Linear Representations of Finite Groups

Randall R. Holmes
Auburn University

0 Introduction

Let G be a finite group, let K be a field, and let V be a finite-dimensional vector space over K. Denote by $\mathrm{GL}(V)$ the group of invertible linear transformations from V to itself. A group homomorphism $\rho : G \to \mathrm{GL}(V)$ is called a **linear K-representation of G in V** (or just a **representation of** G for short).

One gains information about the structure of G by studying the totality of representations of G (i.e., various ρ, V, and K).

EXAMPLE. Suppose $K = \mathbf{C}$. If every "irreducible" representation of G (that is, one admitting no proper "subrepresentation") is of the form $\rho : G \to \mathrm{GL}(V)$ with $\dim V = 1$, then G is abelian (and conversely).

Here are some notable applications of representation theory:

(1) (Burnside) If $|G| = p^a q^b$ (p, q prime), then G is solvable. (Proof given in Section 25.)
(2) (Feit-Thompson) Every group of odd order is solvable.
(3) Classification of Finite Simple Groups. (Proof uses both the "ordinary" theory ($\mathrm{char}\, K = 0$) and the "modular" theory ($\mathrm{char}\, K = p$, prime).)
(4) Quantum mechanics.

Let $\rho : G \to \mathrm{GL}(V)$ be a representation. Define the associated **character** $\chi : G \to K$ by $\chi(a) = \mathrm{tr}\, \rho(a)$. By passing from ρ to the associated character χ, one loses information in general, but enough information is retained to allow proofs of important results. For instance, the theorem of Burnside stated above uses only characters, not actual representations. Much of the power of character theory comes from its deep connections with number theory.

Let KG denote the group ring of G over K (so KG is the vector space over K with basis G made into a ring by using the obvious multiplication). Given a representation $\rho : G \to \mathrm{GL}(V)$ we can make V into a KG-module by putting $a \cdot v = \rho(a)(v)$ ($a \in G$, $v \in V$) and extending this definition linearly to an arbitrary element of KG. It turns out that the study of representations of G over the field K is equivalent (in the category sense) to the study of KG-modules. This brings into representation theory certain aspects of homological algebra and K-theory.

In summary, representation theory involves three interrelated notions: (1) representations, (2) characters, (3) modules.

1 Modules

Let R be a ring with identity 1. A (**left**) R**-module** is an (additive) abelian group M with a function $R \times M \to M$ denoted $(r, m) \mapsto rm$ (or sometimes $r \cdot m$) such that the following hold for all $r, s \in R$, $m, n \in M$:

(1) $r(m+n) = rm + rn$,
(2) $(r+s)m = rm + sm$,
(3) $(rs)m = r(sm)$,
(4) $1m = m$.

One proves for R-modules the natural identities, like $r0 = 0$ for any $r \in R$. (Proof: $r0 = r(0+0) = r0 + r0$; now cancel.)

EXAMPLE. If V is a vector space over a field K, then V is a K-module.

EXAMPLE. If A is an additive abelian group, then A is a $\mathbf{Z}$-module, where ra ($r \in \mathbf{Z}$, $a \in A$) has the usual meaning.

EXAMPLE. Let V be a vector space over the field K and let R be the ring of linear transformations from V to itself. Then V is an R-module by $f \cdot v = f(v)$.

EXAMPLE. Any ring R (with 1) is an R-module with rs ($r, s \in R$) being the given ring multiplication.

Warning: If V is a vector space over the field K, then $\alpha v = 0$ implies $v = 0$ or $\alpha = 0$ ($\alpha \in K$, $v \in V$) since if $\alpha \neq 0$, then $v = \alpha^{-1}\alpha v = \alpha^{-1}0 = 0$. This property does not hold for modules in general. For instance, let $v = \bar{1} \in \mathbf{Z}_2$ and $\alpha = 2 \in \mathbf{Z}$. Then $2 \cdot \bar{1} = \bar{2} = \bar{0}$, but $\bar{1} \neq 0$ and $2 \neq 0$. Furthermore, an arbitrary module need not have a basis.

