(b) Deduce that if L is a simple A-module, then $\mathrm{Hom}_A(L^n, L^n)$ is isomorphic to a matrix ring over a division ring. [Use Schur's Lemma and (a).]

(c) Prove the ring isomorphism $\mathrm{Hom}_A(A, A) \cong A^{opp}$, where A^{opp} is the opposite ring to A (the elements and addition are the same as in A but the value of the product $x \cdot y$ in A^{opp} is yx, computed in A), cf. the end of Section 17.4. [Any homomorphism is determined by its value on 1.]

9. Prove that if S is a simple ring with 1 satisfying D.C.C. on left ideals then $S \cong M_n(\Delta)$ for some division ring Δ. (This result together with Exercise 6 completes the existence part of the proof that (2) implies (5) in Wedderburn's Theorem). [Use Exercises 7 and 8 to show $S^{opp} \cong \mathrm{Hom}_S(L^n, L^n) \cong M_n(D)$ for some division ring D. Then show $S \cong M_n(\Delta)$, where Δ is the division ring D^{opp}.]

10. Prove that Δ and n in the isomorphism $S \cong M_n(\Delta)$ of the previous exercise are uniquely determined by S (proving the uniqueness statement in Wedderburn's Theorem), as follows. Suppose $S = M_n(\Delta) \cong M_{n'}(\Delta')$ as rings, where Δ and Δ' are division rings.

(a) Prove that $\Delta \cong \mathrm{Hom}_S(L, L)$ where L is a minimal left ideal in S. Deduce that $\Delta \cong \Delta'$. [Use Proposition 6(4).]

(b) Prove that a finitely generated (left) module over a division ring Δ has a "basis" (a linearly independent generating set), and that any two bases have the same cardinality. Deduce that $n = n'$. [Mimic the proof of Corollary 4(2) of Section 11.1.]

11. Prove that if R is a ring with 1 such that every R-module is free then R is a division ring.

12. Let F be a field, let $f(x) \in F[x]$ and let $R = F[x]/(f(x))$. Find necessary and sufficient conditions on the factorization of $f(x)$ in $F[x]$ so that R is a semisimple ring. When R is semisimple, describe its Wedderburn decomposition. [See Proposition 16 in Section 9.5.]

13. Let G be the cyclic group of order n and let $R = \mathbb{Q}G$. Describe the Wedderburn decomposition of R and find the number and the degrees of the irreducible representations of G over $\mathbb{Q}$. In particular, show that if $n = p$ is a prime then G has exactly one nontrivial irreducible representation over $\mathbb{Q}$ and this representation has degree $p - 1$. [Recall from the first example in Section 1 that $\mathbb{Q}G = \mathbb{Q}[x]/(x^n - 1)$. Use Proposition 16 in Section 9.5 and results from Section 13.6.]

14. Let p be a prime and let $F = \mathbb{F}_p$ be the field of order p. Let G be the cyclic group of order 3 and let $R = FG$. For each of $p = 2$ and $p = 7$ describe the Wedderburn decomposition of R and find the number and the degrees of the irreducible representations of G over F.

15. Prove that if P is a p-group for some prime p, then P has a faithful irreducible complex representation if and only if $Z(P)$ is cyclic. [Use Exercise 18 in Section 1, Theorem 6.1(2) and Example 3.]

16. Prove that if V is an irreducible FG-module and F is an algebraically closed field then $\mathrm{Hom}_{FG}(V, V)$ is isomorphic to F (as a ring).

17. Let F be a field, let $R = M_n(F)$ and let M be the unique irreducible R-module. Prove that $\mathrm{Hom}_R(M, M)$ is isomorphic to F (as a ring).

18. Find all 2-sided ideals of $M_n(\mathbb{Z})$.

18.3 CHARACTER THEORY AND THE ORTHOGONALITY RELATIONS

In general, for groups of large order the representations are difficult to compute and unwieldy if not impossible to write down. For example, a matrix representation of degree 100 involves matrices with 10,000 entries, and a number of 100 × 100 matrices may be required to describe the representation, even on a set of generators for the group. There are, however, some striking examples where large degree representations have been computed and used effectively. One instance of this is a construction of the simple group J_1 by Z. Janko in 1965 (the existence problem for simple groups was discussed at the end of Section 6.2). Janko was investigating certain properties of simple groups and he found that if any simple group possessed these properties, then it would necessarily have order 175,560 and would be generated by two elements. Furthermore, he proved that a hypothetical simple group with these properties must have a 7-dimensional representation over the field $\mathbb{F}_{11}$ with two generators mapping to the two matrices

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} -3 & 2 & -1 & -1 & -3 & -1 & -3 \\ -2 & 1 & 1 & 3 & 1 & 3 & 3 \\ -1 & -1 & -3 & -1 & -3 & -3 & 2 \\ -1 & -3 & -1 & -3 & -3 & 2 & -1 \\ -3 & -1 & -3 & -3 & 2 & -1 & -1 \\ 1 & 3 & 3 & -2 & 1 & 1 & 3 \\ 3 & 3 & -2 & 1 & 1 & 3 & 1 \end{pmatrix}$$

(note that for any simple group S, every representation of S into $GL_n(F)$ which does not map all group elements to the identity matrix is a faithful representation, so S is isomorphic to its image in $GL_n(F)$). In particular, Janko's calculations showed that the simple group satisfying his properties was unique, if it existed. M. Ward was able to show that these two matrices do generate a subgroup of $GL_7(\mathbb{F}_{11})$ of order 175,560 and it follows that there does exist a simple group satisfying Janko's properties.

