A Structure Theorem for Plesken Lie Algebras over Finite Fields

A Senior Project submitted to
The Division of Science, Mathematics, and Computing
of
Bard College

by
Mona Merling

Annandale-on-Hudson, New York
May, 2009

Abstract

W. Plesken found a simple but interesting construction of a Lie algebra from a finite group. Cohen and Taylor posed themselves the question of what the Plesken Lie algebra, which is the Lie subalgebra of the group algebra $k[G]$ generated by the elements $g - g^{-1}$, could be. The result is very fascinating: It turns out that the Lie algebra decomposition of the Plesken Lie algebra into simple Lie algebras corresponds to the irreducible characters of the group, more preciselyto the types and sizes of characters.

The main idea of the present project was to find a similar decomposition result over a finite field instead of the complex numbers. When we lose algebraic closure, a lot of theorems do not hold anymore, and the problem becomes a lot harder. We take two approaches of reducing the Plesken Lie algebra modulo a prime: On one hand, we use the standard Chevalley basis approach, i.e., we find a Chevalley basis which by definition has integral coeffiecients, consider the $\mathbf{Z}$ lattice it defines and reduce it modulo a prime p. On the other hand, we start with the group algebra $\mathbf{F}_p[G]$ and define the plesken Lie subalgera directly. By comparing the results gotten from the different approaches, we get a fascinating theorem that relates the differences of the Plesken Lie algebra over a finite field of characteristic p to the way in which the prime p behaves in the splitting field of the group G, which is an extension of $\mathbf{Q}$.

Contents

Acknowledgments

I would like to thank John for his tutorial in algebraic number theory, the representation theory class and the great senior project idea he has given me. I would like to thank Greg for his tutorial in Lie algebras. If it had not been for these tutorials and classes, I would not have been able to dwelve so deep into this project.

1
Lie Algebras

This chapter is intended to familiarize the reader with the basic concepts in the theory of Lie algebras, group algebras, representation theory and some more advanced topics in linear algebra. We assume basic knowledge of linear and abstract algebra.

1.1 Basic Definitions and Examples

Lie algebras are vector spaces endowed with an additional operation, called the "bracket operation". The Lie algebras that arise in physics and chemistry have the bracket operation $[x, y] = xy - yx$ for x, y in the underlying vector space and the operations on the right being the ones specific to the application. Lie algebras are in a sense less intuitive than groups; for instance not only are they non-commutative, but they are not associative either. We give a precise definition of a Lie algebra and then we will illustrate the concepts through concrete examples.

Definition 1.1.1. Let k be a field. A **Lie algebra** L over k is a k-vector space L together with a bilinear map

$$[\ ,\ ] : L \times L \to L$$

(called the **bracket** or **commutator**) satisfying:

1. $[x, x] = 0$ for all x in L;

2. $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ for all x, y, z in L. (Jacobi identity)

$\triangle$

Notice that bilinearity and condition (1) give:

$$\begin{aligned} 0 &= [x + y, x + y] \\ &= [x, x + y] + [y, x + y] \\ &= [x, x] + [x, y] + [y, x] + [y, y] \\ &= [x, y] + [y, x], \end{aligned}$$

so we get that anticommutativity:

$$[x, y] = -[y, x] \text{ for all } x, y \in L.$$

We will now give some examples of Lie algebras.

Example 1.1.2. Let V be a finite dimensional vector space of dimension n over a field k. Let $\mathrm{End}(V)$ be the ring of linear maps from V to V. This is also a vector space over k and it can be viewed as a Lie algebra, the so called **general linear Lie algebra**, denoted $\mathfrak{gl}(n, k)$, if we define the bracket by

$$[x, y] = x \circ y - y \circ x \text{ for } x, y \in \mathrm{End}(V),$$

where $\circ$ denotes composition of linear transformations.

Upon choosing a basis for V, the vector space of all $n \times n$ matrices over k with the Lie bracket defined by

$$[x, y] = xy - yx,$$

where the multiplication on the right is the usual product of matrices, coincides with $\mathfrak{gl}(n, k)$. $\Diamond$

We define the notion of a **Lie subalgebra** in the obvious way: A subspace S of L is a subalgebra if it is closed under the bracket operation. Note that any nonzero element $x \in L$ defines a one dimensional Lie subalgebra with trivial multiplication.

Example 1.1.3. Let $\mathfrak{sl}(n,k)$ be the subspace of $\mathfrak{gl}(n,k)$ consisting of the matrices of trace 0. For arbitrary square matrices x and y of trace zero, the matrix $xy - yx$ also has trace 0 since $\mathrm{tr}(xy) = \mathrm{tr}(yx)$. Therefore $\mathfrak{sl}(n,k)$ is closed under the Lie bracket, and therefore it is a Lie algebra, the **special linear algebra**. $\Diamond$

It will be important to observe that any **associative algebra** can be made into a Lie algebra in a natural way. We define an associative algebra first:

Definition 1.1.4. An **algebra** A over a field k is a vector space A over k together with a bilinear map,

$$A \times A \to A,\ (x,y) \mapsto xy.$$

$\triangle$

We call xy the **product** of x and y. Lie algebras are the algebras for which the product satisfies identities (1) and (2) of Definition 1.1.1. In this case, the product is denoted $[x,y]$.

Definition 1.1.5. An algebra A is **associative** if

$$(xy)z = x(yz) \text{ for all } x,y,z \in A.$$

$\triangle$

Definition 1.1.6. An algebra A is **unital** if there is an element 1_A in A such that

$$1_a x = x 1_a \text{ for all nonzero } x \in A.$$

$\triangle$

For example, $\mathfrak{gl}(V)$, the vector space of linear transformations of the vector space V is a unital associative algebra where the product is given by the composition of maps. The identity element is

the identity transformation. Unlike most algebras that one encounters, note that Lie algebras are neither associative nor unital. However, we can turn any associative algebra A into a Lie algebra by defining the following bracket operation:

$$[x, y] = xy - yx \text{ for all } x, y \in A.$$

Note that $\mathrm{End}(V)$ is just a special case of this construction.

We say that a Lie algebra is **abelian** if $[x, y] = [y, x]$ for all x, y in L. Note that this is equivalent to requiring that $[x, y] = 0$ for all x, y in L. A **homomorphism** ϕ of two Lie algebras L, L' is linear map $\phi : L \to L'$ satisfying $\phi([x, y]) = [\phi(x), \phi(y)]$. A very important homomorphism is the **adjoint homomorphism**. We define

$$\mathrm{ad} : L \to \mathfrak{gl}(n, k)$$

by $(\mathrm{ad}\, x)(y) = [x, y]$ for $x, y \in L$. Since the Lie bracket is bilinear, $\mathrm{ad}\, x$ is a linear map for $x \in L$. We also get that the map $x \mapsto \mathrm{ad}\, x$ is also linear. The condition

$$\mathrm{ad}([x, y]) = \mathrm{ad}\, x \circ \mathrm{ad}\, y - \mathrm{ad}\, y \circ \mathrm{ad}\, x \text{ for all } x, y \in L;$$

is equivalent to the Jacobi identity. We thus get that ad is a homomorphism.

1.2 The Group Algebra

In this project we will be concerned with a specific type of Lie algebra, namely a group algebra. We will give the definition of a group algebra and then prove that it is indeed a Lie algebra.

Definition 1.2.1. Let G be a group and k a field. The **group algebra** $k[G]$ is the set of all formal linear combinations of finitely many elements of G with coefficients in k. $\triangle$

The elements of $k[G]$ have the form

$$a_1 g_1 + a_2 g_2 + \cdots + a_n g_n,$$

where $a_i \in k$ and $g_i \in G$ for all i. We can denote this element in general by $\sum_{g \in G} a_g g$, where $a_g = 0$ for all but finitely many elements of G. The group algebra $k[G]$ is an algebra over k with respect

to the addition defined by the rule

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G}(a_g + b_g)g,$$

the product by a scalar given by

$$a\sum_{g\in G} a_g g = \sum_{g\in G}(aa_g)g,$$

and the multiplication

$$(\sum_{g\in G} a_g g)(\sum_{h\in G} b_h h) = \sum_{g\in G, h\in G}(a_g b_h)gh.$$

The multiplication in $k[G]$ is not necessarily a commutative operation. Note that $k[G]$ is a vector space over k and the elements of G form a basis. Moreover, $k[G]$ is an associative algebra with the product that we defined above, so it is a Lie algebra with Lie bracket:

$$[x, y] = xy - yx \text{ for all } x, y \in k[G].$$

W. Plesken suggested looking at the Lie algebra $\mathfrak{L}(G)_k$, the subspace of $k[G]$ which is the linear span of the elements $\hat{g} = g - g^{-1}$ for g in G. It is easy to see that $\widehat{g^{-1}} = -\hat{g}$ and

$$[\hat{g}, \hat{h}] = \widehat{gh} - \widehat{gh^{-1}} - \widehat{g^{-1}h} + \widehat{g^{-1}h^{-1}}.$$

Thus $\mathfrak{L}(G)$ is closed under Lie product, and therefore it is a Lie algebra. We will denote by $\hat{0}$ the zero vector. Every time we write $\mathfrak{L}(G)$ we will mean $\mathfrak{L}(G)_{\mathbf{C}}$. If the field k is different from $\mathbf{C}$ we will always specify it in the notation for the resulting Plesken Lie algebra in order to avoid confusion. Let us consider some examples of Plesken Lie algebras.

Example 1.2.2. Consider the group S_3. Since $(1,2) = (1,2)^{-1}, (1,3) = (1,3)^{-1}$ and $(2,3) = (2,3)^{-1}$, we have

$$\widehat{(1,2)} = \widehat{(1,3)} = \widehat{(2,3)} = \hat{0}.$$

Also, $\widehat{(1,2,3)} = (1,2,3) - (1,3,2)$, so

$$\mathfrak{L}(S_3) = \{\hat{0}, \widehat{(1,2,3)}\} = \operatorname{span}\{\widehat{(1,2,3)}\}.$$

Thus $\dim \mathfrak{L}(S_3) = 1$, and $\mathfrak{L}(S_3)$ is therefore abelian. $\Diamond$

Example 1.2.3. In the same way as in the example above we can see that $\mathfrak{L}(S_4)$ is spanned by $\widehat{(1,2,3)}, \widehat{(1,2,4)}, \widehat{(1,3,4)}, \widehat{(1,2,3,4)}, \widehat{(1,3,2,4)}$ and $\widehat{(1,4,2,3)}$. Thus

$$\mathfrak{L}(S_4) = \{\hat{0}, \widehat{(1,2,3)}, \widehat{(1,2,4)}, \widehat{(1,3,4)}, \widehat{(1,2,3,4)}, \widehat{(1,3,2,4)}, \widehat{(1,4,2,3)}\}.$$

Thus $\dim \mathfrak{L}(S_4) = 7$. $\Diamond$

Example 1.2.4. Consider the quaternion group of order 8:

$$\mathfrak{Q}_8 = \langle i, j | i^2 = j^2, j^4 = 1, i^{-1}ji = j^{-1} \rangle.$$

We can easily see that $\mathfrak{L}(\mathfrak{Q}_8)$ is spanned by $\hat{i}, \hat{j}$ and $\hat{k}$ where $k = ij$. By computing the brackets explicictly, we get

$$[\hat{i}, \hat{j}] = 4\hat{k}, \quad [\hat{j}, \hat{k}] = 4\hat{i}, \quad [\hat{k}, \hat{i}] = 4\hat{j}.$$

By sending the elements $2\hat{i}, 2\hat{j}$, and $2\hat{k}$ to the matrices $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} -i & 0 \\ 0 & i \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right)$ we see that $\mathfrak{L}(\mathfrak{Q}_8)$ is isomorphic to the Lie algebra $\mathfrak{sl}(2, \mathbf{C})$ because the bracket operations on the bases elements are the same. $\Diamond$

1.3 Ideals

In the theory of Lie algebras, ideals play a role similar to that played by normal subgroups in group theory and two-sided ideals in ring theory.

Definition 1.3.1. An **ideal** I of a Lie algebra L is a subspace of L such that $[x, y] \in I$ for all $x \in L, y \in I$.

Since $[x, y] = -[y, x]$, we don't need to distinguish between left and right ideals. The Lie algebra L and 0 are always ideals of L, we call these the trivial ideals.

Example 1.3.2. An example of an ideal which is nontrivial for any non-abelian Lie algebra L, i.e. it is a **proper** ideal of L, is the *center* of L, defined by

$$Z(L) = \{x \in L : [x, y] = 0 \text{ for all } y \in L\}.$$

Note that $L = Z(L)$ if and only if L is abelian.

