises by examining the various $\mathfrak{sl}(2, \mathbf{C})$'s that naturally embed in the semi-simple Lie algebra. This will be important for our study. As usual, fix an alternating, $L_2(q)$ invariant, non-zero 3-form on V so that we have $[,]$ as the corresponding algebra structure. We have already seen in Theorem 1.6.1 that the subalgebra spanned by the vectors f_0 and f_∞ "wants" to be a rank two torus of V with root vectors f_p, $p \in \mathrm{F}_q^*$. Because of this, it is natural to consider the following analogues of $\mathfrak{sl}(2, \mathrm{C})$.

Definition 1.10.1 *Given an alternating, $L_2(q)$ invariant, non-zero 3-form on V, let $\mathfrak{g}_p$ be the subspace of V defined by*

$$\mathfrak{g}_p = span\{f_p, f_{-p}, [f_p, f_{-p}]\}$$

for each $p \in \mathrm{F}_q^*$. Note that $\mathfrak{g}_p = \mathfrak{g}_q$ if and only if $-p = q$.

Define the number

$$d_p = \frac{(f_p, f_{-p}, f_0)(f_p, f_{-p}, f_\infty)}{(f_p, f_{-p})(f_0, f_\infty)}. \tag{1.17}$$

Observe that d_p is non-zero if and only if both terms in the numerator are non-zero.

Within $\mathfrak{g}_p$, single out the following elements:

$$\begin{aligned} x_p &= f_p \\ y_p &= f_{-p} \\ h_p &= [f_p, f_{-p}] \\ &= \frac{(f_p, f_{-p}, f_\infty)}{(f_0, f_\infty)} f_0 + \frac{(f_p, f_{-p}, f_0)}{(f_0, f_\infty)} f_\infty. \end{aligned}$$

Theorem 1.10.1 *Given the above notation, one has*

$$\begin{aligned} [x_p, y_p] &= h_p \\ [h_p, x_p] &= 2d_p x_p \\ [h_p, y_p] &= -2d_p y_p. \end{aligned}$$

In particular, $\mathfrak{g}_p$ is a Lie algebra.

Moreover, if $d_p \neq 0$, then $h_p \neq 0$. Thus by replacing y_p and h_p by y_p/d_p and h_p/d_p, respectively, we see that $\mathfrak{g}_p$ is isomorphic to the three dimensional $\mathfrak{sl}(2, \mathrm{C})$.

Consider what happens when $d_p = 0$ (see Equation 1.17). In the case where only one term in the numerator of d_p is zero, then $h_p \neq 0$ and $\mathfrak{g}_p$ is still a three dimensional algebra, however, h_p is in the center of $\mathfrak{g}_p$. Thus $\mathfrak{g}_p$ is isomorphic to the three dimensional Heisenberg Lie algebra. In the case where both terms in the numerator of d_p are zero, we see that $h_p = 0$ and so $\mathfrak{g}_p$ is the two-dimensional Abelian Lie algebra.

Note that even without V necessarily being a Lie algebra with respect to $[,]$, $\mathfrak{g}_p$ is always a Lie algebra.

Proof. This follows simply from the definitions and Theorem 1.6.1. □

The next goal is to show that if V is both irreducible and a Lie algebra under $[,]$, then each $\mathfrak{g}_p$ is forced to be a $\mathfrak{sl}(2, \mathbf{C})$. We will need the following results.

Lemma 1.10.1 *Suppose that $\pi^2 \neq 1$ and let $(,,)$ be as above. If $(v, v', v'') = 0$ for all $v', v'' \in V$, then $v = 0$.*

Proof. Since $(,,)$ is $L_2(q)$ invariant and since V is an irreducible representation of $L_2(q)$ (Theorem 1.1.1), $v \neq 0$ implies that $(V, v', v'') = 0$ which implies that $(,,) = 0$. However, this contradicts the choice of the non-zero 3-form. □

For the next theorem, recall Definition 1.5.3 for the symbol $|x|$.

Theorem 1.10.2 *For $\pi^2 \neq 1$ and the above notation, the center of V is trivial. In particular, for $r \in \mathbf{P}^1(\mathbf{F}_q)$, (f_r, f_s, f_q) cannot be zero for all $q, s \in \mathbf{P}^1(\mathbf{F}_q)$ where $|r| + |s| + |q| = 0$.*

Proof. The first part comes from Lemma 1.10.1, the definition of $(,,) = ([,],)$, and the non-degeneracy of $(,)$. The second part follows by Theorem 1.6.1. □

Recall Theorem 1.10.1 and suppose that for some p one has $(f_p, f_{-p}, f_0) = 0$ or $(f_p, f_{-p}, f_\infty) = 0$. In other words, suppose that $\mathfrak{g}_p$ is not isomorphic to $\mathfrak{sl}(2, \mathbf{C})$. Our goal is to show that this would imply that f_0 or f_∞, respectively, would be in the center of V and then to use Theorem 1.10.2 to get a contradiction.

In the where $(f_p, f_{-p}, f_0) = 0$ or $(f_p, f_{-p}, f_\infty) = 0$, we claim that it will follow that $f_{\pm a^2 p}$, $a \in \mathbf{F}_q^*$, commute with f_0 or f_∞, respectively. This follows by the invariance of the three form under the powers of the element A, Theorem 1.6.1, and Theorem 1.5.3 part (3).

In the case where -1 is not a square in $\mathbf{F}_q$ (i.e., when $\frac{q-1}{2} = h$ is odd or equivalently when there is only one invariant, alternating three-form), then we are already done (without reference to Jacobi!) since the set $\{\pm a^2\}$ exhausts all of $\mathbf{F}_q^*$. However, we will need to do more work (and definitely require Jacobi) for the case where -1 is a square in $\mathbf{F}_q$. Nevertheless, we record what we have found.

Theorem 1.10.3 *For $\pi^2 \neq 1$ and the above notation, if h is odd (i.e., -1 is not a square in $\mathbf{F}_q$), then each $\mathfrak{g}_p$ is isomorphic to $\mathfrak{sl}(2, \mathbf{C})$.*

For the general case, let us first proceed towards showing that $\mathfrak{g}_p$ cannot be the Abelian two-dimensional algebra if V satisfies Jacobi (noting that by the above theorem, we may assume that -1 is a square in the field). Suppose the Abelian case were possible (Theorem 1.10.1). Then fix some $p_0 \in \mathbf{F}_q^*$ so that $(f_{p_0}, f_{-p_0}, f_0) = (f_{p_0}, f_{-p_0}, f_\infty) = 0$. We define the subspaces:

Definition 1.10.2 *For p_0 fixed in F_q^*, let F_1, F_λ, and $\mathfrak{h}$ be the following subspaces of V*

$$
\begin{aligned}
F_1 &= span\{f_{a^2p_0} | a \in \mathsf{F}_q^*\} \\
F_\lambda &= span\{f_{\lambda a^2 p_0} | a \in \mathsf{F}_q^*\} \\
\mathfrak{h} &= span\{f_0, f_\infty\}.
\end{aligned}
$$

Observe that $V = F_1 \bigoplus \mathfrak{h} \bigoplus \mathsf{F}_\lambda$ and that each of the subspaces is invariant under A and M_x (see Equation 1.3 and Equation 1.5).

Definition 1.10.3 *For $r \in \mathsf{F}_q^*$, define the "root" $\alpha_r \in \mathfrak{h}^*$ to be the linear function defined by the two relations*

$$
\alpha_r(f_\Box) = \frac{(f_r, f_{-r}, f_\Box)}{(f_r, f_{-r})}
$$

where $\Box \in \{0, \infty\}$. Note, that by Theorem 1.6.1 if $h \in \mathfrak{h}$, then

$$
[h, f_r] = \alpha_r(h) f_r.
$$

Lemma 1.10.2 *For $\pi^2 \neq 1$, if V is a Lie algebra and $\mathfrak{g}_{p_0}$ is Abelian, then F_1 and $\mathfrak{h} \bigoplus F_\lambda$ are both ideals in V with $[\mathfrak{h} \bigoplus F_\lambda, F_1] = 0$ and $[\mathfrak{h}, F_\lambda] = F_\lambda$.*

Proof. Throughout we may take $-1 \in \mathsf{F}_q$ to be a square so that if $f_q \in F_x$ then $f_{-q} \in F_x$ where $x \in \{1, \lambda\}$. We will make much use of the Jacobi relation given in Corollary 1.6.1 part (3). Combined with Theorem 1.6.1 and Definition 1.10.3, it says that for $r, s \in \mathsf{F}_q^*$ with $r + s \neq 0$, either

$$
\begin{aligned}
[f_r, f_s] &= 0 \quad \text{or} && (1.18) \\
\alpha_r + \alpha_s - \alpha_{r+s} &= 0. && (1.19)
\end{aligned}
$$

For later convenience, let us note that by using A invariance, one easily checks

$$
\begin{aligned}
\alpha_{a^2 r}(f_0) &= \pi(a)^{-1} \alpha_r(f_0) && (1.20) \\
\alpha_{a^2 r}(f_\infty) &= \pi(a) \alpha_r(f_\infty).
\end{aligned}
$$

By checking the definitions, the fact that we are in the Abelian case just comes down to meaning that $\alpha_{a^2 p_0} = 0$. In particular, $\alpha_{a^2 p_0}(f_\Box) = 0$ where $\Box \in \{0, \infty\}$. But since there is no center (Theorem 1.10.2), neither f_0 nor f_∞ can commute with everything. This in turn gives us that $\alpha_{\lambda a^2 p_0}(f_\Box) \neq 0$ by A invariance and Definition 1.10.3.

Using Theorem 1.6.1 and these facts, let us check the theorem. We already know that $ad(\mathfrak{h})$ will commute with itself, kill F_1, and preserve F_λ (in fact f_0 and f_∞ will not kill anything in F_λ since they preserves the f-basis and must be non-trivial on each $f_{\lambda a^2 p_0}$ to avoid being in the center). Thus we need only consider the action of F_1 and F_λ.

We show first that $[F_1, F_1] \subseteq F_1$. By the Abelian assumption, it is enough to show that $[f_{a^2 p_0}, f_{b^2 p_0}] = 0$ if $a^2 + b^2 = \lambda c^2$ for $a, b, a+b \in \mathsf{F}_q^*$. Thus suppose that $a^2 + b^2 = \lambda c^2$. The left hand side of Equation 1.19 reduces to $\alpha_{\lambda c^2 p_0}$. But by our previous remarks, this is not zero. Hence, Equation 1.18 must hold which gives us that $[f_{a^2 p_0}, f_{b^2 p_0}] = 0$ as desired.

Next we show that $[F_\lambda, F_1] \subseteq F_\lambda$. Suppose that $\lambda a^2 + b^2 = c^2$. Then Equation 1.19 reduces to $\alpha_{\lambda c^2 p_0}$ which, we have seen, is non-zero. Thus, as before, we get $[F_\lambda, F_1] \subseteq F_\lambda$.

At this point, let us make the assumption that $\pi(\lambda)$ is a primitive h'th root of one. This assumption will be in force for the following three paragraphs (see Restriction 1.1.1). After that, we will show why it is sufficient to consider this case. Let us only record that so far (without this assumption) we have already proved:

$$\begin{aligned} [F_1, F_1] &\subseteq F_1 && (1.21) \\ [F_\lambda, F_1] &\subseteq F_\lambda. && (1.22) \end{aligned}$$

Next we show that $[F_\lambda, F_\lambda] \subseteq F_\lambda \bigoplus \mathfrak{h}$. Suppose that $\lambda a^2 + \lambda b^2 = c^2$. Then the left hand side of Equation 1.19 evaluated at f_∞ (f_0 would work equally well) yields $\alpha_{\lambda p_0}(f_\infty)(\pi(a) + \pi(b))$. The first part of this product is non-zero. The second part will be zero if and only if $\pi(a) = -\pi(b)$. If we denote by i some $\sqrt{-1}$ in F_q^*, then this situation will occur if and only if $a = \pm ib$ (note that $\pi(\lambda)$ is a primitive h'th root of unity) so that this will occur if and only if $a^2 = -b^2$. For $c \neq 0$, we must therefore have Equation 1.18 which tells us that the corresponding bracket is zero. For $c = 0$, the bracket will lie in $\mathfrak{h}$. Hence $[F_\lambda, F_\lambda]$ will never have a F_1 component and we have shown that $[F_\lambda, F_\lambda] \subseteq F_\lambda \bigoplus \mathfrak{h}$.

Similarly, we show $[F_\lambda, F_1] \subseteq F_1$. Suppose that $\lambda a^2 + b^2 = \lambda c^2$. In this case, Equation 1.19 evaluated at (say) f_∞ yields $\alpha_{\lambda p_0}(f_\infty)(\pi(a) - \pi(c))$. As before, this can only be zero if $a^2 = c^2$. But this would tell us that $b = 0$ which is not possible. Hence we get $[F_\lambda, F_1] \subseteq F_1$.

We complete the picture in the case of $\pi(\lambda)$ primitive by noting that $F_1 \bigcap F_\lambda = \{0\}$ so that $[F_\lambda, F_1] = 0$ at last. □

It will be useful for us to introduce the following notation for a particular basis for V consisting of eigenvectors for A.

Definition 1.10.4 *Write $\zeta = e^{2\pi i/h}$. Then for $k = 0, 1, \ldots, h-1$, let $w_{1,k}$ and $w_{\lambda,k}$ be as follows.*

$$w_{1,k} \;=\; \sum_{l=1}^{h} \zeta^{-lk} A^k f_{p_0} = \sum_{l=1}^{h} (\zeta^{-k}\pi(\lambda))^l f_{\lambda^{2l} p_0}.$$

$$w_{\lambda,k} = \sum_{l=1}^{h} \zeta^{-lk} A^k f_{\lambda p_0} = \sum_{l=1}^{h} (\zeta^{-k}\pi(\lambda))^l f_{\lambda^{2l+1} p_0}.$$

From this, it is clear that $w_{1,k}$ and $w_{\lambda,k}$ are distinct eigenvectors for A corresponding to the eigenvalue ζ^k. If we also note that f_0 and f_∞ are eigenvectors for A of eigenvalue $\pi(\lambda)$ and $\pi(\lambda)^{-1}$, respectively, then it is clear that the set $\{w_{1,k}, w_{\lambda,k}, f_0, f_\infty \mid k = 0, \dots, h-1\}$ is a basis for V consisting of eigenvectors of A.

Lemma 1.10.3 *Let $m \in 1, \dots, h-1$ be such that $\zeta^m = \pi(\lambda)$. Then for $x \in \{1, \lambda\}$, we have:*
(1) the f_0 component of $Sw_{x,k}$ in the f-basis is $\pi(xp_0)^{-1}\Gamma_{0,1} h\delta^{(h)}_{m+k}$
(2) the f_∞ component of $Sw_{x,k}$ in the f-basis is $h\delta^{(h)}_{m-k}$
(3) $Sf_0 = \pi(p_0)\Gamma_{1,0}[w_{1,-m} + \pi(\lambda)w_{\lambda,-m}] + f_\infty$
(4) $Sf_\infty = 1/q[w_{1,m} + w_{\lambda,m} + f_0]$
where $\delta^{(h)}_r$ denotes 1 if $r = 0 \bmod (h)$ and 0 else.

Proof. These are all simple calculations that follow from Theorem 1.2.1, Definition 1.10.4, and Lemma 1.2.1. We will only work out part (1) since the rest are similar or obvious. The f_0 component of $Sw_{x,k}$ is simply $\sum_{l=1}^{h}(\zeta^{-k}\pi(\lambda))^l\Gamma_{0,x\lambda^{2l}p_0} = \sum_{l=1}^{h}\zeta^{l(m-k)}\Gamma_{0,1}\pi(x\lambda^{2l}p_0)^{-1} = \pi(xp_0)^{-1}\Gamma_{0,1}\sum_{l=1}^{h}\zeta^{-l(m+k)}$ which gives us the desired result. □

Lemma 1.10.4 *With the assumptions of Lemma 1.10.2, there exists k_0 such that $Sw_{1,k_0} = c_{k_0} w_{\lambda,-k_0}$ for some $c_{k_0} \neq 0$.*

Proof. Recall S from Equation 1.6. First we observe that S, A, and M_u generate $L_2(q)$. Since V is an irreducible $L_2(q)$ module, then any proper subspace of V invariant under A and M_u can not be S invariant. Thus, SF_1 must have vectors with components in $\mathfrak{h} \bigoplus F_\lambda$.

In fact, we claim that SF_1 must have vectors with nontrivial components in just F_λ. If this were not so, then we have $SF_1 \subseteq F_1 \bigoplus \mathfrak{h}$. But we will see that this is not possible. First recall the notation m from Lemma 1.10.3 and consider the vectors $w_{1,\pm m}$ in F_1. We will apply S to them.

Since $SAS = A^{-1}$, S will carry a ζ^k eigenvector of A into a ζ^{-k} eigenvector. Thus, *a priori*, we may always write:

$$\begin{aligned} Sw_{1,-m} &= aw_{1,m} + bw_{\lambda,m} + cf_0 \\ Sw_{1,m} &= ew_{q,-m} + fw_{\lambda,-m} + gf_\infty \\ Sw_{\lambda,m} &= e'w_{1,-m} + f'w_{\lambda,-m} + g'f_\infty \end{aligned} \tag{1.23}$$

Where $a, b, c, d, e, f, g, e', f', g'$ are certain numbers in $\mathbf{C}$. By Lemma 1.10.3, we also know c, g, g' explicitly. In particular, none of these are zero. Now using the fact that $S^2 = Id$, we get the following equations by applying Equations 1.23 twice and using Lemma 1.10.3 parts (3) and (4):

$$\begin{aligned} 1 &= ae + be' + c\pi(p_0)\Gamma_{1,0} && (1.24) \\ 0 &= af + bf' + c\pi(\lambda p_0)\Gamma_{1,0} && (1.25) \\ 0 &= ag + bg' + c. && (1.26) \end{aligned}$$

If we were to assume that $SF_1 \subseteq F_1 \bigoplus \mathfrak{h}$, this implies that $b = f = 0$ in Equations 1.23. However, Equation 1.25 then would imply that $c = 0$, but we have already seen that this is not so.

Hence, there exists some non-zero $v_0 \in V$ such that $Sv_0 = v_1 + h + v_\lambda$, written with respect to the decomposition $V = F_1 \bigoplus \mathfrak{h} \bigoplus F_\lambda$, such that $v_\lambda \neq 0$. We have already seen (say in Lemma 1.10.2), that $ad(f_\square)$ does not kill anything in F_λ. On the other hand, it kills everything in $F_1 \bigoplus \mathfrak{h}$. Thus, if we let $v_0' = [f_\square, Sv_0]$, then we see that $v_0' \in F_\lambda$ and is non-zero. However, since S preserves the bracket structure and since F_1 is an ideal, SF_1 is also an ideal. Hence v_0' is also in SF_1. Thus we have shown that $SF_1 \bigcap F_\lambda$ is nontrivial.

To finish the proof, it suffices to note that F_1 and F_λ are A invariant. Since $A^{-1} = A^{h-1}$ and $SAS = A^{-1}$, SF_1 is also A invariant. Thus $SF_1 \bigcap F_\lambda$ is a non-zero A invariant space. Therefore it consists of eigenvectors of A and we are done. □

Lemma 1.10.5 *With the notation from Lemma 1.10.4, either $Sw_{1,m}$ or $Sw_{1,-m}$ is contained in $F_\lambda \bigoplus \mathfrak{h}$.*

Proof. Let k_0 be from Lemma 1.10.4 so that $Sw_{1,k_0} = c_{k_0} w_{\lambda,-k_0}$, $c_{k_0} \neq 0$. We know that $[f_0, w_{\lambda,-k_0}] \neq 0$ so that S applied to it is non-zero. Using Lemma 1.10.3 part (3) and the fact that we are in the Abelian case (so that Lemma 1.10.2 applies), this gives us that $[\pi(p_0)\Gamma_{1,0} w_{1,-m},\ c_{k_0}^{-1} w_{1,k_0}] \neq 0$. Thus we have

$$[w_{1,-m}, w_{1,k_0}] \neq 0. \qquad (1.27)$$

With this done, let us use the notation from Equation 1.23 again and make heavy use of the Abelian case while we consider the following.

$$\begin{aligned} [w_{1,-m}, w_{1,k_0}] &= S^2[w_{1,-m}, w_{1,k_0}] \\ &= S[bw_{\lambda,m} + cf_0,\ c_{k_0} w_{\lambda,-k_0}] \\ &= [be'w_{1,-m} + c\pi(p_0)\Gamma_{1,0} w_{1,-m},\ w_{1,k_0}] \\ &= (be' + c\pi(p_0)\Gamma_{1,0})[w_{1,-m}, w_{1,k_0}]. \end{aligned}$$

Hence Equation 1.27 implies that $be' + c\pi(p_0)\Gamma_{1,0} = 1$. Thus, Equation 1.24 tells us that $ae = 0$. Therefore, we have $a = 0$ or $e = 0$ which is exactly the desired result. □

Theorem 1.10.4 *For $\pi^2 \neq 1$ and $p \in \mathsf{F}_q^*$, if V is a non-trivial Lie algebra, then $\mathfrak{g}_p$ is not Abelian.*

Proof. Suppose not. Then we would be in the position of Lemma 1.10.5. Let us carry over all of its notation so that we have either $Sw_{1,m}$ or $Sw_{1,-m}$ contained in $F_\lambda \bigoplus \mathfrak{h}$. In other words, $ae = 0$. Suppose that $e = 0$ so $Sw_{1,m} \subseteq F_\lambda \bigoplus \mathfrak{h}$. Then we would have:

$$\begin{aligned}[Sw_{1,m}, f_\infty] &= [fw_{\lambda,-m}, f_\infty] \\ &= f[w_{\lambda,-m}, f_\infty].\end{aligned}$$

Thus $[Sw_{1,m}, f_\infty]$ is zero if and only if $f = 0$ since f_∞ does not kill anything in F_λ and $w_{\lambda,-m} \not\subseteq \mathfrak{h}$. However, by applying S to $[Sw_{1,m}, f_\infty]$, we get $[w_{1,m}, (1/q)w_{1,m}]$ which is equal to 0. Since S is invertible, this gives us that $f = 0$. In other words, $e = 0$ implies $f = 0$. But looking at Equation 1.23, this translates to saying that $Sw_{1,-m} = cf_0$. This would imply, though, that $w_{1,-m} = cSf_0$. But this is a contradiction by Lemma 1.10.3.

To see that $a = 0$ also gives a contradiction, repeat the same argument as above, but this time start out with $[Sw_{1,-m}, f_0]$. It is easy to see that everything is similar. Thus we are done. □

Since we have shown that the Abelian possibility of Theorem 1.10.1 cannot occur if V is actually a Lie algebra, this leaves only the possibilities of $\mathfrak{sl}(2, \mathsf{C})$ and the Heisenberg. Next, we will show that Jacobi also excludes the Heisenberg case.

First we need a "nilpotent" argument.

Lemma 1.10.6 *If $\pi^2 \neq 1$ and V a Lie algebra, then for $p, q \in \mathsf{F}_q^*$, there exits n in Z^+ such that $ad(f_p)^n f_q = 0$.*

Proof. First, by Theorem 1.6.1, we observe that $ad(f_p)^n f_q \subseteq \mathsf{C} f_{np+q}$. Suppose $ad(f_p)f_q \neq 0$. Then since Jacobi is satisfied, Equation 1.18 tells us that $\alpha_{p+q} = \alpha_p + \alpha_q$. If $ad(f_p)^2 f_q$ is also non-zero, then $ad(f_p)f_{p+q} \neq 0$. Hence we get $\alpha_{2p+q} = \alpha_p + \alpha_{p+q} = 2\alpha_p + \alpha_q$. In general, suppose $ad(f_p)^n f_q \neq 0$. Using induction, we get

$$\alpha_{np+q} = n\alpha_p + \alpha_q. \tag{1.28}$$

Assume that the lemma is false. Since V is a Lie algebra, we have already seen that each $\mathfrak{g}_p$ must be three-dimensional. In particular, this will give us (see Definition 1.10.3 for α_p, Theorem 1.10.1 for the three-dimensional properties, and Definition 1.10.1 for d_p)

that each α_p is a non-zero element of $\mathfrak{h}^*$. However, by definition of the finite field $\mathbf{F}_q$, there are only a finite number of "roots" α_r, $r \in \mathbf{F}_q^*$. But Equation 1.28 would imply (by taking arbitrary $n \in \mathbf{Z}^+$) that there were an infinite number of distinct "roots". Hence we have a contradiction. □

Next, we present the standard "bracket" relations for $\mathfrak{g}_p$.

Theorem 1.10.5 *In the case where $\mathfrak{g}_p$ is three dimensional, using the notation of Definition 1.10.1, suppose that $[x, f_q] = 0$ for some $q \in \mathbf{F}_q^*$. Then, if we define $v_0 = f_q$ and $v_i = \frac{1}{i!} ad(y)^i v_0$ for $i \in \mathbf{Z}^+$, we have*

$$\begin{aligned} ad(y)v_i &= (i+1)v_{i+1} \\ ad(h)v_i &= (\alpha_q(h) - 2id_p)v_i \\ ad(x)v_i &= (\alpha_q(h) + (1-i)d_p)v_{i-1} \end{aligned}$$

where α_q is given in Definition 1.10.3. In this case,

$$\alpha_q(h) \quad = \quad \frac{(f_p, f_{-p}, f_0)(f_q, f_{-q}, f_\infty) + (f_p, f_{-p}, f_\infty)(f_q, f_{-q}, f_0)}{(f_q, f_{-q})(f_0, f_\infty)}.$$

Note that by Lemma 1.10.6, if $[f_p, f_q]$ were not equal to zero, we could always "push" f_q up (in a non-zero way) with $ad(f_p)$ to some $f_{q'} = f_{np+q}$ so that $[f_p, f_{q'}] = 0$.

Proof. This is just the standard $\mathfrak{sl}(2, \mathbf{C})$ type proof. It follows by induction on the bracket relations given in Theorem 1.10.1 and the Definitions in 1.10.1 and 1.10.3. We omit the details as they are well known. □

We are now in a position to exclude the Heisenberg case.