Let M be an R-module. A subset N of M is an R**-submodule** (written $N \leq M$) if the following hold:

(1) N is a subgroup of M,
(2) $rn \in N$ for all $r \in R$, $n \in N$.

Let M and M' be R-modules. A function $\varphi : M \to M'$ is an R**-homomorphism** if the following hold for all $m, n \in M$, $r \in R$:

(1) $\varphi(m+n) = \varphi(m) + \varphi(n)$,
(2) $\varphi(rm) = r\varphi(m)$.

An R-**isomorphism** is a bijective R-homomorphism. We say that the R-modules M and M' are **isomorphic**, written $M \cong M'$, if there exists an R-isomorphism $\varphi : M \to M'$.

If $\varphi : M \to M'$ is an R-homomorphism, then $\ker \varphi := \varphi^{-1}(0)$ and $\operatorname{im} \varphi := \varphi(M)$ are submodules of M and M', respectively.

If M is an R-module and $N \leq M$, then $M/N := \{m + N \,|\, m \in M\}$ is a module with the induced operations:

$$(m + N) + (m' + N) = (m + m') + N,$$
$$r(m + N) = rm + N.$$

M/N is called the **quotient** (or **factor**) **module** of M by N.

1.1 (First Isomorphism Theorem) *If $\varphi : M \to M'$ is an R-homomorphism, then $M/\ker \varphi \cong \operatorname{im} \varphi$.*

The usual second and third isomorphism theorems are valid as well. In fact, these isomorphism theorems are valid for any Ω-group. (Let Ω be a nonempty set. An Ω-**group** is a group G with a function $\Omega \times G \to G$ for which x(ab)=(xa)(xb) for all $x \in \Omega$, $a, b \in G$. There are obvious notions of Ω-subgroup and Ω-homomorphism. An R-module M is an Ω-group with $\Omega = R$ and $G = M$.)

Let N_1 and N_2 be R-modules. The direct sum

$$N_1 \oplus N_2 = \{(n_1, n_2) \,|\, n_i \in N_i\}$$

is an R-module if we define $r(n_1, n_2) = (rn_1, rn_2)$.

Let M be an R-module and let $N_1, N_2 \leq M$. We say that M is the (**internal**) **direct sum** of N_1 and N_2 (written $M = N_1 \dot{+} N_2$) if the following hold:

(1) $M = N_1 + N_2$,
(2) $N_1 \cap N_2 = \{0\}$.

1.2 *If $M = N_1 \dot{+} N_2$, then $M \cong N_1 \oplus N_2$.*

Proof. The pairing $n_1 + n_2 \leftrightarrow (n_1, n_2)$ is the required correspondence. □

Exercise 1

Let M be an R-module and let $N \leq M$. Prove that if $\varphi : M \to N$ is a homomorphism such that $\varphi(n) = n$ for all $n \in N$, then $M = N \dot{+} \ker \varphi$.

2 The Group Algebra

Let G be a finite group and let K be a field (notation in force from here on). Denote by KG the vector space over K with basis G. So the elements of KG are linear combinations of the form $\sum_{a\in G}\alpha_a a$ with $\alpha_a \in K$. We wish to make KG into a ring, so we define multiplication by

$$\big(\sum_{a\in G}\alpha_a a\big)\big(\sum_{b\in G}\beta_b b\big) = \sum_{a,b\in G}(\alpha_a\beta_b)ab.$$

Note that KG has identity $1e$, where e is the identity element of the group G. We usually write $1a$ as just a ($a \in G$) and thus view G as a subset of KG.

Example. Suppose $G = S_4$ (=symmetric group) and $K = \mathbf{Q}$. Then the following is an example of a computation in KG.

$$\begin{aligned}[3(23)+(1243)]\,&[7(24)-5(13)]\\ &= 21(23)(24) - 15(23)(13) + 7(1243)(24) - 5(1243)(13)\\ &= 21(243) - 15(123) + 7(123) - 5(243)\\ &= 16(243) - 8(123).\end{aligned}$$

A **K-algebra** is a ring A that is also a vector space over K subject to $\alpha(ab) = (\alpha a)b = a(\alpha b)$ for all $\alpha \in K$ and all $a, b \in A$.