Suppose I and J are ideals of a Lie algebra L. Note that $I \cap J$ is a subspace of L, and for $x \in L$ and $y \in I \cap J$, $[x, y] \in I \cap J$, since I and J are ideals. So $I \cap J$ is also an ideal of L.

We define the product of ideals, which is going to generate another very important example. Let

$$[I, J] = \text{span}\{[x, y] : x \in I, y \in J\}.$$

By definition, $[I, J]$ is a subspace of L. If $x \in I, y \in J$ and $u \in L$, the Jacobi identity yields

$$[u, [x, y]] = [x, [u, y]] + [[u, x], y].$$

We know $[u, y] \in J$ since J is an ideal, so $[x, [u, y]] \in [I, J]$. Similarly, $[[u, x], y] \in [I, J]$. Therefore their sum is in $[I, J]$. Let γ be a general element of $[I, J]$, so

$$\gamma = \Sigma c_i [x_i, y_i],$$

where the c_i's are scalars, $x_i \in I$ and $y_i \in J$. Then, for $u \in L$, we get

$$[u, \gamma] = [u, \Sigma c_i [x_i, y_i]] = \Sigma c_i [u, [x_i, y_i]],$$

where $[u, [x_i, y_i]] \in [I, J]$ as shown above. Thus $[u, \gamma] \in [I, J]$; it follows that $[I, J]$ is an ideal of L.

Example 1.3.3. An important example arises if we let $I = J = L$. We call $[L, L]$ the derived algebra of L; it is analogous to the commutator subgroup of a group.

1.3.1 Solvable Ideals

We define a sequence of ideals of L, called the **derived series** of L in the following way:

$$L^{(0)} = L, \tag{1.3.1}$$

$$L^{(1)} = [L, L], \tag{1.3.2}$$

$$L^{(1)} = [L^{(1)}, L^{(1)}], \tag{1.3.3}$$

$$\cdots \tag{1.3.4}$$

$$L^{(i)} = [L^{(i-1)}, L^{(i-1)}]. \tag{1.3.5}$$

Definition 1.3.4. A Lie algebra L is **solvable** if for some $m \geq 1$ we have $L^{(m)} = 0$.

Example 1.3.5. Let $L = \mathfrak{t}(n, k)$ be the Lie algebra of upper triangular $n \times n$ matrices with entries in a field k. Let $x, y \in L$. Then $[x, y] = xy - yx$ has a only zeroes on the diagonal because the diagonals of xy and yx are the same and they cancell out. Thus $[L, L] = \mathfrak{n}(n, k)$, where $\mathfrak{n}(n, k)$ is the Lie algebra of strictly upper triangular $n \times n$ matrices over k. More generally, we get that $L^{(m)}$ has a basis consisting of all the matrix units e_{ij} with $j - i \geq 2^{m-1}$. by using the commutator formula for e_{ij}. So $L^{(m)} = 0$ whenever $2^{-1} > n - 1$. Thus L is solvable.

We give an example of a nonsolvable ideal.

Example 1.3.6. Let $L = \mathfrak{sl}(n, \mathbf{C})$. It is easy to see that $[L, L] = L$, so $L^{(m)} = L$ for all $m \geq 1$, so $\mathfrak{sl}(n, \mathbf{C})$ is not solvable.

We state the following lemma, but we will omit its proof that can be found in [1].

Lemma 1.3.7. *Let L be a finite dimensional Lie algebra. There is a unique maximal solvable ideal of L, i.e. a solvable ideal containing every solvable ideal of L.*

This maximal solvable ideal of L is called the **radical** of L and is denoted $\operatorname{Rad} L$ This suggests the following definition:

Definition 1.3.8. A non-zero Lie algebra L is **semisimple** if it has no non-zero solvable ideals or equivalently if $\operatorname{Rad} L = 0$.

The condition for a Lie algebra to be semisimple is equivalent to requiring that L has no non-zero abelian ideals. This was the original definition of semisimplicity given by Wilhelm Killing.

1.3.2 Nilpotent Ideals

The definition of solvability for Lie algebras is inspired by the corresponding notion in group theory, which dates back to Abel and Galois. However, the notion of nilpotency for groups is more recent and it imitates the corresponding notion for Lie algebras. We define the **lower central series** of a Lie algebra L by

$$L^0 = L, \tag{1.3.6}$$

$$L^1 = [L, L], \tag{1.3.7}$$

$$L^2 = [L, L^1], \tag{1.3.8}$$

$$\cdots \tag{1.3.9}$$

$$L^m = [L, L^{m-1}]. \tag{1.3.10}$$

Definition 1.3.9. The Lie algebra L is called **nilpotent** if $L^m = 0$ for some $m \geq 1$.

Note that since $[L, L] = 0$ for an abelian Lie algebra L, every abelian Lie algebra is nilpotent.

Example 1.3.10. It is not hard to see that $L = \mathfrak{n}(n, k)$, the Lie algebra of strictly upper triangular $n \times n$ matrices over k, is nilpotent: L^1 is spanned by those e_{ij} for which $j - i \geq 2$, L^2 by those e_{ij} for which $j - i \geq 3, \cdots, L^m$ is spanned by those e_{ij} for which $j - i \geq m + 1$. It is then clear that $L^m = 0$ whenever $m + 1 > n - 1$.

Note that we can easily show by induction that $L^{(i)} \subset L^i$ for all i, so all nilpotent Lie algebras are solvable. However, the converse is false. Consider $L = \mathfrak{t}(n, k)$, the Lie algebra of upper triangular $n \times n$ matrices with entries in a field k from example 1.3.5. Recall that we mentioned that $L^{(1)} = L^1$ is $\mathfrak{n}(n, k)$. We can again show inductively that $L^k = [L, L^{m-1}] = L^1$ for all $m \geq 1$. So L is not nilpotent, but we showed in Example 1.3.5 that it is solvable.

The condition for L to be nilpotent is equivalent to requiring that there is some $k \geq 1$ such that $\operatorname{ad} x_i(y) = 0$ for all $i \leq k, y \in L$. In particular, $(\operatorname{ad} x)^k = 0$ for all $x \in L$.

Definition 1.3.11. An element x of a Lie algebra L is ad-**nilpotent** if $\operatorname{ad} x$ is a nilpotent endomorphism. $\triangle$

Recall that an endomorphism is a linear map from a vector space to itself. So, we can conclude that if L is nilpotent, then all its elements are ad-nilpotent. Engel's theorem states that the converse of this statement is also true:

Theorem 1.3.12 (Engel)**.** *If all elements of L are* ad-*nilpotent, then L is nilpotent.*

For the proof of this theorem, once again we refer the reader to [1].

1.3.3 Classification of Simple Ideals

Working over $\mathbf{C}$, we will show that every semisimple Lie algebra is a direct sum of **simple** ideals.

Definition 1.3.13. A **simple Lie algebra** is a Lie algebra L that has no proper ideals.

Note that a simple Lie algebra L is semisimple, since is has no ideals except 0 and itself, and L is nonsolvable.

Due to the work of Killing, Engel, and Cartan, there is a classification theorem for simple Lie algebras over $\mathbf{C}$. We are going to cite it here in order to give to familiarize the reader with it; however, the proof of it is very long and it would divert our attention too much from the main purpose of this thesis. For a proof, we refer the reader again to [1].

Theorem 1.3.14. *With five exceptions, every finite-dimensional Lie algebra over $\mathbf{C}$ is isomorphic to one of the* ***classical Lie algebras****:*

$$\mathfrak{sl}(n, \mathbf{C}), \mathfrak{so}(n, \mathbf{C}), \mathfrak{sp}(2n, \mathbf{C}).$$

The five exceptional Lie algebras are known as $\mathfrak{e}_6$,$\mathfrak{e}_7$,$\mathfrak{e}_8$,$\mathfrak{f}_4$, and $\mathfrak{g}_2$.

The families of classical Lie algebras can be defined as certain subalgebras of $\mathfrak{gl}(n, \mathbf{C})$. It actually turns out that $\mathfrak{so}(n, \mathbf{C})$ and $\mathfrak{sp}(2n, \mathbf{C})$ are subalgebras of $\mathfrak{sl}(2n, \mathbf{C})$.

1.4 Simple Ideals

We say that L is a **direct sum** of ideals $I_1, \cdots, I_t$ provided we have the direct sum of subspaces

$$L = I_1 + \cdots + I_t.$$

Then $[I_i, I_j] \subset I_i \cap I_j = 0$ for $i \neq j$, so the brackets between elements of different ideals are zero. We can thus regard the Lie algebra L as obtained from the Lie algebras I_i by defining Lie products componentwise for the external direct sum of these as vector spaces. We then get a direct sum as Lie algebras:

$$L = I_1 \oplus \cdots \oplus I_t.$$

We call a **simple ideal** is an ideal that is simple as a Lie algebra. We cite the following very useful theorem:

Theorem 1.4.1. *Let L be a complex Lie algebra. Then L is semisimple if and only if there are simple ideals $I_1, \cdots, I_t$ such that*

$$L = I_1 \oplus \cdots \oplus I_t.$$

The proof of Theorem 1.4.1 can be found in [1] and in [3]. The main idea is to define an inner product on L, called the **Killing form**, with respect to which $L = I \oplus I^{\perp}$ for any non-trivial proper ideal I of L. Then we use can use induction in order to show the result of the theorem.

1.5 Cartan Subalgebras

First, we remind the reader that working over an algebraically closed field allows us to consider the Jordan normal form of linear transformations. We use it to define the **Jordan decomposition** of a linear transformation of a finite dimensional vector space over an algebraically closed field:

Lemma 1.5.1. *Let V be a finite dimensional vector space V over an algebraically closed field k, and let $x \in \mathrm{End}(V)$. Then there exist unique elements $x_s, x_n \in \mathrm{End}(V)$ satisfying the conditions:*

1. $x = x_s + x_n$,

2. x_s is semisimple,

3. x_n is nilpotent,

4. x_s and x_n commute.

Definition 1.5.2. The decomposition $x = x_s + x_n$ is called the **Jordan decomposition** of x; we call x_s and x_n the **semisimple part** and the **nilpotent part** of x, respectively. $\triangle$

The proof of Lemma 1.5.1 can be found in [1], and a revision of the Jordan canonical form for complex linear transfomations can be found in Appendix A of [3].

We note that a complex semisimple Lie algera L must have semisimple elements. If L consisted entirely of nilpotent (i.e. ad-nilpotent) elements, then L would be nilpotent by Engel's theorem, and thus L would be solvable. Hence we can find an element in L whose semisimple part x_s is nonzero. If we take the span of such x_s we obtain a subalgebra of L which consists only of semisimple elements, often called a **toral subalgebra**. It turns out that a toral subalgebra of L is abelian (see [1] for a proof). Note that a maximal toral subalgebra exists since L is finite dimensional.

Definition 1.5.3. A Lie subalgebra H of L which consists only of semisimple elements and is maximal with respect to this property is called a **maximal toral subalgebra** or a **Cartan subalgebra**. $\triangle$

1.6 Roots

Let H be a Cartan subalgebra of L. Since H is abelian, $\operatorname{ad}_H L$ is a commuting family of semisimple endomorphisms of L. According to a standard result in linear algebra, $\operatorname{ad}_H L$ is simultaneously diagonalizable. In other words, L is the direct sum of subspaces

$$L_\alpha = \{x \in L \mid [h, x] = \alpha(h)x \text{ for all } h \in H\},$$

where α ranges over H^*. In general, for a subset X of L, we define

$$C_L(X) = \{x \in L \mid [x, X] = 0\}$$

to be the **centralizer** of X. By the Jacobi identity, we get that the centralizer is a subspace of L. Note now that L_0 is simply $C_L(H)$. Clearly, $H \subset C_L(H)$ since H is abelian. We can actually show $H = C_L(H)$. The proof is very technical, and we omit the details. They can be found in [1] and [3].

We denote the set of $\alpha \in H^*$ for which $L_\alpha \neq 0$ by ϕ, and we call the elements of ϕ the **roots** of L with respect to H. It is important to note that there are only finitely many roots. We get a **root space decomposition**:

$$L = H \oplus \coprod_{\alpha \in \phi} L_\alpha.$$

It turns out that ϕ is a root system, namely that ϕ satifies certain axioms that define a root system. We will not going into these details here, since they are not directly relevant to this project. However, we will need the notion of **base of a root system** later on, so we will give a definition for it:

Definition 1.6.1. A subset Δ of ϕ is a **base** if

1. Δ is a basis for the Euclidean space,

2. each root β can be written $\beta = \Sigma k_\alpha \alpha$ where $\alpha \in \phi$ with integral coefficients k_α all nonnegative or all nonpositive.