Lemma 1.10.7 *Let $\pi^2 \neq 1$ and V be a Lie algebra. Then $\mathfrak{g}_p$ is not a Heisenberg algebra.*

Proof. Assume not. Then pick $q' \in \mathbf{F}_q^*$. By Lemma 1.10.6, let $q = np + q'$ be such that $ad(f_p)^n f_{q'} \neq 0$ but $[f_p, f_q] = 0$. We are now in a position to use Theorem 1.10.5 so we will adopt the Theorem's notation. Since $\mathfrak{g}_p$ is a Heisenberg, we know that either (f_p, f_{-p}, f_0) (call this case I) or (f_p, f_{-p}, f_∞) (call this case II) is equal to zero, but not both. In either case, we have $d_p = 0$. Hence, we have the relations

$$\begin{aligned} [f_{-p}, v_i] &= (i+1)v_{i+1} \\ [h, v_i] &= \alpha_q(h)v_i \\ [f_p, v_i] &= \alpha_q(h)v_{i-1} \end{aligned} \tag{1.29}$$

where $v_0 = f_q$ and $v_i = (1/i!)ad(f_{-p})^i v_0$. However, Lemma 1.10.6 tells us that for large i, v_i is zero. Using an i such that $v_i = 0$ but $v_{i-1} \neq 0$, Equation 1.29 tells us that we must have $\alpha_q(h) = 0$. Hence f_p kills each v_i. In particular, looking at the beginning of the proof, we must have $q' = q$. Thus we have $\alpha_{q'}(h) = 0$. However, looking at Theorem 1.10.5 for an explicit form of $\alpha_{q'}(h)$, we must have $(f_{q'}, f_{-q'}, f_0) = 0$ in case I or $(f_{q'}, f_{-q'}, f_\infty) = 0$ in case II. However, q' was arbitrary. Thus, case I implies that f_0 is in the center while case II implies that f_∞ is in the center. Either possibility contradicts Theorem 1.10.2 This finishes the proof. □

Concluding this section, we state:

Theorem 1.10.6 *Assume that $\pi^2 \neq 1$. Suppose there exists a non-zero $L_2(q)$ invariant alternating three-form that makes V into a Lie algebra. Then each $\mathfrak{g}_p$, $p \in \mathsf{F}_q^*$, is isomorphic to $\mathfrak{sl}(2, \mathbf{C})$.*

Proof. This is an immediate corollary of the previous theorem and earlier discussion. □

1.11 Necessity of Rank 2

In this section and the next, we will be able to show that the only time V can be made into a non-trivial Lie algebra is in the cases of A_2, B_2, and G_2. To do this, we will exploit certain "integrality" conditions that will follow from Jacobi. To some degree, the basic reason that only $q = 5, 7, 9, 13$ are allowable stems from the fact that

$$2cos(2\pi i/h)$$

is only an integer for $h = 2, 3, 4, 6$ (Theorem 1.11.2, Equation 1.35).

It will fall out of previous work that the set of $\{\alpha_p\}$ forms a root system. To start, let us make use of Theorem 1.10.6 and Theorem 1.10.1 to redefine the basal elements in $\mathfrak{g}_p$ of Definition 1.10.1.

Definition 1.11.1 *For V a non-trivial Lie algebra and $p \in \mathsf{F}_q^*$, normalize a basis for $\mathfrak{g}_p$ as follows:*

$$\begin{aligned} x_p &= f_p \\ y_p &= \frac{1}{d_p} f_{-p} \\ h_p &= \frac{1}{d_p}[f_p, f_{-p}] \end{aligned}$$

$$= \frac{(f_p, f_{-p})}{(f_p, f_{-p}, f_0)} f_0 + \frac{(f_p, f_{-p})}{(f_p, f_{-p}, f_\infty)} f_\infty$$

Note that this is the "standard e, f, h" basis of $\mathfrak{sl}(2, \mathbb{C})$.

Let us note for future reference the value of a "root" on our new h_p. From the above definition and Definition 1.10.3, we see

$$\alpha_q(h_p) = \frac{(f_p, f_{-p})}{(f_q, f_{-q})}\left(\frac{(f_q, f_{-q}, f_0)}{(f_p, f_{-p}, f_0)} + \frac{(f_q, f_{-q}, f_\infty)}{(f_p, f_{-p}, f_\infty)}\right) \tag{1.30}$$

for $p, q \in \mathbb{F}_q^*$. Now we prove the first integrality condition.

Theorem 1.11.1 *Let V be a non-trivial Lie algebra and let $p, q \in \mathbb{F}_q^*$. Write $r, s \in \mathbb{Z}$ as the largest integers satisfying $ad(f_p)^s f_q \neq 0$ and $ad(f_{-p})^r f_q \neq 0$. Then*

$$\alpha_q(h_p) = -(s - r).$$

In particular, $\alpha_q(h_p)$ is always an integer.

Proof. Since $\mathfrak{g}_p$ is just a $\mathfrak{sl}(2, \mathbb{C})$ and we have renormalized h_p so that it is the standard "h", this is simply a well know fact that follows easily by the bracket relations and finiteness of r and s (see [9]). One way to see this is the following. Using $v_0 = f_{q+sp}$ and the fact that $v_{s+r+1} = 0$ but $v_{s+r} \neq 0$ in Theorem 1.10.5 (with $d_p = 1$), we get $0 = ad(f_{-p})v_{s+r+1} = [\alpha_{q+sp}(h_p) + (1 - (s + r + 1))]v_{s+r}$ so that we must have $0 = \alpha_{q+sp}(h_p) - s - r = \alpha_q(h_p) - s\alpha_p(h_p) - s - r = \alpha_q(h_p) + s - r$ which gives us our result. □

Since our $L_2(q)$ invariant two-form $(,)$ is non-degenerate when restricted to $\mathfrak{h}$, it is a simple matter to transfer all the structure we have on $\mathfrak{h}$ to $\mathfrak{h}^*$. Using the results on the "roots" $\{\alpha_p\}$ and the above integrality condition, it is not too hard to check that the set of α_p is indeed an honest (reduced) root system when V is a Lie algebra. Hence by the dimension of $\mathfrak{h}$, we would get as a corollary that the root system so obtained must be isomorphic to the one of the following root systems: $A_1 + A_1, A_2, B_2, G_2$, or BC_2. Then as a corollary of this, one gets limits on the values of q.

While this line of attack is possible and will be followed up in the next section, most of the time we do not really need to rely on the classification of root systems. Instead, the Jacobi identity forces us into the situation where each $\mathfrak{g}_p$ is a $\mathfrak{sl}(2, \mathbb{C})$. As it turns out, this alone will usually give us that q must be equal to 5, 7, 9, or 13. However, when $q = 5$, then $\pi^2 = 1$ so V is never irreducible. Thus, we will get that only $q = 7, 9, 13$ is possible. (It is easily seen that for $q = 5$, V will split into two copies of $\mathfrak{sl}(2, \mathbb{C})$ as we have already remarked at the end of Section 1.9).

Theorem 1.11.2 *Assume that $\pi_m^2 \neq 1$ and that V_{π_m} is a non-trivial Lie algebra with $\pi_m(\lambda)$ a primitive h'th root of unity, i.e, $(m,h) = 1$. Then $q = 7, 9,$ or 13.*

Proof. Let $p, q \in \mathsf{F}_q^*$. Using Equation 1.30, the fact that $d_r \neq 0$, and the invariance of the two and three-forms with respect to A (see Theorem 1.4.1 and Theorem 1.5.3), let us calculate (by factoring out the $(f_1, f_{-1}, f_\square)$ and $(f_\lambda, f_{-\lambda}, f_\square)$ part in each and canceling where appropriate):

$$\begin{aligned}
\alpha_{q^2}(h_{p^2}) &= \pi(q/p)^2(\pi(p/q) + \pi(p/q)^3) \\
&= \pi(q/p) + \pi(p/q) & (1.31) \\
\alpha_{\lambda q^2}(h_{\lambda p^2}) &= \pi(q/p) + \pi(p/q) & (1.32) \\
\alpha_{q^2}(h_{\lambda p^2}) &= \pi(1/\lambda)(\pi(q/p)\frac{(f_1, f_{-1}, f_\infty)}{(f_\lambda, f_{-\lambda}, f_\infty)} + \pi(p/q)\frac{(f_1, f_{-1}, f_0)}{(f_\lambda, f_{-\lambda}, f_0)}) & (1.33) \\
\alpha_{\lambda q^2}(h_{p^2}) &= \pi(\lambda)(\pi(q/p)\frac{(f_\lambda, f_{-\lambda}, f_\infty)}{(f_1, f_{-1}, f_\infty)} + \pi(p/q)\frac{(f_\lambda, f_{-\lambda}, f_0)}{(f_1, f_{-1}, f_0)}). & (1.34)
\end{aligned}$$

We will only need the first equation for this proof, but we listed the others as they will be useful later. Let $r = q/p$. Then as q and p vary, r will vary over all of F_q^*. Thus Theorem 1.11.1 and Equation 1.31 imply that the expression:

$$\pi(r) + \pi(r)^{-1} \tag{1.35}$$

is always an integer for all $r \in \mathsf{F}_q^*$. However, since $\pi(\lambda)$ is a primitive h'th root of unity, this is the same as saying that

$$2cos(2\pi i/h)$$

is an integer. It is trivial to check that this implies that h = 2, 3, 4, or 6. In turn, this gives us that q = 5, 7, 9, or 13. However, as we have already noted, if $q = 5$, then $\pi^2 = 1$. Hence we must have q = 7,9,or 13 as desired. □

1.12 Structure of the Roots

We note that the condition of Equation 1.35 being an integer is precisely the relation needed when one considers the problem of tiling the plane. And in fact it is clear that the h values 3,4,6 are precisely the only values for which the tiling may be done: for the triangle, the square, and the hexagon. Another way of saying this is that the only Dihedral groups that preserve a lattice in the plane are D_3, D_4, D_6.

Next let us examine the "roots." It will show that only $q = 7, 9, 13$ are allowable under Restriction 1.1.1. To do this we first extract roots and so let us transfer our nondegenerate 2-form $(,)|_{\mathfrak{h}}$ to $\mathfrak{h}^*$. For any $\mu \in \mathfrak{h}^*$, let $u_\mu \in \mathfrak{h}$ be the unique element satisfying $\mu(h) = (u_\mu, h)$ for all $h \in \mathfrak{h}$. With this, we define a non-degenerate symmetric $L_2(q)$ invariant 2-form on $\mathfrak{h}^*$ by letting

$$(\mu, \nu) = (u_\mu, u_\nu)$$

for all $\mu, \nu \in \mathfrak{h}^*$. In particular, for each $p \in \mathsf{F}_q^*$, u_{α_p} is the unique element of $\mathfrak{h}$ such that $\alpha_p(h) = (u_{\alpha_p}, h)$ for all $h \in \mathfrak{h}$. Using the definition of the bracket structure and Definition 1.10.3, we note that $\alpha_p(f_\square) = (f_p, f_{-p}, f_\square)/(f_p, f_{-p}) = ([f_p, f_{-p}], f_\square)/(f_p, f_{-p})$. This gives us

$$u_{\alpha_p} = \frac{[f_p, f_{-p}]}{(f_p, f_{-p})}.$$

Moreover, if we define

$$h_{\alpha_p} = 2u_{\alpha_p}/(\alpha_p, \alpha_p),$$

it is also easy to check that these "coroots" satisfy the relation $h_{\alpha_p} = h_p$ from Definition 1.11.1.

Let us use the standard notation

$$< \mu \mid \nu > = 2(\mu, \nu)/(\nu, \nu).$$

Thus if we write σ_μ for the reflection across the hyperplane perpendicular to μ, we have the usual formula:

$$\sigma_\mu(\nu) = \nu - < \mu \mid \nu > \mu.$$

We will need one more relation. Namely,

$$\begin{aligned} < \alpha_p \mid \alpha_q > &= < h_q \mid h_p > \\ &= \alpha_p(h_q). \end{aligned} \tag{1.36}$$

Since this is the standard phenomenon and since the above is simply a matter of checking the definitions, we leave it to the reader. With this notation, we are now ready to consider root systems.

Theorem 1.12.1 *For $\pi^2 \neq 1$ and V a non-trivial Lie algebra, the set of α_p, $p \in \mathsf{F}_q^*$, form a rank two (reduced) root system of order $q-1$ within their real span.*

Proof. First, let us check that the real span of the α_p really is only two dimensional (over $\mathbf{R}$). To do this, we claim that for $q \in \mathsf{F}_q^*$, the following identity holds:

$$\alpha_q = [2\alpha_q(h_1) - \alpha_q(h_\lambda)\alpha_\lambda(h_1)]\alpha_1 + [2\alpha_q(h_\lambda) - \alpha_q(h_1)\alpha_1(h_\lambda)]\alpha_\lambda. \tag{1.37}$$

To check this equality, merely evaluate both sides at $f_\square$, $\square \in \{0, \infty\}$, using Definition 1.10.3 and Equation 1.30. Since it is an easy calculation, we omit the details. However, Theorem 1.11.1 tells us that we have actually expressed any α_q as an integral linear combination of α_1 and α_λ. In particular, since $\mathbf{Z} \subseteq \mathbf{R}$, the real span of the roots is no more than two dimensional. We will show below that α_1 is not a multiple of α_λ which will give us that the real span is exactly two dimensional as desired.

Let us show that all the roots are distinct and that the only multiples of roots that are still roots are ± 1. This is just the standard argument. First note that by the alternating nature of the three-form, we have:

$$-\alpha_p = \alpha_{-p}. \tag{1.38}$$

Fix $\alpha = \alpha_q$. By Theorem 1.10.6, we know that $\mathfrak{g}_q$ is isomorphic to $\mathfrak{sl}(2, \mathbf{C})$. For each $c \in \mathbf{R}$, let L_c be the real span of all vectors f_p, $p \in \mathsf{F}_q^*$, such that $\alpha_p = c\alpha$. Then put $L = \bigoplus_c L_c$. Thus by the Jacobi identity (see Equation 1.19), $V' = L \bigoplus \mathfrak{h} \subseteq V$ is a finite dimensional representation of $\mathfrak{g}_q$, i.e., of $\mathfrak{sl}(2, \mathbf{C})$, under *ad*. Since we have $ad(h_q)|_{L_c} = (2c)Id$, we must have $c \in \frac{1}{2}\mathbf{Z}$ by elementary $\mathfrak{sl}(2, \mathbf{C})$ theory. Also since $\mathfrak{g}_q + \mathfrak{h} \subseteq V'$ is an invariant subspace of the representation that contains all occurrences of the 0-weight for $ad(h_q)$, we see that 0 and ± 2 exhaust the even roots in V'. In particular, twice a root is not a root. Then we also have half a root is not allowable either since α is a root. In particular, 1 is not a weight. Thus $\mathfrak{sl}(2, \mathbf{C})$ tells us that only $c = \pm 1$ yield non-zero L_c and that $V' = L_1 \bigoplus \mathfrak{h} \bigoplus L_{-1} = \mathfrak{g}_q + \mathfrak{h}$. Since each f_p is distinct, we have shown that each α_q is distinct and that the only multiples of α_q that are roots are $\pm\alpha_q$.

Next, let α and β be two roots. Then if $\beta - r\alpha, \dots \beta + s\alpha$ is the maximal α root sitting through β, then Theorem 1.11.1 has already told us that $\alpha(h_\beta) = r - s$. With this, one easily check that $\sigma_\alpha(\beta)$ is still a root.

Finally, we we have already shown that $< \alpha_p \mid \alpha_q > \in \mathbf{Z}$ by Equation 1.36 and Theorem 1.11.1. This finishes the proof. □

We also prove:

Theorem 1.12.2 *For $\pi^2 \neq 1$ and V a non-trivial Lie algebra, V is semi-simple of rank 2.*

Proof. Since $\pi^2 \neq 1$, V is irreducible. Since $[,]$ is $L_2(q)$ invariant, the first derived algebra of V, $[V, V]$, is invariant and thus either 0 or V. But since there is no center, $[V, V] = V$. In particular, V is not solvable. But since the Killing form (being constructed out of invariant things) is $L_2(q)$ invariant, it must be a multiple of our two-form. In fact, it must be a non-zero multiple by Cartan's criterion. Hence, since the two-form is non-degenerate, the Killing form is non-degenerate. Thus V must be semi-simple. The rest follows basically from Theorem 1.12.1. Another way to see it follows.

We claim that $\mathfrak{h}$ is a maximal Abelian semi-simple subalgebra of V. If not, then by A invariance and the fact that the f-basis diagonalizes $ad(f_0)$ and $ad(f_\infty)$, $\mathfrak{h}$ would commute with all of F_1 or F_λ (see Definition 1.10.2). But we have already seen that this is not possible. Hence we are done since $\mathfrak{h}$ is two dimensional. □

Corollary 1.12.1 *Assume that $\pi_m^2 \neq 1$ and that V_{π_m} is a non-trivial Lie algebra with m subject to Restriction 1.1.1. Then $q = 7, 9$, or 13 and m is an exponent of A_2, B_2, or G_2, respectively.*

Proof. This follows easily from Theorem 1.12.2. Since V has dimension $q+1$ and must be rank two, $q+1$ must be either 6,8,10, or 14. Since we have already seen that 5 is not allowable owing to irreducibility, we have q equal to 7,9, or 13. The exponent statement is obvious for $q = 7, 9$ since the exponents are the only possibilities anyway. For $q = 13$, simply apply Theorem 1.1.1 and Theorem 1.5.4 part (1). □

Corollary 1.12.2 *For $\pi^2 \neq 1$ and V a Lie algebra, the root system obtained from the set of α_p must be isomorphic to A_2, B_2, and G_2, for $q = 7, 9$, and 13, respectively.*

Proof. Corollary 1.12.1 has already told us that the only allowable q are 7, 9, and 13. Now by using Theorem 1.12.2 and Theorem 1.12.1 and noting that in each case we must have 6, 8, and 12 roots (since $\mid \mathsf{F}_q^* \mid = q - 1$), respectively, it is a trivial to check that the above listed root systems are the only rank two possibilities with the correct number of roots. Note: had we not insisted on $\pi^2 \neq 1$, then $A_1 + A_1$ would have been the corresponding root system for $q = 5$. □

Let us look at each of these cases, $q = 7, 9, 13$, to see how the roots are situated.

F_7. As we have seen, the root system must be A_2. Fix $\lambda = -2$ as a generator for F_7^*. Using the fact that $-1 = \lambda^3$ and Equations 1.31, we calculate that $\alpha_1(h_\lambda) = -\alpha_{-1}(h_\lambda) = -\pi(\lambda) - \pi(\lambda)^{-1}$. Since $\pi(\lambda)$ is a primitive third root of unity, this tells us that $\alpha_1(h_\lambda) = 1$. Similarly, we calculate that $\alpha_1(h_{\lambda^5}) = -\alpha_{-1}(h_{\lambda^5}) = 1$. In other words, between α_1 and α_λ and between α_1 and α_{λ^5} there is a 60 degree angle. Thus, up to isomorphism, the root system in this case must be as in Figure 1-1 or Figure 1-2 (this also can be seen using the additive structure of the roots). Note that the roots go around in order of powers of λ and that the element A (multiplication by λ^2) acts as the Coxeter element, rotation by 120°.

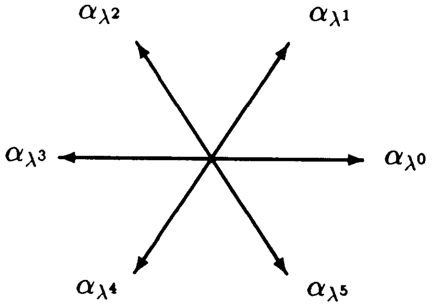

Figure 1-1: $q = 7$, possibility 1

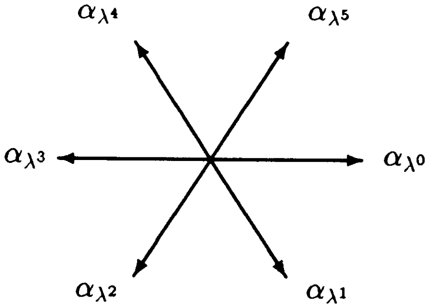

Figure 1-2: $q = 7$, possibility 2

Also, using Equation 1.33, Theorem 1.11.1, and our explicit determination of the roots above, it is now easy to calculate that in either case

$$\begin{aligned}
\frac{(f_1, f_{-1}, f_0)}{(f_\lambda, f_{-\lambda}, f_0)} &= -1 \\
\frac{(f_1, f_{-1}, f_\infty)}{(f_\lambda, f_{-\lambda}, f_\infty)} &= -\pi(\lambda)^2
\end{aligned}$$

by solving two linear equations in two unknowns, e.g., $\alpha_{\lambda^2}(h_\lambda) = 1$ and $\alpha_{\lambda^4}(h_{\lambda^5}) = 1$. In principle, these numbers and $L_2(7)$ invariance (up to normalization) determine the three-form which in turn determines the bracket structure.

Moreover, using the notation of Theorem 3.2.1 and looking at a few character values (say by Theorem 3.3.1), one may say that the representation χ_2 is associated to Figure 1-1 and χ_3 to Figure 1-2 in the standard representations.

F_9: Here we know that the root system must be B_2. First of all, one may check using the definitions and invariance that

$$\begin{aligned}
(\alpha_{c^2q}, \alpha_{c^2q}) &= \frac{2d_{c^2q}}{\pi(c^2q)^2(f_0, f_\infty)} \\
&= \frac{2d_q}{\pi(q)^2(f_0, f_\infty)}. \qquad (1.39)
\end{aligned}$$

In other words, all roots of the form α_{c^2q} have the same length (this can also be seen by A invariance). Fix a generator λ of F_9^* with the property that $\lambda^2 = 1 + \lambda$ and $1 + \lambda^2 = \lambda^7$ (such a generator exists). Then using that the roots must add according to the field (if their sum is another root then $\alpha_p + \alpha_q = \alpha_{p+q}$, $p, q, p+q \in \mathsf{F}_9$) and that all α_{q^2} have the same length, we see that only two possibilities can happen. If α_1 is a short root then we must have the root system isomorphic to the one in Figure 1-3. If α_1 is a long root then we must the root system isomorphic to Figure 1-4. In either case we may calculate (as above for $q = 7$) that in the first case we have:

$$\begin{aligned}
\frac{(f_1, f_{-1}, f_0)}{(f_\lambda, f_{-\lambda}, f_0)} &= -1 - \pi(\lambda) \\
\frac{(f_1, f_{-1}, f_\infty)}{(f_\lambda, f_{-\lambda}, f_\infty)} &= 1 - \pi(\lambda)
\end{aligned}$$

and in the second case

$$\frac{(f_1, f_{-1}, f_0)}{(f_\lambda, f_{-\lambda}, f_0)} = (1 - \pi(\lambda))^{-1}$$

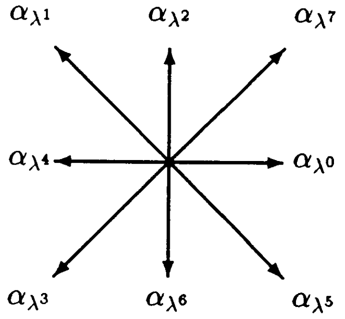

Figure 1-3: $q = 9$ with α_1 short

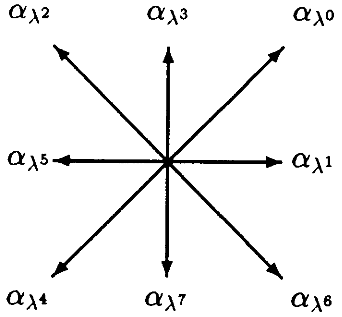

Figure 1-4: $q = 9$ with α_1 long

$$\frac{(f_1, f_{-1}, f_\infty)}{(f_\lambda, f_{-\lambda}, f_\infty)} = (-1 - \pi(\lambda))^{-1}.$$

Moreover, using the notation of Theorem 3.2.1 and looking at a few character values (say by Theorem 3.3.2), one may say that the representation χ_3 is associated to Figure 1-3 and χ_2 to Figure 1-4.

F_{13}: Here we know that the root system must be G_2 and m an exponent of G_2. Again by Equation 1.39 or A invariance, we know that all roots $\alpha_{c^2 q}$ have the same length. Fix a generator $\lambda = 2$. On the roots of the same length, use a similar argument as with the A_2 above. Combining this with the addition being indexed by the field, is trivial to check that again only two possibilities occur. If α_1 happens to be a short root, the roots must be as in Figure 1-5. If α_1 is a long root, then it must be as in Figure 1-6.

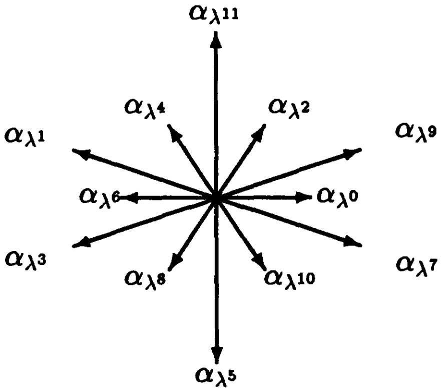

Figure 1-5: $q = 13$ with α_1 short

As before, we can calculate that in the first case:

$$\frac{(f_1, f_{-1}, f_0)}{(f_\lambda, f_{-\lambda}, f_0)} = -3\pi(\lambda)/(1 + \pi(\lambda))$$

$$\frac{(f_1, f_{-1}, f_\infty)}{(f_\lambda, f_{-\lambda}, f_\infty)} = -3\pi(\lambda)^2/(1 + \pi(\lambda))$$

and in the second case we get:

$$\frac{(f_1, f_{-1}, f_0)}{(f_\lambda, f_{-\lambda}, f_0)} = -1/(-1 + \pi(\lambda)^{-2})$$

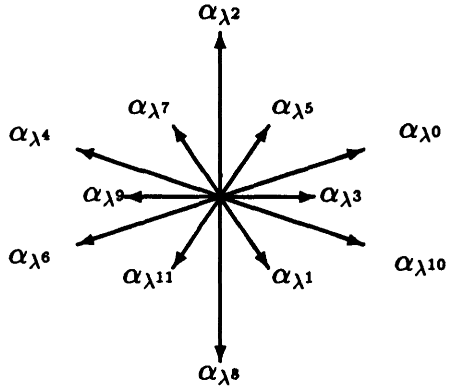

Figure 1-6: $q = 13$ with α_1 long

$$\frac{(f_1, f_{-1}, f_\infty)}{(f_\lambda, f_{-\lambda}, f_\infty)} = 1/(-1 + \pi(\lambda)^{-2}).$$

Moreover, using the notation of Theorem 3.2.1 and looking at a few character values (say by Theorem 3.3.2), one may say that the representation χ_2 is associated to Figure 1-5 and χ_3 to Figure 1-6.