Example. The ring KG is a K-algebra of dimension $|G|$. It is called the **group algebra** of G over K.

Example. If V is a vector space over K, then the ring $\mathrm{End}(V)$ of linear maps from V to itself is a K-algebra.

Example. The ring $\mathrm{Mat}_n(K)$ of $n \times n$ matrices over K is a K-algebra of dimension n^2.

Example. The ring $K[x]$ of polynomials over K is an infinite-dimensional K-algebra.

Let A be a K-algebra with identity 1 ($\neq 0$). We get a ring monomorphism $K \to A$ via $\alpha \mapsto \alpha 1$. (It is nonzero since it sends the identity of K to the identity of A. It is injective since its kernel is an ideal of the field K and is therefore trivial.) We use this monomorphism to view K as a subring of A.

KG-modules. Let V be a vector space over K. A map $G \times V \to V$ by $(a, v) \mapsto av$ is called a **group action** of G on V if the following hold for all $a, b \in G$, $v, w \in V$, and $\alpha \in K$:

(1) $(ab)v = a(bv)$,
(2) $ev = v$,
(3) $a(v + w) = av + aw$,
(4) $a(\alpha v) = \alpha(av)$.

(The first two properties say that the given map defines an action of the group G on the underlying set of the vector space V, while the last two properties say that each element of G acts as a linear operator on V.)

Let V be a KG-module. By restricting the scalars from KG to K, we can view V as a K-module, that is, as a vector space over K. It follows from the module axioms that restricting scalars from KG to G yields a group action $G \times V \to V$ of G on V. The following result says that, conversely, a group action of G on a vector space V induces a KG-module structure on V.

2.1 *Let V be a vector space over K and let $G \times V \to V$ be a group action of G on V. Then V is a KG-module with scalar multiplication given by*

$$\Big(\sum_{a\in G} \alpha_a a\Big)v = \sum_{a\in G} \alpha_a av.$$

(This scalar multiplication is said to be "extended linearly" from the action of G on V.)

Proof. We verify only module axiom (3), namely $(rs)v = r(sv) \quad (r, s \in KG,\ v \in V)$, since the verifications of the other axioms are straightforward. Let $r, s \in KG$ so that $r = \sum_a \alpha_a a$ and $s = \sum_b \beta_b b \in KG$ for some $\alpha_a, \beta_b \in K$. For any $v \in V$, we have

$$\begin{aligned}
(rs)v &= \Big(\sum_{a,b} \alpha_a\beta_b(ab)\Big)v \\
&= \Big(\sum_{c} \big(\sum_{\substack{a,b\\ ab=c}} \alpha_a\beta_b c\big)\Big)v && \text{(collect like terms)} \\
&= \sum_{c} \big(\sum_{\substack{a,b\\ ab=c}} \alpha_a\beta_b\big)cv && \text{(linear extension)} \\
&= \sum_{c}\sum_{a} \alpha_a\beta_{a^{-1}c}cv \\
&= \sum_{a} \alpha_a\big(\sum_{c} \beta_{a^{-1}c}cv\big) \\
&= \sum_{a} \alpha_a\big(\sum_{b} \beta_b(ab)v\big) && (b = a^{-1}c)
\end{aligned}$$

$$
\begin{aligned}
&= \sum_a \alpha_a \big(\sum_b \beta_b a(bv) \big) && \text{((1) of group action)} \\
&= \sum_a \alpha_a a \big(\sum_b \beta_b bv \big) && \text{((3) and (4) of group action)} \\
&= \big(\sum_a \alpha_a a \big) \Big(\big(\sum_b \beta_b b \big) v \Big) && \text{(linear extension, twice)} \\
&= r(sv),
\end{aligned}
$$

so module axiom (3) holds. $\square$

3 Tensor Product and Contragredient

Recall (Section 2) that any KG-module can be viewed as a vector space over K. For us, KG-modules will always be assumed to be finite-dimensional (over K) when viewed thus. Here, we look at two ways of constructing new KG-modules from old ones.