$\triangle$

We end our introduction to Lie algebras here, and continue with an introduction to representation theory.

2
Representation Theory of Finite Groups

2.1 Definitions and Examples

Representation theory studies abstract algebraic objects purely in terms of linear algebra by representing elements as linear transformations of vector spaces. The abstarct object becomes thus concrete. Representation theory is a very powerful tool becaue it reduces problems in abstract algebra to problems in linear algebra which is well understood. We will see later on that the key to understanding the Lie algebra $\mathfrak{L}(G)$ is the study of the irreducible representations of G.

Let G denote a finite group and k an algebraically closed field of characteristic 0. For convenience, one can take k to be $\mathbf{C}$. Let V be a vector space of dimension n over $\mathbf{C}$.

Definition 2.1.1. A **representation** of G is a homomorphism $\rho : G \longrightarrow \mathrm{GL}(V) \simeq \mathrm{GL}_n(\mathbf{C})$. $\triangle$

In other words, the image of ρ gives a "picture" of the group elements in terms of matrices. We make a few more definitions:

Definition 2.1.2. The **degree** of the representation ρ is defined to be the dimension of V. A representation is called **faithful** if $\ker \rho$ is trivial. $\triangle$

In other words, a faithful representation really represent the whole group, and not just some quotient of the group.

Two representations ρ_1, ρ_2 of the same group G on the same vector space V are said to be **equivalent** if there exists a linear transformation $T \in \mathrm{GL}(V)$ such that the following diagram commutes for all $g \in G$.

$$\begin{tikzcd} V \arrow[r, "\rho_1(g)"] \arrow[d, "T"'] & V \arrow[d, "T"] \\ V \arrow[r, "\rho_2(g)"'] & V \end{tikzcd}$$

So ρ_1 and ρ_2 are equivalent if images of ρ_1 and ρ_2 are conjugate.

One of the major goals of representation theory is to classify all representations of a finite group up to equivalence. To do that we'll need the notion of an **irreducible representation**.

Definition 2.1.3. A representation $\rho : G \longrightarrow \mathrm{GL}(V)$ is said to be **irreducible** if there are no nontrivial G-stable subspaces of V, i.e., any subspace W of V for which $\rho(g)W \subset W$ for all g, is either the zero space, or all of V. $\triangle$

Example 2.1.4. The **trivial representation** of a finite non-trivial group G is defined to be the (unfatihful) representation:

$$\rho : G \longrightarrow \mathrm{GL}_1(\mathbf{C}) \simeq \mathbf{C}^\times$$

sending all elements of G to $1 \in \mathbf{C}$. $\Diamond$

Example 2.1.5. Let $G = S_3$ and V a 3-dimensional vector space. Choose a basis $\{e_1, e_2, e_3\}$ of V, and consider the representation $\rho : S_3 \longrightarrow \mathrm{GL}_3(\mathbf{C})$, where each element of S_3 permutes the basis vectors accordingly. It is not hard to check that the image of this representation is:

$$\operatorname{im}\rho = \left\{ \begin{pmatrix} 1&0&0\\0&1&0\\0&0&1 \end{pmatrix}, \begin{pmatrix} 0&1&0\\0&0&1\\1&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&1\\1&0&0\\0&1&0 \end{pmatrix}, \begin{pmatrix} 0&1&0\\1&0&0\\0&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&0\\0&0&1\\0&1&0 \end{pmatrix}, \begin{pmatrix} 0&0&1\\0&1&0\\1&0&0 \end{pmatrix} \right\}.$$

This representation is not irreducible. For example, the line spanned by the vector $(1, 1, 1)$ is G-stable. So is the hyperplane $x + y + z = 0$. In fact, with respect to the new basis $\{e_1 + e_2 + e_3, e_1 - e_3, e_2 - e_3\}$, the representation is visibly reducible. Moreover, these two representations are equivalent, since they just correspond to a change of basis in accordance with our definition above. $\Diamond$

2.2 Characters of Representations

All the data you need to reconstruct a representation up to conjugation is contained in the character table of a group.

Definition 2.2.1. Let $\rho : G \longrightarrow GL(V)$ be a representation. The **character** of ρ, denoted χ_ρ, is defined by $\chi_\rho(g) = \mathrm{tr}(\rho(g))$. $\triangle$

Note that

$$\chi_\rho(1) = \deg(\rho) = \dim(V)$$

since $\rho(1) = I_n$ and $\chi_\rho(1) = tr(I_n) = n$.

We are going to cite a few very important theorems about characters and try to point out their importance. For example, we can define an inner product on characters that is zero for any two characters that are different and 1 exactly when it is applied to two equal characters. Throughout this section, let $\#G$ denote the order of a finite group G.

Definition 2.2.2. Let ρ_1 and ρ_2 be irreducible representations of a finite group G, and let χ_1 and χ_2 be the characters of ρ_1 and ρ_2. We define the following inner product on χ_1 and χ_2:

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{\#G} \sum_{g \in G} \chi_1(g)\overline{\chi_2(g)}$$

We then have the following important property of this inner product:

Theorem 2.2.3 (Othogonality Condition)**.** *Let G, χ_1 and χ_2 be as defined above. Then*

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{\#G} \sum_{g \in G} \chi_1(g)\overline{\chi_2(g)} = \begin{cases} 1 & \text{if } \chi_1 = \chi_2, \\ 0 & \text{otherwise.} \end{cases}$$

We will cite the following theorems, but we will omit their proofs.

Theorem 2.2.4. *The number of irreducible representations (and therefore irreducible characters) is equal to the number of conjugacy classes.*

Theorem 2.2.5. *If $\rho_1, \rho_2, \ldots, \rho_k$ are the irreducible representations of a finite group G with degrees $n_1, n_2, \ldots, n_k$ respectively, then*

$$n_1{}^2 + n_2{}^2 + \cdots + n_k{}^2 = \#G.$$

We begin by proving a theorem that will provide the motivation for looking at character tables, which is the focus of this section.

Theorem 2.2.6. *Let s and t be in the same conjugacy class of a finite group G, and let χ be the character of some representation ρ of G. Then $\chi(s) = \chi(t)$.*

Proof. Since s and t are in the same conjugacy class, there is some $g \in G$ such that $s = gtg^{-1}$. Then $\rho(s) = \rho\left(gtg^{-1}\right) = \rho(g)\rho(t)\rho\left(g^{-1}\right)$. Recalling that $\mathrm{tr}(AB) = \mathrm{tr}(BA)$ for all matrices A and B, we have

$$\chi(s) = \mathrm{tr}\big(\rho(s)\big) = \mathrm{tr}\Big(\rho\big(gtg^{-1}\big)\Big) = \mathrm{tr}\left(\rho(g)\rho(t)\rho(g)^{-1}\right) = \mathrm{tr}\left(\rho(t)\rho(g)^{-1}\rho(g)\right) = \mathrm{tr}\big(\rho(t)\big) = \chi(t).$$

□

This theorem says that the character function is a class function, which means that the character of each representation is constant over each conjugacy class. Therefore, we can summarize the characters of each irreducible representation for each conjugacy class in the form of a table. By convention, we let each column denote a conjugacy class (indicating which class it is simply by heading the column with one representative element from the class), and we let each row stand for an irreducible representation. By Theorem 2.2.4, the table should have as many rows as it has columns. The order in which the rows and columns appear is arbitrary.

Let us construct the character table for the alternating group of order 3, A_3, which is isomorphic to the cyclic group of order 3, $\mathbf{Z}_3$. Since A_3 has three elements, and every element is in its own conjugacy class, the character table for A_3 has three rows and three columns. Every group has a trivial representation, so we can always start by filling up the first row with ones. Since the character of the identity element is the degree of the representation, Theorem 2.2.5 gives us a condition that we can use to fill up the first column—the sum of the squares of the values in the first column must equal the order of the group. In this case, the order of the group is 3, so all the representations are of degree 1, and we fill up the first column with ones.

Since $(123)^3 = (132)^3 = 1$, it follows that $\chi(123) = \chi(132) = \chi(1) = 1$ for every representation's character χ. Therefore, the character values for the two non-trivial representations are the 3rd roots of unity, i.e. 1, $e^{2\pi i/3}$ and $e^{4\pi i/3}$. We have thus constructed our first character table:

A_3	1	(123)	(132)
χ_1	1	1	1
χ_2	1	$e^{2\pi i/3}$	$e^{4\pi i/3}$
χ_3	1	$e^{4\pi i/3}$	$e^{2\pi i/3}$

We can verify that each pair of rows satisfies the orthogonality condition (Theorem 2.2.3). Take the first and second rows, for example:

$$\begin{aligned}
\langle \chi_1, \chi_2 \rangle &= \frac{1}{3} \sum_{g \in A_3} \chi_1(g) \overline{\chi_2(g)} \\
&= \frac{1}{3} \left(1 \cdot \overline{1} + 1 \cdot \overline{e^{2\pi i/3}} + 1 \cdot \overline{e^4 \pi i/3} \right) \\
&= \frac{1}{3} \left(1 + \frac{-1 - i\sqrt{3}}{2} + \frac{-1 + i\sqrt{3}}{2} \right) \\
&= 0. \quad \text{(verified)}
\end{aligned}$$

Below are the character tables for $\mathbf{Z}_4$ and $\mathbf{Z}_2 \times \mathbf{Z}_2$, both of which have only degree 1 representations, and both of which can be constructed in the same way.

$\mathbf{Z}_4$	0	1	2	3
χ_1	1	1	1	1
χ_2	1	i	-1	$-i$
χ_3	1	$-i$	-1	i
χ_4	1	-1	1	-1

$\mathbf{Z}_2 \times \mathbf{Z}_2$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
χ_1	1	1	1	1
χ_2	1	-1	-1	1
χ_3	1	-1	1	-1
χ_4	1	1	-1	-1

Let us turn our attention now to groups in which some conjugacy classes have more than one element. When not all conjugacy classes are of order 1, it is common practice to write the order (i.e. number of elements) of each conjugacy class above the corresponding column.

Let us now construct the character table for the symmetric group of order 6, S_3. We already know two degree-1 representations of S_3—the trivial representation and the alternating representation:

	1	3	2
S_3	1	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1

By Theorem 2.2.4, we know that S_3 has one more character. By Theorem 2.2.5, we deduce that the remaining character is of degree 2, since the sum of the squares of the degrees of the characters must equal the order of the group. We can now apply Theorem 2.2.3 to obtain the following equations:

$$\langle \chi_1, \chi_3 \rangle = \frac{1}{6}\left(1 \cdot 2 + 3 \cdot 1 \cdot \overline{\chi_3(12)} + 2 \cdot 1 \cdot \overline{\chi_3(123)}\right) = 0$$
$$\langle \chi_2, \chi_3 \rangle = \frac{1}{6}\left(1 \cdot 2 + 3 \cdot (-1) \cdot \overline{\chi_3(12)} + 2 \cdot 1 \cdot \overline{\chi_3(123)}\right) = 0$$

Equivalently,

$$2 + 3 \cdot \overline{\chi_3(12)} + 2 \cdot \overline{\chi_3(123)} = 0$$

$$2 - 3 \cdot \overline{\chi_3(12)} + 2 \cdot \overline{\chi_3(123)} = 0$$

Solving for the two unknowns, we find that $\chi_3(12) = \overline{\chi_3(12)} = 0$ and $\chi_3(123) = \overline{\chi_3(123)} = -1$. Thus we have our completed character table for S_3:

	1	3	2
S_3	1	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Alternatively, we could also compute the third row of S_3's character table by considering the permutation representation, which sends (for example) (12) to $\left(\begin{smallmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$. It is easy to see that the character of each permutation under the permutation representation is equal to the number of fixed points held by the permutation (recall that the character is the trace of the representation matrix). The permutation representation is not irreducible—it decomposes into the direct sum of the trivial representation and another irreducible representation that we shall call ρ_3. The characters

of ρ_3 can thus be computed by subtracting the character of the trivial representation (i.e. 1) from the character of the permutation representation (i.e. the number of fixed points), giving us $(3,1,0)-(1,1,1)=(2,0,-1)$.

Constructing the character table for S_4 takes a little more work. S_4 has five conjugacy classes, and thus it also has five irreducible representations. Once again, we use Theorem 2.2.5 to populate the first column. The order of the group is 24; the only way to express this as a sum of squares of five natural numbers is

$$1^2+1^2+2^2+3^2+3^2=1+1+4+9+9=24.$$

The two degree 1 representations are, of course, the trivial and alternating representations, which we label ρ_1 and ρ_2 respectively. We have a degree 2 representation and two degree 3 representations of which to find the characters.

