

Introduction to semisimple rings and the representation theory of finite groups

Pedro Resende

Abstract

Support notes for the MMAC course “Groups, Rings and Modules” of IST in the academic year 2022/2023.

Contents

0	Introduction	3
1	Algebras	3
2	Group algebras and representations	4
3	Maschke’s Theorem	6
4	Simple and semisimple modules	8
5	Semisimple rings	10
6	Simple rings	12
7	Idempotents	15
8	Artin–Wedderburn theorem	17
9	More on group algebras	19
10	More on group representations	21
11	Character theory	22
12	Example: character table of D_8	29
13	Example: character table of D_{14}	32

A Properties of the polynomial algebras	34
B Solutions of exercises	36

0 Introduction

These notes are meant to provide an introduction to the representation theory of finite groups via the notion of semisimple ring and the theorem of Artin–Wedderburn. For further reading see [1–3].

All the rings and ring homomorphisms in these notes are assumed to be unital.

- [1] J. A. Beachy, *Introductory lectures on rings and modules*, London Mathematical Society Student Texts, vol. 47, Cambridge University Press, Cambridge, 1999. MR1723048
- [2] D. S. Dummit and R. M. Foote, *Abstract algebra*, 3rd ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004. MR2286236
- [3] S. Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR1878556

1 Algebras

§1. DEFINITION. Let R be a commutative ring. By an R -algebra is meant a ring A together with a ring homomorphism $\iota : R \rightarrow A$, called the *injection of scalars*, whose image is in the center of A .

§2. DEFINITION. Given two R -algebras $A \equiv (A, \iota_A)$ and $B \equiv (B, \iota_B)$, a *homomorphism of R -algebras* $\varphi : A \rightarrow B$ is a (necessarily unital) homomorphism of rings for which the following diagram commutes (i.e., φ preserves the scalars):

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \iota_A \swarrow & & \searrow \iota_B \\ & R & \end{array} \tag{1}$$

This defines the category of R -algebras, which we denote by $R\text{-Alg}$.

§3. EXAMPLES. Let R be a commutative ring.

1. $M_n(R)$ is an R -algebra with injection of scalars $\iota : R \rightarrow M_n(R)$ given by $r \mapsto rI$ where I is the identity matrix.
2. $R[x]$ is an R -algebra with injection of scalars $\iota : R \rightarrow R[x]$ yielding the polynomial r of degree zero for each $r \in R$.

Note that in these two cases the injection of scalars is injective. In fact in the second example we always regard R concretely as a subring of $R[x]$.

See appendix A for a brief account of the universal property of $R[x]$ and a consequence of it which has already been exploited in our study of Jordan canonical forms.

§4. NOTATION. Any R -algebra A with injection of scalars ι has a structure of R -module whose action $\cdot : R \times A \rightarrow A$ is given, for each $r \in R$ and $a \in A$, by $r \cdot a = \iota(r)a$. Usually we shall just write ra if no confusion may arise. In particular, if R is a field then A is a vector space over R , whose multiplication by scalars is given by the action.

§5. EXERCISE. Prove that a homomorphism φ of R -algebras is the same as a ring homomorphism which is equivariant with respect to the action; that is, such that for all $r \in R$ and $a \in A$,

$$\varphi(ra) = r\varphi(a).$$

§6. EXERCISE. Show that for all $r \in R$ and $a, b \in A$ the action satisfies the following additional conditions:

$$\begin{aligned} r(ab) &= (ra)b \\ r(ab) &= a(rb). \end{aligned}$$

§7. EXERCISE. Show that an R -algebra is the same thing as a ring A which is also an R -module such that the two conditions in the previous exercise hold. (Hint: define $\iota(r) = r1_A$.)

§8. EXERCISE. Let R be a commutative ring, and M an R -module. Show that $\text{End}_R(M)$ is an R -algebra. (Hint: define the action of $r \in R$ on $f \in \text{End}_R(M)$ by $(rf)(m) = rf(m)$.)

2 Group algebras and representations

In what follows, given a ring R and a finite set X , we denote the free R -module on X by RX , and will think of it concretely as consisting of the set of all the formal linear combinations

$$RX = \left\{ \sum_{x \in X} r_x x \mid r_x \in R \right\}.$$

§9. PROPOSITION. Let R be a commutative ring and G a finite group with unit 1_G . The free R -module RG is an R -algebra whose unit coincides with 1_G and whose multiplication is defined by bilinear extension of the multiplication of G :

$$\left(\sum_{g \in G} r_g g \right) \left(\sum_{h \in G} s_h h \right) = \sum_{g, h \in G} r_g s_h gh.$$

Proof. Straightforward. ■

§10. EXERCISE. Let R be a commutative ring. Show that the mapping $A \mapsto A^\times$ yields a functor $U : R\text{-Alg} \mapsto \text{Grp}$.

§11. PROPOSITION. Let R be a commutative ring with unit 1_R , G a finite group, and $\eta : G \rightarrow RG$ the mapping given by $g \mapsto 1_R g$. The pair (RG, η) is a universal arrow from G to the functor U .

Proof. We need to show the following:

1. η defines a group homomorphism $G \rightarrow (RG)^\times$;
2. For any R -algebra A and any group homomorphism $\varphi : G \rightarrow A^\times$ there is a unique homomorphism of R -algebras $\varphi^\sharp : RG \rightarrow A$ whose restriction to $(RG)^\times$ makes the diagram on the left commute:

$$\begin{array}{ccc}
 \text{Grp} & & R\text{-Alg} \\
 \\
 G & \xrightarrow{\eta} & (RG)^\times \\
 & \searrow \varphi & \downarrow U(\varphi^\sharp) \\
 & & A^\times
 \end{array}
 \qquad
 \begin{array}{c}
 RG \\
 \vdots \varphi^\sharp \\
 A
 \end{array}$$

The fact that η is a homomorphism of groups is immediate. For the second condition let $G = \{g_1, \dots, g_n\}$. We define φ^\sharp by

$$\varphi^\sharp(r_1 g_1 + \dots + r_n g_n) = r_1 \varphi(g_1) + \dots + r_n \varphi(g_n).$$

The rest of the proof is left as an exercise: show that φ^\sharp is a homomorphism of R -algebras, and that any other homomorphism of R -algebras $\psi : RG \rightarrow A$ such that $U(\psi) \circ \eta = \varphi$ must coincide with φ^\sharp . ■

§12. DEFINITION. Let F be a field, and $n \in \mathbb{N}$. A *matrix representation of degree n over F* of a group G is a homomorphism of groups

$$\rho : G \rightarrow GL_n(F).$$

Similarly, a *matrix representation of degree n* of an F -algebra A is a homomorphism of F -algebras

$$\pi : A \rightarrow M_n(F).$$

Since $M_n(F)^\times = GL_n(F)$, the restriction $U(\pi)$ is a matrix representation over F of degree n of the group A^\times . Moreover, the universal property of §2.11 shows that there is a bijective correspondence between matrix representations ρ over F of degree n of a finite group G and the matrix representations $\rho^\#$ of degree n of the group algebra FG :

$$\begin{array}{ccc} Grp & & F-Alg \\ & & \\ G & & FG \\ \rho \downarrow & & \downarrow \rho^\# \\ GL_n(F) & & M_n(F) \end{array}$$

§13. EXERCISE. Show that an entirely analogous construction of an R -algebra can be obtained from a finite monoid M , again by taking the multiplication of RM to be defined by bilinear extension of the multiplication of M . Show also that $\eta : M \rightarrow RM$, given by $m \mapsto 1_R m$, defines a universal arrow from M to the forgetful functor $R-Alg \rightarrow Mon$ where Mon is the category of monoids (for each R -algebra A the forgetful functor forgets the additive group structure and the injection of scalars of A , thus keeping only its multiplicative monoid structure).

3 Maschke's Theorem

A fundamental theorem for the study of representations of finite groups hinges on the following property of their algebras:

§14. MASCHKE'S THEOREM (18.1.1 OF [2]). *Let G be a finite group and F a field whose characteristic does not divide $|G|$. Then every FG -module is injective (equivalently, every FG -module is projective).*

Proof. This is equivalent to showing that every injective homomorphism $\psi : U \rightarrow V$ of FG -modules splits. Equivalently, we show that any submodule $U \subset V$ has a direct complement, $V = U \oplus W$, which in turn is equivalent to the existence of a homomorphism of FG -modules $\pi : V \rightarrow U$ such that $\pi(u) = u$ for all $u \in U$.

First, since U is an F -linear subspace of V , there is an F -linear subspace $W_0 \subset V$ such that $V = U \oplus W_0$, and we define $\pi_0 : V \rightarrow U$ to be the corresponding projection to U . This is not necessarily the splitting we are looking for because W_0 is not necessarily a G -invariant subspace (i.e., an FG -submodule), so, equivalently, π_0 is not necessarily G -equivariant.