Tensor Product. Let V and W be KG-modules with bases $\{v_1, \ldots, v_m\}$ and $\{w_1, \ldots, w_n\}$, respectively. Let $V \otimes W$ be the vector space with basis $\{v_i \otimes w_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$. $V \otimes W$ is the **tensor product** of V and W.

For arbitrary $v \in V$, $w \in W$, write $v = \sum_i \alpha_i v_i$, $w = \sum_j \beta_j w_j$ and define $v \otimes w = \sum_{i,j} \alpha_i \beta_j v_i \otimes w_j \in V \otimes W$. (*Caution*: It is not the case that every element of $V \otimes W$ can be expressed in the form $v \otimes w$ with $v \in V$ and $w \in W$.)

3.1 *For all $v, v' \in V$, $w, w' \in W$, and $\alpha \in K$, we have*

(1) $(v + v') \otimes w = v \otimes w + v' \otimes w$,
(2) $v \otimes (w + w') = v \otimes w + v \otimes w'$,
(3) $\alpha(v \otimes w) = (\alpha v) \otimes w = v \otimes (\alpha w)$.

For $a \in G$, the map of basis vectors given by $v_i \otimes w_j \mapsto av_i \otimes aw_j$ extends uniquely to a linear map from $V \otimes W$ to itself, which we denote by $u \mapsto au$ ($u \in V \otimes W$). Then $(a, u) \mapsto au$ defines a group action of G on the vector space $V \otimes W$ (note that once properties (3) and (4) are checked it suffices to verify properties (1) and (2) under the assumption that v is a basis vector). According to 2.1 the linear extension to KG of this action gives V the structure of KG-module.

Contragredient. Let V be a KG-module and set $V^* = \{f : V \to K \mid f \text{ is linear}\}$. V^* is the **dual space** of V. For $a \in G$ and $f \in V^*$, the function $af : V \to K$ defined by $(af)(v) = f(a^{-1}v)$ is an element of V^*. Then the map $(a, f) \mapsto af$ defines a group action of G on the vector space V^*. According to 2.1 the linear extension to KG of this action gives V^* the structure of KG-module. This module is the **contragredient** of V. We have $V \cong V^{**}$ via $v \mapsto (f \mapsto f(v))$.

Remark. These two constructions are available for any Hopf algebra (of which the group algebra is an example), but not for an arbitrary algebra. A Hopf algebra A has a certain algebra homomorphism, $\triangle : A \to A \otimes A$ (comultiplication) and an algebra antihomomorphism $\sigma : A \to A$ (antipode). In the case $A = KG$ we obtain these maps by putting $\triangle(a) = a \otimes a$ and $\sigma(a) = a^{-1}$ ($a \in G$) and extending linearly to KG. Let M and N be A-modules. Then $M \otimes N$ is an $A \otimes A$-module by $(a \otimes b)(m \otimes n) = am \otimes bn$ (even without

the additional Hopf structure); it becomes an A-module by putting $a(m \otimes n) = \triangle(a)(m \otimes n)$. Also, M^* becomes an A-module by putting $(af)(m) = f(\sigma(a)m)$.

4 Representations and Modules

Let $\rho : G \to \mathrm{GL}(V)$ be a representation (Section 0). Putting $av = \rho(a)(v)$ $(a \in G, v \in V)$ we obtain a group action of G on the vector space V. According to 2.1, the linear extension to KG of this action gives V the structure of KG-module.

Conversely, let V be a KG-module. Then V can be viewed as a (finite-dimensional) vector space over K. Define $\rho : G \to \mathrm{GL}(V)$ by $\rho(a)(v) = av$. Then ρ is a well-defined homomorphism, and hence a representation of G. We call ρ the representation **afforded by** V.

We can use the language of categories to make the correspondence described above more precise. Let KG-**mod** denote the category having as objects KG-modules and as morphisms KG-homomorphisms. Let G-**rep** denote the category having as objects representations of G and morphisms described as follows: Given objects $\rho : G \to \mathrm{GL}(V)$, $\rho' : G \to \mathrm{GL}(V')$, the set $\mathrm{Mor}(\rho, \rho')$ of morphisms from ρ to ρ' consists of those linear maps $f : V \to V'$ such that $f \circ \rho(a) = \rho'(a) \circ f$ for all $a \in G$.