Note 1.12.1 As a final observation, we note that the appearance of two possibilities for the root configuration in the above examples is due to our choice of labeling M_1 and M_λ in $L_2(q)$ or in our choice of V_{π_m} and $V_{\pi_{-m}}$. In a sense, they can be interchanged. For more details, see the discussion following Theorem 1.9.1 and Theorems 3.3.1, 3.3.2, and 3.3.3.

Chapter 2

The Geometry of the Cartans

In this chapter we will explore the possibility of using Kostant's conjecture in decomposing the Lie algebra into a sum of Cartans with some invariant properties. To begin, we will state Kostant's conjecture in its full generality.

2.1 The Cartan Subalgebras

Note that if one allows computer proofs, then Kostant's conjecture below has been verified–see the Introduction. For the following, please recall the notation of the Introduction and Section 1.1 and 1.2 so that we have λ a generator for F_q^*, π a multiplicative character of F_q^*, χ an additive character of F_q, V_π a principal series representations, and $\Gamma_{0,1}$ the gamma function depending on π and χ.

Theorem 2.1.1 *(Kostant's Conjecture) Suppose G is a simple complex Lie group with trivial center such that $2h + 1 = q = p^f$ is an odd prime power where h is the Coxeter number of G, then the following holds:*
(1) There is a homomorphism ν embedding:

$$L_2(q) \overset{\nu}{\hookrightarrow} G.$$

(2) Under the Adjoint action of this embedding, $L_2(q)$ decomposes $\mathfrak{g} = Lie(G)$ into a direct sum of principal series representations $V_{\pi_{m_i}}$ (or a component of $V_{\pi_{m_i}}$ in the case that $m_i = h/2$) where $1 \leq m_i \leq h/2$ are the exponents of G less than or equal to $h/2$.
(3) $\nu(A)$ is a Kostant element (globalized Coxeter element) and $\nu(K)$ is a Kac element in G where A is an element of order h and K is an element of order $h+1$ in $L_2(q)$.
(4) There exists a Borel subalgebra of $L_2(q)$ which, under $Ad \circ \nu$, fixes a Cartan subalgebra $\mathfrak{h}$ of $\mathfrak{g}$. An element of order h in the Borel acts as the Coxeter element on $\mathfrak{h}$ and the elements of order p in the Borel act trivially on $\mathfrak{h}$.

Remark 2.1.1 See Sections 1.1 and 1.2 on the e-basis and the f-basis to recall the basic structure and notation of the principal series representations appearing in part (2). In particular, we have a fixed non-trivial additive character χ of F_q. For each exponent m, choose an e-basis $e_u^{(m)}$ (thus by using the same additive character χ we also get an f-basis $f_u^{(m)}$), $u \in \mathsf{P}^1(\mathsf{F}_q)$, for each V_{π_m} just as we did before. Please note that when π_m is understood we will omit the exponents (m) and subscripts m and π. The only additional information needed will be for the case $h/2 \in \mathsf{Z}$ (see Theorem 1.1.1) where $V_{\pi_{h/2}}$ is reducible. In this case, the two irreducible components of $V_{\pi_{h/2}}$ are

$$V_{\pi_{h/2}} = span\{f_{u^2},\, \Gamma_{0,1}f_\infty + f_0 \mid u \in \mathsf{F}_q^*\} \bigoplus span\{f_{\lambda u^2},\, \Gamma_{0,1}f_\infty - f_0 \mid u \in \mathsf{F}_q^*\}$$

where of course the e's, f's, and Γ's all depend on our choice of multiplicative character $\pi_{h/2}$. This is a simple and well known fact to check. For a reference, see [26] §2.5.6.

To begin with, note that the dimensions agree in Theorem 2.1.1 part (3). We will check it in the case that $h/2$ is not an exponent (the other case is similar). First recall that the dimension of $\mathfrak{g}$ is $l(h+1)$ (where l is the rank of $\mathfrak{g}$). Since the dimension of V_{π_m} is $q+1 = 2(h+1)$, the dimensions agree since since there are $l/2$ exponents of G less than $h/2$. Next let us exploit part (4) above.

Lemma 2.1.1 *Under the embedding of $L_2(q)$ in G, a Borel subgroup of $L_2(q)$ fixes a Cartan subalgebra $\mathfrak{h}_\infty$ of $\mathfrak{g}$ and the $L_2(q)$ action on the set of Cartans $\{g\mathfrak{h}_\infty \mid g \in L_2(q)\}$ is equivalent to the action on $\mathsf{P}^1(\mathsf{F}_q)$ by (inverse transpose) linear fractional transformations.*

Proof. If $\mathcal{B}$ is a Borel subalgebra of $L_2(q)$, then it is clear that $L_2(q)/\mathcal{B}$ is just the projective field $\mathsf{P}^1(\mathsf{F}_q)$ (see the discussion in Section 1.1) under the appropriate linear fractional action. Thus we only need to check that there exists a Cartan subalgebra whose stabilizer in $L_2(q)$ is a Borel subalgebra to prove the theorem. Existence of of a Cartan, $\mathfrak{h}_\infty$, fixed by $\mathcal{B}$ is given by Kostant's conjecture part (4). To see that the stabilizer of $\mathfrak{h}_\infty$ in $L_2(q)$ is only $\mathcal{B}$, suppose that more than the Borel fixes the Cartan. If so, then since the Borels are maximal proper subgroups, all of $L_2(q)$ fixes $\mathfrak{h}_\infty$. But then $\mathfrak{h}_\infty$ is a representation of $L_2(q)$ of dimension l. But Kostant's conjecture part (2) also would imply that $\mathfrak{h}_\infty$ would be a sum of principal series representations (or components thereof) and thus would have dimension a multiple of $(h+1)$. In particular, $(h+1)$ would divide l which at the least would give $l \geq (h+1)$ which is a contradiction to the fact that $h > l$. □

In particular, $L_2(q)$ always permutes $(q+1) = 2(h+1)$ Cartans. Since $dim(\mathfrak{g}) = l(h+1)$ and $dim(\mathfrak{h}) = l$, it could be hoped that $\mathfrak{g}$ might be written in some interesting way as a sum of half of these Cartans. This is what we propose to examine. To do this, let us give names to these Cartans and (without loss of generality) pin down a Borel subalgebra of $L_2(q)$.

Definition 2.1.1 *Let $\overline{B}$ be the lower triangular matrices in $L_2(q)$. Let $\mathfrak{h}_\infty$ be a Cartan subalgebra in $\mathfrak{g}$ fixed by $\overline{B}$ as in Theorem 2.1.1 part (4). For each $u \in \mathsf{F}_q^*$, define (via the Ad action of the embedding):*

$$\mathfrak{h}_u = N_{-1/u}\mathfrak{h}_\infty \quad \textit{and} \quad \mathfrak{h}_0 = S\mathfrak{h}_\infty$$

to be the $q+1$ Cartans that $L_2(q)$ permutes according to (inverse transpose) linear fractional transformations where recall

$$N_u = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \textit{ and } S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

from Equations 1.4 and 1.6.

Let us check the uniqueness of the above definition.

Lemma 2.1.2 *$\mathfrak{h}_\infty$ is given uniquely by the joint eigenvectors of eigenvalue one for $\{M_u \mid u \in \mathsf{F}_q\}$ where recall*

$$M_u = \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix}$$

from Equation 1.5.

Explicitly, $\mathfrak{h}_\infty$ will be spanned by its intersection with each irreducible component of $L_2(q)$. In case $m \neq h/2$, each $\mathfrak{h}_\infty \bigcap V_{\pi_m}$ is two dimensional and will be spanned by the two vectors

$$f_0 = \sum_{u \in \mathsf{F}_q} e_u \quad \textit{and} \quad f_\infty = e_\infty .$$

If $m = h/2$, then $h_\infty \bigcap V_{\pi_{h/2}}$ is one dimensional and it is spanned by the appropriately signed vector (see Remark 2.1.1)

$$\Gamma_{0,1} f_\infty \pm f_0 .$$

Proof. By Theorem 2.1.1 part (4), we know that some $\mathfrak{h}_\infty$ exists and that it consists of eigenvectors of eigenvalue one for each M_u. By part (2), we may break up $\mathfrak{g}$ into $l/2$ (respectively $(l+1)/2$ for $h/2$ an exponent) irreducible representations of $L_2(q)$. However, in each such component, $M_u f_v = \chi(uv) f_v$ and $M_u f_\infty = f_\infty$ where χ was the fixed non-trivial additive character of F_q by Theorem 1.2.1. But since χ is non-trivial it is clear that f_v can have eigenvalue one for all M_u if and only if $v = 0, \infty$. Thus only the span of f_0 and f_∞ consists of eigenvectors of eigenvalue one for all M_u. They are the only candidates for being in $\mathfrak{h}_\infty$ within a given irreducible component. But by dimension counting, we see that $\mathfrak{h}_\infty$ must be exactly as described by the lemma. □

Note 2.1.1 In the case that $q = p$, the above proof actually shows that $M = M_1$ (which will now generate all the M_u) is regular and so part (4) of Theorem 2.1.1 is superfluous.

Let us make the following definition:

Definition 2.1.2 *For m an exponent and $u \in \mathbf{P}^1(\mathbf{F}_q)$, define $\mathfrak{h}_u^{(m)}$ to be the subspace*

$$\mathfrak{h}_u^{(m)} = \mathfrak{h}_u \bigcap \textit{(the irreducible component of) } V_{\pi_m}.$$

For $u \in \mathbf{F}_q^*$ and $m \neq h/2$ an exponent, define $h_u^{(m)} \in \mathfrak{h}_u^{(m)}$ to be

$$h_u^{(m)} = N_{\frac{-1}{u}} f_0^{(m)}.$$

Also put $h_\infty^{(m)} = f_0^{(m)}$ and $h_0^{(m)} = S f_0^{(m)}$. Note: *whenever we have a given π_m in mind, we will omit the superscript (m).*

Using Theorem 1.1.2, it is easy to check that since $f_0 = \sum_{z \in \mathbf{F}_q} e_z$,

$$h_u = \pi(u) e_\infty + \sum_{z \in \mathbf{F}_q, z \neq u} \pi_m(\frac{u}{u-z}) e_z$$

for $u \in \mathbf{F}_q^*$ and

$$h_0 = e_\infty + \sum_{z \in \mathbf{F}_q^*} \pi(\frac{-1}{z}) e_z$$

$$h_\infty = \sum_{z \in \mathbf{F}_q} e_z.$$

It is now easy to write down an explicit basis for each $\mathfrak{h}_u$.

Corollary 2.1.1 *Each $\mathfrak{h}_u$ is equal to the direct sum of the $\mathfrak{h}_u^{(m)}$ where m ranges over the exponents of $\mathfrak{g}$ less than or equal to $h/2$. For a given m, an explicit basis for $\mathfrak{h}_u$ is given by*

$$e_u^{(m)} \textit{ and } h_u^{(m)}$$

if $m \neq h/2$ and

$$N_{-1/u}(\Gamma_{0,1} f_0 \pm e_\infty) = \Gamma_{0,1} h_u \pm \pi(u)^{-1} e_u$$

otherwise with the ± according to Lemma 2.1.2.

Proof. This follows immediately from the Definitions 2.1.1 and 2.1.2 and Lemma 2.1.2 since

$$N_{-1/u} f_\infty = \pi(1/u) e_u \text{ and } N_{-1/u} f_0 = h_u.$$

□

2.2 Requirements for the A Decomposition

Let us consider the problem of attempting to decompose $\mathfrak{g}$ into a direct sum of $h+1$ Cartans that will be invariant under A (see Equation 1.3). In other words, since $A\mathfrak{h}_u = \mathfrak{h}_{u/\lambda}$ (see Sections 1.1 and 2.2), we want to know if there is a subset $P_A \subset \mathsf{P}^1(\mathsf{F}_q)$ invariant under multiplication by λ such that *as vector spaces* we have

$$\mathfrak{g} = \bigoplus_{u \in P_A} \mathfrak{h}_u. \tag{2.1}$$

It will turn out the the answer to this question is directly related to some results in number theory.

Since we will be dealing with some sort of A invariance, it is natural to introduce the the following notation for a particular basis of eigenvectors for A.

Definition 2.2.1 *Fix m an exponent of G, $m \neq h/2$, and write $\zeta = e^{2\pi i/h}$. Then for $k = 0, 1, \ldots, h-1$ and $u \in \mathsf{F}_q^*$, let $v_{u,k}^{(m)}$ and $v_{\lambda u,k}^{(m)}$ be as follows.*

$$\begin{aligned} v_{u,k}^{(m)} &= \sum_{l=1}^{h} \zeta^{-lk} A^l e_u^{(m)} = \sum_{l=1}^{h} \zeta^{l(m-k)} e_{u\lambda^{-2l}}^{(m)} \\ v_{\lambda u,k}^{(m)} &= \sum_{l=1}^{h} \zeta^{-lk} A^k e_{\lambda u}^{(m)} = \sum_{l=1}^{h} \zeta^{l(m-k)} e_{u\lambda^{1-2l}}^{(m)}. \end{aligned}$$

From this, it is clear that for any fixed u, $v_{u,k}^{(m)}$ and $v_{\lambda u,k}^{(m)}$ are distinct eigenvectors for A of eigenvalue ζ^k. If we note that $e_0^{(m)}$ and $e_\infty^{(m)}$ are also eigenvectors for A of eigenvalue $\pi_m(\lambda) = \zeta^m$ and $\pi_m(\lambda)^{-1} = \zeta^{-m}$, respectively, then it is clear that the set $\{v_{u,k}^{(m)}, v_{\lambda u,k}^{(m)}, e_0^{(m)}, e_\infty^{(m)} \mid k = 0, \ldots, h-1;$ m ranging over the exponents of $\mathfrak{g} \leq h/2\}$ is a basis for $\mathfrak{g}$ consisting of eigenvectors of A.

As always, when working with an understood π_m, these superscripts will always be suppressed.

Note 2.2.1 Note that the apparent choice of u in the above definition is quite unimportant. In fact, it is easy to check that for $t \in \mathsf{F}_q^*$:

$$v_{t^2x,k}^{(m)} = \pi_{m-k}(t)\, v_{x,k}^{(m)}$$

by writing $t = \lambda^r$ for some $r \in \mathbf{Z}$ and substituting $u = \lambda^{2r}x$ into the above definition:

$$v_{\lambda^{2r}x,k} = \sum_{l=1}^{h} \zeta^{l(m-k)} e_{x\lambda^{-2(l-r)}}$$

$$\begin{aligned} &= \sum_{l'=1}^{h} \zeta^{(l'+r)(m-k)} e_{x\lambda^{-2l'}} \\ &= \zeta^{r(m-k)} v_{x,k}. \end{aligned}$$

But since $\pi_1(\lambda^r) = \zeta^r$ and $\pi_a^b = \pi_{ab}$, the result follows. Thus, for instance, we see that each $v_{u,k}$ is just a non-zero multiple of either $v_{1,k}$ or $v_{\lambda,k}$ depending whether u is a square or not in F_q^*.

Note 2.2.2 Due to the A invariance of each V_{π_m} and Corollary 2.1.1, the question of being able to satisfy Equation 2.1 reduces to being able to satisfy the similar equation within each V_{π_m}. Namely, it is enough to know whether there is a subset $\mathcal{P}_A \subset \mathsf{P}^1(\mathsf{F}_q)$ stable under multiplication by λ such that

$$V_{\pi_m} = \bigoplus_{u \in \mathcal{P}_A} \mathfrak{h}_u^{(m)} \tag{2.2}$$

for each exponent $m \neq h/2$ and similarly for the irreducible component of $V_{\pi_{h/2}}$ if $h/2$ is an exponent.

Let us fix an exponent, m, of G not equal to $h/2$. We will need to define the following numbers that will play a crucial role in our analysis of an A invariant decomposition.

Definition 2.2.2 *For $i = 1,2$, let ψ_i be multiplicative characters of F_q^*. For each $\epsilon \in \mathsf{F}_q^*$ define $c(\psi_1, \psi_2, \epsilon) \in \mathbf{C}$ by*

$$c(\psi_1, \psi_2, \epsilon) = \sum_{x \in \mathsf{F}_q^*, 1-\epsilon x^2 \neq 0} \psi_1(1 - \epsilon x^2)\psi_2(x^2).$$

To get at this number, let us cite some elementary facts from classical number theory. The following definition and theorem are well known, e.g., see [11] chapter 8 §2 and §3.

Definition 2.2.3 *Recall that χ was a fixed non-trivial additive character on F_q. For ψ a multiplicative character on F_q^*, the* Gauss sum *$g(\psi)$ is defined as:*

$$g(\psi) = \sum_{a \in \mathsf{F}_q^*} \chi(a)\psi(a).$$

(Note that $g(\pi)$ is basically our old $q\Gamma_{0,1}$.)

Next, for $i = 1,2$, let ψ_i be multiplicative characters of F_q^*. Then the Jacobi sum *$J(\psi_1, \psi_2)$ is defined as:*

$$J(\psi_1, \psi_2) = \sum_{a+b=1, a,b \in \mathsf{F}_q^*} \psi_1(a)\psi_2(b).$$

Lastly, the Legendre symbol *ρ is the unique non-trivial multiplicative character on F_q^* of order two. It returns $+1$ on the squares and -1 on the non-squares.*

Theorem 2.2.1 *For the finite field F_q and multiplicative characters ψ and ψ_i, $i = 1, 2$,*
(1) if $\psi \neq 1$, $\mid g(\psi) \mid = \sqrt{q}$
(2) if $\psi \neq 1$, $J(1, \psi) = J(\psi, 1) = 0$ and $J(\psi, \psi^{-1}) = -\psi(-1)$
(3) if ψ_i and $\psi_1\psi_2$ are non-trivial, $\mid J(\psi_1, \psi_2) \mid = \sqrt{q}$
(4) if ψ_i and $\psi_1\psi_2$ are non-trivial,

$$J(\psi_1, \psi_2) = \frac{g(\psi_1)g(\psi_2)}{g(\psi_1\psi_2)}.$$

□

We can now check the following lemma.

Lemma 2.2.1 *Recalling that ρ is the Legendre symbol, we have:*

$$c(\psi_1, \psi_2, \epsilon) = \psi_2^{-1}(\epsilon)[J(\psi_1, \psi_2) + \rho(\epsilon)J(\psi_1, \rho\psi_2)].$$

Proof. This is checked by evaluating the definitions. Below we will make use of the substitutions $a = 1 - b$ and $b = \epsilon y$ and the fact that $(1 + \rho)/2$ is one on squares and zero on non-squares.

$$\begin{aligned}
c(\psi_1, \psi_2, \epsilon) &= \sum_{x \in \mathsf{F}_q^*, 1 - \epsilon x^2 \neq 0} \psi_1(1 - \epsilon x^2)\psi_2(x^2) \\
&= 2 \sum_{y \in \mathsf{F}_q^{*2}, 1 - \epsilon y \neq 0} \psi_1(1 - \epsilon y)\psi_2(y) \\
&= 2 \sum_{y \in \mathsf{F}_q^*, 1 - \epsilon y \neq 0} \frac{1 + \rho(y)}{2}\psi_1(1 - \epsilon y)\psi_2(y) \\
&= 2 \sum_{a, b \in \mathsf{F}_q^*, a + b = 1} \frac{1 + \rho(b/\epsilon)}{2}\psi_1(a)\psi_2(b/\epsilon) \\
&= \psi_2^{-1}(\epsilon)[J(\psi_1, \psi_2) + \rho(\epsilon)^{-1}J(\psi_1, \rho\psi_2)].
\end{aligned}$$

□

To apply this to the case at hand, we will need to make one more note.

Note 2.2.3 Recall that for $k \in \mathbb{Z}$, π_k was defined on F_q^* by setting $\pi_k(\lambda) = \zeta^k$ where λ was our fixed generator of F_q^* and $\zeta = e^{2\pi i/h}$. Since $h = (q - 1)/2$, this insures that

$\pi_k(-1) = 1$. In the future, we will want to take a "square root" of π_k. The choice can be made well defined by putting $\xi = e^{2\pi i/(2h)} = e^{2\pi i/(q-1)}$ and defining the *square root* of π_k, written $\pi_{k/2}$, to be the multiplicative character of F_q^* defined by setting $\pi_{k/2}(\lambda) = \xi^k$. In passing, we note that the other "square root" will be $\rho\pi_{k/2}$.

Next we will state the theorem that ties the basic number theory into our discussion.

Theorem 2.2.2 *Recall that m is a fixed exponent $(m \neq h/2)$ and everything is taking place within V_{π_m}. Then for $u \in \mathsf{F}_q^*$,*

$$h_u = e_0 + \pi_m(u)e_\infty + \frac{1}{2h}\sum_{k=1}^{h}[c(\pi_{-m}, \pi_{\frac{m-k}{2}}, 1)v_{u,k} + c(\pi_{-m}, \pi_{\frac{m-k}{2}}, \lambda)v_{\lambda u,k}].$$

Proof. Recalling Definition 2.1.2 and Theorem 1.1.2, we have for $u \in \mathsf{F}_q^*$,

$$\begin{aligned} h_u &= N_{-1/u}f_0 \\ &= N_{-1/u}\sum_{x\in\mathsf{F}_q} e_x \\ &= \pi_m(-u)e_\infty + \sum_{x\in\mathsf{F}_q, x\neq -u} \pi_m(\frac{x+u}{u})e_{\frac{ux}{x+u}} \\ &= \pi_m(u)e_\infty + \sum_{x'\in\mathsf{F}_q, x'\neq u} \pi_m(\frac{u}{u-x'})e_{x'} \qquad (2.3) \end{aligned}$$

where we have used the substitution $x' = \frac{xu}{x+u}$ above which may be written as $x = \frac{x'u}{u-x'}$. However, let us note the following:

$$\begin{aligned} \sum_{n=1}^{h}\zeta^{kn}v_{x,n} &= \sum_{n=1}^{h}\sum_{l=1}^{h}\zeta^{kn}\zeta^{l(m-n)}e_{x/l^{2l}} \\ &= \sum_{l=1}^{h}\zeta^{lm}e_{x/l^{2l}}\sum_{n=1}^{h}z^{n(k-l)} \\ &= \sum_{l=1}^{h}h\delta_{l=k}\zeta^{lm}e_{x/l^{2l}} \\ &= h\zeta^{mk}e_{x/l^{2k}} \\ &= hA^ke_x. \qquad (2.4) \end{aligned}$$

In particular, $e_x = \frac{1}{h}\sum_{n=1}^{h} v_{x,n}$. Substituting this into Equation 2.3 and making use of

Note 2.2.1 gives

$$\begin{aligned}
h_u &= \pi_m(u)e_\infty + \sum_{x\in\mathsf{F}_q, x\neq u} \pi_m(\frac{u}{u-x})\frac{1}{h}\sum_{k=1}^{h} v_{x,k} \\
&= \pi_m(u)e_\infty + e_0 + 1/h\sum_{k=1}^{h}\sum_{x\in\mathsf{F}_q^*, x\neq u} \pi_m(\frac{u}{u-x})v_{x,k} \\
&= \pi_m(u)e_\infty + e_0 + 1/h\sum_{k=1}^{h}\frac{1}{2}[\sum_{z\in\mathsf{F}_q^*, z^2\neq 1} \pi_m(\frac{u}{u-z^2u})v_{z^2u,k} + \sum_{z\in\mathsf{F}_q^*}\pi_m(\frac{u}{u-\lambda z^2u})v_{\lambda z^2u,k}] \\
&= \pi_m(u)e_\infty + e_0 + 1/h\sum_{k=1}^{h}\frac{1}{2}[\sum_{z\in\mathsf{F}_q^*, z^2\neq 1} \pi_m(\frac{u}{u-z^2u})\pi_{m-k}(z)v_{u,k} + \\
&\quad \sum_{z\in\mathsf{F}_q^*}\pi_m(\frac{u}{u-\lambda z^2u})\pi_{m-k}(z)v_{\lambda u,k}] \\
&= e_0 + \pi_m(u)e_\infty + \frac{1}{2h}\sum_{k=1}^{h}[c(\pi_{-m}, \pi_{\frac{m-k}{2}}, 1)v_{u,k} + c(\pi_{-m}, \pi_{\frac{m-k}{2}}, \lambda)v_{\lambda u,k}].
\end{aligned}$$

□

Note 2.2.4 Equation 2.4 also lets us write down a formula for the case $m \neq h/2$:

$$N_{-1/u}(\Gamma_{0,1}f_0 \pm e_\infty) = \Gamma_{0,1}h_u \pm \frac{\pi(u)^{-1}}{h}\sum_{k=1}^{h} v_{u,k}.$$

Coupled with Theorem 2.2.2 to write h_u in terms of $v_{u,k}$ and $v_{\lambda u,k}$, we will be able to decompose the vectors in the case of $m = h/2$.

With this done, we are in position to relate the number theoretic Jacobi sums too the question of decomposing $\mathfrak{g}$ into an A invariant sum of Cartans.

Theorem 2.2.3 *In the case where $h/2$ is not an exponent, we can write $\mathfrak{g} = \bigoplus_{u\in\mathcal{P}_A}\mathfrak{h}_u$ as an A invariant direct vector space sum of Cartans if and only if for each exponent m of G, we have*

$$J(\pi_{-m}, \pi_{\frac{m-k}{2}}) \neq J(\pi_{-m}, \rho\pi_{\frac{m-k}{2}})$$

for all $1 \leq k \leq h$.

Proof. First observe that A acting on $\mathsf{P}^1(\mathsf{F}_q)$ consists of four orbits: $F_0 = \{0\}$, $F_\infty = \{\infty\}$, $F_1 = \{u^2 \mid u \in \mathsf{F}_q^*\}$, and $F_\lambda = \lambda F_1$. Obviously the order of the first two is one and the order of the second two is h. Since A permutes the $\mathfrak{h}_u$, $u \in \mathsf{P}^1(\mathsf{F}_q)$, according to its action on the subscripts, F_0, F_∞, F_1, and F_λ will also describe the orbits of A on the $q+1$ Cartans. If we were to have $\mathfrak{g}$ written as an A invariant direct sum of Cartans as in Equation 2.1, then just by counting dimensions we see that $\mathcal{P}_A$ must consist of one orbit of order one and one orbit of order h. Since the following argument will be true for any of the 2^2 possible combinations of F_0, F_∞, F_1, and F_λ for $\mathcal{P}_A$, let us pick (say) $\mathcal{P}_A = F_\infty \bigcup F_1$ for definiteness and check the theorem in this case (though at the end we will see that the only important distinction between the various $\mathcal{P}_A$'s is whether they contain the element 1 or λ).