In a similar vein, S. Norton, R. Parker and J. Thackray constructed the simple group J_4 of order 86,775,571,046,077,562,880 using a 112-dimensional representation over $\mathbb{F}_2$. This group was shown to be generated by two elements, and explicit matrices in $GL_{112}(\mathbb{F}_2)$ for these two generators were computed in the course of their analysis.

In 1981, R. Griess constructed the largest of the sporadic groups, the so called *Monster*, of order

$$2^{46} \cdot 3^{20} \cdot 5^{9} \cdot 7^{6} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

His proof involves calculations of automorphisms of an algebra over $\mathbb{C}$ of dimension 196,884 and leads to a construction of the Monster by means of a representation of this degree.

By analogy, in general it is difficult to write out the explicit permutations associated to a permutation representation $\varphi : G \to S_n$ for large degrees n. There are, however, numerical invariants such as the signs and the cycle types of the permutations $\pi(g)$ and these numerical invariants might be easier to compute than the permutations themselves (i.e., it may be possible to determine the cycle types of elements without actually having to write out the permutations themselves, as in the computation of Galois groups over $\mathbb{Q}$ in Section 14.8). These invariants alone may provide enough information in a given situation to carry out some analysis, such as prove that a given group is not simple (as illustrated in Section 6.2). Furthermore, the invariants just mentioned do not depend on the labelling of the set $\{1, 2, \ldots, n\}$ (i.e., they are independent of a "change of basis" in S_n) and they are the same for elements that are conjugate in G.

In this section we show how to attach numerical invariants to linear representations. These invariants depend only on the equivalence class (isomorphism type) of the representation. In other words, for each representation $\varphi : G \to GL_n(F)$ we shall attach an element of F to each matrix $\varphi(g)$ and we shall see that this number can, in many instances, be computed without knowing the matrix $\varphi(g)$. Moreover, we shall see that these invariants are independent of the similarity class of φ (i.e., are the same for a fixed $g \in G$ if the representation φ is replaced by an equivalent representation) and that they, in some sense, characterize the similarity classes of representations of G.

Throughout this section G is a finite group and, for the moment, F is an arbitrary field. All representations considered are assumed to be finite dimensional.

Definition.

(1) A *class function* is any function from G into F which is constant on the conjugacy classes of G, i.e., $f : G \to F$ such that $f(g^{-1}xg) = f(x)$ for all $g, x \in G$.

(2) If φ is a representation of G afforded by the FG-module V, the *character* of φ is the function

$$\chi : G \to F \qquad \text{defined by} \qquad \chi(g) = \operatorname{tr}\varphi(g),$$

where $\operatorname{tr}\varphi(g)$ is the trace of the matrix of $\varphi(g)$ with respect to some basis of V (i.e., the sum of the diagonal entries of that matrix). The character is called *irreducible* or *reducible* according to whether the representation is irreducible or reducible, respectively. The *degree* of a character is the degree of any representation affording it.

In the notation of the second part of this definition we shall also refer to χ as the character afforded by the FG-module V. In general, a character is *not* a homomorphism from a group into either the additive or multiplicative group of the field.

Examples

(1) The character of the trivial representation is the function $\chi(g) = 1$ for all $g \in G$. This character is called the *principal* character of G.

(2) For degree 1 representations, the character and the representation are usually identified (by identifying a 1×1 matrix with its entry). Thus for abelian groups, irreducible complex representations and their characters are the same (cf. Corollary 11).

(3) Let $\Pi : G \to S_n$ be a permutation representation and let φ be the resulting linear representation on the basis $e_1, \dots, e_n$ of the vector space V:

$$\varphi(g)(e_i) = e_{\Pi(g)(i)}$$

(cf. Example 4 of Section 1). With respect to this basis the matrix of $\varphi(g)$ has a 1 in the diagonal entry i, i if $\Pi(g)$ fixes i; otherwise, the matrix of $\varphi(g)$ has a zero in position i, i. Thus if π is the character of φ then

$$\pi(g) = \text{the number of fixed points of } g \text{ on } \{1, 2, \dots, n\}.$$

In particular, if Π is the permutation representation obtained from left multiplication on the set of left cosets of some subgroup H of G then the resulting character is called the *permutation character* of G on H.