In order to obtain the required splitting let us begin, for each $g \in G$, by defining another map $g\pi_0g^{-1} : V \rightarrow U$: for all $v \in V$ define

$$g\pi_0g^{-1}(v) = g\pi_0(g^{-1}v).$$

Since π_0 is F -linear and both g and g^{-1} act by linear transformations, the map $g\pi_0g^{-1}$ is F -linear. Also, for each $u \in U$ we have, since U is G -invariant,

$$g\pi_0g^{-1}(u) = g\pi_0(g^{-1}u) = gg^{-1}u = u,$$

so $g\pi_0g^{-1}$ is an F -linear retraction.

Now let $n = |G|$, and let us regard n as an element of F by defining $n = 1 + \dots + 1$ (n times). By hypothesis, $n \neq 0$ in F because the characteristic of F does not divide $|G|$. So n has an inverse n^{-1} , which we denote by $\frac{1}{n}$. Then define $\pi : V \rightarrow U$ to be the ‘‘average’’ of all the maps $g\pi_0g^{-1}$ over G :

$$\pi = \frac{1}{n} \sum_{g \in G} g\pi_0g^{-1}.$$

This is a sum of F -linear maps multiplied by a scalar, so it is an F -linear map. It is also a retraction onto U because for all $u \in U$ we have

$$\pi(u) = \frac{1}{n} \sum_{g \in G} g\pi_0g^{-1}(u) = \frac{1}{n} \sum_{g \in G} u = \frac{1}{n}(nu) = u.$$

Finally, let us prove that π is G -equivariant. Let $h \in G$ and $v \in V$.

$$\begin{aligned}
\pi(hv) &= \frac{1}{n} \sum_{g \in G} g\pi_0(g^{-1}hv) \\
&= \frac{1}{n} \sum_{g \in G} hh^{-1}g\pi_0(g^{-1}hv) \\
&= \frac{1}{n} \sum_{g \in G, k=h^{-1}g} hk\pi_0(k^{-1}v) \\
&= \frac{1}{n} \sum_{g \in G} hg\pi_0(g^{-1}v) \\
&= h \frac{1}{n} \sum_{g \in G} g\pi_0(g^{-1}v) = h\pi(v).
\end{aligned}$$

Notice that in the above derivation k ranges over all the elements of G when g does, which justifies why we could replace k by g (h is fixed). ■

§15. COROLLARY. *Let G be a finite group. Every $\mathbb{C}G$ -module is injective (equivalently, every $\mathbb{C}G$ -module is projective).*

4 Simple and semisimple modules

In order to better understand the properties of the F -algebra FG of a finite group G we need some new concepts.

§16. DEFINITION. Let R be a ring and let M be a nonzero R -module.

1. The module M is *irreducible* (or *simple*) if its only submodules are 0 and M .
2. The module M is *decomposable* if it can be written as $M_1 \oplus M_2$ for two nonzero submodules of M ; otherwise it is *indecomposable*.
3. The module M is *completely reducible* (or *semisimple*) if it is a direct sum of irreducible submodules.
4. If M is a completely reducible module, any direct summand of M is called a *constituent* of M .

§17. SCHUR'S LEMMA. (See also §18.) *Let R be a nonzero ring.*

1. *Any nonzero homomorphism $\varphi : M \rightarrow N$ of simple R -modules is an isomorphism.*
2. *If M is a simple R -module, then $\text{End}_R(M)$ is a division ring.*

Proof. If $\varphi : M \rightarrow N$ is nonzero then $\varphi(M)$ is a nonzero submodule of N , hence it must be N itself. Then $\ker \varphi$ cannot be the whole of M , and thus it must be $\{0\}$, so φ is an isomorphism. Therefore any nonzero $\varphi \in \text{End}_R(M)$ is invertible, so $\text{End}_R(M)$ is a division ring. ■

§18. EXERCISE. Let A be an F -algebra for some field F , and let V be a left A -module.

1. Prove that if $T \in \text{End}_A(V)$ and $\lambda \in F$ is any eigenvalue of T (T is an F -linear map) then the eigenspace E_λ of λ is a nonzero left A -submodule.
2. (SCHUR'S LEMMA FOR ALGEBRAS, cf. §17) Prove that if F is algebraically closed (e.g., $F = \mathbb{C}$) and V is a simple module with $\dim_F(V) \in \mathbb{N}$, then $\text{End}_A(V) \cong F$.

§19. DEFINITION. Let R be a ring. A left ideal of R which is simple as a left R -module is said to be *minimal*.

§20. LEMMA. *Let L be a minimal left ideal of a ring R , and let M be a simple left R -module. If L and M are not isomorphic as left R -modules we have $LM = \{0\}$ (i.e., $L \subset \text{Ann}(M)$).*

Proof. Let $m \in M$. Define $\phi : L \rightarrow M$ by for all $a \in L$

$$\phi(a) = am.$$

This is a left module homomorphism and, by Schur's lemma, it is nonzero if and only if it is an isomorphism. Therefore, if L and M are not isomorphic ϕ must be zero, and it follows that $Lm = \phi(L) = \{0\}$ for all $m \in M$, so $LM = \{0\}$. ■

§21. LEMMA. *Let R be a ring, M a semisimple R -module, and $\varphi : M \rightarrow N$ a surjective homomorphism of R -modules. Then N is semisimple and φ is a retraction.*

Proof. Let $M = \bigoplus_{i \in I} M_i$ with each M_i irreducible. Then N is the sum of the images of the submodules $M_i \subset M$:

$$N = \sum_{i \in I} \varphi(M_i).$$

Since M_i is irreducible, the image $\varphi(M_i)$ is either 0 or isomorphic to M_i , hence itself a simple module. This shows that N is the sum of isomorphic copies of some of the constituents of M . Then for each $i, j \in I$ we must either have $\varphi(M_i) = \varphi(M_j)$ or $\varphi(M_i) \cap \varphi(M_j) = \{0\}$ due to irreducibility of the images, so N is a direct sum of isomorphic copies of some of the constituents of M . This shows both that N is semisimple and that it is a direct summand of M , so φ splits. ■

§22. NOTE. In other words, a quotient of a completely reducible module is a projection onto the direct sum of a subset of the set of constituents.

5 Semisimple rings

Maschke's theorem prompts the question of what properties a ring whose modules are all injective (equivalently, all projective) possesses. This section addresses that.

§23. THEOREM. *Let R be a ring. The following conditions are equivalent.*

1. *Every R -module is injective (equivalently, every R -module is projective).*
2. *Every R -module is semisimple.*
3. *R is a direct sum of minimal left ideals.*
4. *R is a direct sum of finitely many minimal left ideals.*

Proof. (1) \Rightarrow (2). Assume that every R -module is injective, and let M be an R -module. Write $\text{Soc}(M)$ (this is called the *socle* of M) for the sum of all the minimal submodules of M (the simple submodules). Evidently, $\text{Soc}(M)$ is a semisimple module because it is a (necessarily direct) sum of simple modules. Since we are assuming that every module is injective, the inclusion of $\text{Soc}(M)$ into M splits, so there is a submodule $N \subset M$ such that $M = \text{Soc}(M) \oplus N$, and all we need to do is prove that $N = 0$. Let us proceed by assuming that there is an element $n \in N \setminus \{0\}$ and obtain a contradiction. Any chain of

submodules $N' \subset N$ such that $n \notin N'$ has a supremum (their union) which also does not contain n , so by Zorn's lemma there is a maximal submodule $L \subset N$ that does not contain n , and thus $L + Rn$ is the least submodule of N that contains both L and n . Hence, by the fourth isomorphism theorem for modules, in the quotient N/L the submodule $R(n+L)$ is simple. But all the modules are projective, so there is a decomposition $N = N_1 \oplus N_2$ such that $N_1 \cong N/L$, and thus $M = \text{Soc}(M) \oplus N_1 \oplus N_2$, which is a contradiction because N_1 has a simple submodule but $\text{Soc}(M)$ is supposed to contain all the simple submodules of M .

(2) \Rightarrow (3). If every R -module is completely reducible then R itself, regarded as an R -module, is completely reducible, in other words it is a direct sum of minimal left ideals.

(3) \Rightarrow (4). Suppose that R , regarded as an R -module, is completely reducible, and let $(J_i)_{i \in I}$ be a family of minimal left ideals of R such that $R = \bigoplus_{i \in I} J_i$. Then there exists a finite subset $F \subset I$ such that $1 \in \bigoplus_{j \in F} J_j$, so for every element $r \in R$ we have

$$r = r1 \in \bigoplus_{j \in F} J_j.$$

(4) \Rightarrow (1). If R is a direct sum of minimal left ideals, any free R -module is completely reducible because it is a direct sum of copies of R . Hence, since any R -module N is a quotient of a free module, it is a direct summand of a free module due to §21. This shows that every R -module is projective. ■

§24. DEFINITION. A ring satisfying the equivalent conditions of §23 will be called *semisimple*.

§25. REMARK (MASCHKE'S THEOREM). Maschke's theorem is the statement that for any finite group G and any field F whose characteristic does not divide $|G|$, the F -algebra FG is a semisimple ring. In particular, $\mathbb{C}G$ is a semisimple ring.

§26. REMARK. Semisimple rings are often called *semisimple Artinian rings*, as in [1], or *semisimple rings with minimum condition*, as in [2], because some authors use a definition of semisimple ring which is weaker than the one given in these notes.