As previously noted, it suffices to check this statement for each V_{π_m} for each fixed exponent, m. Fix such an $m \neq h/2$. Corollary 2.1.1 tells us that $\mathfrak{h}_u$ is spanned by e_u and h_u. Thus if we let $V_A \subseteq \mathfrak{g}$ be the A invariant vector space

$$V_A = span\{\mathfrak{h}_u | u \in \mathcal{P}_A\},$$

then $V_A = span\{e_x, h_x \mid x \in \mathsf{F}_q^{*2} \bigcup \infty\}$. Since V_A is A invariant, it will be spanned by eigenvectors of A. Thus the question of whether V_A can be equal to $\mathfrak{g}$ reduces to deciding if the vectors e_0, e_∞, $v_{1,k}$, and $v_{\lambda,k}$ are in V_A for every $k = 0, \ldots (h-1)$.

To begin with, V_A contains the $span\{h_\infty, e_x \mid x \in \mathsf{F}_q^{*2} \bigcup \infty\}$. Call this space $V_1 \subseteq V_A$ so that (see Definition 2.2.1 and 2.1.2) V_1 equals the $span\{e_\infty, h_\infty, v_{1,k} \mid k = 0, \ldots (h-1)\}$. This gives us (by $h_\infty = f_0 = e_0 + v_{1,0} + v_{\lambda,0}$ and Definition 2.1.2)

$$V_1 = span\{e_\infty,\ e_0 + v_{\lambda,0},\ v_{1,k} \mid k = 0, \ldots (h-1)\}.$$

Thus the question of whether V_A can be equal to $\mathfrak{g}$ now reduces to deciding if each $v_{\lambda,k}$ is in V_A for every $k = 0, \ldots (h-1)$.

Now V_A is equal to the span of $V_1 \bigcup \{h_x \mid x \in \mathsf{F}_q^{*2}\}$, but by Theorem 2.2.2, we have

$$h_u = e_0 + \pi_m(u) e_\infty + \frac{1}{2h} \sum_{k=1}^{h} [c(\pi_{-m}, \pi_{\frac{m-k}{2}}, 1) v_{u,k} + c(\pi_{-m}, \pi_{\frac{m-k}{2}}, \lambda) v_{\lambda u,k}].$$

Thus, by what we know of V_1 and Note 2.2.1,

$$V_A = \ span\ V_1 \bigcup \{e_0 + \frac{1}{2h} \sum_{k=0}^{h-1} c(\pi_{-m}, \pi_{\frac{m-k}{2}}, \lambda) v_{\lambda u,k} \mid u \in \mathsf{F}_q^{*2}\}.$$

In fact, we will see that the complicated sums in the above expression are more or less A translates of one another (generically by the fact that $A\mathfrak{h}_u = \mathfrak{h}_{u/\lambda^2}$). We will next extract this information with more care.

By Note 2.2.1 and taking $u = \lambda^{2r}$ for $r = 0, \dots (h-1)$,

$$V_A = \ span\ V_1 \bigcup \{e_0 + \frac{1}{2h}\zeta^{rm} \sum_{k=0}^{h-1} c(\pi_{-m}, \pi_{\frac{m-k}{2}}, \lambda)\zeta^{-rk} v_{\lambda,k} \mid r = 0, \dots (h-1)\}.$$

Since $A^s v_{\lambda,k} = \zeta^{sk} v_{\lambda,k}$, we see that we have

$$\begin{aligned} V_A &= \ span\ V_1 \bigcup \{e_0 + \frac{1}{2h}\zeta^{rm} A^{-r} \sum_{k=0}^{h-1} c(\pi_{-m}, \pi_{\frac{m-k}{2}}, \lambda) v_{\lambda,k} \mid r = 0, \dots (h-1)\} \\ &= \ span\ V_1 \bigcup \{\pi_m(\lambda^r) A^{-r}[e_0 + \frac{1}{2h} \sum_{k=0}^{h-1} c(\pi_{-m}, \pi_{\frac{m-k}{2}}, \lambda) v_{\lambda,k}] \mid r = 0, \dots (h-1)\}. \end{aligned}$$

But let us extract the constituent eigenvectors of these A translates. By observing that they are expressed as the sum of eigenvectors under A and using, say, the operators $\sum_k \zeta^{-nk} A^k$ for each n we get:

$$V_A = \ span\ V_1 \bigcup \{e_0 + \frac{1}{2h} c(\pi_{-m}, \pi_{\frac{m}{2}}, \lambda) v_{\lambda,0},\ c(\pi_{-m}, \pi_{\frac{m-k}{2}}, \lambda) v_{\lambda,k} \mid k = 1, \dots (h-1)\}.$$

Thus we arrive at

$$\begin{aligned} V_A \ = \ & span\{e_\infty,\ v_{1,k_1},\ e_0 + v_{\lambda,0},\ e_0 + \frac{1}{2h} c(\pi_{-m}, \pi_{\frac{m}{2}}, \lambda) v_{\lambda,0},\ c(\pi_{-m}, \pi_{\frac{m-k_\lambda}{2}}, \lambda) v_{\lambda,k_\lambda} \mid \\ & k_1 = 0, \dots (h-1),\ k_\lambda = 1, \dots (h-1)\}. \end{aligned} \tag{2.5}$$

If

$$1 \ \neq \ \frac{1}{2h} c(\pi_{-m}, \pi_{\frac{m}{2}}, \lambda), \tag{2.6}$$

we get from Equation 2.5 that V_A is the span of

$$\begin{gathered} \{e_0,\ e_\infty,\ v_{1,k_1},\ v_{\lambda,k_\lambda} \mid k_1, k_\lambda = 0, \dots (h-1) \\ \text{such that } k_\lambda \text{ satisfies } c(\pi_{-m}, \pi_{\frac{m-k_\lambda}{2}}, \lambda) \neq 0\}. \end{gathered} \tag{2.7}$$

We note that by Definition 2.2.1, Note 2.2.2, and Lemma 2.2.1 (using the fact that λ is never a square in F_q^*), we observe that Equation 2.7 finishes the proof of the theorem. All that remains is to verify Equation 2.6 which we will do next.

To verify Equation 2.6, we will make use of the fact that $q = 2h+1$ and $m \neq h/2$. We will also use Lemma 2.2.1 and Theorem 2.2.1 parts (2) and (3). As a general preliminary, let ψ_i, $i = 1, 2$, be multiplicative characters of F_q^* such that ψ_i and $\psi_1\psi_2$ are non-trivial.

Then we have

$$\mid \frac{c(\psi_1, \psi_2, \epsilon)}{2h} \mid \leq \frac{\mid J(\psi_1, \psi_2) \mid + \mid J(\psi_1, \rho\psi_2) \mid}{2h} = \frac{\sqrt{2h+1}}{h}.$$

However, it is easily checked that for $h \geq 3$, $\frac{\sqrt{2h+1}}{h} < 1$ (in fact, equality occurs only at $1 \pm \sqrt{2}$).

When we return to our specifics, we are concerned with $\psi_1 = \pi_{-m}$ and $\psi_2 = \pi_{\frac{m-k}{2}}$. Since $1 \leq m \leq h/2$, we know that $\pi_{-m} \neq 1$. Hence it is easy to see that the conditions $\pi_{-m}, \pi_{\frac{m-k}{2}}, \pi_{-m}\pi_{\frac{m-k}{2}} \neq 1$ amount to the condition that $k \neq \pm m \pmod h$. Using $m \neq h/2$, we may assume that $h \geq 3$. Thus by the above generalities, we have checked Equation 2.6 in the cases where $k \neq \pm m \pmod h$. We will check these two remaining cases separately in the next paragraphs.

In the case where $k = m$, we get: $c(\pi_{-m}, \pi_0, \lambda) = 1(0 - J(\pi_{-m}, \rho))$. Since $m \neq h/2$ (which would correspond to the character $\rho = \rho^{-1}$), $\mid J(\pi_{-m}, \rho) \mid = \sqrt{q}$ and the previous arguments will apply to an even greater degree to check Equation 2.6 in this case.

Finally, in the case where $k = -m$, we get: $c(\pi_{-m}, \pi_m, \lambda) = \pi_m^{-1}(\lambda)(-\pi_{-m}^{-1}(-1) - J(\pi_{-m}, \rho\pi_m))$. Again, $\mid J(\pi_{-m}, \rho\pi_m) \mid = \sqrt{q}$ and by similar arguments as above, we have checked Equation 2.6 in the final case and completed our proof. □

Actually, we have proved more. We state a corollary of the proof:

Corollary 2.2.1 *Let $m \neq h/2$ be an exponent of G and $\mathcal{P}_A \subseteq \mathsf{P}^1(\mathsf{F}_q)$ an A stable subset of order $h+1$. Let*

$$V_A \;=\; span\{\mathfrak{h}_u^{(m)} | u \in \mathcal{P}_A\}. \tag{2.8}$$

Then if $1 \in \mathcal{P}_A$

$$\begin{aligned} V_A \;=\; & \{e_0,\, e_\infty,\, v_{1,k_1},\, v_{\lambda,k_\lambda} \mid k_1, k_\lambda = 0, \ldots (h-1) \\ & \textit{such that } k_\lambda \textit{ satisfies } c(\pi_{-m}, \pi_{\frac{m-k_\lambda}{2}}, \lambda) \neq 0\} \end{aligned}$$

else if $\lambda \in \mathcal{P}_A$

$$\begin{aligned} V_A \;=\; & \{e_0,\, e_\infty,\, v_{1,k_1},\, v_{\lambda,k_\lambda} \mid k_1, k_\lambda = 0, \ldots (h-1) \\ & \textit{such that } k_1 \textit{ satisfies } c(\pi_{-m}, \pi_{\frac{m-k_1}{2}}, \lambda) \neq 0\}. \end{aligned}$$

In particular, $V_A = V_{\pi_m}$ and Equation 2.8 is a direct sum of vector spaces if and only if all the $c(\pi_{-m}, \pi_{\frac{m-k}{2}}, \lambda)$ do not vanish or equivalently if all

$$J(\pi_{-m}, \pi_{\frac{m-k}{2}}) \neq J(\pi_{-m}, \rho\pi_{\frac{m-k}{2}})$$

for $1 \leq k \leq h$.

Proof. See the proof of Theorem 2.2.3 in which all of the above is either proved or proved analogously. □

Note 2.2.5 For the case $m = h/2$, we check Equation 2.8 will always yield $V_A = V_{\pi_{h/2}}$. Making use of Note 2.2.4, we have

$$\begin{aligned} N_{-1/u}(\Gamma_{0,1}f_0 \pm e_\infty) &= \Gamma_{0,1}e_0 + \pi_{h/2}(u)\Gamma_{0,1}e_\infty \\ &\quad + \frac{1}{2h}\sum_{k=0}^{h-1}[(\Gamma_{0,1}c(\pi_{-h/2}, \pi_{\frac{h/2-k}{2}}, 1) \pm 2\pi_{h/2}(u)^{-1})v_{u,k} + \\ &\quad \Gamma_{0,1}c(\pi_{-h/2}, \pi_{\frac{h/2-k}{2}}, \lambda)v_{\lambda u,k}]. \end{aligned}$$

Then by decomposing these into eigenvectors for A as in Theorem 2.2.3 and making use of the fact that each $\mathfrak{h}_u^{(h/2)}$ is now only one dimensional, we see that $V_A = V_{\pi_{h/2}}$ unless both of the following are zero:

$$\Gamma_{0,1}c(\pi_{-h/2}, \pi_{\frac{h/2-k}{2}}, 1) \pm 2\pi_{h/2}(u)^{-1} \quad \text{and}$$

$$\Gamma_{0,1}c(\pi_{-h/2}, \pi_{\frac{h/2-k}{2}}, \lambda).$$

However, using Lemma 2.2.1 and Theorem 2.2.1, it is trivial to see that this is not possible. Hence, the exponent $m = h/2$ (if it is an exponent) will never provide a stumbling block to an A invariant decomposition.

2.3 A Result on Jacobi Sums

In this section we will recall the basic number theory result on determining the prime decomposition of a Gauss sum called the *Stickelberger Relation.* Actually all we will need is a related result on the Jacobi sums. It will enable us to give some explicit information about an A invariant decomposition. Again, the proofs are standard and so will be omitted. A reference for the material in this section is [11] chapter 14.

Definition 2.3.1 *Let* $q = p^f$ *be an odd prime power and* $\xi = e^{\frac{2\pi i}{q-1}}$. *Denote by* D_{q-1} *the ring of integers in* $\mathbb{Q}(\xi)$. *Let* $\mathfrak{B}$ *be a certain prime ideal in* D_{q-1} *lying over* $p\mathbb{Z}$ *in* $\mathbb{Z}$. *Let* ω_m *be the multiplicative character of* $\mathbb{F}_q^*$ *defined on the generator* λ *by* $\omega_m(\lambda) = \xi^m$ *and write* $J(\omega_n, \omega_m)$ *as usual for the Jacobi sum.* Note: *our old* π_m *is* ω_{2m} *in the new notation and our old* $\pi_{\frac{m-k}{2}}$ *is* ω_{m-k}.

Theorem 2.3.1 *Let $1 \leq n, m < q-1$. Then $J(\omega_{-n}, \omega_{-m}) \in D_{q-1}$ and moreover, modulo $\mathfrak{B}$, we have:*

$$J(\omega_{-n}, \omega_{-m}) = -\frac{(m+n)!}{n!\,m!} \quad (\mathfrak{B}).$$

Proof. See for instance [11] chapter 14 exercise 1. □

2.4 The A Invariant Decomposition

In this section we will resolve the question of the existence of an A invariant decomposition of $\mathfrak{g}$ in terms of the $\mathfrak{h}_u$ for the rank two and exceptional groups.

For this it will be easiest to check the following lemma first. The lemma is of obvious importance in light of Theorem 2.3.1. In fact, it is precisely the case for $n = 2$.

Lemma 2.4.1 *Let $q = p^f$ be an odd prime power and recall that $h = \frac{q-1}{2}$. For $1 \leq m < q-1$, in the equations below write the symbol "±" to signify "+" if $m + h < q - 1$ and "–" otherwise. Then modulo $p\mathbb{Z}$, the equality*

$$\frac{(m+2)!}{m!\,2!} = \frac{(m \pm h + 2)!}{(m \pm h)!\,2!} \quad (p)$$

holds if and only if

$$2m + 2 \pm h = 2h \quad (p).$$

Proof. Using the fact that $\mathbb{Z}/p\mathbb{Z}$ is a field and the constraints upon m, the above equality reduces to checking *mod* (p) that:

$$(m+2)(m+1) = (m \pm h + 2)(m \pm h + 1).$$

After one expands this and subtracts the left side from the right, it reduces to:

$$\pm h(2m + 3 \pm h) = 0.$$

The fact that $2h = q - 1 = p^f - 1 = -1$ mod (p) assures us that $h \neq 0$. It also lets us rewrite the equation using $1 = -2h$ (p) to get

$$2m + 2 - 2h \pm h = 0$$

which finishes the proof. □

We will also need this well known fact on Jacobi sums.

Lemma 2.4.2 *Given ψ_i multiplicative characters of F_q^*, then*

$$J(\psi_1, \psi_2) = \psi_1(-1) J(\psi_1, \psi_1^{-1}\psi_2^{-1}).$$

Proof. The idea is that in the expression

$$J(\psi_1, \psi_2) = \sum_{t \in \mathsf{F}_q} \psi_1(t)\psi_2(1-t),$$

one makes the change of variables

$$t = \frac{-t'}{1-t'}.$$

Since this is standard and simple, we omit the rest of the details. □

Corollary 2.4.1 *With the notation of Definition 2.3.1 and $1 \leq m < q-1$ (with the ± convention of Lemma 2.4.1),*

$$J(\pi_1, \omega_m) \neq J(\pi_1, \rho\omega_m)$$

if

$$2m + 2 \pm h \neq 2h \ \ (p).$$

However for $1 \leq n \leq h$,

$$J(\pi_n, \omega_m) = J(\pi_n, \rho\omega_m)$$

if

$$2m + 2n \pm h = 0 \ \ (q-1).$$

Proof. Recall that $\pi_n = \omega_{2n}$. Then the first part is a corollary of Lemma 2.4.1 and Theorem 2.3.1 (using $\overline{\omega_x} = \omega_{-x}$, $\mathfrak{B} \bigcap \mathbf{Z} = p\mathbf{Z}$, and $(m+n)!/(n!\, m!) \in \mathbf{Z}$). For the second, note that ω is of order $q-1$ and that $\pi_n(-1) = 1$. Then we apply Lemma 2.4.2 and solve the equation $\omega_n^{-1}\omega_m^{-1} = \rho\omega_m$. □

Corollary 2.4.2 *Let $1 \leq k \leq h$. Then recalling Definition 2.2.2,*

$$c(\pi_{-1}, \pi_{\frac{1-k}{2}}, \lambda) \neq 0$$

if

$$2k \neq h \ \ (p).$$

Moreover,

$$c(\pi_{-1}, \pi_{\frac{1-k}{2}}, \lambda) = 0$$

if

$$2k = h \quad (q-1).$$

Lastly, for $h \geq 3$, if $q = p^1$ and $1 \leq m \leq h$ is such that $(m,h) = 1$ (that is m and h are relatively prime), then

$$c(\pi_{-m}, \pi_{\frac{m-k}{2}}, \lambda) = 0$$

if and only if h is even and

$$2k = h \quad (\text{exactly}) \ .$$

Proof. The first and second part will just evoke Corollary 2.4.1 and Lemma 2.2.1. To see this for the first part, observe first that by Theorem 2.2.1 part (2) and (3) and Lemma 2.2.1, the first statement is automatically true for $k = 1$. Hence, we may assume $1 < k \leq h$. Now recall that $\pi_{\frac{1-k}{2}} = \omega_{-(k-1)}$ and use $m = k - 1$ in Corollary 2.4.1. Since $1 < k \leq h$, we have $1 \leq m < h$. This will imply that the ± will be a + since we will also have $m + h < 2h = q - 1$. Then the criterion from Corollary 2.4.1 reduces to

$$2(k-1) + 2 + h \neq 2h \ (p)$$

which will reduce to the desired result.

To see that the second part is true, just use the substitutions $m = 1 - k$ and $n = 2$ along with the fact that $2h$ is congruent to 0 modulo $q - 1$.

For the third part, let us first prove it for $m = 1$. As before, we may assume that $1 < k \leq h$. Since $p = q$, there is at most a unique solution to $2k = h\ (p)$ for $1 < k \leq h < p$. Thus by the first two parts of this Corollary and by the range of k, we see that $c(\pi_{-1}, \pi_{\frac{1-k}{2}}, \lambda)$ will be zero if and only if $2k = h\ (p)$ with $1 < k \leq h$. If h is even, then $k = h/2$ is the only time this happens. However, if h is odd, then it is easy to check that the the solution to $2k = h\ (p)$ must have $h < k < p$ which is not allowable. Thus we have finished the last part in the case of $m = 1$. (Actually, one may observe that the distinction between k and $k + h$ does not matter at all because it amounts to picking a different square root of π_{1-k} which will only switch the sign of the corresponding c. One can check through similar reasoning that if $h < k < p - 1$, then the new criterion would come down to solving $2k = 3h\ (p)$. But again, since $2h < 2k, 3h < 4h$ with $4h - 2h = 2h = p - 1$, we see that this cannot be solved for h odd and $h < k < p - 1$.)

For the general case, we simply apply the elements of the Galois group $Gal(\mathbf{Q}(e^{2\pi i/(p-1)})/\mathbf{Q})$. □

Let us record in Table 2.1 a list of the exponents, m_i, and Coxeter numbers, h, for the simple Lie algebras. Such information may be found in many places, e.g., [28].

With this we can state the theorem that tells us when an A invariant decomposition can be found in the case of the Rank Two and Exceptional Lie algebras. We also have

Table 2.1: Exponents and Coxeter Numbers

Type of $\mathfrak{g}$	$m_1, m_2, \ldots m_l$	h	$2h+1$
A_l	1,2,3,... l	$l+1$	$2l+3$
B_l,C_l	1,3,5,... $2l-1$	$2l$	$4l+1$
D_l	1,3,5,... $2l-1, l-1$	$2(l-1)$	$4l-3$
E_6	1,4,5,7,8,11	12	25
E_7	1,5,7,9,11,13,17	18	37
E_8	1,7,11,13,17,19,23,29	30	61
F_4	1,5,7,11	12	25
G_2	1,5	6	13

included the case of A_4 for later comparison (see Corollary 2.6.1).

Theorem 2.4.1 *Let G be one of the following: $A_2, B_2, G_2, A_4, F_4, E_6, E_7, E_8$. Write h for the Coxeter number and $q = 2h+1$. Then given Theorem 2.1.1 with $L_2(q) \hookrightarrow G$, let $\mathcal{P}_A$ be any of the four A stable subsets of order $h+1$ contained in $\mathsf{P}^1(\mathsf{F}_q)$.*

(1) For h odd, i.e, $G = A_2$ or A_4,

$$\mathfrak{g} = \bigoplus_{u \in \mathcal{P}_A} \mathfrak{h}_u \quad \textit{(as vector spaces)} .$$

In particular, an A invariant decomposition of Cartans exists.

(2) For h even, i.e., $G = B_2, G_2, F_4, E_6, E_7, E_8$, an A invariant decomposition does not exist so that $\mathfrak{g}$ may not be written as an A invariant direct sum of Cartans of the form $\mathfrak{h}_u, u \in \mathsf{P}^1(\mathsf{F}_q)$. In particular, if we write

$$\begin{aligned} V_A &= span\{\mathfrak{h}_u | u \in \mathcal{P}_A\} \\ &= span\{\mathfrak{h}_u^{(m)} | u \in \mathcal{P}_A, 1 \leq m \leq h/2 \textit{ exponents } \} \end{aligned}$$

and let θ be 1 if $1 \in \mathcal{P}_A$ and λ otherwise (in which case $\lambda \in \mathcal{P}_A$), then (using Definitions 2.2.1, 2.1.2, and 2.1.1):

(2a) For $G = B_2, G_2, F_4$ and E_8, the exponents are prime to h and $h/2$ is not an exponent. In this case:

$$\mathfrak{g} = V_A \bigoplus span\{v^{(m)}_{\lambda\theta, \frac{h}{2}} | 1 \leq m < h/2 \textit{ exponents } \}.$$

In particular, V_A "misses" being all of $\mathfrak{g}$ by a rank$(\mathfrak{g})/2$ dimensional subspace of the rank$(\mathfrak{g})$ dimensional negative one eigenspace of A.

(2b) For $G = E_7$, the exponents are prime to h, but $h/2$ is an exponent. In this case:

$$\mathfrak{g} = V_A \bigoplus span\{v^{(m)}_{\lambda\theta,\frac{h}{2}} | 1 \leq m < h/2 \textit{ exponents } \}.$$

Thus V_A "misses" being all of $\mathfrak{g}$ by a $(rank(\mathfrak{g})-1)/2$ dimensional subspace of the $rank(\mathfrak{g})$ negative one eigenspace of A.

(2c) For $G = E_6$, two exponents (4 and 8) are not prime to h, but $h/2$ is not an exponent. In this case:

$$\mathfrak{g} = V_A \bigoplus span\{v^{m}_{\lambda\theta,\frac{h}{2}},\ v^{(m_0)}_{\lambda\theta,0} | 1 \leq m < h/2,\ m_0 = 4 \textit{ exponents } \}.$$

Thus, V_A "misses" being all of $\mathfrak{g}$ by a $rank(\mathfrak{g})/2$ dimensional subspace of the $rank(\mathfrak{g})$ dimensional negative one eigenspace of A and *by a one dimensional subspace of the $rank(\mathfrak{g})$ dimensional positive one eigenspace of A.*

Proof. For part (1), simply apply Corollary 2.2.1 and the last part of Corollary 2.4.2.

For part (2a) with G equal to E_8 or G_2, the proof is immediate again from Corollary 2.2.1 and the last part of Corollary 2.4.2.

However, we will also need to invoke the first two parts of Corollary 2.4.2 to finish off the case of $G = B_2$, since for B_2, $q = 3^2$. For this case, we only have $m = 1$ and $1 \leq k \leq 4$. But one trivially checks that the first two parts of Corollary 2.4.2 are enough to completely finish off this case.

Lastly for $G = F_4$, the problem again arises since $q = 5^2$. One proceeds just as above for B_2, however one finds that one case (up to using the Galois group) is undetermined. Namely, the case that needs to be checked is for $m = 1$ and $k = 11$. However, for this case, one may explicitly write out and compute $J(\pi_{-m}, \omega_{k-m}) - J(\pi_{-m}, \rho\omega_{k-m})$. We omit the sum. The reader may check that the answer turns out to be $-2+4i$ which is definitely non-zero. This finishes F_4.

For part (2b), the only reason that it is not as trivial as E_8 and G_2 above, is that $h/2$ is an exponent of E_7. Thus only an *irreducible component* of $V_{\pi_{h/2}}$ appears in the decomposition of E_7 under $L_2(q)$. However, we have already noted in Note 2.2.5 that the $V_{\pi_{h/2}}$ component is never a problem to an A invariant decomposition. Thus as with E_8 and G_2 in part (2), the result is immediate.

For part (2c), two problems arise. The first is that $q = 5^2$ is not a prime and the second is that all the exponents of E_6 are not relatively prime to h. That q is not a prime conceivably could cause problems with the exponents that are prime to h. However, these possible problems have all already been accounted for in part (2) by the calculations for F_4. That leaves only the exponent $m = 4$ (up to the Galois action again) and $1 \leq k \leq h$. For these values, we wish to know exactly when $J(\pi_{-m}, \omega_{k-m}) - J(\pi_{-m}, \rho\omega_{k-m})$ is non-zero. As a first step, one may apply Theorem 2.3.1. The reader may check that the results of those computations check everything we need except for possibly $k = 6, 11$, and 12. As a last step, one explicitly writes out the difference of the Jacobi sums and finds that $k = 6$ and 12 yield zero (only 12 requires a computation since we already knew this for $k = 6$) while $k = 11$ yields a non-zero answer (approximately $7.348 - 2.449i$). This finishes the proof of theorem. □

2.5 The Element of Order $h + 1$

It is well known that $L_2(q)$ contains elements of order $h + 1$. We begin by recalling some basic facts about this element.