We claim that the categories KG-**mod** and G-**rep** are equivalent. Define a functor $F : KG$-**mod**$\to G$-**rep** by

$$F : \begin{cases} V \mapsto \rho, & \text{where } \rho \text{ is afforded by } V, \\ f \mapsto f, & \text{for a } KG\text{-homomorphism } f : V \to V'. \end{cases}$$

We need to check that $F(f) = f \in \mathrm{Mor}(\rho, \rho') = \mathrm{Mor}(F(V), F(V'))$. Clearly f is linear. Also, for $v \in V$ we have

$$\begin{aligned} [f \circ \rho(a)](v) &= f(\rho(a)(v)) = f(av) = af(v) \\ &= \rho'(a)(f(v)) = [\rho'(a) \circ f](v). \end{aligned}$$

We also get a functor $F' : G$-**rep**$\to KG$-**mod** by

$$F' : \begin{cases} \rho : G \to \mathrm{GL}(V) \mapsto V, \\ f \mapsto f. \end{cases}$$

It is easy to check that $F' \circ F = 1_{KG\text{-}\mathbf{mod}}$ and $F \circ F' = 1_{G\text{-}\mathbf{rep}}$, so that KG-**mod**$\cong G$-**rep**, as desired.

Exercise 2

Fill in the details of the "representation $\leftrightarrow$ module" correspondence outlined in the first two paragraphs of this section.

5 Matrix Representations

Let V be a vector space over the field K with (ordered) basis $B = \{v_1, \ldots, v_n\}$. For $v \in V$ we have $v = \sum_i \beta_i v_i$ for uniquely determined $\beta_i \in K$. Write

$$[v]_B = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}$$

(the **coordinate vector of** v **relative to** B).

Let $f : V \to V$ be a linear transformation. For $v \in V$ we have

$$[f(v)]_B = [\alpha_{ij}][v]_B,$$

where $f(v_j) = \sum_i \alpha_{ij} v_i$ $(1 \leq j \leq n)$. We call $[\alpha_{ij}]$ the **matrix of** f **relative to** B.

Now suppose $\rho : G \to \mathrm{GL}(V)$ is a representation of G. For each $a \in G$, let $[\alpha_{ij}(a)]$ be the matrix of $\rho(a)$ relative to B. Then, denoting by $\mathrm{GL}_n(K)$ the group of invertible $n \times n$-matrices over K, we get a homomorphism $R : G \to \mathrm{GL}_n(K)$ by putting $R(a) = [\alpha_{ij}(a)]$. R is called the **matrix representation of** G **afforded by** ρ (or **by** V) **relative to** B.

Example. Let $G = \mathbf{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$. The vector space $V = KG$ is a KG-module (with module product being the ring product in KG). The matrix representation R of G afforded by V relative to the basis $\{\bar{0}, \bar{1}, \bar{2}\}$ is given by

$$R(\bar{0}) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad R(\bar{1}) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad R(\bar{2}) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

Notice that these are "permutation matrices" (exactly one 1 appears in each row and each column with zeros elsewhere).

In general, for any group G the matrix representation R of G afforded by KG relative to the basis G has the property that $R(a)$ is a permutation matrix for each $a \in G$.

Submodules. Let V be a KG-module and let W be a submodule of V. Let $\{v_1, \ldots, v_m\}$ be a basis of W and extend this to get a basis $B = \{v_1, \ldots, v_m, v_{m+1}, \ldots, v_n\}$ of V. If R is the corresponding matrix representation, then for each $a \in G$, $R(a)$ is of block form

$$R(a) = \begin{bmatrix} * & * \\ 0 & * \end{bmatrix}.$$

Let ρ be the representation of G afforded by V. For each $a \in G$, we have $\rho(a)(W) = aW \subseteq W$, so we get a representation $\sigma : G \to \mathrm{GL}(W)$ by defining $\sigma(a) = \rho(a)|_W$ (the **subrepresentation of G afforded by the submodule W of V**). Relative to the basis $\{v_1, \ldots, v_m\}$ of W, σ affords the matrix representation represented by the upper left block in the depiction of $R(a)$ above.