§27. COROLLARY. Let R be a semisimple ring, and M a simple left R -module. Then $M \cong J$ for some minimal left ideal J of R .

Proof. The argument for proving (1) \Rightarrow (2) in §23 is that any left R -module is a direct sum of isomorphic copies of minimal left ideals of R , so if M is a simple module it must be isomorphic to a minimal left ideal. ■

6 Simple rings

§28. DEFINITION. A nonzero ring R is *simple* if it is semisimple and all its minimal left ideals are isomorphic as left R -modules.

§29. COROLLARY. *Any two simple modules over a simple ring R are isomorphic, and they are isomorphic to the minimal left ideals of R .*

Proof. Immediate from §27. ■

§30. EXAMPLE. Let Δ be a division ring, and $R = M_n(\Delta)$. Regard Δ^n as the set of column $n \times 1$ matrices with entries in Δ . Then Δ^n is a left R -module under matrix multiplication, and clearly it is simple. Now note that we have $R = J_1 \oplus \cdots \oplus J_n$ where for each $j = 1, \dots, n$ the left ideal J_j is that of all the matrices whose entries outside the j -column are zero. Then each J_j is isomorphic to Δ^n as a left R -module, so we see that R is a simple ring. Moreover, by §29, every simple R -module is isomorphic to Δ^n . Theorem §36 below will show that every simple ring is of this form up to isomorphism.

§31. THEOREM. *Let R be a simple ring.*

1. *For any minimal left ideals L and M there is $m \in M$ which yields an isomorphism $\varphi : L \rightarrow M$ by $\varphi(b) = bm$ for all $b \in L$. Hence, $Lm = M$.*
2. *$LR = R$.*
3. *R has no two-sided ideals except $\{0\}$ and R .*

Proof. Let L and M be minimal left ideals, and consider the retraction of left R -modules $\pi : R \rightarrow L$ (recall that L is a direct summand of R , so π is the projection). Let $\varphi : L \rightarrow M$ be an isomorphism, and let $m = \varphi(\pi(1))$. Then for all $b \in L$ we have

$$\varphi(b) = \varphi(\pi(b)) = \varphi(\pi(b1)) = b\varphi(\pi(1)) = bm.$$

Since $\varphi \circ \pi : R \rightarrow M$ is surjective, we obtain $Lm = M$. This proves (1), and (2) is an immediate consequence.

Finally, let $I \subset R$ be a two-sided ideal. This is a sum of minimal left ideals, so if $I \neq \{0\}$ we must have $IR = R$ due to (2). This proves (3). ■

§32. NOTATION. If R is a ring, we denote by R^{op} the ring which coincides with R as an abelian group and whose multiplication is that of R with the order reversed; that is, denoting by $x; y$ the product of x and y in R^{op} , we have $x; y = yx$.

§33. LEMMA. *Let R be a ring. Then $R^{\text{op}} \cong \text{End}_R(R)$.*

Proof. Recall the isomorphism of abelian groups $f : R \rightarrow \text{End}_R(R)$ which to each $a \in R$ assigns the unique left R -module homomorphism $f_a : R \rightarrow R$ such that $f_a(1) = a$; that is, $f_a(x) = xa$ for all $x \in R$. Then, writing $a; b$ for the product ba , we obtain

$$f_{a;b}(x) = f_{ba}(x) = xba = (xb)a = f_a(f_b(x)),$$

so we see that $f_{a;b} = f_a \circ f_b$. Therefore, f defines an (evidently unital) isomorphism of rings $f : R^{\text{op}} \rightarrow \text{End}_R(R)$. ■

§34. REMARK. Note that $R = R^{\text{op}}$ if and only if R is commutative, but there may exist isomorphisms $R \cong R^{\text{op}}$ for noncommutative rings. For instance, this happens for any *involutive* ring, by which is meant a ring R equipped with an operation $a \mapsto a^*$ that for all $a, b \in R$ satisfies $(a + b)^* = a^* + b^*$, $a^{**} = a$, and $(ab)^* = b^*a^*$. Then the mapping $a \mapsto a^*$ defines an isomorphism of rings $R \cong R^{\text{op}}$ which moreover is unital because necessarily $1^* = 1$. (Exercise: prove this.) An example of involutive ring is the ring of square matrices $M_n(F)$ for some field F , since the operation of matrix transposition is an involution (check). Hence, $M_n(F)^{\text{op}} \cong M_n(F)$. If $F = \mathbb{C}$, another involution is the operation that to each matrix assigns its adjoint.

§35. LEMMA. *Let Δ be a division ring, and $n \in \mathbb{N}$. Then*

$$M_n(\Delta^{\text{op}}) \cong M_n(\Delta)^{\text{op}}.$$

Proof. The idea is to apply matrix transposition as in §34, but taking into account that the matrices do not necessarily have entries in a commutative ring. Let $A, B \in M_n(\Delta^{\text{op}})$. Writing $(-)^t$ for matrix transposition, we have for all $i, j = 1, \dots, n$

$$\begin{aligned} ((AB)^t)_{ij} &= (AB)_{ji} = \sum_{k=1}^n a_{jk} b_{ki} = \sum_{k=1}^n b_{ki} a_{jk} = \sum_{k=1}^n (B^t)_{ik} (A^t)_{kj} \\ &= (B^t A^t)_{ij} = (A^t; B^t)_{ij}, \end{aligned}$$

so we see that matrix transposition defines a homomorphism of rings

$$(-)^t : M_n(\Delta^{\text{op}}) \rightarrow M_n(\Delta)^{\text{op}}.$$

This is evidently unital, and it is an isomorphism whose inverse is again given by matrix transposition. ■

§36. THEOREM. *Let R be a ring. The following conditions are equivalent:*

1. R is a simple ring.
2. There is a division ring Δ such that $R \cong M_n(\Delta)$ as rings.

Proof. The implication (2) \Rightarrow (1) is simple and has been described in §30, so let us prove the implication (1) \Rightarrow (2). Assume that R is simple, let $R = J_1 \oplus \dots \oplus J_n$ be the decomposition into minimal left ideals, and write J for J_1 . Recall that $\text{End}_R(J)$ is a division ring, by Schur's lemma. The (external) direct sum

$$M := \underbrace{J \oplus \dots \oplus J}_{n \text{ times}}$$

is a left R -module isomorphic to R , so $\text{End}_R(R) \cong \text{End}_R(M)$. Let us prove that there is an isomorphism of rings

$$\text{End}_R(M) \cong M_n(\text{End}_R(J)).$$

Each $\varphi \in \text{End}_R(M)$ is a homomorphism

$$\varphi : J \oplus \dots \oplus J \rightarrow J \oplus \dots \oplus J.$$

Due to the universal properties of the direct sum both as product and coproduct, φ is determined uniquely by a family $\varphi_{ij} \in \text{End}_R(J)$ where $i, j = 1, \dots, n$. Concretely, φ_{ij} is the homomorphism from the j^{th} copy of J in the domain of φ to the i^{th} copy in the codomain. If $\psi \in \text{End}_R(M)$

and we name components $\psi_{ij} \in \text{End}_R(J)$ similarly, the composition $\psi \circ \varphi$ is the homomorphism whose component $(\psi \circ \varphi)_{ij}$ for each $i, j = 1, \dots, n$ is given by

$$(\psi \circ \varphi)_{ij} = \sum_{k=1}^n \psi_{ik} \circ \varphi_{kj}.$$

In other words, there is a homomorphism of rings that sends each $\varphi \in \text{End}_R(M)$ to the matrix $(\varphi_{ij}) \in M_n(\text{End}_R(J))$, which is unital because the identity homomorphism in $\text{End}_R(M)$ is mapped to the $n \times n$ identity matrix with entries in $\text{End}_R(J)$. So we have concluded that

$$\text{End}_R(R) \cong M_n(\text{End}_R(J)).$$

Hence, defining $\Delta = \text{End}_R(J)^{\text{op}}$, from §33 and §35 we obtain

$$R \cong \text{End}_R(R)^{\text{op}} \cong M_n(\text{End}_R(J))^{\text{op}} \cong M_n(\Delta). \quad \blacksquare$$

§37. THEOREM. *Let F be an algebraically closed field, and let A be an F -algebra. The following conditions are equivalent:*

1. A is a simple ring.
2. $A \cong M_n(F)$ as F -algebras.

Proof. Straightforward adaptation of the proof of §36 by taking into account the isomorphism of rings $\text{End}_A(J) \cong F$ for any simple A -module J (cf. Schur's lemma for algebras in §18). \blacksquare

7 Idempotents

§38. DEFINITION. The *center* of a ring R , denoted by $Z(R)$, is the set of elements $r \in R$ such that $rs = sr$ for all $s \in R$.

§39. EXERCISE. Show that $Z(R)$ is a commutative subring of R .

§40. DEFINITION. Let R be a ring.

1. An element e in R is called an *idempotent* if $e^2 = e$.
2. Idempotents e and f are *orthogonal* if $ef = fe = 0$; in particular, orthogonal idempotents commute.