Theorem 2.5.1 *Let F_q be a finite field of $q = p^f$ elements, p an odd prime, with λ a fixed generator of F_q^*. Recall that $h = (q-1)/2$. Then:*
(1) $L_2(q)$ contains an element K of order $h + 1$.
(2) (After conjugation), one may realize $\langle K \rangle$, the cyclic group generated by K, as the set of all elements of the form

$$K_{\sigma,\nu} = \begin{pmatrix} \sigma & \nu \\ \lambda\nu & \sigma \end{pmatrix}$$

where $\sigma, \nu \in \mathsf{F}_q$ satisfy the equality

$$\sigma^2 - \lambda\nu^2 = 1.$$

Moreover, $K_{\sigma,\nu} = K_{\sigma',\nu'}$ if and only if $(\sigma, \nu) = \pm(\sigma', \nu')$.
(3) The $q + 1$ solutions to the equation $\sigma^2 - \lambda\nu^2 = 1$ may be parameterized by letting t vary over $\mathsf{P}^1(\mathsf{F}_q)$ and setting

$$\sigma = \frac{1 + \lambda t^2}{1 - \lambda t^2} \text{ and } \nu = \frac{2t}{1 - \lambda t^2}.$$

Conversely, given σ and ν, one may solve backwards with

$$t = \frac{\nu}{\sigma + 1}.$$

Proof. Since this is well known and only involves easy calculations, we will simply give convenient references. For part (1), one may consult [8] §38. For parts (2) and (3), see [26] §2.5. □

At this point, we have three special subgroups suggestively called $\mathcal{K}$, $\mathcal{A}$, and $\mathcal{N}$ of orders $h + 1$, h, and $2h + 1$, respectively. K generates $\mathcal{K}$, A (Equation 1.3) generates

$\mathcal{A}$, and N_{x_i} (Equation 1.4), $x_i \in \mathsf{F}_q^*$ for $1 \leq i \leq f$ such that the x_i form a basis for F_q over F_p, generate $\mathcal{N}$. We would like to be able to write down an "Iwasawa" $\mathcal{KAN}$ decomposition of $L_2(q)$. However, this is not quite true. In a sense we need two of them as we shall see. First we need some tools.

Definition 2.5.1 *We will call the set of all solutions (σ, ν) to the equation $\sigma^2 - \lambda\nu^2 = 1$ over the field F_q the* circle of radius one.

Define a map v taking the circle of radius one to $\mathsf{P}^1(\mathsf{F}_q)$ by

$$v(\sigma, \nu) = \frac{\lambda\nu}{\sigma}.$$

By the obvious identification, we will also extend the notion of v by letting v act on the set of $K_{\sigma,\nu}$ by setting $v(K_{\sigma,\nu}) = v(\sigma, \nu)$. It is clear that this is well defined by 2.5.1 part (2).

Lemma 2.5.1 *The map*

$$v : \{K_{\sigma,\nu} \mid (\sigma, \nu) \in \text{ circle of radius one } \} \rightarrow \mathsf{P}^1(\mathsf{F}_q)$$

is injective and thus

$$\mid image(v) \mid = h + 1 = \frac{q+1}{2}.$$

Moreover,

$$image(v) = \{-\lambda, \frac{2t\lambda}{1 + \lambda t^2} \mid t \in \mathsf{F}_q\}.$$

Proof. First we check that v is injective. Suppose $\lambda\nu/\sigma = \lambda\nu'/\sigma'$ where (σ, ν) and (σ', ν') are both on the circle of radius one. First of all, we see that $\sigma = 0$ if and only if $\sigma' = 0$. In this case, we then get $\nu^2 = \nu'^2 = -1/\lambda$ so that $\nu = \pm\nu'$. Thus, $K_{0,\nu} = K_{0,\nu'}$ and this case is done. Thus we may suppose that $\sigma \neq 0$. In this case, we may solve $\sigma^2 - \lambda\nu^2 = 1$ and get $\lambda\nu^2/\sigma^2 = 1 - 1/\sigma^2$ and similarly for (σ', ν'). Now our original equality, $\lambda\nu/\sigma = \lambda\nu'/\sigma'$, obviously implies that $\lambda\nu^2/\sigma^2 = \lambda\nu'^2/\sigma'^2$. Since we are in the case $\sigma \neq 0$, this then implies $1 - 1/\sigma^2 = 1 - 1/\sigma'^2$. Thus we have $\sigma = \pm\sigma'$. Then our original equality says that $\nu = \pm\nu'$ also. Thus (by Theorem 2.5.1) we have $K_{\sigma,\nu} = K_{\sigma',\nu'}$ and we have shown that v is injective. For the last part, simply apply part (3) of Theorem 2.5.1. □

Recall some of the material of Section 1.1. We have $\mathcal{AN} = \mathcal{B}$ the Borel of upper triangular matrices in $L_2(q)$ and recall that $L_2(q)/\mathcal{B}$ was identified with $\mathsf{P}^1(\mathsf{F}_q)$. To proceed, one may use the elementary decomposition:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{cases} \begin{pmatrix} 1 & 0 \\ \frac{c}{a} & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}\begin{pmatrix} 1 & \frac{b}{a} \\ 0 & 1 \end{pmatrix} & a \neq 0 \\ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} -b^{-1} & 0 \\ 0 & -b \end{pmatrix}\begin{pmatrix} 1 & -bd \\ 0 & 1 \end{pmatrix} & a = 0. \end{cases}$$

The reader may check this easily using $ad - bc = 1$. With this decomposition, the *residue* of the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $L_2(q)/\mathcal{B}$ (identified with $\mathsf{P}^1(\mathsf{F}_q)$) is simply the ratio c/a. Moreover, since each element of $\mathcal{B}$ is uniquely written in the form $\mathcal{AN}$, then by breaking up $L_2(q)$ into its $\mathcal{B}$ cosets, one sees that the above decomposition is unique. In other words, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in L_2(q)$ can be uniquely written in the form $M_{c/a}\mathcal{AN}$ (see Equation 1.5 and 1.6 and let $M_\infty = S$). It is now apparent why the map v was introduced.

Theorem 2.5.2 *Let s_0 be any fixed element in $\mathsf{P}^1(\mathsf{F}_q)$ not in the image of v (see Lemma 2.5.1). Then $L_2(q)$ admits an "Iwasawa" decomposition as follows. Every element of $L_2(q)$ may be uniquely written as either $\mathcal{KAN}$ or as $\mathcal{K}M_{s_0}\mathcal{AN}$ so that one has*

$$L_2(q) = \mathcal{KAN} \coprod \mathcal{K}M_{s_0}\mathcal{AN}$$

where $\coprod$ stands for disjoint union.

Proof. By the above discussion, we know that $K_{\sigma,\nu}\mathcal{B} = M_{v(\sigma,\nu)}\mathcal{B}$. As a result, the only question remaining for uniqueness of a $\mathcal{KB}$ decomposition is whether $v(K_{\sigma,\nu})$ is injective, but this has already been answered in Lemma 2.5.1. Moreover, by counting, we see that $\mathcal{KB}$ takes care of exactly half of $L_2(q)$-the order of $L_2(q)$ is $2(h+1)(h)(2h+1)$. Next, suppose $X \in \mathcal{KB} \bigcap \mathcal{K}M_{s_0}\mathcal{B}$. Then X may be written as $KB = K'M_{s_0}B'$. Rewriting yields $M_{s_0} = K''B''$. However, the left side is in a different coset of $L_2(q)/\mathcal{B}$ than the right side (by the choice of s_0). Hence, we must have $\mathcal{KB} \bigcap \mathcal{K}M_{s_0}\mathcal{B} = \emptyset$. Again by counting, we will finish the proof if we can show that when an element can be written in the form $\mathcal{K}M_{s_0}\mathcal{B}$, then it is unique.

To do this, it suffices to show that given (σ, ν) on the circle of radius one and $a \neq 0$ that the equality

$$\pm\begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix} = \begin{pmatrix} \sigma & \nu \\ \lambda\nu & \sigma \end{pmatrix}\begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix}\begin{pmatrix} a & n \\ 0 & a^{-1} \end{pmatrix}$$

can only be solved in the case of $\sigma, a = \pm 1$ and $\nu = n = 0$ (note that the ±'s arise since we are working in PSL instead of just SL). However, one can check that the right hand side multiplies out to give

$$\begin{pmatrix} a(\sigma + s\nu) & n(\sigma + s\nu) + a^{-1}\nu \\ a(\lambda\nu + s\sigma) & n(\lambda\nu + s\sigma) + a^{-1}\sigma \end{pmatrix}.$$

Thus we have four equations to solve. They are:

$$\begin{aligned} \pm 1 &= a(\sigma + s\nu) \\ \pm 0 &= n(\sigma + s\nu) + a^{-1}\nu \\ \pm s &= a(\lambda\nu + s\sigma) \\ \pm 1 &= n(\lambda\nu + s\sigma) + a^{-1}\sigma. \end{aligned}$$

The first and third tell us that $\pm a^{-1} = \sigma + s\nu$ and $\pm sa^{-1} = \lambda\nu + s\sigma$, respectively. Applying these to the second and fourth give us $a^{-1}(\pm n + \nu) = 0$ and $a^{-1}(\pm sn + \sigma) = \pm 1$, respectively. Thus we must have $\nu \pm n = 0$ and $a = \pm(\sigma \pm sn)$. Of course we then have $1 = aa^{-1} = (\sigma \pm sn)(\sigma + s\nu) = (\sigma - s\nu)(\sigma + s\nu) = \sigma^{-} s^2\nu^2$. But since $\sigma^2 - \lambda\nu^2 = 1$, this implies $1 = 1 + \nu^2(\lambda - s^2)$ which gives us either $\lambda = s^2$ or $\nu = 0$. The first is quite impossible since λ is a generator of F_q^* and so not a square. Thus we have $\nu = 0$. In turn, one then sees that this will give us $\sigma^2 = 1$ so that $\sigma = \pm 1$. This also will give that $a = \pm 1$ and $n = 0$ so we are done. □

2.6 The K Invariant Decomposition

In this section again assume we are in the setting of Kostant's conjecture 2.1.1 so that we have an embedding of $L_2(q) \hookrightarrow G$. By the previous section, we have a cyclic subgroup $\mathcal{K}$ of $L_2(q)$ of order $h+1$. As we did with the subgroup $\mathcal{A}$, we would like to examine the possibility of writing $\mathfrak{g}$ as a vector space direct sum

$$\mathfrak{g} = \bigoplus_{u \in \mathcal{P}_K} \mathfrak{h}_u \tag{2.9}$$

where $\mathcal{P}_K \subseteq \mathsf{P}^1(\mathsf{F}_q)$ is a $\mathcal{K}$ invariant subset. We note that since $\mid \mathsf{P}^1(\mathsf{F}_q) \mid = 2(h+1)$, there are two possible choices for $\mathcal{P}_K$.

Just as with $\mathcal{A}$, we will find that this is not always possible. However, the question for the $\mathcal{K}$ invariant decomposition so far admits less of a general theory than the corresponding question for the $\mathcal{A}$ invariant decomposition.

There are two reasons for this. The first is that $\mathcal{A}$ has an elementary and explicit generator, namely

$$A = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}.$$

However, in general we may not be so explicit for $\mathcal{K}$. Even though Theorem 2.5.1 allows us to write $\mathcal{K} = \{K_{\sigma,\nu} \mid (\sigma,\nu)$ on the circle of radius one $\}$, we are still not able to pinpoint a generator in general. Moreover, even if we did have a generator, its powers are not nearly as nice as, say, the powers of A in $\mathcal{A}$.

The second reason is that where the study of eigenvalues of A led to summing products of $2h$'th roots of unity and thus to the well studied topic of Jacobi sums, the study of the eigenvalues of $K_{\sigma,\nu}$ leads to the summing of h'th roots unity times $h+1$'th roots of unity. This is not so well understood.

Thus we do not have so general a theory or criterion for the existence of a $\mathcal{K}$ invariant decomposition. However, as with the $\mathcal{A}$ decomposition, we state the following theorem which answers the question in the case of the rank two and exceptional Lie algebras (again, the case of A_4 is also included for the sake of comparison).

Theorem 2.6.1 *Let G be one of the following: $A_2, B_2, G_2, A_4, F_4, E_6, E_7, E_8$. Write h for the Coxeter number and $q = 2h+1$. Then given Theorem 2.1.1 with $L_2(q) \hookrightarrow G$, let $\mathcal{P}_K$ be any of the two K stable subsets of order $h+1$ contained in $\mathbf{P}^1(\mathbf{F}_q)$ where K is a generator of $\mathcal{K}$.*

(1) For $h+1$ even, i.e., A_2 and A_4, $\mathfrak{g}$ may not be written as a $\mathcal{K}$ invariant direct sum of Cartans of the form $\mathfrak{h}_u, u \in \mathbf{P}^1(\mathbf{F}_q)$.

To be a bit more precise, any span$\{\mathfrak{h}_u | u \in \mathcal{P}_K\}$ misses being all of $\mathfrak{g}$ by a rank$(\mathfrak{g})/2$ dimensional subspace of the rank$(\mathfrak{g})$ dimensional negative one eigenspace of K.

(2) For $h+1$ odd, i.e., B_2, F_4, G_2, E_6, E_7, and E_8,

$$\mathfrak{g} = \bigoplus_{u \in \mathcal{P}_K} \mathfrak{h}_u$$

as vector spaces. In particular, a K invariant decomposition exists.

Proof. First, just as in Note 2.2.2, we observe that a $\mathcal{K}$ invariant decomposition of $\mathfrak{g}$ as a direct sum of $\mathfrak{h}_u$ is equivalent to the corresponding decomposition of V_{π_m} as a direct sum of $\mathfrak{h}_u^{(m)}$ for all exponents $1 \le m \le h/2$.

Next, we remark that our current proof is quite inelegant. We are forced to check these statements in a direct manner using Theorem 1.1.2, Definition 2.1.2, Corollary 2.1.1, and Theorem 2.5.1. However, the methods are fairly easy to compute (though time consuming) and do yield the desired information. Since the calculations become complicated, we will only give the details for a few typical examples.

Let us check part (1). For $G = A_2$, we have: $q = 7, h = 3, h+1 = 4, m = 1$, and

$\zeta = e^{2\pi i/3}$. One can also take $\lambda = 5 \in \mathbf{F}_q^*$ and

$$K = K_{2,3} = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix} \in L_2(q).$$

Then one checks that the possible choices for $\mathcal{P}_K$ are either $\{0,3,4,\infty\}$ or $\{1,2,5,6\}$. Since the choice will not matter, let us choose the first to be $\mathcal{P}_K$ and write $\mathcal{P}_K^c$ for the second. Next, one computes $h_\infty = e_0 + e_1 + e_2 + e_3 + e_4 + e_5 + e_6$ and $h_0 = e_1 + \zeta^2 e_2 + \zeta e_3 + \zeta e_4 + \zeta^2 e_5 + e_6 + e_\infty$. Using the fact that $M_{-u} h_0 \subseteq \mathbf{C}^* \mathfrak{h}_u$ and the fact that $M_x e_y = e_{y-x}$, this allows us to trivially the rest of the $\mathfrak{h}_u$'s.

If we write $V_K = span\{\mathfrak{h}_u | u \in \mathcal{P}_K\}$, we want to know if V_K can be equal to A_2. By the nature of $\mathfrak{h}_u$, we know that $V_K = span\{e_u, h_u \mid u \in \mathcal{P}_K\}$. If we write out these eight vectors in terms of the e-basis, it is simple to check the rank of the resulting matrix. In fact, by observing that these eight vectors already contain the $e_u, u \in \mathcal{P}_K$, it is obvious that the only part of this matrix that needs to be checked with care is the part determined by the rows indexed by the $h_u, u \in \mathcal{P}_K$, and the columns indexed by the $e_u, u \in \mathcal{P}_K^c$. We record that part here:

$$\begin{pmatrix} 1 & z^2 & z^2 & 1 \\ z & z^2 & 1 & z^2 \\ z^2 & 1 & z^2 & z \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

It is easy to check that this matrix has rank three and not four. Thus we have shown that $dim(V)$ is seven and not the necessary eight to yield $\mathfrak{g}$ as a K invariant direct sum.

Let us go further and find where the actual defect is. Since V_K is K invariant, it will be a sum of eigenvectors of K. Since we know that the $e_u, u \in \mathcal{P}_K$ are in V_K, we know that each eigenvalue of K appears at *least* once (out of a possible two). By the fact that $dim(\mathfrak{g}) - dim(V) = rank(\mathfrak{g})/2 = 1$, we know that we are only "missing" one eigenvector. It is easy to check that the vector $\sum_{i=1}^{h+1}(-1)^{i+1} K^i e_1 = e_1 - e_6 + \zeta e_5 - \zeta e_6$ is not in V (using, say, the above matrix). Since the vector is an eigenvector for K_K of eigenvalue -1, we are done.

For $G = A_4$, we have: $q = 11, h = 5, h+1 = 6, m = 1,2$ and $\zeta = e^{2\pi i/5}$. One can also take $\lambda = 2 \in \mathbf{F}_q^*$ and $K = K_{5,-1}$. This gives as a choice for $\mathcal{P}_A$ either $\{0,4,5,6,7,\infty\}$ or $\{1,2,3,8,9,10\}$. One can also compute $h_0^{(1)} = e_1 + \zeta^4 e_2 + \zeta^2 e_3 + \zeta^3 e_4 + \zeta e_5 + \zeta e_6 + \zeta^3 e_7 + \zeta^2 e_8 + \zeta^4 e_9 + e_1 0 + e_\infty$ for $m = 1$ (for $m = 2$ apply the Galois map to get the corresponding element). Since everything proceeds exactly as before for A_2, we omit the details.

Let us now check part (2). For $G = B_2$, we have: $q = 9, p = 3, h = 4, h+1 = 5, m = 1$, and $\zeta = e^{2\pi i/4}$. Take λ to be a generator for $\mathbf{F}_q^*$. As a recurrence relation to relate the multiplication to addition, one may take λ to satisfy $\lambda^2 = 1 + \lambda$. Then one may choose $K = K_{\lambda,1}$ which will give the two choices for $\mathcal{P}_K$ as either $\{0, \lambda^3, \lambda^4, \lambda^7, \lambda^8\}$ or $\{\infty, \lambda, \lambda^2, \lambda^5, \lambda^6\}$. Let us choose the first and note that one may check that the choice does not matter. Lastly one may check that $h_0 = \zeta^3 e_\lambda + \zeta^2 e_{\lambda^2} + \zeta e_{\lambda^3} + e_{\lambda^4} + \zeta^3 e_{\lambda^5} + \zeta^2 e_{\lambda^6} + \zeta e_{\lambda^7} + e_{\lambda^8} + e_\infty$.

Again, let $V_K = span\{\mathfrak{h}_u | u \in \mathcal{P}_K\}$. Just as we did for part (1), we could write down a five by five matrix and see that it has full rank in order to finish the proof for this case. This is in fact easy, but we will do it another way. Namely, we already know that $e_0 \subseteq V$. If we also could get e_∞ in V_K, then by the nature of the K orbits above, we would be done. In fact, this is possible. To wit, one may check that

$$\frac{1}{6}[2h_0 + (1+\zeta)h_{\lambda^2} + (1-\zeta)h_{\lambda^4} + (1+\zeta)h_{\lambda^7} + (1-\zeta)h_{\lambda^8}]$$

is equal to e_∞ modulo $\langle \mathcal{K} e_0 \rangle$. Thus we have that $\mathfrak{g}$ admits a K invariant decomposition and we are done with this case.

For $G = G_2$, we have: $q = 13, h = 6, h + 1 = 7, m = 1$, and $\zeta = e^{2\pi i/6}$. One may take $\lambda = 2 \in \mathbf{F}_q^*$ and $K = K_{3,2}$. The $\mathcal{P}_K$ is either $\{0, 2, 3, 6, 7, 10, 11\}$ of $\{\infty, 1, 4, 5, 8, 9, 12\}$. Say that we choose the first. One may also check that $h_0 = e_1 + \zeta^5 e_2 + \zeta^2 e_3 + \zeta^4 e_4 + \zeta^3 e_5 + \zeta e_6 + \zeta e_7 + \zeta^3 e_8 + \zeta^4 e_9 + \zeta^2 e_{10} + \zeta^5 e_{11} + e_{12} + e_\infty$. As above, we may either write down a matrix or display e_∞ as an element of V_K. We choose the later. Explicitly, one may check that

$$\frac{1}{39}[(11-6\zeta)h_0 + (1+3\zeta)h_2 + (4-z)h_3 + (9+\zeta)h_6 + (9+\zeta)h_7 + (4-\zeta)h_{10} + (1+3\zeta)h_{11}]$$

does the trick.

We will not explicitly compute any of the remaining cases for two reasons. The first is that they are long and complicated. The second is that no insight is gained in grinding them out. We only make the following remarks that will allow the reader to perform the analogous calculations.

For $G = E_8$, we have: $q = 61, h = 30, h = 31, m = 1, 7, 11, 13$, and $\zeta = e^{2\pi i/30}$. One may take $\lambda = 2 \in \mathbf{F}_q^*$ and $K = K_{8,1}$. Using the Galois group, it is enough to check $m = 1$. The same techniques work as above. Since the calculations are very long and add no more insight, we shall omit them.

For $G = F_4$, we have: $q = 25, p = 5, h = 12, h + 1 = 13, m = 1, 5$, and $\zeta = e^{2\pi i/12}$. One may take the generator $\lambda \in \mathbf{F}_q^*$ to satisfy the relation $\lambda^2 = 3 + \lambda$ and one may take $K = K_{\lambda^{11},1}$. As above, one need only check the case $m = 1$ and the same techniques will work.

For $G = E_6$, we have everything the same as above except for $m = 1, 4, 5$. By the above, this leaves only $m = 4$ to be checked. It is done in the same fashion and works.

For $G = E_7$, we have: $q = 37, h = 18, h + 1 = 19, m = 1, 5, 7, 9$, and $\zeta = e^{2\pi i/18}$. One may take $\lambda = 2 \in \mathbb{F}_q^*$ and $K = K_{15,1}$. With these, checking $m = 1$ is done as above. It takes care of all the cases except $m = h/2 = 9$. For this exponent, recall that we only get "half" of corresponding induced representation. However, it is trivial to check from general principals (just as with Theorem 2.4.1 and the element A) that the K invariant decomposition is always valid within the *irreducible component* of $V_{\pi_{h/2}}$. □

Now let us make a note that compares Theorem 2.6.1 and Theorem 2.4.1.

Corollary 2.6.1 *Let G be one of the following: $A_2, A_4, B_2, G_2, F_4, E_6, E_7$, or E_8. Write h for the Coxeter number and $q = 2h + 1$. Then with respect to Theorem 2.1.1 and the embedding of $L_2(q) \hookrightarrow G$, $\mathfrak{g}$ admits an invariant decomposition as vector spaces*

$$\mathfrak{g} = \bigoplus_{u \in \mathcal{P}_A} \mathfrak{h}_u$$

by the Kostant element (globalized Coxeter element) A if and only if h is odd. Similarly, $\mathfrak{g}$ admits an invariant decomposition as vector spaces

$$\mathfrak{g} = \bigoplus_{u \in \mathcal{P}_K} \mathfrak{h}_u$$

by the Kac element K if and only if $h + 1$ is odd.

Therefore either the Kostant or Kac decomposition will always work (depending on the parity of h), but the two cases are mutually exclusive.

Moreover, the primary reason for the failure of one of these decompositions to exist has to do with a shortfall in the negative one eigenspace of the element A or K, respectively.

Chapter 3

Restricting to $L_2(q)$ in Rank Two

In this chapter we will want to determine what happens when a representation of G is restricted to $L_2(q)$ in the rank two case. It will be useful to first introduce the following notation.

3.1 Elements of Finite Order

Following Kac (see [12], [24] §4, or [28] §4.4.8), we recall a convenient classification of the elements of finite order in a simply connected simple Lie group G. We shall not provide proofs since this material is rather easy and is classical (the main ingredient in its proof is knowledge of a fundamental region of the affine Weyl group). Let us set up the notation in the following paragraphs.

Notation: First write $(,)$ for the (transpose of the) Killing form on the dual of a Cartan subalgebra $\mathfrak{h}^*$. Then for $\alpha, \beta \in \mathfrak{h}^*$, recall the notation

$$\langle \alpha, \beta \rangle = \frac{2(\alpha, \beta)}{(\beta, \beta)}.$$

Choose $\Pi = \{\alpha_i \mid i = 1, \dots l\}$ to be a simple base in Δ^+, the set of positive roots, where $l = rank(\mathfrak{g})$. We also have the ***fundamental weights*** $\pi_{\alpha_i} \in \mathfrak{h}^*$ defined by $\langle \pi_{\alpha_i}, \alpha_j \rangle = \delta_{i,j}$. We may define the *coroots* $\alpha_i^\vee \in \mathfrak{h}$ by requiring $\alpha(\alpha_i^\vee) = \langle \alpha, \alpha_i \rangle$ for all $\alpha \in \mathfrak{h}^*$. Lastly, we have the dual fundamental weights $\pi_{\alpha_i}^\vee \in \mathfrak{h}$ defined by the relations $\alpha_i(\pi_{\alpha_j}^\vee) = \delta_{i,j}$.

Write $\tilde{\Gamma}$ for the extended Dynkin diagram of G. There are l nodes of $\tilde{\Gamma}$ associated to the standard Dynkin diagram via Π and a 0'th node associated to the negative of the highest long root ξ. If we write $\xi = \sum_{i=1}^{l} n_i \alpha_i$ and define $n_0 = 1$, then $n_0, \dots n_l$ are called the *numerical marks* of $\tilde{\Gamma}$. Moreover, it is standard to call any node of $\tilde{\Gamma}$ a *tip* if its corresponding numerical mark is 1. In the case of the rank two Lie groups, the numerical marks are $(1,1,1)$, $(1,2,1)$, and $(1,2,3)$ for A_2, B_2, and G_2, respectively, where the 2 corresponds to the short root (α) in B_2 and the 3 corresponds to the short root (α) in G_2.