One of the degree 3 representations can be found using the fixed-point trick described earlier, such that we get

$$(4,2,1,0,0)-(1,1,1,1,1)=(3,1,0,-1,-1).$$

We call this representation ρ_4. To find the other degree-3 representation, we observe that $\rho_2\otimes\rho_4$ yields an irreducible representation, and compute the characters of the new representation by multiplying the characters of ρ_2 and ρ_4.

Finally, we can use Theorem 2.2.3 to obtain four equations with our four remaining unknown character values, which we can solve to obtain the following table:

	1	6	8	6	3
S_4	1	(12)	(123)	(1234)	(12)(34)
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	2	0	-1	0	2
χ_4	3	1	0	-1	-1
χ_5	3	-1	0	1	-1

You will notice, of course, that the top-left 3-by-3 subtable is identical to the character table for S_3, which should come as no surprise since $S_3=S_4/(1\cup B\cup C)$ where B is the conjugacy class that contains (1234), and C is the conjugacy class that contains (12)(34).

Similarly, to build the character table for A_4, we can start by filling in values from A_3, since $A_4 = A_3/\{1, (12)(34), (13)(24), (14)(23)\}$. We can then complete the second and third rows by applying Theorem 2.2.3 to $\langle \chi_1, \chi_2 \rangle$ and $\langle \chi_1, \chi_3 \rangle$. The fourth row can be computed using either the fixed point trick or Theorems 2.2.4 and 2.2.3, to produce:

	1	4	4	3
A_4	1	(123)	(132)	(12)(34)
χ_1	1	1	1	1
χ_2	1	$e^{2\pi i/3}$	$e^{4\pi i/3}$	1
χ_3	1	$e^{4\pi i/3}$	$e^{2\pi i/3}$	1
χ_4	3	0	0	-1

Constructing character tables by hand can be a long and tedious process, especially when dealing with larger groups. Fortunately, several mathematics software packages now have the ability to automatically generate character tables. One such program is MAGMA, which can be accessed online at `http://magma.maths.usyd.edu.au/calc`.

Now consider the group $G = \mathrm{PSL}(2, 7)$, which is the unique group of order 168. We can compute its character table using the algebra system MAGMA: G has 6 conjugacy classes, MAGMA gives the sizes of these and the order of their elements when it generates the character table

Class	1	2	3	4	5	6
Size	1	21	56	42	24	24
Order	1	2	3	4	7	7
χ_1	1	1	1	1	1	1
χ_2	3	-1	0	1	z	z^3
χ_3	3	-1	0	1	z^3	z
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 $z = -e^{\frac{6\pi i}{7}} - e^{\frac{5\pi i}{7}} - e^{\frac{4\pi i}{7}} - e^{\frac{2\pi i}{7}}$.

2.2.1 Real, Complex and Symplectic Characters

An irreducible representation $\rho : G \to GL(V)$ is exactly one of the following:

1. Complex: χ_ρ is not real-valued; V does not have a G-invariant nondegenerate bilinear form.

2. Real: $V = V_0 \otimes \mathbf{C}$, a real representation; V has a G-invariant symmetric nondegenerate bilinear form.

3. Symplectic: χ_ρ is real, but V is not real; V has a G-invariant skew-symmetric nondegenerate bilinear form.

Furthermore, a character χ of G is **real, symplectic** or **complex** according to the type of its associated irreducible representation. An equivalent way of defining the type of a representation is the following. If χ is the character of an irreducible representation, then

$$\frac{1}{\#G}\sum_{g\in G}\chi(g^2) = \begin{cases} 0 & \text{if } \chi \text{ is complex} \\ 1 & \text{if } \chi \text{ is real} \\ -1 & \text{if } \chi \text{ is symplectic.} \end{cases}$$

Example 2.2.7. Recall that the character table of A_3 is:

A_3	1	(123)	(132)
χ_1	1	1	1
χ_2	1	$e^{2\pi i/3}$	$e^{4\pi i/3}$
χ_3	1	$e^{4\pi i/3}$	$e^{2\pi i/3}$

Then,

$$\begin{aligned} \frac{1}{\#A_3}\sum_{g\in A_3}\chi_1(g^2) &= \frac{1}{3}(\chi_1(1) + \chi_1((123)^2) + \chi_1((132)^2) && (2.2.1)\\ &= \frac{1}{3}(\chi_1(1) + \chi_1((132)) + \chi_1((123)) && (2.2.2)\\ &= \frac{1}{3}(1+1+1) && (2.2.3)\\ &= 1 && (2.2.4) \end{aligned}$$

So χ_1 is real. Now we compute the type of χ_1:

$$\begin{aligned} \frac{1}{\#A_3}\sum_{g\in A_3}\chi_2(g^2) &= \frac{1}{3}(\chi_2(1) + \chi_2((123)^2) + \chi_2((132)^2) && (2.2.5)\\ &= \frac{1}{3}(\chi_2(1) + \chi_2((132)) + \chi_2((123)) && (2.2.6)\\ &= \frac{1}{3}(1 + e^{4\pi i/3} + e^{2\pi i/3}) && (2.2.7)\\ &= 0 && (2.2.8) \end{aligned}$$

So χ_2 is complex. Similarly, we get that χ_3 is complex.

Now we end the chapters on background material, and we go right into the heart of this project in the next two chapters.

3
The Plesken Lie Algebra of a Group

3.1 Reduction mod p of arbitrary complex Lie algebras

Lie algebras over fields of prime characteristic behave quite differently from complex Lie algebras. The classification of simple Lie algebras over $\mathbf{C}$ doe snot generalise. For example, one can show that $\mathfrak{sl}(n,k)$ is not simple if the characteristic of k divides n. Moreover, new simple Lie algebras have been discovered over fields of prime characteristic that do not have any analogues in characteristic zero.

Example 3.1.1. We will define the **Witt algebra** $W(1)$. The Witt algebra $W(1)$ over $\mathbf{F}_p$ is p-dimensional with basis

$$e_{-1}, e_0, \cdots, e_{p-2}$$

and Lie bracket

$$\begin{cases} (j-i)e_{i+j} & -1 \leq i+j \leq p-2 \\ 0 & \text{otherwise.} \end{cases}$$

When $p = 2$, this algebra is the 2-dimensional non-abelian Lie algebra. $W(1)$ is simple for $p \geq 3$. For $p = 3$, $W(1)$ is isomorphic to $\mathfrak{sl}(2, \mathbf{F}_p)$. However, if $p > 3$, we can see by considering the known dimensions of the classical Lie algebras, that $W(1)$ is not isomorphic to any of them.

$\Diamond$

We will describe the methos of reducing a Lie algebra L over $\mathbf{C}$ mod p. It turns out that we can construct L "over $\mathbf{Z}$"; L has a basis for which the structure constants are integral, called a **Chevalley basis**. We need the following proposition in order to define this basis:

Proposition 3.1.2. *It is possible to choose root vectors $x_\alpha \in L_\alpha (\alpha \in \phi)$ satisfying:*

1. $[x_\alpha, x_{-\alpha}] = h_\alpha$.
2. *If $\alpha, \beta, \alpha+\beta \in \phi, [x_\alpha, x_\beta] = c_{\alpha,\beta} x_{\alpha+\beta}$, then $c_{\alpha,\beta} = c_{-\alpha,-\beta}$. For any such choice of root vectors, the scalars $c_{\alpha,\beta}(\alpha, \beta, \alpha+\beta \in \phi)$ automatically satisfy:*
3. $c^2_{\alpha,\beta} = q(r+1)\frac{(\alpha+\beta,\alpha+\beta)}{(\beta,\beta)}$, *where $\beta - r\alpha, \cdots, \beta + r\alpha$ is the α string through β.*

Proof. See [1]. □

Definition 3.1.3. A **Chevalley basis** of L is a basis $\{x_\alpha, \alpha \in \phi; h_i, 1 \leq i \leq l\}$ for which the x_α satisfy Proposition 3.1.2 , while $h_i = h_{\alpha_i}$ for some base $\Delta = \{\alpha_1, \cdots, \alpha_l\}$.

Chevalley proved that the structure constants corresponding to this basis lie entirely in $\mathbf{Z}$:

Theorem 3.1.4 (Chevalley)**.** *Let $\{x_\alpha, \alpha \in \phi; h_i, 1 \leq i \leq l\}$ be a Chevalley basis of L. Then the resulting structure constants lie in $\mathbf{Z}$.*

The $\mathbf{Z}$-span $L(\mathbf{Z})$ of a Chevalley basis $\{x_\alpha, h_i\}$ is a lattice in L, independent of the choice of Δ. $L(\mathbf{Z})$ is a Lie algebra over $\mathbf{Z}$ under the bracket inherited from L; note that Chevalley's theorem ensures closure. The tensor product

$$L^{\otimes \mathbf{F}_p} = L(\mathbf{Z}) \otimes_{\mathbf{Z}} \mathbf{F}_p$$

is defined: $L^{\otimes \mathbf{F}_p}$ is a vector space over $\mathbf{F}_p$ with basis $\{x_\alpha \otimes 1, h_i \otimes 1\}$. Moreover, the bracket operation in $L(\mathbf{Z})$ induces a Lie algebra structure on $L^{\otimes \mathbf{F}_p}$: we just reduce the structure constants mod p.

3.2 The Plesken Lie Algebra over $\mathbf{C}$ vs. a finite field

Recall that the Lie algebra $\mathfrak{L}(G)_k$ is the subspace of the group algebra $k[G]$ that is the span of the elements $\hat{g} = g - g^{-1}$ for g in G. Also, recall that if we avoid the subscript in the notation of the

Plesken Lie algebra, we mean the field $\mathbf{C}$. In [2], Cohen and Taylor prove the following theorem under the condition that $k = \mathbf{C}$:

Theorem 3.2.1. *The Lie algebra $\mathfrak{L}(G)$ admits the decomposition*

$$\mathfrak{L}(G) = \bigoplus_{\chi \in \mathfrak{R}} \mathfrak{o}(\chi(1)) \oplus \bigoplus_{\chi \in \mathfrak{Sp}} \mathfrak{sp}(\chi(1)) \oplus \bigoplus_{\chi \in \mathfrak{C}} {}'\mathfrak{gl}(\chi(1))$$

where $\mathfrak{R}, \mathfrak{Sp}$ and $\mathfrak{C}$ are the sets of irreducible characters of real, symplectic, and complex types, respectively, and where the prime signifies that there is just one summand $\mathfrak{gl}(\chi(1))$ for each pair $\{\chi, \bar{\chi}\}$ from $\mathfrak{C}$.

Example 3.2.2. To illustrate the theorem, consider the group A_5. We can compute the character table of A_5 using Magma, for instance. The group A_5 has 5 characters, all of real type, of degrees 1,3,3,4,5. So, by the above theorem $\mathfrak{L}(A_5)$ decomposes in the following way:

$$\mathfrak{L}(A_5) = \mathfrak{o}(1, \mathbf{C}) \oplus \mathfrak{o}(3, \mathbf{C}) \oplus \mathfrak{o}(3, \mathbf{C}) \oplus \mathfrak{o}(4, \mathbf{C}) \oplus \mathfrak{o}(5, \mathbf{C}).$$

By adding up the dimensions, we get that $\dim \mathfrak{L}(A_5) = 22$. $\diamondsuit$

Is is possible to anticipate what the dimension of $\mathfrak{L}(G)_k$ is going to be? It is not hard to see that the answer is yes. First, observe that the dimension of $\mathfrak{L}(G)_k$ will be the same regardless of the field k we work over. More precisely, the Lie algebra will be spanned by half of the elements of order not equal to 2 or the identity, since $\hat{g} = g - g^{-1} = \hat{0}$ if and only if g has order 2, and $\hat{h} = h - h^{-1} = -\hat{h^{-1}}$ for all $h \in G$. So in our previous example

$$\dim \mathfrak{L}(A_5)_k = (\#\text{elements in } A_5 - \#\text{elements of order } 2 - 1)/2 = 22.$$

Looking at how the bracket acts on the basis vectors of $\mathfrak{L}(G)_k$, we see that the structure constants will not be different if $k = \mathbf{F}_p$ as long as the characteristic is not equal to 2. Recall that

$$[\hat{g}, \hat{h}] = \hat{gh} - \widehat{gh^{-1}} - \widehat{g^{-1}h} + \widehat{g^{-1}h^{-1}}.$$

We can easily show that if three of the terms on the right hand side of the equation are equal, the forth one has to also be equal to them. Thus we cannot get multiples of 3 of the basis vectors as the

result of applying the bracket operation to two basis vectors of $\mathfrak{L}(G)_k$. However, we have already seen that we can get multiples of 2 of the basis vectors when we apply the bracket operation to basis vectors. Recall that if G is the quaternion group $\mathfrak{Q}_8$, then

$$[\hat{i}, \hat{j}] = 4\hat{k}, \quad [\hat{j}, \hat{k}] = 4\hat{i}, \quad [\hat{k}, \hat{i}] = 4\hat{j}.$$

This raises the following question: If we have a certain decomposition of $\mathfrak{L}(G)_{\mathbf{C}}$ and we know that the brackets are preserved on the basis vectors if we change the field $\mathbf{C}$ to $\mathbf{F}_p$ with characteristic not equal to 2, do we get the same decomposition? If the answer is yes, it would be interesting to see what the irreducibles in the decomposition correspond to, since the representations of G over $\mathbf{F}_p$ will have different characters.

