elements of each class, $h^{-1}X_ih = X_i$, i.e., X_i commutes with all group elements. This proves that $X_i \in Z(\mathbb{C}G)$.

We show the X_i's form a basis of $Z(\mathbb{C}G)$, which will prove $s = \dim_{\mathbb{C}} Z(\mathbb{C}G) = r$. Since the X_i's are linearly independent it remains to show they span $Z(\mathbb{C}G)$. Let $X = \sum_{g\in G} \alpha_g g$ be an arbitrary element of $Z(\mathbb{C}G)$. Since $h^{-1}Xh = X$,

$$\sum_{g\in G} \alpha_g h^{-1}gh = \sum_{g\in G} \alpha_g g.$$

Since the elements of G form a basis of $\mathbb{C}G$ the coefficients of g in the above two sums are equal:

$$\alpha_{hgh^{-1}} = \alpha_g.$$

Since h was arbitrary, every element in the same conjugacy class of a fixed group element g has the same coefficient in X, hence X can be written as a linear combination of the X_i's.

We summarize these results in the following theorem.

Theorem 10. Let G be a finite group.

(1) $\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \times M_{n_2}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C})$.

(2) $\mathbb{C}G$ has exactly r distinct isomorphism types of irreducible modules and these have complex dimensions $n_1, n_2, \ldots, n_r$ (and so G has exactly r inequivalent irreducible complex representations of the corresponding degrees).

(3) $\sum_{i=1}^{r} n_i^2 = |G|$.

(4) r equals the number of conjugacy classes in G.

Corollary 11.

(1) Let A be a finite abelian group. Every irreducible complex representation of A is 1-dimensional (i.e., is a homomorphism from A into $\mathbb{C}^{\times}$) and A has $|A|$ inequivalent irreducible complex representations. Furthermore, every finite dimensional complex matrix representation of A is equivalent to a representation into a group of diagonal matrices.

(2) The number of inequivalent (irreducible) degree 1 complex representations of any finite group G equals $|G/G'|$.

Proof: If A is abelian, $\mathbb{C}A$ is a commutative ring. Since a $k \times k$ matrix ring is not commutative whenever $k > 1$ we must have each $n_i = 1$. Thus $r = |A|$ (= the number of conjugacy classes of A). Since every $\mathbb{C}A$-module is a direct sum of irreducible submodules, there is a basis such that the matrices are diagonal with respect to this basis. This establishes the first part of the corollary.

For a general group G, every degree 1 representation, φ, is a homomorphism of G into $\mathbb{C}^{\times}$. Thus φ factors through G/G'. Conversely, every degree 1 representation of G/G' gives, by composition with the natural projection $G \to G/G'$, a degree 1 representation of G. The degree 1 representations of G are therefore precisely the irreducible representations of the abelian group G/G'. Part (2) is now immediate from (1).

Examples

(1) The irreducible complex representations of a finite abelian group A (i.e., the homomorphisms from A into $\mathbb{C}^\times$) can be explicitly described as follows: decompose A into a direct product of cyclic groups

$$A \cong C_1 \times \cdots \times C_n$$

where $|C_i| = |\langle x_i \rangle| = d_i$. Map each x_i to a (not necessarily primitive) $d_i{}^{\text{th}}$ root of 1 and extend this to all powers of x_i to give a homomorphism. Since there are d_i choices for the image of each x_i, the number of distinct homomorphisms of A into $\mathbb{C}^\times = GL_1(\mathbb{C})$ defined by this process equals $|A|$. By Corollary 11, these are all the irreducible representations of A. Note that it is necessary that the field contain the appropriate roots of 1 in order to realize these representations. An exercise below explores the irreducible representations of cyclic groups over $\mathbb{Q}$.

(2) Let $G = S_3$. By Theorem 10 the number of irreducible complex representations of G is three (= the number of conjugacy classes of S_3). Since the sum of the squares of the degrees is 6, the degrees must be 1, 1 and 2. The two degree 1 representations are immediately evident: the trivial representation and the representation of S_3 into $\{\pm 1\}$ given by mapping a permutation to its sign (i.e., $\sigma \mapsto +1$ if σ is an even permutation and $\sigma \mapsto -1$ if σ is an odd permutation). The degree 2 representation can be found by decomposing the permutation representation on 3 basis vectors (described in Section 1) into irreducibles as follows: let S_3 act on the basis vectors e_1, e_2, e_3 of a vector space V by permuting their indices. The vector $t = e_1 + e_2 + e_3$ is a nonzero fixed vector, so t spans a 1-dimensional G-invariant subspace (which is a copy of the trivial representation). By Maschke's Theorem there is a 2-dimensional G-invariant complement, I. Note that the permutation representation is not a sum of degree 1 representations: otherwise it could be represented by diagonal matrices and the permutations would commute in their action — this is impossible since the representation is faithful and G is non-abelian. Thus I cannot be decomposed further, so I affords *the* irreducible 2-dimensional representation. Indeed, I is the "augmentation" submodule described in Section 1:

$$I = \{w \in V \mid w = \alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3 \quad \text{with} \quad \alpha_1 + \alpha_2 + \alpha_3 = 0\}.$$