Let g be an element of finite order N in G and let M be the order of $Ad(g)$ on $\mathfrak{g} = Lie(G)$. We will be able to classify the conjugacy class of g by conjugating to a Cartan subalgebra and looking at its "log" within the fundamental region of the affine Weyl group (see [24] §4). In particular, it is known that there exists unique nonnegative integers $[s_0, \ldots s_l]$ (each s_i corresponding to the ith node of $\tilde{\Gamma}$) with $gcd(s_0, \ldots s_l) = 1$ such that

$$M = \sum_{i=0}^{l} n_i s_i \tag{3.1}$$

so that if we define $x \in \mathfrak{h}$ by requiring it to have the barycentric coordinates

$$\alpha_i(x) = \frac{s_i}{M}$$

for $i = 1, \ldots l$, then g is conjugate to $exp(2\pi i x)$. Thus we have attached to the conjugacy class of g a set of integers $[s_0, \ldots s_l]$.

To follow the process backwards, start with a sequence $[s_0, \ldots s_l]$ of non-negative integers with $gcd(s_0, \ldots s_l) = 1$. Define M by Equation 3.1. Then let

$$x = \frac{1}{M} \sum_{i=1}^{l} s_i \pi_{\alpha_i}^{\vee}$$

and take $g = exp(2\pi i x)$ to get back the original element (up to conjugacy). (In to order retrieve N, the order of g in G, see [24] §4 and Table 6.)

Let us formalize some very convenient notation.

Definition 3.1.1 *In the following sections, we will allow ourselves to refer to an element g of finite order by referring the the corresponding sequence $[s_0, \ldots s_l]$ via the process in the preceding paragraphs.*

For our applications, we will really be concerned with $Ad(G)$. For this purpose, we note the following theorem.

Theorem 3.1.1 *Two elements $[s_0, \ldots s_l]$ and $[s_0', \ldots s_l']$ are $Ad(G)$ conjugate if and only if their entries differ by a permutation on the tips.*

Proof. The result will follow quickly after observing that $[s_0'', \ldots s_l'']$ will be in the center of G if and only if $[s_0'', \ldots s_l''] = [0, \ldots, 0, 1, 0, \ldots 0]$ where the 1 corresponds to a tip of $\tilde{\Gamma}$. For details, see [24] §4. □

Note 3.1.1 Let us note the following facts. First of all, $[s_0, \dots s_l]$ will be regular if and only if each s_i is non-zero since a regular element does not lie on the Weyl chamber walls. Second, the element $[1, \dots 1]$ is a Kostant element since it is regular and has Ad order h. Third, $[2, 1, \dots 1]$ is a Kac element since it is also regular and has Ad order $h + 1$. For more details, see [24] §6.

3.2 Character Values of the Finite Group

At this point, we will record the character tables for $L_2(7), L_2(9)$, and $L_2(13)$. They will be useful for both notation and later use.

Theorem 3.2.1 *The following tables (Table 3.1, 3.2, and 3.3) are the character tables for $L_2(q)$, $q = 7, 9, 13$, respectively. The first line is a representative of each conjugacy class of $L_2(q)$ in terms of our old notation, the second line is the order of the element, the third line is the number of elements within the conjugacy class, and the remaining lines are the character tables.*

Table 3.1: $L_2(7)$

	I	S	A	K	M_1	M_λ
ord elt:	1	2	3	4	7	7
ord conj:	1	21	56	42	24	24
χ_1	1	1	1	1	1	1
χ_2	3	-1	0	1	b_7	b_7^{**}
χ_3	3	-1	0	1	b_7^{**}	b_7
χ_4	6	2	0	0	-1	-1
χ_5	7	-1	1	-1	0	0
χ_6	8	0	-1	0	1	1

where $b_7 = \frac{-1+i\sqrt{7}}{2}$ and $b_7^{**} = \frac{-1-i\sqrt{7}}{2}$

Proof. This is easily gleamed from, say, [7], [8] §38, or [26] §2.5 and our previous knowledge of S, A, K, and M. For the names of the representations, χ_i, and their character values, we have tried to follow the notation of the ATLAS. □

According to Kostant's Conjecture 2.1.1, we have $L_2(q) \hookrightarrow G$ where $q = 7, 9, 13$ and $G = A_2, B_2, G_2$, respectively. In Chapter 1 these embeddings were derived in great detail.

Table 3.2: $L_2(9)$

	I	S	A	K	K^2	M_1	M_λ
ord elt:	1	2	4	5	5	3	3
ord conj:	1	45	90	72	74	40	40
χ_1	1	1	1	1	1	1	1
χ_2	5	1	-1	0	0	2	-1
χ_3	5	1	-1	0	0	-1	2
χ_4	8	0	0	$-b_5$	$-b_5^*$	-1	-1
χ_5	8	0	0	$-b_5^*$	$-b_5$	-1	-1
χ_6	9	1	1	-1	-1	0	0
χ_7	10	-2	0	0	0	1	1

where $b_5 = \frac{-1+\sqrt{5}}{2}$ and $b_5^* = \frac{-1-\sqrt{5}}{2}$

For these rank two cases, we will find the character values for irreducible representations of G restricted to $L_2(q)$. Let us fix some general notation.

Notation: Let G be a rank two simple complex Lie group with trivial center. Write $\mathfrak{g}$ for $Lie(G)$ and $\mathfrak{h}$ for a fixed Cartan subalgebra of $\mathfrak{g}$. In addition, fix a positive Weyl chamber and $\alpha, \beta \in \mathfrak{h}^*$ as the corresponding basis of simple positive roots. When it matters, we will take α to be the short root. We will then write Π for the simple roots, Δ for the set of all roots, and Δ^+ for the positive ones. We also have $\pi_\alpha, \pi_\beta \in \mathfrak{h}^*$ as the corresponding fundamental weights, see Section 3.1. (All of these choices will eventually be made explicit for each G).

Definition 3.2.1 *Index all the finite dimensional irreducible representations of $\mathfrak{g}$ by the set of all dominant integral weights. Explicitly, we may index the representations by pairs of non-negative integers (m, n) to which we associate the representation $\Lambda(m, n)$ on a vector space $V(m, n)$ whose highest weight is $m\pi_\alpha + n\pi_\beta$.*

The representations of G are precisely those representations $\Lambda(m, n)$ that descend to G. (It is only different if G is not simply connected). We will use the same notation for the representation of the group as for the algebra.

In the following, we will have the opportunity to make use of the Weyl character formula. For convenience, we record it below. Write W for the Weyl group of G and $\rho = \frac{1}{2}\sum_{\alpha \in \Delta^+} \alpha$. fix a representation with highest weight Λ. Then for $x \in \mathfrak{h}$, the character of the representation, χ_Λ, with highest weight Λ is given by

$$\chi_\Lambda(exp(x)) = \frac{\sum_{\sigma \in W} sgn(\sigma) e^{[\sigma(\Lambda+\rho)](x)}}{\sum_{\sigma \in W} sgn(\sigma) e^{[\sigma(\rho)](x)}} \tag{3.2}$$

Table 3.3: $L_2(13)$

	I	S	A^2	A	K	K^2	K^3	M_1	M_λ
ord elt:	1	2	3	6	7	7	7	13	13
ord conj:	1	91	182	182	156	156	156	84	84
χ_1	1	1	1	1	1	1	1	1	1
χ_2	7	-1	1	-1	0	0	0	$-b_{13}$	$-b_{13}^*$
χ_3	7	-1	1	-1	0	0	0	$-b_{13}^*$	$-b_{13}$
χ_4	12	0	0	0	$-y_7$	$-y_7^{*2}$	$-y_7^{*4}$	-1	-1
χ_5	12	0	0	0	$-y_7^{*4}$	$-y_7$	$-y_7^{*2}$	-1	-1
χ_6	12	0	0	0	$-y_7^{*2}$	$-y_7^{*4}$	$-y_7$	-1	-1
χ_7	13	1	1	1	-1	-1	-1	0	0
χ_8	14	2	-1	-1	0	0	0	1	1
χ_9	14	-2	-1	1	0	0	0	1	1

where $b_{13} = \frac{-1+\sqrt{13}}{2}$, $b_{13}^* = \frac{-1-\sqrt{13}}{2}$, $y_7 = 2\cos(2\pi i/7)$, and $y_7^{*n} = 2\cos(2n\pi i/7)$

whenever $e^{\alpha(x)} \neq 1$ for all roots $\alpha \in \Delta$, i.e., whenever the denominator is non-zero.

Let us now introduce some notation that will be very useful in the next section.

Definition 3.2.2 *For any prime power p^f, define the function $R_{(p^f)} : \mathbb{Z} \hookrightarrow \{0, \pm 1\}$ by*

$$R_{(p^f)}(a) = \begin{cases} 0 & \text{if } a = 0 \mod p \\ 1 & \text{if } a \text{ is a square in } \mathbb{Z}/p^f\mathbb{Z} \text{ and } a \neq 0 \mod p \\ -1 & \text{if } a \text{ is not a square in } \mathbb{Z}/p^f\mathbb{Z} \text{ and } a \neq 0 \mod p \end{cases}$$

Note that for $f = 1$, R_p restricted to $\mathbb{Z}/p\mathbb{Z}^*$ is just the Legendre symbol, *ρ.*

For any positive integer k, define the number $\delta^{(k)}_{condition} \in \{0, 1\}$ to be

$$\delta^{(k)}_{condition} = \begin{cases} 0 & \text{if condition is not satisfied mod } k \\ 1 & \text{if condition is satisfied mod } k \end{cases}$$

Note that this is more or less the Dirac *delta function on the condition mod k.*

We will also need one more lemma on Gauss sums (recall Definition 2.2.3 for $g(\psi)$).

Lemma 3.2.1 *For χ a fixed non-trivial additive character on F_q and ρ the Legendre symbol, then for any $a \in \mathsf{F}_q^*$, one has*

$$\sum_{u \in \mathsf{F}_q^{*2}} \chi(au) = \frac{1}{2}[\rho(a)g(\rho) - 1].$$

Proof. This follows trivially by writing

$$\sum_{u \in \mathsf{F}_q^{*2}} \chi(au) = \sum_{v \in \mathsf{F}_q^*} \chi(av) \frac{\rho(v) + 1}{2}.$$

□

3.3 Character Values in the Lie Group

Theorem 3.3.1 *For the embedding of $L_2(7) \hookrightarrow A_2$, the restriction of the character $\chi_{\Lambda(m,n)}$ to $L_2(7)$ is given by the equations below. Note that $\Lambda(m,n)$ descends to $PSL(3,\mathbf{C})$ only if $m = n$ mod 3. These character values below correspond to the embedding in Figure 1-1. For the other embedding of Figure 1-2, switch the role of M_1 and M_λ in the following.*

$$\begin{aligned}
\chi_{\Lambda(m,n)}(I) &= \frac{1}{2}(m+1)(n+1)(m+n+2) \\
\chi_{\Lambda(m,n)}(S) &= \frac{(-1)^{m+n}}{2}[(n+1)R_{(2)}(m+1) + (m+1)R_{(2)}(n+1)] \\
\chi_{\Lambda(m,n)}(A) &= -\delta^{(3)}_{m=n} R_{(3)}(m+n+2) \\
\chi_{\Lambda(m,n)}(K) &= \frac{1}{2}[R_{(4)}(m+1) + R_{(4)}(n+1) - R_{(4)}(m+n+2)] \\
\chi_{\Lambda(m,n)}(M_1) &= \frac{1}{2}[R_{(7)}(s) - R_{(7)}(r) + (\delta^{(7)}_{r=0} - \delta^{(7)}_{s=0})i\sqrt{7}] \\
\chi_{\Lambda(m,n)}(M_\lambda) &= \overline{\chi_{\Lambda(m,n)}(M_1)}
\end{aligned}$$

where

$$r = m - 2n - 1 \text{ and } s = 2m - n + 1.$$

Proof. First of all, by our earlier discussion of the rank two case for $q = 7$, if we need to be explicit, we may take our simple base of roots for $\mathfrak{sl}(3,\mathbf{C})$ to be $\alpha = \alpha_{\lambda^0}$ and $\beta = \alpha_{\lambda^2}$ where $\lambda = -2$ (see Figure 1-1). Of course in this case, half sum of the positive roots, ρ, is equal to $\alpha + \beta$. The fundamental weights are $\pi_\alpha = 1/3(2\alpha + \beta)$

and $\pi_\beta = 1/3(\alpha + 2\beta)$. For m, n non-negative integers, we have the dominant weight $\Lambda(m,n) = m\pi_\alpha + n\pi_\beta$. Thus $\Lambda(m,n) = 1/3(2m+n)\alpha + 1/3(m+2n)\beta$. For convenience, let us call

$$x = 1/3(2m+n)$$

$$y = 1/3(m+2n)$$

so that $\Lambda(m,n) = x\alpha + y\beta$. Of course x, y depend on m, n, but we shall suppress this in the notation.

By this we see that $\Lambda(m,n)$ will be in the root lattice if and only if $m = n \ mod\ 3$. Thus if we wish the representation of $\mathfrak{sl}(3, \mathbb{C})$ with highest weight $\Lambda(m,n)$ to descend to the Adjoint group of A_2 $(PSL(3, \mathbb{C}))$, then we must require that $m = n \ mod\ 3$. Since we are only interested in $L_2(7) \hookrightarrow PSL(3, \mathbb{C})$, we will make this assumption. (However, it is not really necessary since in actuality, we really have $L_2(7) \hookrightarrow SL(3, \mathbb{C})$—see Section 1.9 on the discussion of $q = 7$—and in fact the character values given above are correct without this assumption).

Let us make use of the Weyl character formula. In this case the Weyl group is isomorphic to D_3, the Dihedral group. Now if we have an element x in the Cartan subalgebra $\mathfrak{h}$ with

$$\alpha(x) = a \text{ and } \beta(x) = b,$$

then one may quickly verify that $\chi_{\Lambda(m,n)}(exp(x))$ is

$$\frac{n_1 - n_2}{d + \overline{d}} \tag{3.3}$$

whenever the denominator is non-zero where

$$n_1 = e^{a(x+1)+b(y+1)} + e^{-a(x+1)+b(x-y)} + e^{a(-x+y)-b(x+1)}$$

$$n_2 = e^{-a(y+1)-b(x+1)} + e^{a(x+1)+b(x-y)} + e^{a(-x+y)+b(y+1)}$$

$$d = e^{a+b} + e^{-a} + e^{-b}.$$

We may now calculate the character values. To begin with, the character value for the identity I is simply the dimension. This is standard (see for instance §24.3 of [9]).

Next comes the character value for S. Since S is non-trivial and has order 2 (recalling Definition 3.1.1 and Theorem 3.1.1), up to conjugacy, the only possibility for S is $[0,1,1]$. Thus S is conjugate to $exp[2\pi i(\pi_\alpha^\vee + \pi_\beta^\vee)/2]$. But this is the same as $exp[2\pi i(\pi_\alpha^\vee - \pi_\beta^\vee))/2]$. If we let $\theta = 2\pi i/2$, we would like to put $a = \theta$ and $b = -\theta$ into Equation 3.3. But of course S is not regular so this is not quite legal. Instead, we will put $a = t\theta$ and $b = -t\theta$ and consider the limit as $t \to 1$ in Equation 3.3. For this, we apply L'Hopital's rule. The reader may check that this gives us a character value of:

$$-\frac{1}{4}[(-1)^{m+1}(m+1) - (-1)^{-m-n-2}(m+n+2) + (-1)^{n+1}(n+1)].$$

If one then simplifies this and considers the various cases of m and n being even and odd, the result given in the theorem will follow.

Next, let us compute the character value of A. By Note 3.1.1, we already know that A is conjugate to $[1,1,1]$ since A is a Kostant element (Theorem 2.1.1 part (3)). Thus if we let $\theta = 2\pi i/3$, we may apply Equation 3.3 directly with $a = b = \theta$. If one is careful and remembers that $x+y, x-2y, 2x-y$ are all integers, then one may verify that the result is

$$\frac{1}{3(\zeta^{-1}-\zeta)}[\zeta^{m+n-1}(1+\zeta^{-m+n}+\zeta^{m-n}) - \zeta^{-m-n+1}(1+\zeta^{-m+n}+\zeta^{m-n})]$$

where $\zeta = e^{\theta}$. This however, will reduce to the given result.

Next, let us consider the character on K. Again, by Note 3.1.1, we already know that K is conjugate to $[2,1,1]$ since K is a Kac element (Theorem 2.1.1 part (3)). Thus, if we let $\theta = 2\pi i/4$, we may apply Equation 3.3 directly with $a = b = \theta$. The resulting formula is very similar to the one for A given above, however, with a different value for θ. Using that $e^{\theta} = i$, one may check that the result in the theorem is correct.

Next, let us consider the character on M_1. Using Figure 1-1, it is easy to find a "log" for M_1 since it is trivial on $\mathfrak{h}_{\infty}$. We let $\theta = 2\pi i/7$ and take $a = \theta$ and $b = 4\theta$. When this is exponentiated, it has the correct eigenvectors and eigenvalues. Thus it is our desired "log". Now applying Equation 3.3 yields

$$\frac{\sum_{u \in \mathbf{F}_q^{*2}} \chi(ru) - \sum_{u \in \mathbf{F}_q^{*2}} \chi(su)}{-\sum_{v \in \mathbf{F}_q^*} \chi(v)\rho(v)}$$

where we have set

$$r = m - 2n - 1 \text{ and } s = 2m - n + 1$$

and we recall that χ is the additive character on $L_2(7)$ determined by $\chi(1) = e^{\theta}$ and that ρ is the Legendre symbol (Definition 2.2.3). Applying Lemma 3.2.1, Definition 2.2.3, and Theorem 2.2.1 part (1), we can rewrite our above equation. If one checks the various cases of r, s being either zero or non-zero, the result will follow. (Note: though Theorem 2.2.1 already tells us that $g(\rho)\overline{g(\rho)} = q$, in fact one can also check that in fact $g(\rho)^2 = \rho(-1)q$— see [26] §2.5 equation 5.5.7.)

The character of M_λ could be done in a similar fashion as M_1 above. However, it is much easier to observe that the result follows from the character table in Theorem 3.2.1.

Lastly, if we were to have chosen Figure 1-2 (basically conjugating everything by an outer automorphism), then it is easily checked that this simply amounts to switching the roles of M_1 and M_λ. □

Theorem 3.3.2 *For the embedding of $L_2(9) \hookrightarrow B_2$, the restriction of the character $\chi_{\Lambda(m,n)}$ to $L_2(9)$ is given below. Note that (m,n) must be in $2\mathbb{Z} \times \mathbb{Z}$ in order for $\Lambda(m,n)$ to be a representation of $SO(5,\mathbb{C})$. Therefore make this assumption. Also, the following character values correspond to the root configuration in Figure $1-3$. To get the ones corresponding to Figure $1-4$, simply switch the roles of M_1 and M_λ.*

$$\begin{aligned}
\chi_{\Lambda(m,n)}(I) &= \frac{1}{3!}(m+1)(n+1)(m+n+2)(m+2n+3) \\
\chi_{\Lambda(m,n)}(S) &= \frac{(-1)^{\frac{m}{2}}}{2}[(n+1)+(m+1)R_{(2)}(n+1)] \\
\chi_{\Lambda(m,n)}(A) &= \delta^{(4)}_{a,b\in 0,1} - \delta^{(4)}_{a,b\in 2,3} \\
\chi_{\Lambda(m,n)}(K) &= \delta^{(5)}_{(m,n)\neq(4,4)}\delta^{(5)}_{m=n} - \delta^{(5)}_{m-n=2} \\
\chi_{\Lambda(m,n)}(K^2) &= \chi_{\Lambda(m,n)}(K) \\
\chi_{\Lambda(m,n)}(M_1) &= \frac{1}{3}[(m+n+2)R_{(3)}(n+1)-(n+1)R_{(3)}(m+n+2)] \\
\chi_{\Lambda(m,n)}(M_\lambda) &= \frac{1}{3}[(m+2n+3)R_{(3)}(m+1)-(m+1)R_{(3)}(m+2n+3)]
\end{aligned}$$

where

$$a = -\frac{m}{2} + 2n \text{ and } b = \frac{m}{2} - n.$$

Proof. By our earlier discussion of the rank two case for $q = 9$, if we need to be explicit, we may take our simple base of roots for $\mathfrak{so}(5,\mathbb{C})$ to be $\alpha = \alpha_{\lambda^0}$ (the short root) and $\beta = \alpha_{\lambda^1}$ (the other case is $\alpha = \alpha_{\lambda^1}$ (the short root) and $\beta = \alpha_{\lambda^2}$) where $\lambda^2 + \lambda = 1$ and $1 + \lambda^2 = \lambda^7$ (see Figure 1-3, Figure 1-4, and the surrounding discussion). Of course, $\rho = \pi_\alpha + \pi_\beta$ and one may calculate that the fundamental weights are $\pi_\alpha = \alpha + \beta/2$ and $\pi_\beta = \alpha + \beta$. Thus for m, n non-negative integers, we have the dominant integral weight $\Lambda(m,n) = m\pi_\alpha + n\pi_\beta$. Thus $\Lambda(m,n) = (m+n)\alpha + (m/2+n)\beta$. For convenience, let us call

$$x = m + n$$

$$y = m/2 + n.$$

Then we have $\Lambda(m,n) = x\alpha + y\beta$. Of course x, y depend on m, n, but we shall suppress this in the notation. We see that $\Lambda(m,n)$ will be in the root lattice if and only if $m = 0$ *mod* 2. Thus if we wish the representation of $\mathfrak{so}(5,\mathbb{C})$ with highest weight $\Lambda(m,n)$ to descend to the Adjoint group of B_2, $SO(5,\mathbf{C})$, then we must require that m is even. Since we only have $L_2(9) \hookrightarrow SO(5,\mathbf{C})$, we will make this assumption—see Section 1.9 on the discussion of $q = 9$.

Let us make use of the Weyl character formula. In this case the Weyl group is isomorphic to D_4, the Dihedral group. If we have an element x in the Cartan subalgebra $\mathfrak{h}$ with

$$\alpha(x) = a \text{ and } \beta(x) = b,$$

then one may quickly calculate $\chi_{\Lambda(m,n)}(exp(x))$. For this, let

$$n_1 = e^{a(x+2)+b(y+3/2)} + e^{a(x-2y-1)+b(x-y+1/2)} - e^{a(-x+2y+1)+b(y+3/2)} - e^{a(x+2)+b(-y+1/2)}$$

and

$$d = e^{2a+3b/2} + e^{-a+b/2} - e^{a+3b/2} - e^{2a+b/2}$$

then one has $\chi_{\Lambda(m,n)}(exp(x))$ equal to

$$\frac{n_1 + \overline{n}}{d + \overline{d}} \tag{3.4}$$

whenever the denominator is non-zero.

The character value for the identity I is simply the dimension. This is standard (see for instance §24.3 of [9]).

Next, let us find the character value on S. Recalling Definition 3.1.1 and Theorem 3.1.1, up to conjugacy, the only non-trivial elements of order 2 are $[0,1,0]$ and $[1,0,1]$. However, the trace of an element $exp(x)$ on the Adjoint representation is simply

$$l + \sum_{\gamma \in \Delta} e^{\gamma(x)}$$

for $x \in \mathfrak{h}$. Using the character table in Theorem 3.2.1 and the fact that the Adjoint representation is irreducible under $L_2(9)$ (see Theorem 2.1.1 part(2)), one may easily check that S must have trace -2 and that only $[1,0,1]$ will satisfy this condition. Thus S is conjugate to $exp[2\pi i(0\pi_\alpha^\vee + \pi_\beta^\vee)/2]$. But this is the same as $exp[2\pi i(2\pi_\alpha^\vee - \pi_\beta^\vee)/2]$. Thus if we let $\theta = 2\pi i/2$, we would like to put $a = 2\theta$ and $b = \theta$ into Equation 3.4. But of course S is not regular so this is not possible. Instead, we will put $a = 2t\theta$ and $b = t\theta$ and consider the limit as $t \to 1$ using L'Hopital's rule. The reader may check that this gives us a character value of:

$$\frac{-1}{2}[(-1)^y(-x + y - 1/2) + (-1)^{x+y}(-y - 3/2)].$$

Then checking the even and odd possibilities, the desired answer is obtained.

Next let us find the character value on A. We already know that A is conjugate to $[1,1,1]$. Thus we let $\theta = 2\pi i/4$ and $a = b = \theta$. Then Equation 3.4 will yield

$$\frac{1}{2}\frac{(\zeta^0+\zeta^x)(\zeta^{-1+x+y}+\zeta^{2x-y})}{(\zeta^0+\zeta^3)}$$

where $\zeta = e^\theta$. This in turn, will be equal to the above result.

Let us find the character value on K. Again, we know that K is conjugate to $[2,1,1]$ so that if we let $\theta = 2\pi i/5$, we can put $a = b = \theta$ in Equation 3.4. One may check that this yields

$$\frac{1}{5}(\delta^{(5)}_{x+y+1\neq 0} - 4\delta^{(5)}_{x+y+1=0} + 4\delta^{(5)}_{x-3y=0} - \delta^{(5)}_{x-3y\neq 0}).$$

Further calculation gives

$$\delta^{(5)}_{(x,y)\neq(3,1)}(-\delta^{(5)}_{x+y+1=0} + \delta^{(5)}_{x-3y=0})$$

which will simplify to the expression in the theorem.

For the character value on K^2, simply observe that in B_2, K and K^2 are conjugate.

Next, consider the character on M_1. Using Figure 1-3, it is easy to find a "log" for M_1 in $\mathfrak{h}_\infty$. We let $\theta = 2\pi i/3$ and would like to take $a = \theta$ and $b = 0\theta$ (or $a = 0\theta$ and $b = \theta$ for the second case) so that $e^a = \chi(\lambda^0)$ and $e^b = \chi(\lambda^1)$ (for the additive character χ, we write any element of $u \in \mathsf{F}_q$ uniquely in the form $u = k + l\lambda$, $k, l \in \mathbb{Z}_3$, and define $\chi(u) = e^{k\theta}$). When this is exponentiated, it has the correct eigenvectors and eigenvalues. Thus it is our desired "log". Unfortunately, M_1 is no longer regular since $q \neq p$ (M_1 has order 3 not order 9). Thus we use L'Hopital's rule as $t \to 0$ with $a = \theta$ and $b = 2t\theta$ in Equation 3.4 to get

$$\frac{-1}{3(\xi-\xi^{-1})}[(m+1)(\xi^{2+m+n}-\xi^{1-m-n})+(m+n+2)(\xi^{-n+2}-\xi^{n-2})]$$

where $\xi = e^\theta$. The result will then follow. (If we were in the second case, then one easily checks that the role of M_1 and M_λ are reversed in the above equation).