3.3 Chevalley Bases for Plesken Lie Algebras

The main goal of this section is to show that given a direct sum decomposition of Lie algebras over $\mathbf{C}$, reducing the sum mod p comes down to reducing each summand mod p. Hence we will be able to get an analogue of Theorem 3.2.1 over a finite field, and we can then start investigating how the direct summands mod p arise.

Given a Chevalley basis for $\mathfrak{L}(G)$, we will show that it yields Chevalley bases for the simple ideals of $\mathfrak{L}(G)$ in its direct sum decomposition. Since all the direct summands are themselves simple, they correspond to the simple ideals of $\mathfrak{L}(G)$. In order to prove the claim, we show that the brackets between elements of the same ideal are 0 and that each root vector lies in just one of the simple ideals in the decomposition. It will then follow that the Chevalley basis for $\mathfrak{L}(G)$ splits into Chevalley bases for each direct summand.

Lemma 3.3.1. *Let the Lie algebra L decompose as*

$$L = L_1 \oplus \cdots \oplus L_n,$$

where the L_i's are the simple ideals of L. Then $[L_i, L_j] = 0$ for all i, j.

Proof. Assume $x_i \in L_i$ and $x_j \in L_j$. Then $[x_i, x_j] \in L_i \cap L_j$. But $L_i \cap L_j$ is a subideal of L_i and L_j both of which are simple, so $[x_i, x_j] = 0$ for all $x_i \in L_i$ and $x_j \in L_j$. □

Lemma 3.3.2. *Let the Lie algebra L decompose as $L = L_1 \oplus \cdots \oplus L_n$ with $n \geq 2$, where the L_i's are the simple ideals of L. Then each root vector of L lies in precisely one of the L_i's.*

Proof. Let x_α be a root vector of L corresponding to a root α, so that $[h, x_\alpha] = \alpha(h)x_\alpha$ for all $h \in H$. Suppose

$$x_\alpha = x_{\alpha_1} + \cdots + x_{\alpha_n}$$

where $x_{\alpha_i} \in L_i$ and at least least two of them are nonzero, say $x_{\alpha_j} \neq 0$ and $x_{\alpha_k} \neq 0$. Then

$$[h, x_{\alpha_1}] + \cdots + [h, x_{\alpha_n}] = \alpha(h)x_{\alpha_1} + \cdots + \alpha(h)x_{\alpha_n},$$

for all $h \in H$. Since $[h, x_{\alpha_i}] \in L_i$, by the uniqueness of the decomposition of each element of L into a sum of elements of the L_i's, we get

$$[h, x_{\alpha_i}] = \alpha(h)x_{\alpha_i}, \text{ for all } h \in H, \text{ for all } i.$$

It follows that $x_{\alpha_i} \in L_\alpha$ for all i, and since the root space L_α is one-dimensional, we get $x_{\alpha_i} = \lambda x_{\alpha_j}$ for all i, j. Thus the ideals $\langle x_{\alpha_i} \rangle$ and $\langle x_{\alpha_j} \rangle$ are equal for all i, j. But since the L_i's are simple and $x_{\alpha_j} \neq 0$ and $x_{\alpha_k} \neq 0$, it follows that $\langle x_{\alpha_j} \rangle = L_j$ and $\langle x_{\alpha_k} \rangle = L_k$. So $L_j = L_k$, a contradiction. □

For convenience's sake we will prove the following results for an arbitrary Lie algebra L that decomposes into semisimple ideals L_1 and L_2. Inductively, the results will follow for $\mathfrak{L}(G)$ with its direct sum decomposition.

We now prove that the direct sum decomposition of a Lie algebra yields a direct sum decomposition of the Cartan subalgebras.

Lemma 3.3.3. *Let the Lie algebra L be the direct sum of simple ideals $L = L_1 \oplus L_2$ and let H, H_1, H_2 be the Cartan subalgebras of L, L_1 and L_2 respectively. Then $H_1 \oplus H_2 = H$.*

Proof. Clearly, $H_1 \oplus H_2$ is abelian and consists of semisimple elements. Suppose, for contradiction, that $H_1 \oplus H_2$ is not maximal, and that

$$H_1 \oplus H_2 \subsetneq H.$$

Let $h \in H$, but suppose that $h \notin H_1 \oplus H_2$. Then $h = l_1 + l_2$ for $l_1 \in L_1$ and $l_2 \in L_2$. If either l_1 or l_2 were not semisimple, then the nilpotent part in the Jordan decomposition of h would be non-zero, which contradicts the fact that h is semisimple. Thus l_1 and l_2 are semisimple, so $l_1 \in H_1$ and $l_2 \in H_2$. Hence $h \in H_1 \oplus H_2$, a contradiction. □

Corollary 3.3.4. *If $L = L_1 \oplus L_2$ the dual space of the Cartan subalgebra H^* decomposes as $H_1^* \oplus H_2^*$.*

So, in general, if $L = L_1 \oplus \cdots \oplus L_n$, we have a decomposition of the dual spaces of the Cartan algebras $H^* = H_1^* \oplus \cdots \oplus H_n^*$. We can consider projections from L onto L_i. We define

$$\pi_i : L \to L_i$$

such that π_i is a projection onto L_i, i.e., $\pi_i^2 = \pi_i$. For any $x \in L$, we know that x has a unique representation $x = x_1 + \cdots + x_n$ for $x_i \in L_i$. Then

$$\pi_i(x) = x_i.$$

Similarly, define

$$\pi_i^* : H^* \to H_i^*$$

to be projections onto H_i^* for all i.

Lemma 3.3.5. *Let the Lie algebra L be the direct sum of simple ideals $L = L_1 \oplus \cdots \oplus L_n$, and assume the root vector x_α corresponding to a root α lies in L_i. Then α lies in H_i, the Cartan subalgebra of L_i, and hence α is a root for L_i and x_α is a root vector for L_i.*

Proof. Since $\alpha \in \phi$ where ϕ is a root system for L, then $L_\alpha \neq 0$. So, there is a nonzero $x \in L_\alpha$. Then

$$[h, x] = \alpha(h)x \text{ for all } h \in H.$$

Then

$$[h_j, x] = \alpha(h_j)x \text{ for all } h_j \in H_j,$$

since $H_j \subset H$. Thus $L_{\alpha_j} \neq 0$. So α_j is a root for L_j for all j. By Corollary 3.3.4 $\alpha = \alpha_1 + \cdots + \alpha_n$ for $\alpha_j \in H_j^*$. Since x_α is a root vector we have

$$[h, x_\alpha] = \alpha(h)x_\alpha \text{ for all } h \in H.$$

Choose $h_j \in H_j$, i.e., $\pi_j(h_j) = h_j$. Then

$$\pi_j([h_j, x_\alpha]) = [\pi_j(h_j), \pi_j(x_\alpha)] = [h_j, x_\alpha] = \alpha(h_j)x_\alpha = (\alpha_1(h_j) + \cdots + \alpha_n(h_j))x_\alpha = \alpha_i(h_j)x_\alpha,$$

since $\pi_k(h_j) = 0$ for all $k \neq j$. We can conclude that $\pi_j^*(\alpha) = \alpha_j$ is a root for L_j for all j and x_α a root vector for it. Suppose, for contradiction, that there was a nonzero $\alpha_k \neq \alpha_i$. Then $x_\alpha \in L_{\alpha_k} \subset L_k$, a contradiction, since $x_\alpha \in L_i$. Note that since $\alpha_k = 0$ for all $k \neq i$, and $\alpha = \alpha_1 + \cdots + \alpha_n$ is nonzero, we get $\alpha = \alpha_i$. So α is a root for L_i and x_α is a root vector for L_i.

□

Lemma 3.3.2 and Lemma 3.3.5 say that the root vectors in a Chevalley basis for L split into disjoint sets of root vectors for the L_i's, the simple ideals in the decomposition of L, and also that the corresponding root vectors also split disjointly into root systems for H_i's, the Cartan subalgebras of the ideals in the decomposition of L. It is not hard to see that a base Δ for a root system ϕ of L also splits disjointly into bases for the root systems of the L_i's. We are going to make this precise in the next lemma by showing that the image of Δ under π_i^* is a base for the root system of L_i. Note that the elements of Δ are just roots and we have already proved that the image of a root α under π_i^* is nonzero and equal to α only for the i for which its corresponding root vector x_α lies in L_i.

Lemma 3.3.6. *The image of Δ under π_i^* is a base for the root system of L_i.*

Proof. Let $\Delta_i = \pi_i^*(\Delta)$, so

$$\Delta_i = \{\pi_1(\alpha) : \alpha \in \Delta\}.$$

For any $\alpha \in \Delta$, $\alpha = \alpha_1 + \cdots + \alpha_n$ for $\alpha_i \in H_i^*$, so

$$\pi^*(\alpha) = \pi^*(\alpha_1 + \cdots + \alpha_n) = \alpha_i \in \phi_i.$$

Also, for every root $\beta \in \Delta_i$,

$$\beta = \sum k_\alpha \alpha,$$

with $\alpha' s \in \Delta$. So,

$$\beta = \pi_i^*(\beta) = \pi_i^*(\sum k_\alpha \alpha) = \sum k_\alpha \pi_i^*(\alpha).$$

Hence Δ_i is a base for ϕ_i where ϕ_i is a root system for L_i. □

In order to illustrate the previous lemmas, we can consider a possible example. Assume that the Lie algebra L decomposes into the simple ideals L_1 and L_2, so

$$L = L_1 \oplus L_2.$$

Assume that $\phi = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5\}$ is a root system for L. Let x_{α_i} be the corresponding root vector for α_i. By Lemma 3.3.2 we know that each root vector lies in precisely one of L_1 or L_2. Suppose that $x_{\alpha_1}, x_{\alpha_2}, x_{\alpha_3} \in L_1$ and $x_{\alpha_4}, x_{\alpha_5} \in L_2$. Then by Lemma 3.3.5, $\alpha_1, \alpha_2, \alpha_3 \in \phi_1$ and $\alpha_4, \alpha_5 \in \phi_2$ where ϕ_1 and ϕ_2 are root sytems for L_1 and L_2, respectively. Assume that $\Delta = \{\alpha_1, \alpha_2, \alpha_4\}$ is a basis for ϕ. Then, by Lemma 3.3.6 $\{\alpha_1, \alpha_2\}$ is a basis for ϕ_1 and $\{\alpha_4\}$ is a basis for ϕ_2.