Clearly $e_1 - e_2$ and $e_2 - e_3$ are independent vectors in I, hence they form a basis for this 2-dimensional space. With respect to this basis of I we obtain a matrix representation of S_3 and, for example, this matrix representation on two elements of S_3 is

$$(1\,2) \mapsto \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad (1\,2\,3) \mapsto \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

(3) We decompose the regular representation over $\mathbb{C}$ of an arbitrary finite group. Recall that this is the representation afforded by the left $\mathbb{C}G$-module $\mathbb{C}G$ itself. By Theorem 10, $\mathbb{C}G$ is first of all a direct product of two-sided ideals:

$$\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \times M_{n_2}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C}).$$

Now by Proposition 6(4) each $M_{n_i}(\mathbb{C})$ decomposes further as a direct sum of n_i isomorphic simple left ideals. These left ideals give a complete set of isomorphism classes of irreducible $\mathbb{C}G$-modules. Thus the regular representation (over $\mathbb{C}$) of G decomposes as *the direct sum of all irreducible representations of G, each appearing with multiplicity equal to the degree of that irreducible representation.*

We record one additional property of $\mathbb{C}G$ which we shall prove in Section 19.2.

Theorem 12. The degree of each complex irreducible representation of a finite group G divides the order of G, i.e., in the notation of Theorem 10, each n_i divides $|G|$ for $i = 1, 2, \dots, r$.

In the next section we shall describe the primitive central idempotents of $\mathbb{C}G$ in terms of the group elements.

EXERCISES

Let G be a finite group and let R be a ring with 1.

1. Prove that conditions (1) and (2) of Wedderburn's Theorem are equivalent.
2. Prove that (3) implies (2) in Wedderburn's Theorem. [Let Q be a submodule of an R-module N. Use Zorn's Lemma to show there is a submodule M maximal with respect to $Q \cap M = 0$. If $Q + M = N$, then (2) holds; otherwise let M_1 be the complete preimage in N of some simple module in N/M not contained in $(Q + M)/M$, and argue that M_1 contradicts the maximality of M.]
3. Prove that (4) implies (3) in Wedderburn's Theorem. [Let N be a nonzero R-module. First show N contains simple submodules by considering a cyclic submodule. Then use Zorn's Lemma applied to the set of direct sums of simple submodules (appropriately ordered) to show that N contains a maximal completely reducible submodule M. If $M \neq N$ let M_1 be the complete preimage in N of a simple module in N/M and contradict the maximality of M.]
4. Prove that (5) implies (4) in Wedderburn's Theorem. [Use the methods in the proofs of Propositions 6 and 8 to decompose each R_i as a left R-module.]

The next six exercises establish some general results about rings and modules that imply the remaining implication of Wedderburn's Theorem: (2) implies (5). In these exercises assume R satisfies (2): every R-module is injective.

5. Show that R has the descending chain condition (D.C.C.) on left ideals. Deduce that R is a finite direct sum of left ideals. [If not, then show that as a left R-module R is a direct sum of an infinite number of nonzero submodules. Derive a contradiction by writing the element 1 in this direct sum.]
6. Show that $R = R_1 \times R_2 \times \cdots \times R_r$ where R_j is a 2-sided ideal and a simple ring (i.e., has no proper, nonzero 2-sided ideals). Show each R_j has an identity and satisfies D.C.C. on left ideals. [Use the preceding exercise to show R has a minimal 2-sided ideal R_1. As a left R-module $R = R_1 \oplus R'$ for some left ideal R'. Show R' is a right ideal and proceed inductively using D.C.C.]
7. Let S be a simple ring with 1 satisfying D.C.C. on left ideals and let L be a minimal left ideal in S. Show that $S \cong L^n$ as left S-modules, where $L^n = L \oplus \cdots \oplus L$ with n factors. [Argue by simplicity that $LS = S$ so $1 = l_1 s_1 + \cdots + l_n s_n$ for some $l_i \in L$ and $s_i \in S$ with n minimal. Show that the map $(x_1, \dots, x_n) \mapsto x_1 s_1 + \cdots + x_n s_n$ is a surjective homomorphism of left S-modules; use the minimality of L and n to show it is an injection.]
8. Let A be any ring with 1, let L be any left A-module and let L^n be the direct sum of n copies of L with itself.
   (a) Prove the ring isomorphism $\mathrm{Hom}_A(L^n, L^n) \cong M_n(D)$, where $D = \mathrm{Hom}_A(L, L)$ (multiplication in the ring $\mathrm{Hom}_A(X, X)$ is function composition, cf. Proposition 2(4) in Section 10.2).