3. A set E of idempotents is *orthogonal* if e and f are orthogonal for all $e \neq f$ in E .
4. A *partition* of an idempotent f is a finite orthogonal set of nonzero idempotents $\{e_1, \dots, e_n\}$ such that $e_1 + \dots + e_n = f$.
5. An idempotent e is *primitive* if it cannot be written as a sum of two nonzero orthogonal idempotents.
6. The idempotent e is a *primitive central idempotent* of R if it is a primitive idempotent of the subring $Z(R)$ (it cannot be written as a sum of nonzero orthogonal idempotents $e, f \in Z(R)$).

§41. EXAMPLE. Let X be a set and R the commutative ring of real valued functions on X . A function $f \in R$ is an idempotent if and only if $f(x)^2 = f(x)$ for all $x \in X$, which means either $f(x) = 0$ or $f(x) = 1$; that is, f is the characteristic function χ_Y of a subset $Y \subset X$. The product of two such functions corresponds to the intersection of subsets, $\chi_Y \chi_Z = \chi_{Y \cap Z}$, and orthogonal projections correspond to disjoint subsets. The ring identity is the function with constant value 1, and a partition of the identity corresponds precisely to a partition of X by nonempty subsets. The primitive idempotents are the characteristic functions of singleton subsets, so they correspond bijectively with the points of X .

§42. EXERCISE. Let R be a ring such that $R = A \oplus B$ (internal direct sum) for two additive subgroups $A, B \subset R$ such that $a^2 \in A$ for all $a \in A$ and $b^2 \in B$ for all $b \in B$ (for instance, A and B could be subrings). Show that the components of 1 in A and B are orthogonal idempotents.

§43. EXERCISE. Let $e \in R$ be an idempotent such that the cyclic left module Re equals a direct sum of left submodules $J \oplus K$. Show that the components of e in J and K are orthogonal idempotents.

§44. EXERCISE. Let R be a ring, and let $\{e_1, \dots, e_n\}$ be a partition of 1. Prove that R is a direct sum of left ideals

$$R = J_1 \oplus \dots \oplus J_n$$

where $J_i = Re_i$ for each $i = 1, \dots, n$.

§45. EXERCISE. Prove the converse of the previous exercise: any decomposition of R as a direct sum of left ideals $J_1 \oplus \cdots \oplus J_n$ arises as in the previous exercise from a partition of 1.

§46. EXERCISE. Let Δ be a division ring, let $n \in \mathbb{N}$, let $R = M_n(\Delta)$, and let I be the identity matrix (the 1 of R). Prove the following assertions:

1. $Z(R) = \{\alpha I \mid \alpha \in Z(\Delta)\}$, and $Z(R)$ is a field isomorphic to $Z(\Delta)$ (so if Δ is a field we have $Z(R) \cong \Delta$).
2. The only central idempotent in R is I (in particular, I is a primitive central idempotent).

8 Artin–Wedderburn theorem

Let R be a semisimple ring. For each isomorphism class $i = \{M_1, \dots, M_s\}$ (as left R -modules) of minimal left ideals of R , we can form its sum $R_i = M_1 + \cdots + M_s = M_1 \oplus \cdots \oplus M_s$, and thus obtain a decomposition of R by left ideals

$$R = R_1 \oplus \cdots \oplus R_r$$

where r is the number of isomorphism classes of minimal left ideals of R and any two minimal left ideals of R are isomorphic as left modules if and only if they are contained in the same component R_i .

§47. DEFINITION. Using the above notation, each component R_i of a semisimple ring R will be called a *Wedderburn component* of R , and the direct decomposition $R = R_1 \oplus \cdots \oplus R_r$ is the *Wedderburn decomposition* of R .

§48. REMARK. A simple ring is the same as a semisimple ring which has exactly one Wedderburn component.

§49. THEOREM. *Let R be a semisimple ring, and let $R = R_1 \oplus \cdots \oplus R_r$ be its Wedderburn decomposition. Then*

1. R_i is a two-sided ideal of R for all $i = 1, \dots, r$,
2. There is a unique partition of 1 by central idempotents z_1, \dots, z_r in R such that each $R_i = z_i R$ for all $i = 1, \dots, r$,
3. R_i is a simple ring with unit z_i , for all $i = 1, \dots, r$,
4. R is isomorphic to the direct product of simple rings $R_1 \times \cdots \times R_r$.

Proof. Let us prove (1). Each R_i is a left ideal, so let us prove that it is also a right ideal. Let $a \in R$ and $m \in R_i$. Let $a = a_1 + \cdots + a_r$ be the decomposition of a over the Wedderburn components of R ; that is, $a_j \in R_j$ for each $j = 1, \dots, r$. Then

$$ma = ma_1 + \cdots + ma_r,$$

and thus $ma_j \in R_j$ for all $j = 1, \dots, r$. Let $j \neq i$, and consider the direct decompositions of R_i and R_j into minimal left submodules:

$$\begin{aligned} R_i &= J_1 \oplus \cdots \oplus J_s, \\ R_j &= K_1 \oplus \cdots \oplus K_t. \end{aligned}$$

Then $m = m_1 + \cdots + m_s$ for unique components $m_k \in J_k$, and $a_j = b_1 + \cdots + b_t$ for unique components $b_l \in K_l$, so

$$ma_j = \sum_{k=1}^s \sum_{l=1}^t m_k b_l,$$

and $m_k b_l \in K_l$ for each k and l . But $j \neq i$ implies that J_k and K_l are not isomorphic, and thus by §20 we must have $m_k b_l = 0$. Hence, for all $j \neq i$ we have $ma_j = 0$, and thus $ma \in R_i$, showing that R_i is a two-sided ideal.

Let us prove (2). Recall from §44 and §45 that there is a unique partition $1 = z_1 + \cdots + z_r$ such that $R_i = Rz_i$ for each $i = 1, \dots, r$. But the R_i 's are also right ideals, and by the same reasoning of §44 and §45 the partition of 1 over the direct decomposition is also such that $R_i = z_i R$ for all $i = 1, \dots, r$, and thus $z_i a = a$ for all $a \in R_i$. Since for $j \neq i$ and $a \in R_j$ we must have $az_i = z_i a = 0$, it follows that each z_i is a central idempotent.

Let us prove (3). Being an ideal, each R_i is also a subring. The condition $R_i = Rz_i$ shows that for all $a \in R_i$ we have $az_i = a$ because there must be $b \in R_i$ such that $a = bz_i$, and thus $az_i = bz_i^2 = bz_i = a$. Similarly, the condition $R_i = z_i R$ shows that for all $a \in R_i$ we have $z_i a = a$, so R_i is a ring with unit z_i . Since, by construction, all the minimal left submodules of R_i are isomorphic, we conclude that R_i is a simple ring.

Finally, let us prove (4). Let $a, b \in R$, and write

$$a = a_1 + \cdots + a_r \quad \text{and} \quad b = b_1 + \cdots + b_r$$

for the unique decompositions into Wedderburn components. Since, as we have seen, $a_i b_j = 0$ for all $i \neq j$, it follows that

$$ab = a_1 b_1 + \cdots + a_r b_r.$$

Therefore R is isomorphic to the direct product of rings $R_1 \times \cdots \times R_r$. ■

§50. COROLLARY (ARTIN–WEDDERBURN THEOREM). *Let R be a ring. The following conditions are equivalent:*

1. R is semisimple.
2. $R \cong M_{n_1}(\Delta_1) \times \cdots \times M_{n_r}(\Delta_r)$ for some choice of integers $n_i \in \mathbb{N}$ and division rings Δ_i , $i = 1, \dots, r$.

Moreover, the numbers n_i are unique, and the division rings Δ_i are unique up to isomorphism (up to permutations of factors in the Wedderburn decomposition of R).

§51. COROLLARY (ARTIN–WEDDERBURN THEOREM FOR ALGEBRAS). *Let F be an algebraically closed field, and A be an F -algebra. The following conditions are equivalent:*

1. A is a semisimple ring.
2. $A \cong M_{n_1}(F) \times \cdots \times M_{n_r}(F)$ for a unique choice of integers $n_i \in \mathbb{N}$.

§52. EXERCISE. Give an example of a finite dimensional \mathbb{C} -algebra which is not semisimple.

9 More on group algebras

From the Artin–Wedderburn theorem for algebras (§51) and Maschke’s theorem (§14, §25) we immediately obtain:

§53. COROLLARY. *Let G be a finite group, and F an algebraically closed field. Then*

$$FG \cong M_{n_1}(F) \times \cdots \times M_{n_r}(F)$$

for a unique choice of $r, n_1, \dots, n_r \in \mathbb{N}$.