Lemma 3.3.7. *If the Lie algebra L is a direct sum of simple ideals $L = L_1 \oplus \cdots \oplus L_n$, then* $\mathrm{Chev}(L) = \mathrm{Chev}(L_1) \coprod \cdots \coprod \mathrm{Chev}(L_n)$ *where* $\mathrm{Chev}(L_i)$ *is a Chevalley basis for L_i.*

Proof. Let $\mathrm{Chev}(L) = \{x_\alpha, \alpha \in \phi; h_i, 1 \leq i \leq l\}$ be a Chevalley basis for L. By Lemma 3.3.2 we get that each $x_\alpha \in L_i$ for just one of the ideals L_i. Since $[x_\alpha, x_{-\alpha}] = h_\alpha$, we get also that $h_\alpha \in L_i$. By Lemma 3.3.5 and Lemma 3.3.6 it follows that $\mathrm{Chev}(L)$ is partitioned into disjoint sets $\mathrm{Chev}(L_i) = \{x_{\alpha_i}, \alpha_i \in \phi_i; h_j, 1 \leq j \leq m\} \subset L_i$ where ϕ_i is a root system for L_i and $h_j = h_{\alpha_{i_j}}$ for some base of ϕ_1 $\Delta_1 = \{\alpha_{i_1}, \cdots, \alpha_{i_m}\}$. It is not hard to see that $\mathrm{Chev}(L_i)$ is a basis for L_i: Its elements are linearly independent and if the dimension of L_i were greater than its cardinality,

then $\sum_i \dim(L_i) \geq \dim(L)$, a contradiction. It is clear that the x_{α_i}'s satisfy Proposition 3.1.2, so $\mathrm{Chev}(L_i)$ is indeed a Chevalley basis for L_i. $\square$

Corollary 3.3.8. *The* $\mathbf{Z}$*-span* $L(\mathbf{Z})$ *of* $\mathrm{Chev}(L)$ *is the sum of the* $L_i(\mathbf{Z})$*'s, the* $\mathbf{Z}$*-span of the Chevalley bases for the* L_i*'s.*

Theorem 3.3.9. *If the Lie algebra* L *is a direct sum of simple ideals* $L = L_1 \oplus \cdots \oplus L_n$*, then*

$$L^{\otimes \mathbf{F}_p} = L_1^{\otimes \mathbf{F}_p} \oplus \cdots \oplus L_n^{\otimes \mathbf{F}_p}.$$

Proof. By Corollary 3.3.8 we have

$$L(\mathbf{Z}) = L_1(\mathbf{Z}) \oplus \cdots \oplus L_n(\mathbf{Z}),$$

where $L_i(\mathbf{Z})$ is the $\mathbf{Z}$-span of the Chevalley basis for L_i. By the distributivity of the tensor product, we get

$$L(\mathbf{Z}) \otimes \mathbf{F}_p = (L_1(\mathbf{Z}) \otimes \mathbf{F}_p) \oplus \cdots \oplus L_n(\mathbf{Z}) \otimes \mathbf{F}_p).$$

$\square$

We can conclude that reducing the Plesken Lie algebra mod p via the Chevalley basis amounts to reducing each direct summand in its decomposition mod p. We will investigate in the next section when using this method of reduction mod p yields the same result that we would obtain by starting with $\mathbf{F}_p[\mathbf{C}]$ and considering the Plesken Lie subalgebra. When they are the same, we will then have a decomposition theorem analogous with the one over $\mathbf{C}$.

4
$\mathfrak{L}(G)_{\mathbf{F}_p}$ vs. $\mathfrak{L}(G)^{\otimes \mathbf{F}_p}$

4.1 Decomposition Theorems

The central question of this chapter is whether taking the Plesken subalgebra of $\mathbf{F}_p[G]$ yields the same result as reducing the Plesken Lie algebra $\mathfrak{L}(G)$, the subalgebra of $\mathbf{C}[G]$ mod p by tensoring the $\mathbf{Z}$-span of the Chevalley basis with $\mathbf{F}_p$. It is not obvious that they do not have to be the same. We will give an example of how this can fail to be true in a few moments. Another subtlely we have to note first is that reducing the classical Lie algebras $\mathfrak{sl}(n, \mathbf{C})$, $\mathfrak{o}(n, \mathbf{C})$ and $\mathfrak{sp}(n, \mathbf{C})$ mod p via the Chevalley basis we do not know a priori that the results are going to coincide with $\mathfrak{sl}(n, \mathbf{F}_p)$, $\mathfrak{o}(n, \mathbf{F}_p)$ and $\mathfrak{sp}(n, \mathbf{F}_p)$. It is not hard to see, however, that they actually do (and they should; otherwise our method of reducing mod p would be inconsistent). Recall that the classical algebras are matrix algebras; it is not hard to write down Chevalley bases for them that are matrices with 0-1 entries, so it will be clear that the multiplication tables of $\mathfrak{sl}(n, \mathbf{F}_p)$, $\mathfrak{o}(n, \mathbf{F}_p)$ and $\mathfrak{sp}(n, \mathbf{F}_p)$ and the Lie algebras resulting from the mod p reduction via the Chevalley basis will be the same, since the bases are the same, and both methods of creating the multiplication tables are to reduce the structure constants mod p.

We take a moment to remind the reader of the notation we have used so far because it will be of particular importance in this chapter:

- $\mathfrak{L}(G)_k$ is the Plesken Lie algebra as a subalgebra of $k[G]$. If we omit the subscript, then it is understood that $k = \mathbf{C}$,

- $\mathfrak{L}(G)^{\otimes \mathbf{F}_p} = (\mathfrak{L}(G))(\mathbf{Z}) \otimes_{\mathbf{Z}} \mathbf{F}_p$, the tensor product of the $\mathbf{Z}$-span of the Chevalley basis of the complex Lie algebra $\mathfrak{L}(G)$ with $\mathbf{F}_p$.

We now give an example of how $\mathfrak{L}(G)_{\mathbf{F}_p}$ and $\mathfrak{L}(G)^{\otimes \mathbf{F}_p}$ can fail to be the same:

Example 4.1.1. Recall that $\mathfrak{L}(A_5)$ decomposes in the following way:

$$\mathfrak{L}(A_5) = \mathfrak{o}(1, \mathbf{C}) \oplus \mathfrak{o}(3, \mathbf{C}) \oplus \mathfrak{o}(3, \mathbf{C}) \oplus \mathfrak{o}(4, \mathbf{C}) \oplus \mathfrak{o}(5, \mathbf{C}).$$

Then we have

$$\mathfrak{L}(A_5)^{\otimes \mathbf{F}_{13}} = \mathfrak{o}(1, \mathbf{F}_{13}) \oplus \mathfrak{o}(3, \mathbf{F}_{13}) \oplus \mathfrak{o}(3, \mathbf{F}_{13}) \oplus \mathfrak{o}(4, \mathbf{F}_{13}) \oplus \mathfrak{o}(5, \mathbf{F}_{13}).$$

The classical Lie algebra $\mathfrak{o}(n, k)$ is an exception in that it is not simple, but it decomposes into two irreducibles of size 3. The other direct summand are all simple. Thus the sizes of the irreducible components in the direct sum are 3, 3, 3, 3 and 10. However, by computing $\mathfrak{L}(A_5)_{\mathbf{F}_{13}}$ with a MAGMA program whose commented code you can find in the appendix, we get that it decomposes into a direct sum of Lie algebras of sizes 6, 6 and 10 that cannot further be decomposed. Thus $\mathfrak{L}(A_5)_{\mathbf{F}_{13}}$ and $\mathfrak{L}(A_5)^{\otimes \mathbf{F}_{13}}$ are not the same.

Note that by combining Theorem 3.2.1 and Theorem 3.3.9, we get the following result:

Theorem 4.1.2. *The Lie algebra $\mathfrak{L}(G)^{\otimes \mathbf{F}_p}$ admits the decomposition*

$$\mathfrak{L}(G)^{\otimes \mathbf{F}_p} = \bigoplus_{\chi \in \mathfrak{R}} \mathfrak{o}(\chi(1), \mathbf{F}_p) \oplus \bigoplus_{\chi \in \mathfrak{Sp}} \mathfrak{sp}(\chi(1), \mathbf{F}_p) \oplus \bigoplus_{\chi \in \mathfrak{C}} {}'\mathfrak{gl}(\chi(1), \mathbf{F}_p)$$

where $\mathfrak{R}, \mathfrak{Sp}$ and $\mathfrak{C}$ are the sets of irreducible characters of real, symplectic, and complex types, respectively, of the complex representations of G, and where the prime signifies that there is just one summand $\mathfrak{gl}(\chi(1))$ for each pair $\{\chi, \bar{\chi}\}$ from $\mathfrak{C}$.

The proof of Theorem 3.2.1 rests on the following result applied to the field $k = \mathbf{C}$, which is discussed in detail in [4]:

Theorem 4.1.3. *If* $\operatorname{char} k \nmid \#G$*, then the algebra* $k[G]$ *is semisimple. More precisely,*

$$k[G] = \operatorname{End}(V_1) \oplus \cdots \oplus \operatorname{End}(V_r)$$

where V_1*,...,*V_r *are a set of representatives of the irreducible* G*-modules, i.e.,* $\rho_i : G \to \mathrm{GL}(V_i)$ *are the irreducible representations of* G*.*

The $\operatorname{End}(V_i)$ are two-sided ideals of the algebra $k[G]$ and they are also ideals with respect to the Lie product. We can then generalize the result of theorem 3.2.1 to any finite field $\mathbf{F}_p$ as long as $p \nmid \#G$. We get the following theorem:

Theorem 4.1.4. *The Lie algebra* $\mathfrak{L}(G)_{\mathbf{F}_p}$ *admits the decomposition*

$$\mathfrak{L}(G)_{\mathbf{F}_p} = \bigoplus_{\chi \in \mathfrak{R}} \mathfrak{o}(\chi(1), \mathbf{F}_p) \oplus \bigoplus_{\chi \in \mathfrak{Sp}} \mathfrak{sp}(\chi(1), \mathbf{F}_p) \oplus \bigoplus_{\chi \in \mathfrak{C}} {}'\mathfrak{gl}(\chi(1), \mathbf{F}_p)$$

where $\mathfrak{R}, \mathfrak{Sp}$ *and* $\mathfrak{C}$ *are the sets of irreducible characters of real, symplectic, and complex types, respectively, of the representations of* G *over* $\mathbf{F}_p$*, and where the prime signifies that there is just one summand* $\mathfrak{gl}(\chi(1))$ *for each pair* $\{\chi, \bar{\chi}\}$ *from* $\mathfrak{C}$*.*

Note that the only difference in Theorem 4.1.2 and Theorem 4.1.4 is that the ideals in the direct sum correspond to *complex characters* in the decomposition of $\mathfrak{L}(G)^{\otimes \mathbf{F}_p}$ and they correspond to *characters of representations over* F_p in the decomposition of $\mathfrak{L}(G)_{\mathbf{F}_p}$. We will thus want to compare complex representations to modular ones, and see when they are the same.

4.2 Complex Characters vs. Modular Characters

We are going to look at characters of representations mod p and see how they differ from the complex ones. We are going to introduce some new concepts as we need them, and prove some results that we will need in the following section in order to establish when $\mathfrak{L}(G)^{\otimes \mathbf{F}_p}$ and $\mathfrak{L}(G)_{\mathbf{F}_p}$ are the same. A condition that we will always keep from this point on is that p does not divide the order of the group G since Theorem **??** requires it.

Let K be an extension of a field k and imagine we have the following set-up:

- R is a k-algebra,
- M is an R-module,
- $R' = K \otimes_k R$,
- $M' = K \otimes_k M$ is an R'-module.

Now we can give the following definitions:

Definition 4.2.1. An irreducible R-module M is **absolutely irreducible** if M' is irreducible for every extension K of k.

Definition 4.2.2. A field $K \supseteq k$ is a **splitting field** for R if every irreducible R'-module is absolutely irreducible.

We are now going to explain these concepts in the language that we will use them. Recall from the previous section that $k[G]$ is a k-module and that the irreducible $k[G]$, sometimes called simply G-modules, are the $\mathrm{End}(V_i)$ where $\rho_i : G \to GL(V_i)$ are the irreducible representations of G over k.

Notice that the splitting field of $k[G]$ is the smallest field for which all the irreducible representations of G over k are realizable. For example, the character table given by MAGMA for A_5 is:

Class	1	2	3	4	5
Size	1	15	20	12	12
Order	1	2	3	5	5
χ_1	1	1	1	1	1
χ_2	3	-1	0	z	z^2
χ_3	3	-1	0	z^2	z
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

where $z = \zeta_5^3 + \zeta_5^2 + 1$ and $\zeta_5 = e^{\frac{2\pi i}{5}}$. So

$$z = \zeta_5 + \zeta_5^4 = \zeta_5 + \zeta_5^{-1} = 2\cos(\frac{2\pi}{5}) = \frac{\sqrt{5}-1}{2}.$$

It turns out that the splitting field of A_5 is $\mathbf{Q}(\sqrt{5})$.

Let us see what happens if the splitting field for $\mathbf{C}[G]$ is $\mathbf{Q}$, i.e., if we can realize all the irreducible representations over $\mathbf{Q}$. Since the matrices in the representations have rational entries, their traces will also be rational. Thus the characters are rational. We can actually deduce something stronger, namely that the character values are integers. We will need the following lemma in the proof of this result.

