On a Certain Lie Algebra Defined by a Finite Group

Arjeh M. Cohen and D. E. Taylor

1. **INTRODUCTION.** Some years ago W. Plesken told the first author of a simple but interesting construction of a Lie algebra from a finite group. The authors posed themselves the question as to what the structure of this Lie algebra might be. In particular, for which groups does the construction produce a simple Lie algebra? The answer is given in the present paper; it uses some textbook results on representations of finite groups, which we explain along the way.

Little knowledge of the theory of Lie algebras is required beyond the definition of a Lie algebra itself and the definitions of simple and semisimple Lie algebras. Thus this exposition may serve as the basis for some entertaining examples or exercises in a graduate course on the representation theory of finite groups.

2. **THE PLESKEN LIE ALGEBRA OF A GROUP.** Let G be a finite group. As with any associative algebra, the group algebra $\mathbb{C}[G]$ over the field $\mathbb{C}$ of complex numbers can be made into a Lie algebra by means of the bracket product: $[a, b] = ab - ba$. The Lie algebra $\mathcal{L}(G)$ suggested by Plesken is the subspace that is the linear span of the elements $g - g^{-1}$ for g in G. Indeed, setting $\hat{g} = g - g^{-1}$ we 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 $\mathcal{L}(G)$ is closed under the Lie product, and therefore it is a Lie algebra.

Let L be a Lie algebra. The algebra L is *Abelian* if $[x, y] = 0$ for all x and y in L. A subspace I of L is an *ideal* if $[x, y]$ belongs to I for all x in I and all y in L. The Lie algebra L is *simple* if its dimension is at least two and if $\{0\}$ and L are its only ideals. It is *semisimple* if $\{0\}$ is the only Abelian ideal. In characteristic 0 a Lie algebra is semisimple if and only if it is the direct sum of ideals that are simple Lie algebras.

The Lie algebra $\mathfrak{gl}(n)$ is the space of all linear transformations of $\mathbb{C}^n$, where the Lie product is defined by $[x, y] = xy - yx$. The subalgebra $\mathfrak{sl}(n)$ of linear transformations with trace zero is a simple Lie algebra except when n is 1.

If $n \geq 1$ and if β is a nondegenerate alternating or symmetric form, then the subspace of $\mathfrak{gl}(n)$ consisting of all x such that $\beta(xu, v) + \beta(u, xv) = 0$ for all u and v is a Lie algebra (see Humphreys [3, p. 3]). When β is alternating, n is necessarily even, and we have the *symplectic* Lie algebra $\mathfrak{sp}(n)$; when β is symmetric, we have the *orthogonal* Lie algebra $\mathfrak{o}(n)$. If $n \geq 2$, almost all these Lie algebras are simple: the exceptions are $\mathfrak{o}(2)$, which is Abelian and $\mathfrak{o}(4)$, which is semisimple. The algebras $\mathfrak{sl}(n)$, $\mathfrak{sp}(n)$, and $\mathfrak{o}(n)$ are the *classical* simple Lie algebras. Cartan showed that a simple Lie algebra over $\mathbb{C}$ is either classical or one of five exceptions. He used the symbols A_n, B_n, C_n, D_n, E_6, E_7, E_8, F_4, and G_2 to denote the simple Lie algebras. For the classical algebras, $\mathfrak{sl}(n+1)$ is of type A_n, $\mathfrak{sp}(2n)$ is of type C_n, $\mathfrak{o}(2n+1)$ is of type B_n, and $\mathfrak{o}(2n)$ is of type D_n. Not all are distinct: it is true that $\mathfrak{sl}(2) \simeq \mathfrak{sp}(2) \simeq \mathfrak{o}(3)$, $\mathfrak{sp}(4) \simeq \mathfrak{o}(5)$, and $\mathfrak{sl}(3) \simeq \mathfrak{o}(6)$.

3. **SMALL EXAMPLES.** Before addressing the question of simplicity directly, we examine some small examples. Since $\hat{g} = 0$ if and only if $g^2 = 1$, the dimension of $\mathcal{L}(G)$ is half the number of elements g in G such that $g^2 \neq 1$. (This already suggests that Schur-Frobenius theory might be involved.) Since the dimension of a smallest nontrivial simple Lie algebra is three, this should serve as a guide to possible examples.