From here on we shall assume, without loss of generality, that the underlying algebraically closed field F is \mathbb{C} . Let G be a finite group whose complex group algebra is

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

Then $\mathbb{C}G$ is a complex vector space of dimension $n_1^2 + \cdots + n_r^2$ and $Z(\mathbb{C}G)$ has dimension r . The latter is easy to see because the center of each Wedderburn component $M_{n_i}(\mathbb{C})$ is isomorphic to \mathbb{C} , and thus the center of $\mathbb{C}G$ is

isomorphic to \mathbb{C}^r . In terms of block diagonal matrices, $\mathbb{C}G$ is isomorphic to the ring of complex block diagonal matrices

$$\begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ & & \ddots & \\ 0 & 0 & \cdots & A_r \end{pmatrix}$$

where for each $k = 1, \dots, r$ the matrix A_k is of dimension $n_k \times n_k$, and $Z(\mathbb{C}G)$ is isomorphic to the subring of $\mathbb{C}G$ such that, for each $k = 1, \dots, r$, the matrix A_k is a scalar matrix $\lambda_k I_k$ with $\lambda_k \in \mathbb{C}$, where I_k is the $n_k \times n_k$ identity matrix.

§54. THEOREM. *Let G be a finite group whose complex group algebra is*

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

Then r (the number of Wedderburn components of $\mathbb{C}G$) equals the number of conjugacy classes of G .

Proof. Let $\mathcal{K}_1, \dots, \mathcal{K}_s$ be the distinct conjugacy classes of G . For each i let

$$X_i = \sum_{g \in \mathcal{K}_i} g \in \mathbb{C}G.$$

Note that the set $\{X_1, \dots, X_s\}$ is linearly independent. Moreover, the condition $h^{-1}\mathcal{K}_i h = \mathcal{K}_i$ implies that $h^{-1}X_i h = X_i$ for all $i = 1, \dots, s$, so $X_i \in Z(\mathbb{C}G)$. In order to conclude that $r = s$ we only need to prove that the X_i 's span $Z(\mathbb{C}G)$. Let then $X = \sum_{g \in G} \alpha_g g$ be an arbitrary element of $Z(\mathbb{C}G)$, for coefficients $\alpha_g \in \mathbb{C}$. Centrality implies that $h^{-1}Xh = X$ for all $h \in G$, so

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

But as g ranges over G so does $h^{-1}gh$, and the coefficient of g in the left hand side summation is $\alpha_{hgh^{-1}}$, so we conclude that $\alpha_{hgh^{-1}} = \alpha_g$ for all $h \in G$. This means that the function $\alpha : G \rightarrow \mathbb{C}$ is a class function (i.e., constant in each conjugacy class — cf. §59), so X is a linear combination of the X_i 's. ■

§55. COROLLARY. *Let A be a finite abelian group. Then $\mathbb{C}A \cong \mathbb{C}^{|A|}$.*

Proof. This is immediate because any matrix ring $M_n(\mathbb{C})$ is noncommutative if and only if $n > 1$, and the number of conjugacy classes is $|A|$, so

$$\mathbb{C}A \cong \overbrace{\mathbb{C} \times \cdots \times \mathbb{C}}^{|A| \text{ times}}. \blacksquare$$

10 More on group representations

Since any representation of a finite group G is completely reducible, it follows that any finite dimensional left $\mathbb{C}G$ -module V is a finite direct sum of simple submodules $V = V_1 \oplus \cdots \oplus V_s$, so choosing an appropriate basis of V we obtain a representation

$$\pi : G \rightarrow GL_n(\mathbb{C})$$

where for each $g \in G$ the matrix $\pi(g)$ is a block diagonal matrix

$$\begin{pmatrix} \pi_1(g) & 0 & \cdots & 0 \\ 0 & \pi_2(g) & \cdots & 0 \\ & & \ddots & \\ 0 & 0 & \cdots & \pi_s(g) \end{pmatrix}$$

with each $\pi_i(g)$ being a square matrix of dimension $m_i \times m_i$ where m_i is the dimension of V_i . So the degree of the representation is the sum $n = m_1 + \cdots + m_s$.

In such a basis, then, π factors through a product of linear groups, so we can regard it as a map

$$\pi : G \rightarrow GL_{m_1}(\mathbb{C}) \times \cdots \times GL_{m_s}(\mathbb{C}).$$

Then each projection $\pi_i : GL_{m_1}(\mathbb{C}) \times \cdots \times GL_{m_s}(\mathbb{C}) \rightarrow GL_{m_i}(\mathbb{C})$ gives us the irreducible representation

$$\pi_i \circ \pi : G \rightarrow GL_{m_i}(\mathbb{C}),$$

which is a matrix representation corresponding to the simple FG -module V_i .

Moreover, the irreducible representations of G correspond, up to isomorphism, precisely to the projections of $\mathbb{C}G$ onto its Wedderburn components:

§56. COROLLARY. *Let G be a finite group whose complex group algebra is*

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

Then G has precisely r distinct isomorphism classes of irreducible representations, each corresponding to one of the r projections

$$\pi_i : \mathbb{C}G \rightarrow M_{n_i}(\mathbb{C}).$$

So any simple direct component (= minimal submodule) of an FG -module V must have complex dimension n_i for some $i = 1, \dots, r$.

It can also be shown that the degree of each irreducible representation (i.e., each n_i) is a divisor of $|G|$ (cf. Theorem 18.2.12 of [2], which is proved only in section 19).

§57. COROLLARY. *Let A be an abelian group. The irreducible representations of A are all of degree 1, they are group homomorphisms $\pi : A \rightarrow \mathbb{C}^\times$ and there are exactly $|A|$ many of them corresponding to the projections $\mathbb{C}A \cong \mathbb{C}^{|A|} \rightarrow \mathbb{C}$.*

§58. COROLLARY. *Let G be a finite group. The irreducible representations of G with degree 1 (i.e., the homomorphisms $\pi : G \rightarrow \mathbb{C}^\times$) correspond bijectively to the irreducible representations of the abelianization of G ,*

$$\pi : G/[G, G] \rightarrow \mathbb{C}^\times,$$

so there are exactly $|G/[G, G]|$ isomorphism classes of irreducible representations of G with degree 1.

Proof. This follows immediately from the universal property of the abelianization, which establishes a bijection between homomorphisms $G \rightarrow A$ to abelian groups A and homomorphisms $G/[G, G] \rightarrow A$. ■

11 Character theory

The following is a streamlined version of the material of sections 18.3 and 19.1 of [2]. Contrary to the approach in [2], here for simplicity the underlying field will always be \mathbb{C} .

In the remainder of this note all the representations will be assumed to be of finite degree, and G always denotes a finite group.

§59. DEFINITION. By a (complex valued) *class function* on G is meant a function $f : G \rightarrow \mathbb{C}$ that is constant on each conjugacy class: $f(g^{-1}xg) = f(x)$ for all $x, g \in G$ (cf. §54).

§60. PROPOSITION.

1. The set \mathcal{C} of all the class functions is a linear subspace of the space \mathbb{C}^G of all the complex valued functions on G .
2. A basis of \mathcal{C} is formed by the characteristic functions of the conjugacy classes; that is, a basic class function equals 1 on a given class and 0 on all the others.
3. Hence, \mathcal{C} has dimension r , where r is the number of conjugacy classes.

Proof. Clear. ■

§61. REMARK. Since G is a basis of $\mathbb{C}G$, each class function f is the restriction to G of the unique linear map $f : \mathbb{C}G \rightarrow \mathbb{C}$ such that

$$f\left(\sum_{g \in G} \alpha_g g\right) = \sum_{g \in G} \alpha_g f(g).$$

Hence, class functions will also be regarded as linear maps on $\mathbb{C}G$, so the linear space \mathcal{C} of class functions can be identified with a linear subspace of the dual space $(\mathbb{C}G)^*$.

§62. DEFINITION.

1. If $\varphi : G \rightarrow GL(V)$ is a representation, the *character* of φ is the function

$$\chi : G \rightarrow \mathbb{C}$$

defined by $\chi(g) = \text{tr } \varphi(g)$ for each $g \in G$.

2. The character χ is *reducible* or *irreducible* according to whether φ is a reducible or irreducible representation, respectively, and the *degree* of χ is the degree of φ (i.e., the dimension of V).

§63. NOTE. $\text{tr}(T)$ (or just $\text{tr } T$) is the trace of a complex linear transformation $T : V \rightarrow V$; that is, $\text{tr}(T)$ is the sum of the complex eigenvalues of T (repeated in the sum according to their multiplicities) or, equivalently, the sum of the diagonal entries of any matrix representation of T .

§64. EXAMPLE. Consider the canonical permutation representation of S_n on the set $X = \{1, \dots, n\}$. Each permutation $\sigma : X \rightarrow X$ extends uniquely to a linear isomorphism $\sigma^\# : \mathbb{C}^n \rightarrow \mathbb{C}^n$ which in the canonical basis is represented by a permutation matrix (i.e., a matrix whose entries are either 0 or 1 and which has exactly one 1 in each row and in each column). This defines a representation $\pi : S_n \rightarrow M_n(\mathbb{C})$. Letting χ be the associated character, for each $\sigma \in S_n$ the value $\chi(\sigma)$ is the number of fixed points of σ .