Lastly, M_λ could be done in a similar fashion to M_1 above. However, it is much easier to observe that the result follows from the character table in Theorem 3.2.1. □

Theorem 3.3.3 *For the embedding of $L_2(13) \hookrightarrow G_2$, the restriction of the character $\chi_{\Lambda(m,n)}$ to $L_2(13)$ is given below. The following character values correspond to the root configuration in $Figure\ 1-5$. To get the ones corresponding to $Figure\ 1-6$, switch the* *roles of* M_1 *and* M_λ.

$$\begin{aligned}
\chi_{\Lambda(m,n)}(I) &= \frac{1}{5!}(m+1)(n+1)(m+n+2)(m+2n+3)(m+3n+4)(2m+3n+5) \\
\chi_{\Lambda(m,n)}(S) &= \frac{1}{16}[(-1)^m(m+1)(m+2n+3)+(-1)^n(n+1)(2m+3n+5)+ \\
&\quad (-1)^{n+m}(m+n+2)(m+3n+4)] \\
\chi_{\Lambda(m,n)}(A^2) &= \frac{1}{9}[(m+1)R_{(3)}(m+2n+3)+(2m+3n+5)R_{(3)}(n+1) \\
&\quad -(m+3n+4)R_{(3)}(m+n+2)] \\
\chi_{\Lambda(m,n)}(A) &= \delta^{(6)}_{b=\pm 1}(\delta^{(6)}_{a-3}-\delta^{(6)}_{a}+\delta^{(6)}_{a+b-3})-\delta^{(6)}_{a=\pm 1}(\delta^{(6)}_{b-3}-\delta^{(6)}_{b}+\delta^{(6)}_{a+b-3}) \\
\chi_{\Lambda(m,n)}(K) &= \delta^{(7)}_{m,n\neq -1}(-\delta^{(7)}_{3m-2n+1}+\delta^{(7)}_{m-n}) \\
\chi_{\Lambda(m,n)}(K^2) &= \chi_{\Lambda(m,n)}(K) \\
\chi_{\Lambda(m,n)}(K^3) &= \chi_{\Lambda(m,n)}(K) \\
\chi_{\Lambda(m,n)}(M_1) &= \frac{1}{2}[R_{(13)}(s)-R_{(13)}(r)+(\delta^{(13)}_{r=0}-\delta^{(13)}_{s=0})\sqrt{13}] \\
\chi_{\Lambda(m,n)}(M_\lambda) &= \frac{1}{2}[R_{(13)}(s)-R_{(13)}(r)-(\delta^{(13)}_{r=0}-\delta^{(13)}_{s=0})\sqrt{13}]
\end{aligned}$$

where

$$a = 3m+5n+2 \text{ and } b = 2m+5n+1$$

$$r = 4m+7n-2 \text{ and } s = 3m+7n-3.$$

Proof. First of all, by our earlier discussion of the rank two case for $q = 13$, if we need to be explicit, we may take our simple base of roots for G_2 to be $\alpha = \alpha_{\lambda^0}$ (the short root) and $\beta = \alpha_{\lambda^1}$ (the other case is $\alpha = \alpha_{\lambda^3}$ (the short root) and $\beta = \alpha_{\lambda^4}$) where $\lambda = 2$ (see Figure 1-5 and Figure 1-6). Of course, $\rho = \pi_\alpha + \pi_\beta$ and one may calculate that the fundamental weights are $\pi_\alpha = 2\alpha + \beta$ and $\pi_\beta = 3\alpha + 2\beta$. For m, n non-negative integers, we have the dominant integral weight $\Lambda(m,n) = m\pi_\alpha + n\pi_\beta$. Thus $\Lambda(m,n) = (2m+3n)\alpha + (m+2n)\beta$. For convenience, let us call

$$x = 2m+3n$$

$$y = m+2n.$$

Then we have $\Lambda(m,n) = x\alpha + y\beta$. Of course x, y depend on m, n, but we shall suppress this in the notation. By this we see that $\Lambda(m,n)$ will is always in the root lattice for any m, n non-negative integers.

Let us make use of the Weyl character formula. In this case the Weyl group is isomorphic to D_6, the Dihedral group. Now if we have an element x in the Cartan subalgebra $\mathfrak{h}$ with

$$\alpha(x) = a \text{ and } \beta(x) = b,$$

then one may quickly calculate $\chi_{\Lambda(m,n)}(exp(x))$. For this, if we let

$$n_1 = e^{a(x+5)+b(y+3)} + e^{a(-x+3y+4)+b(-x+2y+2)} + e^{a(-2x+3y-1)+b(-x+y-2)}$$

$$n_2 = e^{a(-x+3y+4)+b(y+3)} + e^{a(-2x+3y-1)+b(-x+2y+1)} + e^{a(-x-5)+b(-x+y-2)}$$

$$d_1 = e^{5a+3b} + e^{4a+b} + e^{-a-2b}$$

$$d_2 = e^{4a+3b} + e^{-a+b} + e^{-5a-2b}$$

then we get $\chi_{\Lambda(m,n)}(exp(x))$ as

$$\frac{n_1 + n_2 + \overline{n_1} + \overline{n_2}}{d_1 + d_2 + \overline{d_1} + \overline{d_2}} \tag{3.5}$$

whenever the denominator is non-zero.

For S, by Definition 3.1.1, the only possibility is $[0,1,0]$. Thus if we put $\theta = 2\pi i/2$, we would like to put $a = 0$ and $b = \theta$. But this is the same as $a = 2\theta$ and $b = \theta$. Thus we may calculate the character on S by taking the limit as $t \to 1$ with $a = 2t\theta$ and $b = \theta$. This time we will have to use L'Hopital's rule twice on Equation 3.5. It will end up giving us

$$\frac{-1}{16}[(-1)^{y+1}(-y-3)(-2x+3y-1)+(-1)^{x+1}(x-2y-1)(-x-5)+(-1)^{x+y}(x-y+2)(x-3y-4)].$$

This is easily checked to be the said result.

Next we need the character on A^2. By Definition 3.1.1, the only possibility for a non-trivial order three element is $[1,1,0]$. Let $\theta = 2\pi i/3$. We would like to put $a = 0$ and $b = \theta$, but this gives the same thing as $a = -3\theta$ and $b = \theta$. Of course A^2 is not regular so we must instead take $a = -3t\theta$ and $b = t\theta$ and let $t \to 1$. Then L'Hopital's rule on Equation 3.5 yields

$$\frac{1}{9}[(2x - 3y + 1)R_{(3)}(y) + (x + 5)R_{(3)}(-x - y + 1) + (-x + 3y + 4)R_{(3)}(-x + y + 1)]$$

which will quickly yield the desired result.

Next we move on to A. By Note 3.1.1 we can let $\theta = 2\pi i/6$ and $a = b = \theta$ in Equation 3.5. This gives us

$$\frac{-1}{6}(\zeta^t + \zeta^u + \zeta^{u-t} + \zeta^{-t} + \zeta^{-u} + \zeta^{-u+t} + \zeta^v + \zeta^w + \zeta^{w-v} + \zeta^{-v} + \zeta^{-w} + \zeta^{-w+v})$$

where

$$t = x + y + 2 \text{ and } u = 4x + 5y + 5$$

and

$$v = 3t - u \text{ and } w = t + 2b.$$

Though it is a complicated calculation, one may check the various possibilities to see that the stated result follows.

Let us compute K. By Note 3.1.1, we can let $\theta = 2\pi i/7$ and $a = b = \theta$ in Equation 3.5. This gives us

$$\frac{-1}{7}(6\delta^{(7)}_{x+y+1=0} - \delta^{(7)}_{x+y+1\neq 0} - 6\delta^{(7)}_{-x+4y=0} + \delta^{(7)}_{-x+4y\neq 0}).$$

This may then be examined to give the result in the theorem.

For K^2 and K^3, one observes that in G_2, all of these elements are conjugate.

Next, let us consider the character on M_1. Using Figure 1-5, it is easy to find a "log" for M_1 in $\mathfrak{h}_\infty$. Thus we let $\theta = 2\pi i/7$ and take $a = \theta$ and $b = 2\theta$ ($a = 8\theta$ and $b = 3\theta$ in the second case). When this is exponentiated, it has the correct eigenvectors and corresponding eigenvalues. Thus it is our desired "log". Now applying Equation 3.5 yields

$$\frac{\sum_{u\in \mathbf{F}_q^{*2}} \chi(ru) - \sum_{u\in \mathbf{F}_q^{*2}} \chi(su)}{-\sum_{v\in \mathbf{F}_q^{*}} \chi(v)\rho(v)}$$

where we have set

$$r = x + 2y - 2 \text{ and } s = -x + 5y - 3$$

and we recall that χ is the additive character on $L_2(13)$ determined by $\chi(1) = e^\theta$ and that ρ is the Legendre symbol (Definition 2.2.3). Applying Lemma 3.2.1, Definition 2.2.3, and Theorem 2.2.1 part (1), we can rewrite our above equation. If one checks the various cases of r, s being either zero or non-zero, the result will follow. (If one takes the second case, then r, s will both be changed by a non-square in the numerator and the denominator will change by -1. This will amount to taking the algebraic conjugate in the formulas or just switching the role of M_1 and M_λ above.)

Lastly, M_λ could be done in a similar fashion to M_1 above. However, it is much easier to observe that the result follows from the character table in Theorem 3.2.1. □

As a consistency check of Theorems 3.3.1, 3.3.2, and 3.3.3, one can easily verify that the character values of irreducible representations on the Kostant and Kac elements A

and K all lie within the set $\{0, \pm 1\}$ as required by Theorem 0.0.2. Secondly, one sees that the following theorem also holds true in our above work:

Theorem 3.3.4 *For G a simple Lie groups and $x \in G$ an element of finite order, the set of character values $\chi_{(V,\pi)}(x)$ as (V, π) runs through all irreducible representations of G is finite if and only if x is regular.*

Proof. This theorem is taken directly from [24] Proposition 6.1. The proof simply uses the Weyl character formula for the easy direction and cites the [12] for the other. □

In particular, this agrees with our above characters for $L_2(q)$ in G since the elements I and S for $L_2(7)$, the element's I, S, M_1, and M_λ for $L_2(9)$, and the elements I, S, and A^2 for $L_2(13)$ are all not regular in the corresponding Lie group. These are precisely the conjugacy classes that take on an infinite number of character values. The other elements are all regular and all have only a finite number of character values.

3.4 Finite Group Invariant Theory

In this section, we recall some basic terminology and standard facts about the invariants of finite groups. Since this is classical, we will refer the reader to [10], [31], and [30] for details and proofs.

Notation: throughout this section, let L be a finite group of *order* $\mid L \mid = l$ contained in some $GL(V)$ where V is a complex vector space of dimension m, called the *degree* of L. We will write $S = S(V)$ for the polynomial algebra on V and S_i for the homogeneous polynomials of degree i in S. In other words, if we fix a basis $x_1, \ldots x_m$ of V, then we may identify S with polynomials in the variables $x_1, \ldots x_m$, i.e., $S = \mathbb{C}[x_1, \ldots x_m]$. Of course the action of L on V yields an action of L on each S_i and S by letting $(gf)(x) = f(g^{-1}x)$ where $f \in S$ and $x \in V$.

We may break S up uniquely into its *isotypic* components:

$$S = \bigoplus_{\chi} S^L_\chi$$

where the sum is over the set of irreducible complex characters χ of L (the traces of irreducible representations of L) and we write S^L_χ for the isotypic component of S corresponding to the character χ of L. If we write ϵ for the trivial character of L, then the set S^L_ϵ will be abbreviated to simply S^L. It is obviously a subalgebra of S and is called the *algebra of invariants.* Clearly

$$S^L = \{f \in S \mid gf = f \text{ for all } g \in L\}.$$

Similarly, in the special case where the character χ of L is a homomorphism from L to C, then one also has $f \in S^L_\chi$ if and only if $gf = \chi(g)f$ for all $g \in L$. In this case, the elements of S^L_χ are called *semi-invariants* or *χ-invariants.*

One has the standard basic theorem:

Theorem 3.4.1 *If L has degree m and order l, then there are precisely m algebraically independent invariants (over* C*) in S^L and as an algebra, S^L is generated by no more than $\begin{pmatrix} l+m \\ m \end{pmatrix}$ homogeneous invariants of degree not exceeding l. Moreover, S^L_χ is finitely generated as a S^L-module by homogeneous polynomials of degree not exceeding l.*

□

A useful way to encode certain data about the algebra S^L is the following Hilbert polynomial. It is a special case of the *Molien series.*

Definition 3.4.1 *The* Poincaré *polynomial $F_L(t)$ is the formal polynomial given by*

$$F_L(t) = \sum_{i=0}^{\infty} H_i t^i$$

where H_i is the multiplicity of the trivial representation of L in S_i.

It is well known by a theorem of Hilbert that $F_L(t)$ is a rational function of t. It is also trivial that

$$F_L(t) = \frac{1}{l}\sum_{g\in L} \frac{1}{det(I - tg)},$$

however, we will not need this. Instead, there is an easy way to express $F_L(t)$ in terms of generators of the ring S^L. This result is included in the next theorem part (2). Part (1) merely states that S^L is a *Cohen-Macaulay* algebra.

Theorem 3.4.2 *(1) Let $\theta_1, \ldots \theta_m$ be any set of homogeneous invariants of positive degree such that S^L is finitely generated over* C*$[\theta_1, \ldots \theta_m]$ (such objects always exist), then $\theta_1, \ldots \theta_m$ are algebraically independent and S^L is a finitely generated free module over* C*$[\theta_1, \ldots \theta_m]$. That is, there exist homogeneous $\eta_1, \ldots \eta_s \in S^L$ such that*

$$S^L = \bigoplus_{i=1}^{s} \eta_i \mathrm{C}[\theta_1, \ldots \theta_m].$$

(2) If θ_j has degree d_j and η_i has degree e_i, then

$$F_L(t) = \frac{\sum_{i=1}^{s} t^{e_i}}{\prod_{j=1}^{m}(1 - t^{d_j})}.$$

(3) If we arrange the degrees so that $0 = e_1 \leq e_2 \leq \dots e_s$ and let μ be the least degree of a det^{-1}-invariant, then

$$e_s = \sum_{i=1}^{m}(d_i - 1) - \mu.$$

In particular, $e_s \leq \sum_{i=1}^{m}(d_i - 1)$ with equality occurring if and only if $L \subseteq SL(V)$.
(4) The d_j may be taken to divide l if so desired.
(5) The action of L on the quotient ring $S/(\theta_1, \dots \theta_m)$ is isomorphic to s times the regular representation of L.

□

For a given finite group $L \subseteq GL(V)$, there are explicit ways to construct elements $\theta_1, \dots \theta_m$ in the above theorem (see e.g., [31], page 483). However, we will not make use of these techniques in general. Instead, let us select a particularly nice class of finite groups.

Definition 3.4.2 *For $g \in L \subseteq GL(V)$, g is called a* pseudo-reflection *if exactly one eigenvalue of g is not equal to one. Moreover, we will call L a* finite reflection group *if L is generated by its pseudo-reflections.*

The key theorem about finite reflection groups is the following.

Theorem 3.4.3 *For L a finite subgroup of $GL(V)$, there exist m algebraically independent (homogeneous) invariants $\theta_1, \dots \theta_m$ such that $S^L = \mathbf{C}[\theta_1, \dots \theta_m]$ if and only if L is a reflection group.*

□

Moreover, quite a bit is known about the invariants of these groups. In fact, knowledge of the pseudo-reflections gives nice information in general.

Theorem 3.4.4 *(1) For any L, let the notation be as in Theorem 3.4.2. Also denote by r the number of pseudo-reflections contained in L. Then one has*

$$sl = \prod_{i=1}^{m} d_i$$

$$rs + 2\sum_{i=1}^{s} e_i = s(\sum_{i=1}^{m} d_i - m).$$

Also, the Laurent expansion of $F_L(t)$ about $t = 1$ begins as

$$\frac{1}{l}(1-t)^{-m} + \frac{r}{2l}(1-t)^{-m+1} + O((1-t)^{-m+2}).$$

(2) In particular, if L is a finite reflection group with $S^L = \mathbb{C}[\theta_1, \ldots \theta_m]$, then

$$l = \prod_{i=1}^{m} d_i,$$

$$r = \sum_{i=1}^{m}(d_i - 1),$$

$$F_L(t) = \frac{1}{\prod_{i=1}^{m}(1-t^{d_i})}.$$

□

A fact we will not make use of is that if L is a finite reflection group and if b_i is the number of elements in L with precisely i eigenvalues unequal to one, then

$$\sum_{i=0}^{m} b_i t^i = \prod_{j=1}^{m}(1 + (d_j - 1)t).$$

Another nice fact about reflection groups is that knowledge of S^L gives very good knowledge of any S^L_χ. In fact, one theorem is that if χ is a homomorphism, then S^L_χ is a free S^L-module of rank one. Moreover, a generator, called f_χ, can be written down explicitly using reflection hyperplanes (so $S^L_\chi = f_\chi S^L$). We will not do this here even though it is simple, but we will use the notation f_χ again in Theorem 3.4.5. We note only that in the case of $\chi = det^{-1}$, there is an alternate description of $f_{det^{-1}}$, namely as the Jacobian of $\theta_1, \ldots \theta_m$:

$$f_{det^{-1}} = det(\partial\theta_i/\partial x_j) \tag{3.6}$$

(up to a non-zero scalar).

Lastly, there is a theorem due to Stanley that will be useful. Before stating it, we simply note that there is a chain of technical conditions that a ring can satisfy with the following names and hierarchy: *polynomial ring ⇒ hypersurface ⇒ complete intersection ⇒ Gorenstein ⇒ Cohen-Macaulay.* Only the last of these have we really defined. It will not be worth our time to go deeper into these matters, however the interested reader may consult [31] for more details. Instead, we will allow ourselves to use the words to state the following theorem since the part that we will make use of will be explicitly spelled out in the text of the theorem.

Theorem 3.4.5 *(Stanley) Suppose $H = L \bigcap SL(V)$ where $L \subseteq GL(V)$ is a finite reflection group. If the index $[L : H]$ is a prime power, then S^H is a complete intersection. If $[L : H]$is a prime p, then S^H is a hypersurface; indeed, if $S^L = \mathbb{C}[\theta_1, \ldots \theta_m]$ and $\eta = f_\chi$ for the character $\chi = det$, then $S^H = \mathbb{C}[\theta_1, \ldots \theta_m](1 \bigoplus \eta \bigoplus \ldots \eta^{p-1})$.*

□

To give some idea of what the word hypersurface means in this context, we give the following. It has to do with the fact that if one chooses a set $\gamma_1, \ldots \gamma_t$ of minimal generators of a ring (here $t = m + 1$), then there is precisely one relation among the γ_i's (called a *syzygie of the first kind.* In other words, in the above theorem for the second case, one has generators $\theta_1, \ldots \theta_m, \eta$ and there is some polynomial relation P so that $\eta^p = P(\theta_1, \ldots \theta_m, \eta)$. Thus S^L is basically $\mathbb{C}[\theta_1, \ldots \theta_m, \eta]/\langle \eta^p - P(\theta_1, \ldots \theta_m, \eta)\rangle$, in other words, a "hypersurface."

3.5 The Cartan Polynomials

To begin with, let us make some notes about Cartan powers. To do this, we will look at various one parameter families of representations. In general, let G be a complex simple Lie group. Denote by $R(\psi)$ the irreducible representation of G with highest weight ψ. Then one may may form the vector space

$$R = \bigoplus_{n=0}^{\infty} R(\psi^n). \tag{3.7}$$

By making use of the fact that R is simply the *Cartan powers* of a single representation $R(\psi)$, one may put an algebra structure on R. To be a bit more specific, observe that within $R(\psi_1) \otimes R(\psi_2)$, $R(\psi_1\psi_2)$ appears exactly once. Then the multiplication of $R(\psi^{n_1})$ and $R(\psi^{n_2})$ within R is simply defined to be the tensor product of the two followed by projection onto the $R(\psi^{n_1+n_2})$ component.

The resulting algebra structure is well known. Let X be the G-orbit of the highest weight in $R(\psi)^*$, the dual of $R(\psi)$, and set $Y = \overline{X}$, the closure of X. Write $S(Y)$ for the restriction of the polynomials on $R(\psi)^*$ to Y. It turns out that the regular functions on X are isomorphic to $S(Y)$ which in turn is isomorphic to the algebra R.

Let us start with some general notations that will apply in all cases.

Definition 3.5.1 *Fix L to be one of the groups $L_2(q)$ for $q = 7, 9, 13$ so that we have L embedded inside a simple Lie group G or rank two (A_2, B_2, or G_2, respectively). Also* *fix an irreducible highest weight module $R(\psi)$ with highest weight ψ. Then forming the one-parameter algebra of Cartan powers R as in Equation 3.7, we may define a formal polynomial P_χ for each irreducible character χ of L by*

$$P_\chi(t) = \sum_{i=0}^{\infty} H_i t^i$$

where H_i is the multiplicity of the χ-isotypic component of L acting on $R(\psi^i)$ inside of R.

Of course, the above polynomials are very much related to the Poincaré polynomials discussed in Definition 3.4.1.

Next let us define an extension of the polynomials P_χ using the character formulas that we have already calculated. We will use the Schur orthogonality relations which tell us that if a representation of L has character χ_1, then the multiplicity of χ_2 in it is given by

$$\frac{1}{\mid L \mid} \sum_{g \in L} \chi_1(g)\overline{\chi_2(g)}. \tag{3.8}$$

Using this equation formally in conjunction with Theorems 3.3.1, 3.3.2, and 3.3.3, one is able to extend the polynomials P_χ:

Definition 3.5.2 *Continue the notation from Definition 3.5.1. For $i \geq 0$, we may write the differential of the weight ψ^i in the form $im\pi_\alpha + in\pi_\beta$ for some non-negative integers m, n (see the notation in Section 3.1). These integers may be put into Theorems 3.3.1, 3.3.2, and 3.3.3, respectively, to give the character of L acting on $R(\psi^i)$. If we call this character χ_i for $i \geq 0$, then we formally extend these definitions to the cases $i < 0$ by directly putting $im\pi_\alpha + in\pi_\beta$ into the character formulas for $i < 0$. Using these new χ_i for $i \in \mathbf{Z}$, we define the formal Laurent series Q_χ for each irreducible character χ of $L_2(q)$ to be*

$$Q_\chi(t) = \sum_{i=-\infty}^{\infty} H_i t^i$$

where H_i is the number that results from Equation 3.8 applied to $\chi_1 = \chi$ and $\chi_2 = \chi_i$. In particular, the coefficients of Q_χ of positive degree are the same as the coefficients of P_χ.

The reason for introducing Q_χ is that it will allow us to do some calculations. To see why this is so, we introduce one more piece of notation. For a formal Laurent series $q(t) = \sum_{i=-\infty}^{\infty} q_i t^i$, we will write $q^{a,b}(t) = q_a t^a + q_{a+1} t^{a+1} + \ldots q_b t^b$ where $a, b \in \mathbf{Z} \bigcup \{\pm\infty\}$ with $a \leq b$. In particular, $Q_\chi^{a,b}$ is the part of Q_χ that has degree between (and including) a and b. For instance, $P_\chi = Q_\chi^{0,\infty}$.

What will happen is that by looking at Theorems 3.3.1, 3.3.2, and 3.3.3, we will easily be able to find a polynomial D of some degree d such that

$$DQ_\chi \ = \ 0. \tag{3.9}$$

Then writing $Q_\chi = P_\chi + Q_\chi^{-\infty,-1}$, we get

$$DP_\chi = -DQ_\chi^{-\infty,-1}.$$

However, since D is a polynomial of degree d and P_χ is a formal polynomial, by looking at degrees, this becomes

$$DP_\chi \ = \ -(DQ_\chi^{-d,-1})^{0,d-1}. \tag{3.10}$$

The advantage to this formula is that it is very useful for computations since (once D is known), then after computing d terms of coefficients of Q_χ we have an explicit formula for P_χ.

3.6 Some Invariants of A_2

The finite group in this section will be $L = L_2(7)$ inside of $SL(3,\mathbf{C})$. Of course it sits in $SL(3,\mathbf{C})$ in two distinct ways. We shall choose the embedding as in Theorem 3.3.1 (the other is just the dual).

The one-parameter family that we will concentrate the most on is the Cartan powers of one of the standard three dimensional representations. This is because they will yield the simplest results. Let us take in Equation 3.7 ψ to have differential π_α (see Theorem 3.3.1) and form the one parameter family of representations R of $SL(3,\mathbf{C})$, i.e., of the standard representation. If we had chosen the other three dimensional representation, π_β, everything would be made into its dual. Next, we would like to examine the restriction of the $SL(3,\mathbf{C})$ action on R to the finite group $L_2(7)$. Our goal is to calculate the formal polynomials $P_{\chi_i}(t)$ in Definition 3.5.1 where $1 \leq i \leq 6$ (see the notation of Theorem 3.2.1) and to find the algebra structure of $R^{L_2(7)}$, the isotypic component of the trivial representation.