If g and h commute in G, then $[\hat{g}, \hat{h}] = 0$ and therefore $[\mathcal{L}(G), \mathcal{L}(G)] = 0$ whenever G is Abelian. Furthermore, if A is an Abelian subgroup of index 2 in G and x is an element of order 2 such that $xax = a^{-1}$ for all a in A, then every element of $G \setminus A$ has order 2. This implies that $\mathcal{L}(G) = \mathcal{L}(A)$, so $[\mathcal{L}(G), \mathcal{L}(G)] = 0$ in this case as well. For example, for the symmetric group Sym(3) on three letters with $A = \mathrm{Alt}(3)$ and x any transposition, we find that the dimension of $\mathcal{L}(\mathrm{Sym}(3))$ is one and it is spanned by $(1,2,3) - (1,3,2)$. Furthermore, in general, the linear span of $\hat{z}$, for z in $Z(G)$, is an Abelian ideal of $\mathcal{L}(G)$ that is trivial if and only if $Z(G)$ is an elementary Abelian 2-group.

The considerations so far show that in searching for nontrivial simple examples we can ignore Abelian groups, dihedral groups, and groups whose centres are not elementary Abelian 2-groups. The smallest group not covered by these restrictions is the quaternion group of order 8:

$$Q_8 = \langle\, a, b \mid a^2 = b^2, b^4 = 1, a^{-1}ba = b^{-1} \,\rangle.$$

In this case $\dim \mathcal{L}(Q_8) = 3$, and setting $c = ab$ we have

$$[\hat{a}, \hat{b}] = 4\hat{c}, \quad [\hat{b}, \hat{c}] = 4\hat{a}, \quad [\hat{c}, \hat{a}] = 4\hat{b}.$$

Thus $\mathcal{L}(Q_8)$ is the simple Lie algebra $\mathfrak{sl}(2)$. The elements $2\hat{a}$, $2\hat{b}$, and $2\hat{c}$ correspond to the matrices $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $\begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}$, and $\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$.

4. **BILINEAR FORMS AND THE ADJOINT MAP.** The key to understanding the group algebra $\mathbb{C}[G]$ (hence $\mathcal{L}(G)$) is the study of the irreducible representations of G. In this section we introduce the material on representations and bilinear forms that we need for the structural analysis of $\mathcal{L}(G)$ carried out in the next section.

Suppose that V is a G-module. The *character* of V is the complex valued function, defined on G, that assigns each element g of G to the trace of the linear transformation that g induces on V. If χ is the character of V, its complex conjugate $\overline{\chi}$ is the character of the dual space V^*, which is a G-module with G-action given by $g\varphi(v) = \varphi(g^{-1}v)$. Then $\chi = \overline{\chi}$ if and only if V is isomorphic to V^*.

If $\theta : V \to V^*$ is a linear transformation, then $\beta(u,v) = \theta(v)u$ is a bilinear form on V. Furthermore, every bilinear form β on V arises in this way, and θ is an isomorphism if and only if β is nondegenerate. It is clear that β is preserved by G if and only if θ is a G-module homomorphism. Therefore, if V is an irreducible G-module, then by Schur's lemma there is at most one nonzero bilinear form β (up to a scalar multiple) preserved by G. Moreover, if β is G-invariant, the alternating form $(u,v) \mapsto \beta(u,v) - \beta(v,u)$ and the symmetric form $(u,v) \mapsto \beta(u,v) + \beta(v,u)$ are also G-invariant. Consequently, if V is irreducible, β is either alternating or symmetric.

An irreducible G-module V is said to be of *real* (respectively, *symplectic*) *type* if G preserves a nondegenerate symmetric (respectively, alternating) form on V. If G is not of real or symplectic type, then we have shown that the only bilinear form on V preserved by G is 0. In this case V is said to be of *complex type*. Furthermore, the character χ of V is of *real*, *symplectic*, or *complex* type according to the type of V.

If f belongs to $\mathrm{End}(V)$, the *transpose* of f is the element f^* of $\mathrm{End}(V^*)$ defined by $f^*\varphi = \varphi f$. Suppose that β is nondegenerate, and $\theta(v)u = \beta(u,v)$. The map σ defined by

$$\sigma(f) = \theta^{-1} f^* \theta$$

is an anti-automorphism of $\mathrm{End}(V)$. The definition of σ is equivalent to the requirement that

$$\beta(u, \sigma(f)v) = \beta(f(u), v) \tag{1}$$

for all u and v in V and all f in $\mathrm{End}(V)$. That is, $\sigma(f)$ is the *adjoint* of f with respect to β. This formula shows that the nonzero scalar multiples of β give rise to the same anti-automorphism σ and that σ^{-1} is the anti-automorphism corresponding to the opposite form $\beta'(u,v) = \beta(v,u)$.