§65. EXAMPLE. A representation $\pi : D_{2n} \rightarrow M_2(\mathbb{C})$ is obtained by specifying

$$\begin{aligned}\pi(r) &= \begin{pmatrix} \cos 2\pi/n & -\sin 2\pi/n \\ \sin 2\pi/n & \cos 2\pi/n \end{pmatrix} \\ \pi(s) &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\end{aligned}$$

The corresponding character satisfies

$$\begin{aligned}\chi(r) &= 2 \cos 2\pi/n \\ \chi(s) &= 0\end{aligned}$$

§66. MORE EXAMPLES OF CHARACTERS. See section 18.3 of [2].

§67. LEMMA.

1. Any two equivalent representations of G have the same character.
2. The character of any representation of G is a class function.
3. For any character χ , the value $\chi(1)$ is the degree of χ .

Proof. 1. By definition, $\varphi, \psi : G \rightarrow GL_n(\mathbb{C})$ are equivalent matrix representations if and only if for each $g \in G$ the matrices $\varphi(g)$ and $\psi(g)$ are similar, so they have the same trace.

2. If $x, g \in G$ and $\varphi : G \rightarrow GL_n(\mathbb{C})$ is a representation,

$$\operatorname{tr} \varphi(g^{-1}xg) = \operatorname{tr}(\varphi(g)^{-1}\varphi(x)\varphi(g)) = \operatorname{tr} \varphi(x).$$

3. $\chi(1)$ is the trace of an identity matrix, so it equals the degree of χ . ■

§68. PROPOSITION. Let V_1 and V_2 two finite dimensional $\mathbb{C}G$ -modules with characters χ_1 and χ_2 , respectively. Then the character of $V_1 \oplus V_2$ is $\chi_1 + \chi_2$.

Proof. For some choice of bases of V_1 and V_2 let

$$\varphi_1 : G \rightarrow M_{n_1}(\mathbb{C}) \quad \text{and} \quad \varphi_2 : G \rightarrow M_{n_2}(\mathbb{C})$$

be the corresponding matrix representations. Then the matrix representation $\varphi : G \rightarrow M_{n_1+n_2}(\mathbb{C})$ afforded by the module $V_1 \oplus V_2$, with respect to the union of the two bases, is by block diagonal matrices

$$\begin{pmatrix} \varphi_1(g) & 0 \\ 0 & \varphi_2(g) \end{pmatrix}$$

and thus the character of φ is given by

$$\chi(g) = \text{tr } \varphi(g) = \text{tr } \varphi_1(g) + \text{tr } \varphi_2(g) = \chi_1(g) + \chi_2(g). \quad \blacksquare$$

§69. COROLLARY. *The character of a representation is the sum of the (irreducible) characters of the constituents appearing in a direct sum decomposition.*

§70. NOTATION. Suppose

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

and let M_1, \dots, M_r be the simple $\mathbb{C}G$ -modules that correspond, respectively, to the irreducible representations $\pi_i : \mathbb{C}G \rightarrow M_{n_i}(\mathbb{C})$ for each $i = 1, \dots, r$. Any finite dimensional $\mathbb{C}G$ -module V is a direct sum of copies of the M_i 's, and each M_i appears in the decomposition with a certain multiplicity $a_i \in \mathbb{N}$; that is,

$$V \cong \overbrace{M_1 \oplus \cdots \oplus M_1}^{a_1 \text{ times}} \oplus \cdots \oplus \overbrace{M_r \oplus \cdots \oplus M_r}^{a_r \text{ times}}.$$

Henceforth let us abbreviate this by

$$a_1 M_1 \oplus \cdots \oplus a_r M_r.$$

Hence, letting χ_i be the irreducible character corresponding to each M_i , and χ the character corresponding to V , we obtain

$$\chi = a_1 \chi_1 + \cdots + a_r \chi_r,$$

and any such sum of irreducible characters is the character of some representation.

§71. THEOREM. *Two representations are equivalent if and only if they have the same character.*

Proof. We have already seen that equivalent representations have the same character, so only the converse needs proving. Suppose that

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

For simplicity of terminology let us regard the above isomorphism as being an inequality. Let M_1, \dots, M_r be the simple $\mathbb{C}G$ -modules that correspond to the irreducible representations of $\mathbb{C}G$, and let χ_1, \dots, χ_r be the corresponding irreducible characters. Let z_1, z_2, \dots, z_r be the idempotents $(I, 0, \dots, 0)$, $(0, I, \dots, 0)$, \dots , $(0, 0, \dots, I)$. These are r central idempotents of $\mathbb{C}G$ that form a linearly independent set, so they yield a basis of $Z(\mathbb{C}G)$. Let us write z^1, \dots, z^r for the dual basis; that is, each linear map $z^i : Z(\mathbb{C}G) \rightarrow \mathbb{C}$ is uniquely defined for all $j \neq i$ by

$$z^i(z_i) = 1 \quad \text{and} \quad z^i(z_j) = 0.$$

Now note that for any $m \in M_i$ we have $z_i m = m$ and, if $j \neq i$, $z_j m = 0$. Then for each $i \neq j = 1, \dots, r$ we have

$$\chi_i(z_i) = n_i \quad \text{and} \quad \chi_i(z_j) = 0.$$

In other words, for each $i = 1, \dots, r$, the restriction $\chi'_i : Z(\mathbb{C}G) \rightarrow \mathbb{C}$ of the irreducible character $\chi_i : \mathbb{C}G \rightarrow \mathbb{C}$ satisfies

$$\chi'_i = n_i z^i.$$

Hence, the maps χ'_i form a basis of the dual space $(Z(\mathbb{C}G))^*$, so there are at least r distinct irreducible characters. But, since any two equivalent irreducible representations have the same character, and there are exactly r equivalent classes of irreducible representations, there are at most r distinct characters, and thus there are exactly r distinct characters; in other words, for all $i, j = 1, \dots, r$, we have $\chi_i = \chi_j$ if and only if $\chi'_i = \chi'_j$. ■

§72. COROLLARY. *The irreducible characters of G form a basis of the complex vector space \mathcal{C} of complex valued class functions on G .*

Proof. Let $\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C})$. Since \mathcal{C} has dimension r , and there are r linearly independent irreducible characters, which are class functions, the conclusion follows. ■

§73. NOTE. The set of characters consists of all the linear combinations of irreducible characters

$$a_1 \chi_1 + \cdots + a_r \chi_r$$

with coefficients taken from $\mathbb{Z}_{\geq 0}$, whereas the space of all the class functions consists of all the complex linear combinations of irreducible characters.

§74. EUCLIDEAN STRUCTURE. Let $\theta, \psi : G \rightarrow \mathbb{C}$ be class functions. Define

$$\langle \theta, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \theta(g) \overline{\psi(g)}.$$

It is easily seen that this defines a complex inner product (i.e., a positive definitive Hermitian sesquilinear form) on the vector space of class functions: for $\alpha, \beta \in \mathbb{C}$

1. $\langle \alpha\theta_1 + \beta\theta_2, \psi \rangle = \alpha\langle \theta_1, \psi \rangle + \beta\langle \theta_2, \psi \rangle,$
2. $\langle \theta, \psi \rangle = \overline{\langle \psi, \theta \rangle}$
(so also $\langle \theta, \alpha\psi_1 + \beta\psi_2 \rangle = \overline{\alpha}\langle \theta, \psi_1 \rangle + \overline{\beta}\langle \theta, \psi_2 \rangle$),
3. $\langle \theta, \theta \rangle \geq 0,$
4. If $\langle \theta, \theta \rangle = 0$ then $\theta = 0$.

(This is the canonical inner product on $\mathbb{C}^{|G|}$ divided by $|G|$.)

§75. LEMMA. Let M_1, \dots, M_r be the simple modules of $\mathbb{C}G$ (one per isomorphism class), and let z_1, \dots, z_r be the primitive orthogonal central idempotents of $\mathbb{C}G$ such that z_i acts as the identity on M_i , and let χ_i be the irreducible character afforded by M_i . Then

$$z_i = \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g^{-1})g.$$

Moreover, for any character ψ and $g \in G$ we have $\psi(g^{-1}) = \overline{\psi(g)}$, and $\psi(g)$ is a sum of roots of 1 in \mathbb{C} .

Proof. See propositions 13 and 14 of section 18.3 of [2]. ■

§76. ORTHOGONALITY RELATIONS. Using the previous results, after a bit of work one proves the following (see theorems 15 and 16 of section 18.3 of [2]):

§77. THEOREM (FIRST ORTHOGONALITY RELATION FOR GROUP CHARACTERS). The irreducible characters of G form an orthonormal basis (with respect to the inner product defined above).

§78. THEOREM (SECOND ORTHOGONALITY RELATION FOR GROUP CHARACTERS). Letting χ_1, \dots, χ_r be the irreducible group characters of G , for all $x, y \in G$ we have

$$\sum_{i=1}^r \chi_i(x) \overline{\chi_i(y)} = \begin{cases} |C_G(x)| & \text{if } x \text{ and } y \text{ are conjugate in } G \\ 0 & \text{otherwise.} \end{cases}$$

§79. EXERCISE. Show that the product of two characters is itself a character. (Suggestion: if θ and ψ are the characters afforded by $\mathbb{C}G$ -modules V and W , show that $\theta\psi$ is the character afforded by $V \otimes_{\mathbb{C}} W$ — cf. Proposition 17 of section 18.3 of [2].)