Keep the notation above and assume there exists a submodule W' of V such that $V = W \dot{+} W'$. Also assume that $\{v_{m+1}, \ldots, v_n\}$ is a basis for W'. Then B is still a basis for V and for each $a \in G$, $R(a)$ is of block form

$$R(a) = \begin{bmatrix} * & 0 \\ 0 & * \end{bmatrix}.$$

Tensor Products. Let V and W be KG-modules with bases $\{v_1, \ldots, v_m\}$, $\{w_1, \ldots, w_n\}$, respectively. Then $\{v_i \otimes w_j\}$ is a basis for $V \otimes W$. Order this set lexicographically: $\{v_1 \otimes w_1, v_1 \otimes w_2, \ldots, v_2 \otimes w_1, v_2 \otimes w_2, \ldots\}$. Let $[\alpha_{ij}]$ and $[\beta_{kl}]$ be the matrix representations afforded by V and W, respectively, relative to the given bases. We wish to determine the matrix representation $[\gamma_{ij,kl}]$ afforded by $V \otimes W$ relative to the above basis. By definition, for each $a \in G$, we have

$$a(v_k \otimes w_l) = \sum_{i,j} \gamma_{ij,kl}(a) v_i \otimes w_j.$$

But also,

$$\begin{aligned} a(v_k \otimes w_l) &= av_k \otimes aw_l \\ &= \big(\sum_i \alpha_{ik}(a) v_i\big) \otimes \big(\sum_j \beta_{jl}(a) w_j\big) \\ &= \sum_{i,j} \alpha_{ik}(a)\beta_{jl}(a) v_i \otimes w_j. \end{aligned}$$

Since $\{v_i \otimes w_j\}$ is linearly independent, we have $\gamma_{ij,kl}(a) = \alpha_{ik}(a)\beta_{jl}(a)$. The matrix $[\gamma_{ij,kl}(a)]$ is called the **tensor** (or **Kronecker**) **product** of the matrices $[\alpha_{ik}(a)]$ and $[\beta_{jl}(a)]$, written $[\alpha_{ik}(a)] \otimes [\beta_{jl}(a)]$.

Example.

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \otimes \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 2 & 4 & 6 \\ 4 & 5 & 6 & 8 & 10 & 12 \\ 7 & 8 & 9 & 14 & 16 & 18 \\ 3 & 6 & 9 & 4 & 8 & 12 \\ 12 & 15 & 18 & 16 & 20 & 24 \\ 21 & 24 & 27 & 28 & 32 & 36 \end{bmatrix}.$$

Exercise 3

Let V be a KG-module. Let $[\alpha_{ij}]$ be the matrix representation of G afforded by V relative to the basis $\{v_1, \ldots, v_n\}$. Let $[\alpha^*_{ij}]$ be the matrix representation of G afforded by the contragredient module V^* (Section 3) relative to the "dual basis" $\{v^*_1, \ldots, v^*_n\}$ (so $v^*_i(v_j) = \delta_{ij}$ = Kronecker delta). Express $[\alpha^*_{ij}]$ in terms of $[\alpha_{ij}]$.

6 Schur's Lemma

From Section 8 on we will assume $K = \mathbf{C}$. In this section and the next, we see why this assumption simplifies matters. We begin by reviewing "algebraically closed fields" and "eigenvalues."

Algebraically Closed Fields. The field K is **algebraically closed** if each nonconstant $f \in K[x]$ ($=$ set of polynomials in x over K) has a zero.

EXAMPLE. The field $\mathbf{R}$ of real numbers is not algebraically closed since x^2+1 has no zero.

Remark. If α is a zero of $f \in K[x]$, then $x-\alpha$ is a factor. (Proof: Use division algorithm.) So, using induction on the degree of f, we have that K is algebraically closed if and only if each nonconstant $f \in K[x]$ can be written in the form $f = \alpha_0(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ ($\alpha_i \in K$).