Suppose that there is no nondegenerate bilinear form preserved by G. Then V and V^* are not isomorphic as G-modules. However, the map $Q : V \oplus V^* \to \mathbb{C}$ for which $(u,\varphi) \mapsto \varphi(u)$ is a G-invariant quadratic form and the G-invariant symmetric form β defined by $\beta(u+\varphi, v+\psi) = \varphi(v) + \psi(u)$ is known as the *polar form* of Q.

To complete the description of σ we consider the situation where V is a G-module and β is a nondegenerate G-invariant bilinear form on V. For g in G we have $\beta(u, \sigma(g)) = \beta(gu, v) = \beta(u, g^{-1}v)$ for all u and v in V. Thus $\sigma(g) = g^{-1}$, where we identify g with the automorphism induced by g on V. In particular, σ is an *anti-involution* of $\mathrm{End}(V)$. In the next section we apply this observation to the group algebra of G.

5. **THE STRUCTURE OF $\mathcal{L}(G)$.** The group algebra $\mathbb{C}[G]$ can be written as a direct sum of two-sided ideals:

$$\mathbb{C}[G] = I_1 \oplus I_2 \oplus \cdots \oplus I_r.$$

In fact, we may take $I_i = \mathrm{End}(V_i)$, where $V_1, V_2, \ldots, V_r$ are a set of representatives for the irreducible G-modules. The I_i are also ideals with respect to the Lie product on $\mathbb{C}[G]$.

If χ_i is the character of V_i, its complex conjugate $\overline{\chi_i}$ is the character of the dual space V_i^*. When $\chi_i \neq \overline{\chi_i}$, we can choose the notation so that $V_i^* = V_j$ for some j different from i; in this case we put $i^* = j$.

Theorem 5.1. *The Lie algebra $\mathcal{L}(G)$ admits the decomposition*

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

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 $\{\chi, \overline{\chi}\}$ from $\mathfrak{C}$.

Proof. The calculations of the previous section show that either V_i or $V_i \oplus V_{i^*}$ carries a nondegenerate bilinear form β_i according to whether or not V_i is isomorphic to V_i^*. These forms combine to provide a nondegenerate G-invariant form β on $V = \bigoplus_i V_i$, hence an anti-involution σ of $\mathbb{C}[G]$ such that $\sigma(g) = g^{-1}$ for all g in G. The Lie algebra $\mathcal{L}(G)$ is just the -1-eigenspace of this anti-involution. It follows from equation (1) that

$$\mathcal{L}(G) = \{\, f \in \mathbb{C}[G] : \beta(f(u), v) + \beta(u, f(v)) = 0 \text{ for all } u \text{ and } v \text{ in } V \,\}.$$

Accordingly, if V_i is of real or symplectic type, the image of $\mathcal{L}(G)$ under the projection of $\mathbb{C}[G]$ onto I_i consists of all linear transformations h in $\mathrm{End}(V_i)$ such that $\beta_i(h(u), v) + \beta_i(u, h(v)) = 0$ for all u and v in V_i; that is, the image is the full Lie algebra of the form β_i.

Let $d_i = \chi_i(1)$ be the dimension of V_i. If V_i is of real type, the image of $\mathcal{L}(G)$ under the projection of $\mathbb{C}[G]$ onto I_i is $\mathfrak{o}(d_i)$, which has dimension $d_i(d_i - 1)/2$. Similarly, if V_i is of symplectic type, the image of $\mathcal{L}(G)$ is $\mathfrak{sp}(d_i)$, a Lie algebra of dimension $d_i(d_i + 1)/2$.

If V_i is of complex type, then σ interchanges I_i and I_{i^*}. In this case the image of $\mathcal{L}(G)$ in $I_i \oplus I_{i^*}$ is the d_i^2-dimensional Lie algebra $\mathfrak{gl}(d_i)$. ☐

The *Schur-Frobenius indicator* $\nu(\chi)$ of χ is defined to be 1, -1, or 0 according to whether χ is of real, symplectic, or complex type.

Example. The dimensions of the irreducible representations of the group $\mathrm{SL}(3, 2)$ of three by three non-singular matrices over the field of two elements are 1, 3, 3, 6, 7, and 8 and the Schur-Frobenius indicators of their characters are 1, 0, 0, 1, 1, and 1, respectively (see [1, p. 3]). Thus the Lie algebra of this group is the direct sum of simple Lie algebras of types $\mathfrak{gl}(3)$, $\mathfrak{o}(6)$, $\mathfrak{o}(7)$, and $\mathfrak{o}(8)$ and the dimension of its centre is one.