§80. CHARACTER TABLES. The information about characters can be conveniently recorded in a *character table*, as in the following example for $Z_2 = \langle x \mid x^2 = 1 \rangle$. The columns are labeled by representatives of the conjugacy classes and the rows are labelled by irreducible characters, so character tables are square matrices. But there is an additional row (“sizes”) which records the size of the conjugacy class of each representative:

classes:	1	x
sizes:	1	1
χ_1	1	1
χ_2	1	-1

§81. EXAMPLE. The character table of $Z_3 = \langle x \mid x^3 = 1 \rangle$ is, given a primitive cubic root ζ of 1 (so $\zeta^2 = \bar{\zeta}$),

classes:	1	x	x^2
sizes:	1	1	1
χ_1	1	1	1
χ_2	1	ζ	ζ^2
χ_3	1	ζ^2	ζ

§82. EXAMPLE. The character table of S_3 is:

classes:	1	(1 2)	(1 2 3)
sizes:	1	3	2
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Notice that the left column of any character table lists the degrees of each character. So, for instance, we see in this example that the three irreducible characters of S_3 have degrees 1, 1, and 2, respectively. Taking into account that $S_3 \cong D_6$, the character χ_3 is easy to understand in terms of the representation of D_{2n} in §65:

$$\begin{aligned}\pi((1\ 2\ 3)) &= \begin{pmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix} \\ \pi((1\ 2)) &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\end{aligned}$$

Let us use the table to confirm that the norm of χ_3 is 1:

$$\begin{aligned}\|\chi_3\|^2 &= \langle \chi_3, \chi_3 \rangle \\ &= \frac{1}{6} \sum_{\sigma \in S_3} |\chi_3(\sigma)|^2 \\ &= \frac{1}{6} (d_1 |\chi_3(1)|^2 + d_2 |\chi_3((1\ 2))|^2 + d_3 |\chi_3((1\ 2\ 3))|^2),\end{aligned}$$

where d_1 , d_2 and d_3 are the sizes of the conjugacy classes of 1, (1 2) and (1 2 3), which are listed in the character table. So

$$\|\chi_3\|^2 = \frac{1}{6} (|\chi_3(1)|^2 + 3|\chi_3((1\ 2))|^2 + 2|\chi_3((1\ 2\ 3))|^2) = \frac{1}{6}(4 + 2 \times 1) = 1.$$

§83. REMARK. Non-isomorphic groups can have the same character table. This is the case for D_8 and Q_8 , for instance. For these and other examples see section 19.1 of [2].

12 Example: character table of D_8

Let us compute the character table for D_8 . First we need to compute the conjugacy classes. Since $Z(D_8) = \{1, r^2\}$, there are exactly two singleton conjugacy classes, namely $\mathcal{O}_1 = \{1\}$ and $\mathcal{O}_{r^2} = \{r^2\}$. Since $\langle r \rangle \leq C_{D_8}(r)$ and r is not central, Lagrange's theorem forces $|C_{D_8}(r)| = 4$, so

$$|\mathcal{O}_r| = |D_8 : C_{D_8}(r)| = 2.$$

Then, noting that

$$sr s^{-1} = sr s = s^2 r^{-1} = r^3,$$

we conclude that $\mathcal{O}_r = \{r, r^3\}$. Now consider s . Its centralizer satisfies

$$\langle s \rangle \leq C_{D_8}(s),$$

so again by Lagrange's theorem the order of the centralizer must be either 2 or 4 (it cannot be 8 because s is not central). Since both 1 and r^2 commute with s , it follows that the order of the centralizer is 4, and thus $|O_s| = 2$. Let us compute a conjugate of s :

$$rsr^{-1} = sr^{-2} = sr^2.$$

Hence, $O_s = \{s, sr^2\}$. There are only two elements of D_8 to account for, sr and sr^3 , which are not central, so the remaining conjugacy class is $O_{sr} = \{sr, sr^3\}$. Hence, we have found five conjugacy classes, with orders 1, 1, 2, 2, and 2. Then there are five equivalence classes of irreducible representations, and thus

$$\mathbb{C}D_8 \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_5}(\mathbb{C})$$

with $\sum_{i=1}^5 n_i^2 = 8$. The only possibility is to have four n_i 's equal to 1 and the other equal to 2, so we conclude that D_8 has, up to equivalence of representations, four irreducible representations of degree 1 and one irreducible representation of degree 2. One representation of degree 1 is the trivial representation $G \rightarrow \mathbb{C}^\times$, whose character χ_1 satisfies $\chi_1(g) = 1$ for all $g \in D_8$ (note that for any finite group there is such a trivial irreducible character of degree one). The irreducible representation of degree 2 is the usual matrix representation ρ by $\pi/2$ rotations and a reflection:

$$\rho(r) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \rho(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

The matrices of the other representatives of conjugacy classes are:

$$\rho(r^2) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad \rho(sr) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

This gives us the following incomplete character table, where χ_5 is the only irreducible character of degree 2, corresponding to the representation π :

classes:	1	r	r^2	s	sr
sizes:	1	2	1	2	2
χ_1	1	1	1	1	1
χ_2	1				
χ_3	1				
χ_4	1				
χ_5	2	0	-2	0	0

Another obvious irreducible representation of degree 1 sends r to 1 and s to -1 , for it is immediate that this respects the relations of D_8 (in fact the

same would be true for any D_{2n}). The corresponding character χ_2 is given in the following table:

classes:	1	r	r^2	s	sr
sizes:	1	2	1	2	2
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1				
χ_4	1				
χ_5	2	0	-2	0	0

(The fact that $\chi_1 \neq \chi_2$ ensures that the two irreducible representations are not equivalent.) Another irreducible representation of degree 1 can be obtained by letting both r and s correspond to a rotation of π in the complex plane; in other words, both r and s are assigned to $-1 \in \mathbb{C}^\times$, corresponding to the irreducible character χ_3 :

classes:	1	r	r^2	s	sr
sizes:	1	2	1	2	2
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	-1	1	-1	1
χ_4	1				
χ_5	2	0	-2	0	0

(At each stage verify that the first orthogonality relations are satisfied, and that the norm of each line is 1 — remember that the sizes of the conjugacy classes must be accounted for.) There is only one irreducible character missing from our table, again of degree 1. Note that the assignments $r \mapsto -1$ and $s \mapsto 1$ also respect the relations of D_8 , so we conclude the character table:

classes:	1	r	r^2	s	sr
sizes:	1	2	1	2	2
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	-1	1	-1	1
χ_4	1	-1	1	1	-1
χ_5	2	0	-2	0	0

§84. EXERCISE. Revisit Exercise §82 seeing S_3 as the dihedral group D_6 , using similar ideas as those which we used for D_8 .

13 Example: character table of D_{14}

Similarly to any dihedral group, there are two irreducible representations of degree 1, namely the trivial one that assigns every group element to 1 (which exists for every finite group), and the irreducible representation $\rho : D_{14} \rightarrow \mathbb{C}^\times$ defined by $\rho(r) = 1$ and $\rho(s) = -1$. In order to move further, let us compute the conjugacy class \mathcal{O}_g for each $g \in D_{14}$. The reasoning is again based on computing centralizers and applying Lagrange's theorem, so now we shall abbreviate a bit.

$|\mathcal{O}_r| = 2$ (this is true for any D_{2n} , $n \geq 3$). A conjugate of r is $sr s = r^6$, so $\mathcal{O}_r = \{r, r^6\}$.

Since $\langle r \rangle$ is cyclic of prime order, the centralizers of all the powers r^2, \dots, r^5 have order 7, so again the orbits of these elements have order 2. Hence, $\mathcal{O}_{r^2} = \{r^2, r^5\}$ because $sr^2s = r^5$, and $\mathcal{O}_{r^3} = \{r^3, r^4\}$ because $sr^3s = r^4$.

Next, we consider the centralizer of s : since in D_{14} the reflection s commutes with no power of r , and also with no element of the form sr^k with $k = 1, \dots, 6$, $C_{D_{14}}(s) = \{1, s\}$, so $|\mathcal{O}_s| = 7$. Hence, \mathcal{O}_s consists of all the seven elements of order 2.