It will be easy find the formal polynomials P_{χ_i} using Equation 3.10. By Theorem 3.3.1, we find the characters values on the various conjugacy classes for $R(k\pi_\alpha)$ to be

$$\begin{aligned}
\chi_{\Lambda(k,0)}(I) &= (k+2)(k+1)/2 \\
\chi_{\Lambda(k,0)}(S) &= (-1)^{k+1}[(k+1) + R_2(k+1)]/2 \\
\chi_{\Lambda(k,0)}(A) &= \delta^{(3)}_{k=0} \\
\chi_{\Lambda(k,0)}(K) &= [R_4(k+1) + 1 - R_4(k+2)]/2
\end{aligned}$$

$$\begin{aligned}
\chi_{\Lambda(k,0)}(M_1) &= [R_7(k+4) - R_7(k-1) + (\delta^{(7)}_{k=1} - \delta^{(7)}_{k=3})i\sqrt{7}]/2 \\
\chi_{\Lambda(k,0)}(M_\lambda) &= [R_7(k+4) - R_7(k-1) - (\delta^{(7)}_{k=1} - \delta^{(7)}_{k=3})i\sqrt{7}]/2.
\end{aligned}$$

Since Q_{χ_i} (Definition 3.5.2) is put together term by term using the above character values and the Schur Orthogonality relations, it will be true that the polynomial

$$D(t) = (1-t^4)(1-t^6)(1-t^{14})$$

will satisfy

$$D(t)Q_{\chi_i}(t) = 0.$$

For instance, $(1-t^{14})Q_{\chi_i}(t)$ will "kill" the contribution from the elements M_1 and M_λ since 14 is a multiple of 7 (the choice of 14 instead of the apparently simpler 7 will be discussed later). Similarly, multiplying by $(1-t^4)$ will "kill" the contribution of K. The combination of $(1-t^4)(1-t^6)$ will "kill" the S part (we need to apply an even degree twice since there is also a linear dependence on k for the character of S) and the total $(1-t^4)(1-t^6)(1-t^{14})$ will kill the quadratic dependence on k of I.

Thus using Equation 3.10, we may compute the formal polynomials P_{χ_i}. Since the proof is just a matter of calculating a finite number of terms and multiplying polynomials, we will omit the calculations in the following theorem.

Theorem 3.6.1 *The Cartan powers of the representation π_α of $SL(3,\mathbf{C})$ restricted to $L_2(7)$ yield the formal polynomials*

$$P_{\chi_i}(t) = \frac{p_{\chi_i}(t)}{(1-t^4)(1-t^6)(1-t^{14})}$$

where the polynomials p_{χ_i} are given by

$$\begin{aligned}
p_{\chi_1}(t) &= 1 + t^{21} \\
p_{\chi_2}(t) &= t + t^8 + t^9 + t^{11} + t^{16} + t^{18} \\
p_{\chi_3}(t) &= t^3 + t^5 + t^{10} + t^{12} + t^{13} + t^{20} \\
p_{\chi_4}(t) &= t^2 + t^4 + t^6 + t^8 + t^9 + t^{10} + t^{11} + t^{12} + t^{13} + t^{15} + t^{17} + t^{19} \\
p_{\chi_5}(t) &= t^3 + t^5 + t^6 + t^7 + t^8 + t^9 + t^{10} + t^{11} + t^{12} + t^{13} + t^{14} + t^{15} + t^{16} + t^{18} \\
p_{\chi_6}(t) &= t^4 + t^5 + t^6 + 2t^7 + t^8 + t^9 + t^{10} + t^{11} + t^{12} + t^{13} + 2t^{14} + t^{15} + t^{16}.
\end{aligned}$$

□

We note only that of course the polynomial $D(t)$ used above is not unique. Many others will work and some will greatly simplify the above results. For instance, one can check that with this denominator $(1-t^2)(1-t^3)(1-t^4)(1-t^7)$, one may also write the formal polynomials above as

$$P_{\chi_i}(t) = \frac{p'_{\chi_i}(t)}{(1-t^2)(1-t^3)(1-t^4)(1-t^7)}$$

where the polynomials p'_{χ_i} are given by

$$\begin{aligned} p'_{\chi_2}(t) &= t - t^3 - t^4 + t^6 + t^7 - t^{10} \\ p'_{\chi_3}(t) &= t^3 - t^6 - t^7 + t^9 + t^{10} - t^{12} \\ p'_{\chi_4}(t) &= t^2 - t^5 + t^8 - t^{11} \\ p'_{\chi_5}(t) &= t^3 - t^{10} \\ p'_{\chi_6}(t) &= t^4 + t^5 - t^8 - t^9. \end{aligned}$$

We have omitted p'_{χ_1} since it is considerable worse with this denominator. However, the others are much simpler. The particular choice of $D(t) = (1-t^4)(1-t^6)(1-t^{14})$ in the above theorem is related to the fact that we are actually dealing with something very close to a finite reflection group and the numbers $4, 6, 14$ are related to the minimal generators.

To see this, let us momentarily view $L = L_2(7)$ as sitting in $SL(3, \mathbb{C})$ by the dual of our three dimensional representation (whose differential will be π_β). Then if we write L' for the subgroup in $GL(3, \mathbb{C})$ generated by L and $\pm I$, the order of L' will be $2(168) = 336$. We have already seen that L has 21 elements of order 2 (Theorem 3.2.1) so that L' will have $42 + 1$ elements of order 2 with only $21 + 1$ of them having determinant -1. It is clear that 21 of these elements make up the set of all reflections of $L' \subseteq GL(3, \mathbb{C})$. It is also classically known and easy to verify that these reflections generate L' (see [30] §4.6). Thus we have that L' is a finitely generated reflection group with 21 reflections. Hence, with the notation of Section 3.4, we know that the ring of invariants of L', $S(R(\pi_\beta))^{L'}$ is of the form $\mathbb{C}[\theta_1, \theta_2, \theta_3]$ (Theorem 3.4.3). Moreover, Theorem 3.4.4 part (2) tells us that if we write d_i for the degree of θ_i, that $336 = d_1 d_2 d_3$ and $21 = d_1 + d_2 + d_3 - 3$. One may quickly check that the only possible solution is $d_1 = 4, d_2 = 6, d_3 = 14$. Thus,

$$F_{L'}(t) = \frac{1}{(1-t^4)(1-t^6)(1-t^{14})}.$$

Next, we of course have the order of L' in L is 2, a prime, and since $L' \bigcap SL(3, \mathbb{C}) = L$, we are in a position to apply Theorem 3.4.5. Using the fact that *det* maps L' to $\{\pm 1\}$

and Equation 3.6, to get the degree of $f_{det} = f_{det^{-1}}$ to be 21, we get

$$F_L(t) = \frac{1 + t^{21}}{(1 - t^4)(1 - t^6)(1 - t^{14})}.$$

This, of course looks suspiciously like our result for $P_{\chi_1}(t)$ in Theorem 3.6.1.

The reason stems from our discussion in Section 3.5. Since the orbit of the highest weight vector in the three dimensional representation under $SL(3, \mathbf{C})$ is everything but zero, its closure is all of $\mathbf{C}^3$. Therefore the algebra of Cartan powers, R, is isomorphic to $S(\mathbf{C}^3)$ as $SL(3, \mathbf{C})$ graded modules and algebras. Hence we have R^L isomorphic to $S^L(\mathbf{C}^3)$. Thus, by the above results, R has elements $\theta_4, \theta_6, \theta_{14}, \theta_{21}$ of degrees $4, 6, 14, 21$, respectively, so that the first three are algebraically independent and

$$R = \mathbf{C}[\theta_4, \theta_6, \theta_{14}](1 \bigoplus \theta_{21})$$

with $\theta_{21}^2 \in \mathbf{C}[\theta_4, \theta_6, \theta_{14}]$. Now the structure of $S^L(3, \mathbf{C})$ is classically known. Springer ([30] §4.6.5) has worked out by some explicit computations that the generators may be chosen so that

$$\theta_{21}^2 + \theta_{14}^3 + \theta_6^7 \in \theta_4 \, S^L(\mathbf{C}^3).$$

To give an idea of what these invariants are, we note that the degree 6 invariant is basically the Klein curve of genus three, $x^3y + y^3z + z^3x$, and the degree 6 invariant is basically the Wronskian of this.

We observe that if we had looked at the Cartan powers of π_β instead of π_α, the whole story would be the same except one should switch χ_2 and χ_3 everywhere (this follows by duality).

Last, we give some indication of why the Cartan powers of π_α are the only "nice" ones. For instance, one of the next simplest cases is the case of Cartan powers of $\rho = \pi_\alpha + \pi_\beta$. In fact, the characters on this one-parameter family are very nice. Using Theorem 3.3.2 they are:

$$\begin{aligned}
\chi_{\Lambda(k,k)}(I) &= (k+1)^3 \\
\chi_{\Lambda(k,k)}(S) &= (k+1)R_2(k+1) \\
\chi_{\Lambda(k,k)}(A) &= R_3(k+1) \\
\chi_{\Lambda(k,k)}(K) &= R_4(k+1) \\
\chi_{\Lambda(k,k)}(M_1) &= R_7(k+1) \\
\chi_{\Lambda(k,k)}(M_\lambda) &= R_7(k+1).
\end{aligned}$$

However, one may check, by techniques similar to Theorem 3.6.1 that the formal polynomials may be written as

$$P_{\chi_i}(t) = \frac{p_{\chi_i}}{(1-t^2)(1-t^3)(1-t^4)(1-t^7)}$$

where the polynomials p_{χ_i} are given by

$$\begin{aligned}
p_{\chi_1}(t) &= 1 - t^2 + t^5 + 2t^6 + 2t^8 + t^9 - t^{12} + t^{14} \\
p_{\chi_2}(t) &= t^3 + 2t^4 + 3t^5 + 2t^6 + 2t^7 + 2t^8 + 3t^9 + 2t^{10} + t^{11} \\
p_{\chi_3}(t) &= p_{\chi_2}(t) \\
p_{\chi_4}(t) &= 2t^2 + 2t^3 + 4t^4 + 4t^5 + 4t^6 + 4t^7 + 4t^8 + 4t^9 + 4t^{10} + 2t^{11} + 2t^{12} \\
p_{\chi_5}(t) &= t^2 + 3t^3 + 3t^4 + 5t^5 + 6t^6 + 6t^7 + 6t^8 + 5t^9 + 3t^{10} + 3t^{11} + t^{12} \\
p_{\chi_6}(t) &= t + t^2 + 2t^3 + 4t^4 + 5t^5 + 7t^6 + 8t^7 + 7t^8 + 5t^9 + 4t^{10} + 2t^{11} + t^{12} + t^{13}.
\end{aligned}$$

The denominator used appears to give the simplest form of these rational functions. Already everything is more complicated. However, the worst part comes when one tries to look for generators for R^L. Just by writing out a few terms of $P_{\chi_1}(t)$ and looking at dimensions, one may check that as an algebra, R^L has *at least* generators in degrees 3, 4, 5, two in 6, two in 7, four in 8, two in 9, and three in degree 10. Therefore, R^L has at least 16 generators and is quite intractable. The problem appears to be related to the fact that in the Adjoint representation, L is no longer related to a reflection group.

3.7 Some Invariants of B_2

Let us look at $L = L_2(9)$ embedded in $SO(5, \mathbf{C})$. In this case, the best series to examine will be the Cartan powers of π_β, i.e., of the standard five dimensional representation.

First we calculate the characters of the conjugacy classes of L. For this, Theorem 3.3.2 tells us that the on $R(k\pi_\beta)$ we get:

$$\begin{aligned}
\chi_{\Lambda(0,k)}(I) &= (k+1)(k+2)(2k+3)/6 \\
\chi_{\Lambda(0,k)}(S) &= [(k+1) + R_{(2)}(k+1)]/2 \\
\chi_{\Lambda(0,k)}(A) &= \delta^{(4)}_{k=0} - \delta^{(4)}_{k=1} \\
\chi_{\Lambda(0,k)}(K) &= \delta^{(5)}_{k=0} - \delta^{(5)}_{k=3} \\
\chi_{\Lambda(0,k)}(K^2) &= \chi_{\Lambda(0,k)}(K) \\
\chi_{\Lambda(0,k)}(M_1) &= [(k+2)R_{(3)}(k+1) - (k+1)R_{(3)}(k+2)]/3 \\
\chi_{\Lambda(0,k)}(M_\lambda) &= [(2k+3) - R_{(3)}(2k+3)]/3.
\end{aligned}$$

Next, one sees from this (just as we did in Section 3.6) that if $D(t) = (1-t^3)(1-$

$t^4)(1-t^5)(1-t^6)$, that $D(t)Q_{\chi_i}(t) = 0$. The results of applying Equation 3.10 to this yields the following theorem. Again, the trivial calculations will be omitted.

Theorem 3.7.1 *The Cartan powers of the representation π_β of $SO(5, \mathbf{C})$ restricted to $L_2(9)$ yield the formal polynomials*

$$P_{\chi_i}(t) = \frac{p_{\chi_i}(t)}{(1-t^3)(1-t^4)(1-t^5)(1-t^6)}$$

where the polynomials p_{χ_i} are given by

$$\begin{aligned}
p_{\chi_1}(t) &= 1 + t^{15} \\
p_{\chi_2}(t) &= t + t^2 + t^3 + t^4 + t^5 + t^{10} + t^{11} + t^{12} + t^{13} + t^{14} \\
p_{\chi_3}(t) &= t^3 + t^5 + 2t^6 + t^7 + x^8 + 2t^9 + t^{10} + t^{12} \\
p_{\chi_4}(t) &= t^4 + 2t^5 + 2t^6 + 3t^7 + 3t^8 + 2t^9 + 2t^{10} + t^{11} \\
p_{\chi_5}(t) &= t^4 + 2t^5 + 2t^6 + 3t^7 + 3t^8 + 2t^9 + 2t^{10} + t^{11} \\
p_{\chi_6}(t) &= t^2 + t^3 + 2t^4 + t^5 + 2t^6 + 2t^7 + 2t^8 + 2t^9 + t^{10} + 2t^{11} + t^{12} + t^{13} \\
p_{\chi_7}(t) &= t^3 + t^4 + 2t^5 + 3t^6 + 3t^7 + 3t^8 + 3t^9 + 2t^{10} + t^{11} + t^{12}.
\end{aligned}$$

□

As with $SL(3, \mathbf{C})$, a more tidy denominator would have been given by, say, $D(t) = (1-t^3)^2(1-t^4)(1-t^5)$. However, there is a reason for the above choice. Again, the answer deals with a closely associated finite reflection group. We will sketch the correspondence.

The first step is to make use of the classic isomorphism of $L_2(9)$ with A_6, the *alternating group on 6 letters* (see [7]). The reason this is useful is because the symmetric group S_6 acts as a finite reflection group (of course even as a Weyl group) on $\mathbf{C}^5$. It is well known by the theory of symmetric polynomials that the degrees of the invariants of this action are $2, 3, 4, 5, 6$. Since we may pick A_6 out as $S_6 \bigcap SL(5, \mathbf{C})$, we may apply Theorem 3.4.5 and Equation 3.6 to get that the ring of invariants of A_6 acting on $\mathbf{C}^5$ to be isomorphic to

$$\mathbf{C}[\theta_2, \theta_3, \theta_4, \theta_5, \theta_6](1 \bigoplus \theta_{15})$$

where θ_d is a generator of degree d with the only relation being of the form θ_{15}^2 a polynomial in the θ's.

We would like to make use of our discussion in Section 3.5 of the Cartan powers. First, let X be the $O(5, \mathbf{C})$ orbit of the highest weight vector in $\mathbf{C}^5$ (everything is self dual here). Then $X = \{(z_1, \ldots z_5) \mid z_i \in \mathbf{C}, z_1^2 + \ldots z_5^2 = 0\}$. Let j_2 be the second degree polynomial $z_1^2 + \ldots z_5^2$. By classical separation of variables for the orthogonal group or by the more general techniques in [15], one knows that $S(\mathbf{C}^5) = j_2 S(\mathbf{C}^5) \bigoplus H$, where H are the *harmonic* polynomials. One knows that $j_2 S(\mathrm{C}^5)$ is a prime ideal in $S(\mathrm{C}^5)$ so that the restriction of $S(\mathrm{C}^5)$ to X is the same as looking at $S(\mathrm{C}^5)$ projected onto $S(\mathrm{C}^5)/j_2 S(\mathrm{C}^5)$. However by our earlier discussion, this restriction is just the algebra of Cartan powers.

Since j_2 is a second degree invariant of $O(5, \mathrm{C})$, we may of course take j_2 to be the degree two invariant for A_6. Hence, if we look at $S^{A_6}(\mathrm{C}^5)/j_2 S^{A_6}(\mathrm{C}^5)$, it is easy to see that we are really looking at $R^{L_2(9)}(\pi_\beta)$. But since we have seen that we may identify θ_2 with j_2, we finally get that $R^{L_2(9)}(\pi_\beta)$ is isomorphic to

$$\mathrm{C}[\theta_3, \theta_4, \theta_5, \theta_6](1 \bigoplus \theta_{15})$$

where the degree of θ_d is d with the only relation being of the form θ_{15}^2 the corresponding polynomial in the θ's. Thus we recover the polynomial $P_{\chi_1}(t)$ in Theorem 3.7.1 and the basic algebraic structure of $R^L(\pi_\beta)$.

Lastly, this appears to be the best one-parameter family. Probably the next best is $2\pi_\alpha$ (the 10 dimensional Adjoint representation). One can write down the formal polynomials for it easy enough, but the answers are quite unpleasant. Moreover, the situation for generators in R^L is much worse. One may check by dimensions that R^L must have generators *at least* in degrees: two in 4, three in 6, two in 7, and four in degree 9 which already gives at least 26 generators. Things become even worse in other one-parameter families. For instance in the 2ρ (81 dimensional) family, one quickly checks that there are already eight generators in degree 2, twenty three in degree 3, and wildly out of control thereafter. As before with the $SL(3, \mathrm{C})$ case, it seems that we are only able to get simple results when there is a finite reflection group somehow involved.

3.8 Some Invariants of G_2

For G_2, there are apparently no simple one-parameter families to consider. To show how bad things are, we will calculate for the reader the polynomials P_{χ_1} for three of the simplest families using Theorem 3.3.3 and Equation 3.10.

The first family we will consider is $R(\pi_\alpha)$ where π_α is the standard 7 dimensional representation. One may check that P_{χ_1} is given by

$$\frac{p(t)}{D(t)}$$

where

$$D(t) = (1 - t^2)^2(1 - t^3)(1 - t^6)(1 - t^7)(1 - t^{13})$$

and

$$p(t) \;=\; 1 - 2t^2 - t^3 + 2t^4 + 2t^5 - t^6 - 2t^7 + 2t^8 + 3t^9 + t^{10}$$

$$-2t^{11} + 2t^{13} + 2t^{14} + 2t^{15} - 2t^{17} + t^{18} + 3t^{19} + 2t^{20}$$
$$-2t^{21} - t^{22} + 2t^{23} + 2t^{24} - t^{25} - 2t^{26} + t^{28}.$$

As one can see, this is quite horrible. One may check that R^L has generators at least in degree 4, two in 6, one in 7, two in 8, two in 9, five in 10, four in 11, seven in 12, eight in 13, ten in 14, and that is just the start.

The second family we will consider is $R(\pi_\beta)$ where π_β is the 14 dimensional Adjoint representation. One may check that P_{χ_1} is given by

$$\frac{p(t)}{D(t)}$$

where

$$D(t) = (1-t^2)^2(1-t^3)(1-t^6)(1-t^7)(1-t^{13})$$

and

$$\begin{aligned} p(t) &= 1 - 2t^2 - t^3 + 2t^4 + 2t^5 + 3t^6 + t^7 + 4t^8 + 6t^9 + 6t^{10} \\ &\quad +4t^{11} + 7t^{12} + 7t^{13} + 9t^{14} + 10t^{15} + 9t^{16} + 7t^{17} + 7t^{18} + 4t^{19} + 6t^{20} \\ &\quad +6t^{21} + 4t^{22} + t^{23} + 3t^{24} + 2t^{25} + 2t^{26} - t^{27} - 2t^{28} + t^{30}. \end{aligned}$$

As one can see, this is quite horrible. One may check that R^L has generators at least in degree 4, six in 6, four in 7, thirteen in 8, fifteen in 9, twenty-four in 10, and that is also just the start.

The last family we will consider is $R(\rho)$ where $\rho = \pi_\alpha + \pi_\beta$ is 64 dimensional. One may check that in this case P_{χ_1} is given by

$$\frac{p(t)}{D(t)}$$

where

$$D(t) = (1-t^2)^3(1-t^3)^2(1-t^6)(1-t^7)(1-t^{13})$$

and

$$\begin{aligned} p(t) &= 1 - t^2 + 3t^3 + 13t^4 + 30t^5 + 60t^6 + 98t^7 \\ &\quad +145t^8 + 188t^9 + 219t^{10} + 238t^{11} + 224t^{12} + 242t^{13} + 186t^{14} + 140t^{15} \\ &\quad +97t^{16} + 53t^{17} - 53t^{19} - 97t^{20} - 140t^{21} - 186t^{22} - 224t^{23} \\ &\quad -242t^{24} - 238t^{25} - 219t^{26} - 188t^{27} - 145t^{28} - 98t^{29} \\ &\quad -60t^{30} - 30t^{31} - 13t^{32} - 3t^{33} + t^{34} - t^{36}. \end{aligned}$$

Again, this is horrible and the list of necessary generators for R^L is really quite outrageous.

The idea of these three calculations is to say that there does not seem to be any simple one parameter families (as far as their polynomials are concerned) for G_2. Looking back at the last two sections, this appears to be related to the fact that no finite reflection groups are involved. (For a classification of such objects, see [29]). One possible idea for cleaning up the results is to look at functions restricted to a different space than the orbit of the highest weight. This area does not seem to have been very much explored to date.

Bibliography

[1] A. V. Alekseevskiĭ. On gradings of simple Lie algebras connected with groups generated by transvections. *Amer. Math. Soc. Transl. (2)*, 151:1–40, 1992.

[2] T. Brocker and T. tom Dieck. *Representations of Compact Lie Groups.* Springer-Verlag, 1985.

[3] A. M. Cohen and D. B. Wales. Finite subgroups of $G_2(\mathbf{C})$. *Comm. Algebra*, 11(4):441–459, 1983.

[4] A. M. Cohen and D. B. Wales. Finite subgroups of $E_6(\mathbf{C})$ and $F_4(\mathbf{C})$. preprint, 1992.

[5] A. M. Cohen and D. B. Wales. Finite simple subgroups of semisimple complex Lie groups–a survey. preprint, 1994.

[6] Arjeh M. Cohen, Jr. Robert L. Griess, and Bert Lisser. The groups $L(2, 61)$ embeds in the Lie group of type E_8. *Comm. Algebra*, 21(6):1889–1907, 1993.

[7] J. H. Conway, R. T. Curtis, et al. *Atlas of Finite Groups.* Clarendon Press, Oxford, 1985.

[8] Larry Dornhoff. *Group Representation Theory: Part A.* Marcel Dekker, Inc., 1971.

[9] James E. Humphreys. *Introduction to Lie Algebras and Representation Theory.* Springer-Verlag, 1972.

[10] James E. Humphreys. *Reflection Groups and Coxeter Groups.* Cambridge University Press, 1990.

[11] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory.* Springer-Verlag, 1990.

[12] Victor G. Kac. Simple Lie groups and the Legendre symbol. In R. K. Amayo, editor, *Algebra: Carbondale 1980, Proceedings*, pages 110–123. Springer-Verlag, 1980. Lecture Notes in Math., 848.

[13] Peter B. Kleidman and A. J. E. Ryba. Kostant's conjecture holds for E_7: $L_2(37) < E_7(\mathbf{C})$. *J. Algebra*, 161:535–540, 1993.

[14] Bertram Kostant. The principal 3-dimensional subgroup and the Betti numbers of a complex simple Lie group. *Amer. J. of Math.*, pages 973–1032, Oct. 1959.

[15] Bertram Kostant. Lie group representations on polynomial rings. *Amer. J. of Math.*, 85:327–404, 1963.

[16] Bertram Kostant. On Macdonald's η-function formula, the Laplacian, and generalized exponents. *Adv. in Math.*, 20:179–212, 1976.

[17] Bertram Kostant. A tale of two conjugacy classes. Colloquium Lecture of the Amer. Math. Soc., 1983. in preparation.

[18] Bertram Kostant. The McKay correspondence, the Coxeter element, and representation theory. In *Societe Math. de France*, pages 209–255, 1985.

[19] A. I. Kostrikin. Invariant lattices in Lie algebras and their automorphism groups. In Kai N. Cheng and Yu K. Leong, editors, *Group Theory.* Proceedings of the Singapore Group Theory Conference, June 8-19, 1987, 1989.

[20] A. I. Kostrikin, I. A. Kostrikin, and V. A. Ufnarovskiǐ. Orthogonal decompositions of simple Lie algebras. *Soviet Math. Dokl.*, 24(2):292–297, 1981.

[21] A. I. Kostrikin, I. A. Kostrikin, and V. A. Ufnarovskiǐ. Multiplicative decompositions of simple Lie algebras. *Soviet Math. Dokl.*, 25(1):23–27, 1982.

[22] A. I. Kostrikin, I. A. Kostrikin, and V. A. Ufnarovskiǐ. On decompositions of classical Lie algebras. *Proc. Steklov Inst. Math.*, 166(1):117–133, 1986.

[23] A. Meurman. An embedding of $PSL(2,13)$ in $G_2(\mathbf{C})$. In *Article in Lie Algebras and Related Topics, SLN 933.* Lecture Notes in Mathematics 933, 1982.

[24] R. V. Moody and J. Patera. Characters of elements of finite order in Lie groups. *SIAM J. Alg. Disc. Meth.*, 5(3):359–383, September 1984.

[25] R. V. Moody, J. Patera, and R. T. Sharp. Character generators for elements of finite order in simple Lie groups A_1, A_2, A_3, B_2, and G_2. *J. Math. Phys.*, 24(10):2387–2396, October 1983.

[26] M. A. Naimark and A. I. Štern. *Theory of Group Representations.* Springer-Verlag, 1982.

[27] Mohammad Ali Najafi. Clifford algebra structure on the cohomology algebra of compact symmectric spaces. Master's thesis, MIT, February 1979.

[28] A. L. Onishchik and E. B. Vinberg. *Lie Groups and Algebraic Groups.* Springer-Verlag, 1990.

[29] G. C. Shephard and J. A. Todd. Finite unitary reflection groups. *Canad. J. Math.*, 6:274–304, 1954.

[30] T. A. Springer. *Invariant Theory, Lecture Notes in Mathematics #585.* Springer-Verlag, 1970.

[31] Richard P. Stanley. Invariants of finite groups and their applications to combinatorics. *Bull. (New Series) Amer. Math. Soc.*, 1(3):475–511, May 1979.

[32] J. G. Thompson. A conjugacy theorem for E_8. *J. Algebra*, 38:525–530, 1976.