Lemma 4.2.3. *If $f(x) \in \mathbf{Z}[x]$ factors as $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbf{Q}[x]$, then $g(x), h(x) \in \mathbf{Z}[x]$.*

Proof. Firstly, note that for any monic polynomial $p(x) \in \mathbf{Q}[x]$ such that

$$p(x) = x^n + \frac{a_{n-1}}{b_{n-1}}x^{n-1} + \cdots + \frac{a_0}{b_0}$$

where each fraction $\frac{a_i}{b_i}$ is in lowest terms, if we multiply by b where b is the least common multiple of the b_i, we clear all denominators. Note that b is the unique integer such that $bp(x)$ has integer coefficients that are relatively prime. Now let c be the least common multiple of the denominators of the coefficients of $g(x)$ and let d be the least common multiple of the denominators of the coeffiecients of $h(x)$. Suppose that there is some prime p that divides every coefficient of $(cg(x))(dh(x))$. Then

$$(cg(x))(dh(x)) \equiv 0 \pmod{p},$$

and since $\mathbf{F}_p[x]$ is an integral domain this implies that either

$$cg(x) \equiv 0 \pmod{p}$$

or

$$dh(x) \equiv 0 \pmod{p}.$$

However, this contradicts our previous claim that $cg(x)$ and $dh(x)$ have coefficients that are relatively prime. We can therefore conclude that $(cg(x))(dh(x))$ has relatively prime integer coefficients. On the other hand, note that since $f(x)$ is monic it already satisfies the condition that all its coefficients are relatively prime. Since there is a unique integer multiple of $f(x)$ that has this property,

and

$$(cg(x))(dh(x)) = (cd)f(x),$$

it follows that $cd = 1$. But both c and d are integers, so $c = d = \pm 1$. Thus $g(x), h(x) \in \mathbf{Z}[x]$. $\square$

Lemma 4.2.4. *If the splitting field for* $\mathbf{C}[G]$ *is* $\mathbf{Q}$*, then all the character values are integeters.*

Proof. Let χ be an irreducbile character of G corresponding to an irreducible representation ρ, and let $g \in G$. Suppose that the order of g is e. The $g^e = 1$, so $\rho(g)^e = I$. Since $\rho(g)$ is a root of $X^e - I$, its minimal polynomial must divide $X^e - I$. Since $\rho(g)$ has rational entries, by definition its minimal polynomial $m_{\rho(g)}(X)$ has rational coeffiecients. Since it is a divisor of $X^e - I$, it must then be a product of cyclotomical polynomials, so it must have integer coefficients. Let $c_{\rho(g)}(X)$ be the characteristic polynomial of $\rho(g)$. By the Rational Canonical Form,

$$c_{\rho(g)}(X) = m_1(X)m_2(X)\cdots m_r(X)$$

, where $m_i(X) \in \mathbf{Q}[X]$ are all monic polynomials and

$$m_1(X)|m_2(X)|\cdots|m_r(X),$$

and $m_r(X) = m_{\rho(g)}(X)$. By Lemma 4.2.3, all $m_i(X) \in \mathbf{Z}[X]$. Thus $c_{\rho(g)}(X) \in \mathbf{Z}[X]$. Since $\mathrm{tr}(\rho(g)) = \chi(g)$ is the coefficient of X^{e-1} in $c_{\rho(g)}(X)$, it must then be an integer. $\square$

We are going to introduce the notion of an algebraic integer and a ring of integers in the next section, and we will prove that in general the character values are algebraic integers. More precisely, they will take values in the ring of integers of the splitting field of $\mathbf{C}[G]$. Since the ring of integers of $\mathbf{Q}$ is $\mathbf{Z}$, we have just proved this result for the particular case in which the splitting field of $\mathbf{C}[G]$ is $\mathbf{Q}$.

By Proposition 43 in [4], if $p \nmid \#G$, then the characters of the representations over $\mathbf{F}_p$ are the reduction mod p of the complex characters. If the characer values are integers, the reduction mod p means what we intuitively understand by it. A more detailed discussion of this result and its

proof are beyond the scope of this project; we refer the reader to [4]. The result will be very useful, though.

Lemma 4.2.5. *If the splitting field for* $\mathbf{C}[G]$ *is* $\mathbf{Q}$*, then the reduction mod* p *of a complex character* χ *will have the same type if* $p \neq 2$*.*

Proof. If the splitting field for $\mathbf{C}[G]$ is $\mathbf{Q}$, then the characters of the complex representations have integer values. Let χ' denote the reduction mod p of a complex character χ. Then,

$$\frac{1}{\#G}\sum_{g\in G}\chi'(g^2) = \frac{1}{\#G}\sum_{g\in G}(\chi(g^2)(\text{mod } p)) \tag{4.2.1}$$

$$= \frac{1}{\#G}(\sum_{g\in G}\chi(g^2))(\text{mod } p) \tag{4.2.2}$$

$$= \begin{cases} 0 \pmod p & \text{if } \chi \text{ is complex} \\ 1 \pmod p & \text{if } \chi \text{ is real} \\ -1 \pmod p & \text{if } \chi \text{ is symplectic.} \end{cases} \tag{4.2.3}$$

Thus χ' has the same type as χ if $p \neq 2$.

□

Since we can just reduce the integer valued characters of irreducible complex representations mod p, we will have the same number of modular representations, and the dimensions of the modular representations will remain the same. Then, it follows that if $p \neq 2$ and $p \nmid \#G$, the characters that index the decompositions of $\mathfrak{L}(G)_{\mathbf{F}_p}$ and $\mathfrak{L}(G)^{\otimes \mathbf{F}_p}$ in Theorem 4.1.4 and Theorem 4.1.2 have the same sizes and types. Thus the decompositions will be the same if $\mathbf{Q}$ is the splitting field of $\mathbf{C}[G]$.

4.3 Prime Splitting

If K is the splitting field of $\mathbf{C}[G]$, then we will obtain that $\mathfrak{L}(G)_{\mathbf{F}_p}$ and $\mathfrak{L}(G)^{\otimes \mathbf{F}_p}$ are the same provided that p splits completely in the ring of integers of K. We now introduce the notions of ring of integers of a number field and of prime splitting. We will give a very broad discussion of these concepts; we will mention the motivation behind them, and we will cite the result that we will need. However, for details and a rigorous treatment of number fields, we refer the reader to [5].

Definition 4.3.1. A **number field** is a finite extension of **Q**.

Definition 4.3.2. A complex number is an **algebraic integer** if it is a root of some monic polynomial with coefficients in $\mathbb{Z}$.

Definition 4.3.3. The **ring of integers** of a number field K, denoted by $\mathcal{O}_K$, is the set of all algebraic integers in K.

We can illustrate these concepts in the following diagram:

$$\begin{array}{ccc} \mathcal{O}_K & \subset & K \\ | & & | \\ \mathbf{Z} & \subset & \mathbf{Q} \end{array}$$

One of the most useful properties of **Z** is that every integer factors uniquely into primes. Does this generalize to $\mathcal{O}_K \subset K$, i.e., does every element of K decompose unique into irreduciles? The answer is no. Let us give an example of the failure of $\mathcal{O}_K$ to be a unique factorization domain (UFD).

Example 4.3.4. Let $K = Q(\sqrt{-5})$. It turns out that the ring of integers of K is $R = Z[\sqrt{-5}]$. Consider the factorization of 6 in $Z[\sqrt{-5}]$. On the one hand, $6 = 2 \cdot 3$. We can check that both 2 and 3 are irreducible in R. On the other hand, $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, and both of these factors are also irreducible. Thus we found two distinct factorizations of the element 6 into irreducibles of R, so R is not a UFD.

However, we can work around this problem. Kummer repaired unique factorization with his theory of ideal numbers. In modern terms, we use the somewhat simpler method of factorization into ideals. Specifically, the factorizations above are only using principal ideals, and it turns out that R is not a principal ideal domain, i.e., not every ideal is generated by a single element. We need the non-principal ideals in order to solve the factorization problem. Let us look again at the same example, but this time considering the factorization of the ideals generated by the elements we considered before.

Example 4.3.5. This is how the following ideals factor into prime ideals:

$$(2) = (2, 1+\sqrt{-5})^2, \tag{4.3.1}$$

$$(3) = (3, 1-\sqrt{-5})(3, 1+\sqrt{-5}), \tag{4.3.2}$$

$$(1+\sqrt{-5}) = (2, 1+\sqrt{-5})(3, 1-\sqrt{-5}), \tag{4.3.3}$$

$$(1+\sqrt{-5}) = (2, 1+\sqrt{-5})(3, 1+\sqrt{-5}). \tag{4.3.4}$$

In particular,

$$(6) = (2)(3) = (2, 1+\sqrt{-5})^2(3, 1-\sqrt{-5})(3, 1+\sqrt{-5}),$$

and

$$(6) = (1+\sqrt{-5})(1-\sqrt{-5}) = (2, 1+\sqrt{-5})(3, 1-\sqrt{-5})(2, 1+\sqrt{-5})(3, 1+\sqrt{-5}).$$

Note that we have unique factorization into prime ideals.

The key fact is that $\mathcal{O}_K$ is a Dedekind domain for any number field K, and every ideal in a Dedekind domain has unique factorization into prime ideals. For a definition of Dedekind domain and a proof of this result, see [5] and [8].

We have already seen in the above example that even though 2 and 3 are primes in $\mathbf{Z}$ they are not prime in $\mathbf{Z}[\sqrt{-5}]$. The behavior of primes in extensions is a central question in the study of number fields. We will consider the case of an extension $K/\mathbf{Q}$, in which case the relevant ideals are of the form $p\mathcal{O}_K$ for rational primes p. If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ and p is a rational prime, we say that p **lies above** p if $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$. It can be shown that every non-zero prime of $\mathcal{O}_K$ lies above a unique prime of $\mathbf{Z}$, and that the primes of $\mathcal{O}_K$ lying above p are precisely those ideals occurring in the prime factorization of $p\mathcal{O}_K$. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ lying over $p \in Z$. Let e be the exact power of p dividing $p\mathcal{O}_K$. We call e the ramification index of $\mathfrak{p}/p$ and write it as $e(\mathfrak{p}/p)$. The factorization of $p\mathcal{O}_K$ is thus

$$p\mathcal{O}_K = \prod_{\mathfrak{p}\cap\mathbf{Z}=p\mathbf{Z}} \mathfrak{p}^{e(\mathfrak{p}/p)}.$$

We will also need a way to measure the relative "sizes" of ideals. The most natural way is to consider the residue field $\mathcal{O}_K/\mathfrak{p}$. We can show that this is a finite field of order p^f for some f; however, the

proof of this claim is non-trivial and can be found in [5] and [8]. We define the **inertial degree** $f(\mathfrak{p}/p)$ to be this integer f. We will be interested in those primes that **split completely** in $\mathcal{O}_K$, i.e., those primes for which all the $e(\mathfrak{p}/p) = 1$ and $f(\mathfrak{p}/p) = 1$.

We are going to show how to explicitly factor primes in a number ring in the particular case when $\mathcal{O}_K = Z[\alpha]$ for some $\alpha \in \mathcal{O}_K$, with minimal polynomial $f(x) \in Z[x]$, and illustrate it through an example. Let K be a number field of degree n. Let p be a prime of $\mathbf{Z}$. We wish to explicitly determine the factorization of the ideal $p\mathcal{O}_K$ of $\mathcal{O}_K$. Let

$$\bar{f}(x) = \bar{g_1}(x)^{e_1} \cdots \bar{g_r}(x)^{e_r}$$

be the factorization of $\bar{f}(x)$ into irreducibles in $\mathbf{F}_p[x]$. We will write $g_i(x)$ for any lift of $\bar{g_i}$ to $\mathbf{Z}[x]$. Let f_i be the degree of $\bar{g_i}$; so we have $\sum e_i f_i = n$. The main results that we are going to use are that each ideal

$$\mathfrak{p}_i = (p, g_i(\alpha))$$

of $\mathcal{O}_K$ is prime, and

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

Furthermore,

$$f(\mathfrak{p}_i/p) = f_i.$$

The proofs of all these results can be found in [5] and [8]. We now give an example of how to factor a prime ideal of $\mathbf{Z}$ in a number ring.

Example 4.3.6. Let $K = \mathbf{Q}(\sqrt[3]{2})$; it turns out that $\mathcal{O}_K = \mathbf{Z}[\sqrt[3]{2}]$. We can therefore factor primes by factoring $x^3 - 2$ modulo p. For example,

$$x^3 - 2 \equiv x^3 \pmod 2;$$

this yields the ideal factorization

$$(2) = (2, \sqrt[3]{2})^3.$$

To give an example of a prime that splits completely, we get

$$x^3 - 2 \equiv (x-11)(x-24)(x-27) \pmod{31},$$

so we get the ideal factorization

$$(31) = (31, \sqrt[3]{2} - 11)(31, \sqrt[3]{2} - 24)(31, \sqrt[3]{2} - 27).$$

Note that since the polynomials $x-11$, $x-24$ and $x-27$ in the factorization of x^3-2 have degree 1, we get that

$$f((31, \sqrt[3]{2} - 11)/31) = f((31, \sqrt[3]{2} - 24)/31) = f((31, \sqrt[3]{2} - 27)/31) = 1,$$

and note that all the exponents in the factorization of the ideal (31) are equal to 1, so we have

$$e((31, \sqrt[3]{2} - 11)/31) = e((31, \sqrt[3]{2} - 24)/31) = e((31, \sqrt[3]{2} - 27)/31) = 1.$$

Thus 31 splits completely in $\mathcal{O}_K$.