Summarizing, there are 5 conjugacy classes:

- $\mathcal{O}_1 = \{1\}$
- $\mathcal{O}_r = \{r, r^6\}$
- $\mathcal{O}_{r^2} = \{r^2, r^5\}$
- $\mathcal{O}_{r^3} = \{r^3, r^4\}$
- $\mathcal{O}_s = \{s, sr, sr^2, sr^3, sr^4, sr^5, sr^6\}$

Since two of the irreducible characters must have degree 1, the squares of the remaining three irreducible characters must add up to 12, so they are all of degree 2. This leads us to the first incomplete character table:

classes:	1	r	r^2	r^3	s
sizes:	1	2	2	2	7
χ_1	1	1	1	1	1
χ_2	1	1	1	1	-1
χ_3	2				
χ_4	2				
χ_5	2				

The remaining three irreducible representations can be based on rotation and permutation matrices, the “standard” one being

$$\rho_3(r) = \begin{pmatrix} \cos(2\pi/7) & -\sin(2\pi/7) \\ \sin(2\pi/7) & \cos(2\pi/7) \end{pmatrix} \quad \rho_3(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

The two other irreducible representations can be obtained by duplicating and triplicating the rotation “speed”:

$$\rho_4(r) = \begin{pmatrix} \cos(4\pi/7) & -\sin(4\pi/7) \\ \sin(4\pi/7) & \cos(4\pi/7) \end{pmatrix} \quad \rho_4(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$\rho_5(r) = \begin{pmatrix} \cos(6\pi/7) & -\sin(6\pi/7) \\ \sin(6\pi/7) & \cos(6\pi/7) \end{pmatrix} \quad \rho_5(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Note that as the powers of r range from $1 = r^0$ to r^6 and then back to 1 the representation ρ_3 performs one full rotation, whereas ρ_4 and ρ_5 perform two and three full rotations, respectively. So the intuition behind these being nonequivalent representations resembles that of single, double and triple loops being distinct in the fundamental group of the 1-sphere. The quickest way to confirm that the representations are not equivalent is to verify that their characters are different:

classes:	1	r	r^2	r^3	s
sizes:	1	2	2	2	7
χ_1	1	1	1	1	1
χ_2	1	1	1	1	-1
χ_3	2	$2 \cos(2\pi/7)$	$2 \cos(4\pi/7)$	$2 \cos(6\pi/7)$	0
χ_4	2	$2 \cos(4\pi/7)$	$2 \cos(8\pi/7)$	$2 \cos(12\pi/7)$	0
χ_5	2	$2 \cos(6\pi/7)$	$2 \cos(12\pi/7)$	$2 \cos(18\pi/7)$	0

This becomes more visible if we choose all angles to lie in the upper half plane:

classes:	1	r	r^2	r^3	s
sizes:	1	2	2	2	7
χ_1	1	1	1	1	1
χ_2	1	1	1	1	-1
χ_3	2	$2 \cos(2\pi/7)$	$2 \cos(4\pi/7)$	$2 \cos(6\pi/7)$	0
χ_4	2	$2 \cos(4\pi/7)$	$2 \cos(6\pi/7)$	$2 \cos(2\pi/7)$	0
χ_5	2	$2 \cos(6\pi/7)$	$2 \cos(2\pi/7)$	$2 \cos(4\pi/7)$	0

§85. EXERCISE. Verify that ρ_4 and ρ_5 are indeed representations (check that the defining relations are respected), and that they are irreducible.

§86. EXERCISE. Verify that the following defines an irreducible representation of D_{14} :

$$\rho(r) = \begin{pmatrix} \cos(2\pi/7) & \sin(2\pi/7) \\ -\sin(2\pi/7) & \cos(2\pi/7) \end{pmatrix} \quad \rho(s) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

To which of the representations ρ_3 , ρ_4 , or ρ_5 is it equivalent? Describe an explicit isomorphism of modules that proves the equivalence.

§87. EXERCISE. Can you generalize the D_{14} example so as to describe the character table of any dihedral group D_{2p} for a prime p ?

Appendix

A Properties of the polynomial algebras

§88. PROPOSITION. *Let R be a commutative ring. For any R -algebra A and any $a \in A$ there is a unique homomorphism of R -algebras*

$$\psi_a : R[x] \rightarrow A$$

such that $\psi_a(x) = a$.

Proof. Explicitly, for each polynomial with coefficients in R

$$p(x) = r_n x^n + \cdots + r_1 x + r_0$$

we define $\psi_a(p)$ by “evaluating p at a ” in the only sensible way:

$$\psi_a(p) = “p(a)” = r_n a^n + \cdots + r_1 a + r_0 1.$$

The rest of the proof is left as an exercise: verify that ψ_a is a homomorphism of R -algebras and that if $\xi : R[x] \rightarrow A$ is any other homomorphism of R -algebras that sends x to a then necessarily $\xi = \psi_a$. ■

§89. NOTE. This proposition shows that the inclusion mapping $\eta : \{x\} \rightarrow R[x]$ is a universal arrow from the set $\{x\}$ to the forgetful functor $R\text{-Alg} \rightarrow \text{Set}$; that is, for all R -algebras A and all maps $\{x\} \rightarrow A$ (i.e., all elements

$a \in A$) there is a unique homomorphism of R -algebras $\psi_a : R[x] \rightarrow A$ that makes the diagram on the left commute:

$$\begin{array}{ccc}
 \text{Set} & & R\text{-Alg} \\
 \\
 \{x\} & \xrightarrow{\eta} & R[x] \\
 & \searrow_{x \mapsto a} & \downarrow \psi_a \\
 & & A
 \end{array}
 \qquad
 \begin{array}{c}
 R[x] \\
 \vdots \psi_a \\
 A
 \end{array}$$

In other words, $R[x]$ is the *free R -algebra* on a single generator x .

§90. EXAMPLE. Let R be a commutative ring. The previous universal property gives us the well known fact (already seen in the lectures) that an $R[x]$ -module is “the same” as an R -module M together with an element $\varphi \in \text{End}_R(M)$.

In order to see this, first consider an $R[x]$ -module M . This is also an R -module by change of ring along the injection of scalars $\iota : R \rightarrow R[x]$ (in other words, the action of R is the action of $R[x]$ restricted to degree zero polynomials); and, letting $\sigma : R[x] \rightarrow \text{End}(M)$ be the representation by endomorphisms afforded by the action, the image $\sigma(R[x])$ is contained in $\text{End}_{R[x]}(M)$ because $R[x]$ is commutative, so it is also contained in $\text{End}_R(M)$. Hence, define φ to be $\sigma(x)$.

Conversely, let M be an R -module and $\varphi \in \text{End}_R(M)$. Again because R is commutative, the endomorphism representation is by endomorphisms of R -modules:

$$\sigma : R \rightarrow \text{End}_R(M).$$

Note that σ coincides with the injection of scalars of $\text{End}_R(M)$ as an R -algebra, for the definition of ι in terms of the R -action on M is

$$\iota(r) = r1_{\text{End}_R(M)},$$

so for all $m \in M$

$$\iota(r)(m) = (r1_{\text{End}_R(M)})(m) = r(1_{\text{End}_R(M)}(m)) = rm = \sigma(r)(m).$$

Since $\text{End}_R(M)$ is an R -algebra, the universal property above tells us that there is a unique homomorphism of R -algebras

$$\sigma_\varphi : R[x] \rightarrow \text{End}_R(M)$$

such that $\sigma_\varphi(x) = \varphi$, and this makes M an $R[x]$ -module because $\text{End}_R(M) \subset \text{End}(M)$.

It is now clear that there is a bijection between the class of $R[x]$ -modules and the class of pairs (M, φ) where M is an R -module and $\varphi \in \text{End}_R(M)$. Explicitly, given an R -module M and $\varphi \in \text{End}_R(M)$, the action of $R[x]$ is given by, for all $m \in M$,

$$(r_n x^n + \cdots + r_1 x + r_0)m = r_n \varphi^n(m) + \cdots + r_1 \varphi(m) + r_0 m,$$

where $\varphi^i = \varphi \circ \cdots \circ \varphi$ i times.

B Solutions of exercises

§91. SOLUTION OF §18. Writing λx instead of $\lambda \cdot x$ for the action of $\lambda \in F$ on $x \in V$, we have:

1. Let $x \in E_\lambda$ and $a \in A$. Then $T(ax) = aT(x) = a\lambda x = \lambda ax$, so $ax \in E_\lambda$. This shows that E_λ is a left A -submodule of V , and E_λ is nonzero by definition of eigenspace (it must contain an eigenvector, which by definition has to be a nonzero vector).
2. Let $T : V \rightarrow V$ be a homomorphism of left A -modules. In particular, T is an F -linear map, so it has an eigenvalue λ because F is algebraically closed (and $\dim(V)$ is both finite and nonzero). By 1 above, the eigenspace E_λ is a nonzero A -submodule of V , so it coincides with V because V is simple. Hence, $T(x) = \lambda x$ for all $x \in V$. This establishes the envisaged bijective correspondence between F and $\text{End}_A(V)$, which moreover is: clearly a homomorphism of abelian groups; clearly unital; and it preserves multiplication, for if $T_1(x) = \lambda_1 x$ and $T_2(x) = \lambda_2 x$ for all $x \in V$ then $T_1 \circ T_2(x) = \lambda_1(\lambda_2 x) = (\lambda_1 \lambda_2)x$.

§92. SOLUTION OF §42. Let f and g be the elements of A and B , respectively, such that $1 = f + g$. Then

$$g^2 = (1 - f)^2 = 1 - f - f + f^2 = g - f + f^2,$$

so

$$g^2 - g = f^2 - f.$$

But $f^2 - f \in A$ and $g^2 - g \in B$, so $f^2 - f = g^2 - g = 0$. This shows that both f and g are idempotents. Then

$$fg = f(1 - f) = f - f^2 = f - f = 0 \quad \text{and} \quad gf = (1 - f)f = f - f^2 = 0.$$

So $\{f, g\}$ is a partition of 1.