On computing the dimension of $\mathcal{L}(G)$ we obtain the following well-known formula (see Isaacs [4, p. 51]):

Corollary 5.2. *If t is the number of involutions (i.e., elements of order 2) in G, then*

$$t + 1 = \sum_{i=1}^{r} \nu(\chi) d_i,$$

Proof. In the proof of Theorem 5.1 we showed that if V_i is of real or symplectic type, the dimension of the image of $\mathcal{L}(G)$ in I_i is $d_i(d_i - \nu(\chi_i))/2$, and if V_i is of complex type, the dimension of the image of $\mathcal{L}(G)$ in $I_i \oplus I_{i^*}$ is d_i^2. Thus

$$\dim \mathcal{L}(G) = \sum_{i=1}^{r} d_i(d_i - \nu(\chi_i))/2.$$

Combining this with the observation from section 3 that

$$\dim \mathcal{L}(G) = (|G| - t - 1)/2,$$

where t is the number of involutions in G, we see that

$$\sum_{i=1}^{r} d_i^2 - \sum_{i=1}^{r} d_i \nu(\chi_i) = |G| - t - 1.$$

But $|G| = \sum_i d_i^2$, so the first terms cancel, and we obtain the required equality. □

6. **WHEN IS $\mathcal{L}(G)$ SIMPLE?.** Assume, until further notice, that $\mathcal{L}(G)$ is a simple Lie algebra and, in particular, that $\dim \mathcal{L}(G) \geq 3$. The following result is a corollary of Theorem 5.1:

Corollary 6.1. *If $\mathcal{L}(G)$ is simple, then all linear characters of G are real, and G has a unique irreducible character of degree greater than 1, which is of real or symplectic type.*

Proof. The group algebra $\mathbb{C}[G]$ is a direct sum of two-sided ideals I_j, which are also ideals with respect to the Lie product. From the proof of Theorem 5.1 we have $\mathcal{L}(G) \cap I_j \neq \{0\}$ for some j. By assumption, $\mathcal{L}(G)$ is simple, whence I_j is the *unique* ideal such that $\mathcal{L}(G) \subseteq I_j$ and $\mathcal{L}(G) \cap I_i = \{0\}$ when $i \neq j$. The Lie algebra $\mathfrak{gl}(n)$ has a one-dimensional centre and is not simple. It follows that G has no representations of complex type and that $d_i = 1$ if $i \neq j$. Thus V_j is of real or symplectic type, and $\mathcal{L}(G)$ is $\mathfrak{o}(d_j)$ or $\mathfrak{sp}(d_j)$. □

A group G is an *extraspecial* 2*-group* if $G' = Z(G)$ has order 2 and G/G' is an elementary Abelian 2-group. In [2, Theorem 5.2] it is shown that for each n there are just two extraspecial 2-groups of order 2^{1+2n}, namely,

$$\mathbf{2}_+^{1+2n} = \underbrace{D_8 \circ D_8 \circ \cdots \circ D_8}_{n \text{ factors}}$$

and

$$\mathbf{2}_-^{1+2n} = \underbrace{Q_8 \circ D_8 \circ \cdots \circ D_8}_{n \text{ factors}},$$

where D_8 is the dihedral group of order 8, Q_8 is the quaternion group of order 8, and $\circ$ denotes a central product (see Gorenstein [2, p. 29]).

Now we have enough information to prove our main result:

Theorem 6.2. *Except in two cases the Lie algebra $\mathcal{L}(G)$ of a finite group G is simple if and only if G is an extraspecial 2-group. The two exceptions are the dihedral group D_8 and the central product $Q_8 \circ Q_8 \simeq D_8 \circ D_8$.*

Proof. Suppose that $\mathcal{L}(G)$ is simple. Then all the linear characters of G are real, so G/G' has no element whose order is greater than 2; that is, G/G' is an elementary Abelian 2-group. Furthermore there is only one irreducible character of G that is not linear. Now G' has at least two conjugacy classes, and all conjugates of x in G belong to the coset xG'. Therefore G has at least $|G/G'|+1$ conjugacy classes. But G has exactly $|G/G'|+1$ characters, from which it follows that all nonidentity elements of G' are conjugate. Thus G' is an elementary Abelian p-group for some prime p.

If $x \notin G'$, then the coset xG' consists of a single conjugacy class in G and hence $x \notin Z(G)$; that is, $Z(G) \subseteq G'$. The linear span of $\hat{z}$ for z in $Z(G)$ is an Abelian ideal of $\mathcal{L}(G)$ which in this case must be trivial. Thus $Z(G)$ is either the identity subgroup or an elementary Abelian 2-group.