Let us now consider what happens if a prime p splits completely in the ring of integers $\mathcal{O}_K$ of K, where K is the splitting field of $\mathbf{C}[G]$ for a finite group G. Analogously to Lemma 4.2.4, the characters of G over $\mathbf{C}$ will be algebraic integers of K, i.e., the characters will take values in $\mathcal{O}_K$.

Lemma 4.3.7. *If K is the splitting field of $\mathbf{C}[G]$ for a finite group G, then the characters of G over $\mathbf{C}$ take values in $\mathcal{O}_K$.*

Proof. Let χ be a character of an irreducible complex representation ρ of G. By definition, $\chi(g)$ is the trace of the matrix $\rho(g)$ for any $g \in G$. Hence $\chi(g)$ is the sum of the eigenvalues of $\rho(g)$ which are algebraic integers. Thus $\chi(g)$ is an algebraic integer, but by the definition of K, $\chi(g) \in K$, so $\chi(g) \in \mathcal{O}_K$. □

Lemma 4.3.8. *If a prime p splits completely in the ring of integers $\mathcal{O}_K$ of K, where K is the splitting field of $\mathbf{C}[G]$ for a finite group G, then the reduction modulo p of the character values lies in $\mathbf{F}_p$.*

Proof. Recall from before that $\mathcal{O}_K/p\mathcal{O}_K \cong \mathbf{F}_{p^f}$ for some integer f. (For proof, see [5].) So, the residues modulo p of elements in $\mathcal{O}_K$ lie in $\mathbf{F}_{p^f}$. By definition, a prime p splits completely if $f = 1$. Then, $\mathcal{O}_K/p\mathcal{O}_K \cong \mathbf{F}_p$, thus the reduction modulo p of the character values lies in $\mathbf{F}_p$. $\square$

This result guarantess that the dimensions of the representations over $\mathbf{F}_p$ will be the same when p splits completely in $\mathcal{O}_K$, and also, if $p \neq 2$, the proof of the following lemma will go through idetically to the one of Lemma 4.2.5. We restate the lemma in its more general form:

Lemma 4.3.9. *If the a prime p splits completely in $\mathcal{O}_K$ where $\mathcal{O}_K$ is the ring of integers of the splitting field K of $\mathbf{C}[G]$, then the reduction mod p of a complex character χ will have the same type if $p \neq 2$.*

Again, since the dimension and types of characters are preserved under reduction modulo p of complex characters, if $p \neq 2$, $p \nmid \#G$ and p splits completely in $\mathcal{O}_K$, the decompositions of $\mathfrak{L}(G)_{\mathbf{F}_p}$ and $\mathfrak{L}(G)^{\otimes \mathbf{F}_p}$ will coincide.

4.4 An Example

Let us give an example of a group whose splitting field is K, an extension of Q, and see how $\mathfrak{L}(G)_{\mathbf{F}_p}$ and $\mathfrak{L}(G)^{\otimes \mathbf{F}_p}$ compare for primes p that split completely in $\mathcal{O}_K$ and for primes p that do not split in $\mathcal{O}_K$.

Example 4.4.1. Again, let $G = A_5$, the alternating group on 5 elements. Recall from a previous example that the spliting field of $\mathbf{C}[A_5]$ is $\mathbf{Q}[\sqrt{5}]$. It turns out that the ring of integers of $\mathbf{Q}[\sqrt{5}]$ is $\mathbf{Z}[\sqrt{5}]$. The order of A_5 is 60, so we will rule out from the beginning the primes 2,3, and 5 since they divide the order of the group. Recall from another previous example that we have the following decomposition:

$$\mathfrak{L}(A_5)^{\otimes \mathbf{F}_p} = \mathfrak{o}(1, \mathbf{F}_p) \oplus \mathfrak{o}(3, \mathbf{F}_p) \oplus \mathfrak{o}(3, \mathbf{F}_p) \oplus \mathfrak{o}(4, \mathbf{F}_p) \oplus \mathfrak{o}(5, \mathbf{F}_p).$$

As we mentioned before, $\mathfrak{o}(n,k)$ decomposes into two simple Lie algebras of size 3, and the other direct summands are all simple. In particular, the sizes of the irreducible components in the direct sum are 3, 3, 3, 3 and 10.

First, let $p = 13$. The polynomial $x^2 - 5$ is irreducible modulo 13, so the ideal (13) does not factor in $\mathcal{O}_K$, i.e., it is a prime ideal. Note that for a prime to split completely in $\mathcal{O}_K$ it would have to factor into two distinct factors since the degree of the extension is 2. So 3 does not split in $\mathcal{O}_K$. Using MAGMA, we get that the sizes of the irreducible components in the decomposition of $\mathfrak{L}(A_5)_{\mathbf{F}_{13}}$, we get 6,6,10. Thus we do not even have the same number of components and we get different sizes compared to the irreducibles in the decomposition of $\mathfrak{L}(A_5)^{\otimes \mathbf{F}_{13}}$. Thus the two algebras are not the same.

Now let $p = 11$. Factoring $x^2 - 5$ modulo 11 we get

$$x^2 - 5 \equiv (x+4)(x+7) \pmod{11},$$

so we get the ideal factorization

$$(11) = (5, \sqrt{5}+4)(5, \sqrt{5}+7).$$

Since both exponents in the factorization are 1, the prime 11 splits completely in $\mathbf{Z}[\sqrt{5}]$. Using MAGMA, we can easily verify that in this case $\mathfrak{L}(A_5)_{\mathbf{F}_{11}}$ is the same as $\mathfrak{L}(A_5)^{\otimes \mathbf{F}_{11}}$.

It makes sense that we can reduce $\sqrt{5}$ modulo p if and only if 5 is a square mod p, i.e., when $x^2 - 5$ has a root mod p. We can generalize these results further for this particular example. By quadratic reciprocity (see [5]) we get that a prime p splits completely in $\mathcal{O}_K$ if and only if

$$p \equiv 1, 4 \pmod{5}.$$

Thus we get that $\mathfrak{L}(A_5)^{\otimes \mathbf{F}_p}$ and $\mathfrak{L}(A_5)_{\mathbf{F}_p}$ are the same if and only if $p \equiv 1, 4 \pmod{5}$.

4.5 When are $\mathfrak{L}(G)^{\otimes \mathbf{F}_p}$ and $\mathfrak{L}(G)_{\mathbf{F}_p}$ the same?

We have shown in the previous section that under certain assumptions $\mathfrak{L}(G)^{\otimes \mathbf{F}_p}$ and $\mathfrak{L}(G)_{\mathbf{F}_p}$ are the same if the splitting field of $\mathbf{C}[G]$ is $\mathbf{Q}$, or if it is an extension of $\mathbf{Q}$, K such that p splits completely in the ring of integers of K. We summarize this result as the following theorem:

Theorem 4.5.1. *If $p \neq 2$ and $p \nmid \#G$ the Lie algebras $\mathfrak{L}(G)^{\otimes \mathbf{F}_p}$ and $\mathfrak{L}(G)_{\mathbf{F}_p}$, as defined in the beginning of section 4.2 are the same if*

- *the splitting field of $\mathbf{C}[G]$ is $\mathbf{Q}$, or*
- *the splitting field of $\mathbf{C}[G]$ is K, an extension of $\mathbf{Q}$ and p splits completely in the ring of integers of K.*

We have taken two approaches to defining a modular Plesken Lie algebra. On one hand, we have reduced the complex Pleasken Lie algebra mod p by taking the $\mathbf{Z}$-span of the Chevalley basis and tensoring it with $\mathbf{F}_p$ and we have shown that this preserves the decomposition of the Lie algebra into simple ideals. On the other hand, we have started with the group algebra $\mathbf{F}_p[G]$ and we have defined the Plesken Lie algebra analogously to the complex one, i.e., as a subalgebra of $\mathbf{F}_p[G]$ that is the linear span of the elements $g - g^{-1}$. We are mostly interested in how the modular Plesken Lie algebra over $\mathbf{F}_p$ decomposes, so we have investigated when it is the same with the reduction mod p of the complex one, since we already knew the decomposition of this one. The previous theorem summarizes our main result, and illustrates that this problem involves not only Lie algebra theory and modular Lie algebra theory, but also representation theory, modular character theory, and algebraic number theory such as prime splitting.

5
APPENDIX

We provide the MAGMA code that we used in order to compute the Plesken Lie algebra as a subalgebra of $\mathbf{F}_p[G]$, and compute its deocmposition into irreducible direct summands. Each line of code is commented.

The main reason for which we include this code is that there is no straightforward way to define the Plesken Lie algebra in MAGMA, and working with their functions turned out to be a difficut task because of the types of this programming language. The main object that we are interested in, the Plesken Lie algebra, is a Lie algebra that is a subalgebra of a group algebra. There are different types for this object in MAGMA (GenAlgebra, GrpAlgebra, AssAlgebra, LieAlgebra) and we have to be careful when we try to combine functions that are defined for specific types because they are not inherited. Figuring out why some things initially did not work as expected was not very easy because of the poor documentation MAGMA offers on types. Therefore, the key to making the following code work was to realize that when we have to define functions going from one type to the other, and specify what the maps are, and later on apply the maps or their inverses to elements in order to convey them the right types for the functions that we are using on them.

First we define G to be a finite group.

FG := GroupAlgebra(GF(37), G);

We define the group algebra $\mathbf{F}_{37}[G]$.

L1,h:=Algebra(FG);

We redefine the type of FG to Algebra in order to be able to use function that only define din MAGMA for the type Algebra. h encodes the map going from one type to the other.

FFG,f:=LieAlgebra(L1);

We redefine the type of L1 to LieAlgebra in order to be able to use function that only define din MAGMA for the type LieAlgebra. f encodes the map going from one type to the other.

L:=[];

We define an empty list L.

for g in G do

We start to iterate over the elements in G, i.e., we start a loop.

if Order(g) ne 2 and Order(g) ne 1 and Inverse(g) notin L then

We filter for non identity elements with order not equal to 2 and sort out their inverses.

Append(L,g);

The elements that qualify are appended to the list L. **end if;**

end for;

We end the if statement and for loop.

LL:=[];

We define an empty list LL.

for g in L do

We start a for loop over the elements in our previous list L.

Append(LL,FG!g-FG!g^{-1}**);**

For each $g \in G$ that is in our list L we append $g - g^{-1}$ to LL as an element of the group algebra FG.

end for;

We end the for loop.

LLL:=[];

We define an empty list LLL.

for g in LL do

We start a loop over the elements in the list LL.

Append(LLL, (g@h)@f);

To each element in LL we apply the functions h and f, i.e., we change its type to Algebra element and LieAlgebra element and we append it to LLL.

end for;

We end the for loop.

P:=sub⟨FFG|LLL⟩;

We define our Plesken Lie algebra to be the subalgebra of FFG, the group algebra $\mathbf{F}_{37}$, generated by the elements in the list LLL.

P;

We ask for a description of P.

DirectSumDecomposition(P);

This command give us the direct sum decomposition into irreducibles of P.

Bibliography

[1] James Humphreys, *Introduction to Lie Algebras and Representation Theory*, Springer, New York, 1972.

[2] Arjeh Cohen and D.E Taylor, *On a Certain Lie Algebra Defined by a Finite Group.*

[3] Karin Erdmann and Mark J. Wildon, *Introduction to Lie Algebras*, Springer, New York.

[4] Jean-Pierre Serre, *Linear Representations of Finite Groups*, Springer, New York, 1977.

[5] Daniel Marcus, *Number Fields*, Springer, New York, 1975.

[6] Steven Weintraub, *Representation Theory of Finite Groups: Algebra and Arithmetic*, American Mathematical Society, Providence, Rhode Island, 2003.

[7] William Fulton and Joe Harris, *Representation Theory*, Springer, New York, 1991.

[8] Tom Weston, *Algebraic Number Theory Notes.*

[9] John Cullinan, *Representation Theory Lecture Notes.*