Suppose at first that $p \neq 2$. If S is a Sylow 2-subgroup of G, then G is the semidirect product of G' and S, where S acts faithfully on G' by conjugation (i.e., only the identity element of S commutes with every element of G'). Therefore the elements of S are simultaneously diagonalizable (regarding G' as a vector space over the field of p elements). However, S acts transitively on G', so the only possibility is that $|G'| = 3$, whence G is the symmetric group Sym(3). This case was considered in section 3, where it was shown that $\mathcal{L}(\mathrm{Sym}(3))$ is not simple.

We have proved that G is a 2-group. Let m be the degree of the unique nonlinear character of G. Then $|G| = |G/G'| + m^2$, and m is a power of 2. Hence $m^2 = |G/G'|(|G'| - 1)$ and consequently $|G'| = 2$. Thus we have established that $G' = Z(G)$ and that G/G' is elementary Abelian (i.e., G is an extraspecial 2-group of order 2^{1+2n}, where $m = 2^n$). Consequently, G is isomorphic to either $\mathbf{2}_+^{1+2n}$ or $\mathbf{2}_-^{1+2n}$.

We have seen before that $\mathcal{L}(D_8)$ is not simple. Moreover, it turns out that $\mathcal{L}(Q_8 \circ Q_8) = \mathcal{L}(D_8 \circ D_8)$ is the direct sum of two copies of a Lie algebra of type $\mathfrak{sl}(2)$. On the other hand, in all other cases the Lie algebra is simple.

If G_n denotes $\mathbf{2}_+^{1+2n}$ or $\mathbf{2}_-^{1+2n}$, then $G_{n+1} = G_n \circ D_8$. We infer that if t_n is the number of involutions in G_n, then t_n satisfies the recurrence relation

$$t_{n+1} = 2^{1+2n} + 2t_n + 1.$$

The groups D_8 and Q_8 contain five involutions and one involution, respectively. Thus $\mathbf{2}_+^{1+2n}$ contains $m^2 + m - 1$ involutions, hence

$$\dim \mathcal{L}(\mathbf{2}_+^{1+2n}) = m(m-1)/2.$$

Similarly, $\mathbf{2}_-^{1+2n}$ contains $m^2 - m - 1$ involutions, hence

$$\dim \mathcal{L}(\mathbf{2}_-^{1+2n}) = m(m+1)/2.$$

(These values can also be derived from the number of singular vectors in an orthogonal geometry over the field of two elements; see Taylor [5, p. 146].)

It follows that

$$\mathcal{L}(\mathbf{2}_+^{1+2n}) \simeq \mathfrak{o}(2^n), \quad \mathcal{L}(\mathbf{2}_-^{1+2n}) \simeq \mathfrak{sp}(2^n).$$

□

As a bonus, our main structure theorem provides the following answer to the question about the semisimplicity of $\mathcal{L}(G)$:

Theorem 6.3. *The Lie algebra $\mathcal{L}(G)$ of the finite group G is semisimple if and only if G has no complex characters and every character of degree 2 is of symplectic type.*

Proof. The Lie algebra $\mathfrak{gl}(n)$ has a centre of dimension one, so if $\mathcal{L}(G)$ is semisimple it follows from Theorem 5.1 that G has no complex characters. Furthermore, the only orthogonal or symplectic Lie algebra that is not semisimple is the Lie algebra $\mathfrak{o}(2)$ of orthogonal 2×2 matrices. In our context this is the Lie algebra arising from a real character of degree 2. □

7. **ACKNOWLEDGEMENT.** This paper was written during visits by the authors to Sydney and Eindhoven, respectively. We thank the University of Sydney and the Technische Universiteit Eindhoven for their hospitality.

References.

1. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *The Atlas of Finite Groups*, Clarendon Press, Oxford, 1985; also available at: `http://web.mat.bham.ac.uk/atlas/v2.0/`.
2. D. Gorenstein, *Finite Groups*, Harper & Row, New York, 1968.
3. J. E. Humphreys, *Introduction to Lie Algebras and Representation Theory*, Graduate Texts in Mathematics, vol. 9, Springer-Verlag, New York, 1972.
4. I. M. Isaacs, *Character Theory of Finite Groups*, Academic Press, New York, 1976.
5. D. E. Taylor, *The Geometry of the Classical Groups*, Sigma Series in Pure Mathematics, vol. 9, Heldermann Verlag, Berlin, 1992.

Arjeh M. Cohen, Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, PO Box 513, 5600 MB Eindhoven, The Netherlands
E-mail address: `A.M.Cohen@tue.nl`

D. E. Taylor, Department of Mathematics and Statistics, University of Sydney, NSW 2006, Australia
E-mail address: `D.Taylor@maths.usyd.edu.au`