6.1 FUNDAMENTAL THEOREM OF ALGEBRA. *The field* $\mathbf{C}$ *of complex numbers is algebraically closed.*

PROOF. The name given to this theorem is a bit of a misnomer since there is no known "purely algebraic" proof. Nor is it likely that there could be such since the complex numbers are constructed from the real numbers, which are defined as the completion of the rational numbers, and so topology ultimately enters in. Here is a quick proof using complex analysis.

Liouville's Theorem states that every bounded entire (i.e., differentiable) function $f : \mathbf{C} \to \mathbf{C}$ is constant. Suppose $f \in \mathbf{C}[x]$ has no zero. Since $|f(x)| \to \infty$ as $|x| \to \infty$ and $\operatorname{im} f$ is bounded away from zero, $1/f$ is bounded (and clearly entire). Therefore, by Liouville's Theorem, $1/f$ is constant, so that f is as well. $\square$

Eigenvalues. Let V be a vector space over K and let $f : V \to V$ be a linear transformation. An element α of K is an **eigenvalue** of f if $f(v) = \alpha v$ for some *nonzero* $v \in V$. If the matrix A represents f relative to some basis B of V, then

$$\begin{aligned} \alpha \in K \text{ is an eigenvalue of } f &\iff f(v) = \alpha v \text{ for some } v \neq 0 \\ &\iff [f(v)]_B = \alpha[v]_B \text{ for some } v \neq 0 \\ &\iff A[v]_B = \alpha[v]_B \text{ for some } v \neq 0 \end{aligned}$$

$$\iff (A-\alpha I)[v]_B = 0 \text{ for some } v \neq 0$$
$$\iff (A-\alpha I) \text{ is not invertible}$$
$$\iff \det(A-\alpha I) = 0,$$
$$\iff \alpha \text{ is a zero of the polynomial } g(x) = \det(A-xI).$$

In particular, if K is algebraically closed, then each linear transformation $f : V \to V$ has an eigenvalue.

Now that the background material has been reviewed, we turn to the main subject of the section.

A nonzero KG-module V is **simple** if it has no (nonzero) proper submodule. If V is simple and it affords the representation ρ, we say that ρ is **irreducible**. In other words, a representation is irreducible if it admits no (nonzero) proper subrepresentation in the sense of Section 5.

6.2 Schur's Lemma. *Let V and W be simple KG-modules and let $f : V \to W$ be a homomorphism.*

(1) *If $V \ncong W$, then $f = 0$.*
(2) *Assume K is algebraically closed. If $V = W$, then $f = \alpha 1_V$ for some $\alpha \in K$ (so f is a "homothety").*

Proof. (1) Assume $f \neq 0$. Since $\ker f$ is a submodule of V not equal to V, we must have $\ker f = 0$, so that f is injective. Similarly, $\operatorname{im} f$ is a submodule of W not equal to 0, so $\operatorname{im} f = W$ implying f is surjective. Thus, $V \cong W$.

(2) Assume $V = W$. Since K is assumed to be algebraically closed, f has an eigenvalue, say α. Then $\ker(f - \alpha 1_V) \neq 0$. Since V is simple, we get $f - \alpha 1_V = 0$, whence $f = \alpha 1_V$. □

7 Maschke's Theorem

Let R be a ring and let M be a nonzero R-module. A sequence

$$0 = M_0 < M_1 < \cdots < M_n = M$$

of submodules of M is called a **composition series** if each factor M_i/M_{i-1} is simple (i.e., has no proper (nonzero) submodule). If M has a composition series as above, then the simple factors M_i/M_{i-1} $(1 \leq i \leq n)$ are called the **composition factors** of M. (By the Jordan-Hölder Theorem, which applies to Ω-groups and hence to R-modules, composition factors are independent of the chosen composition series and are hence well-defined.) It is possible to have two nonisomorphic modules with the same composition factors.

EXAMPLE. The $\mathbf{Z}$-modules $\mathbf{Z}_4$ and $\mathbf{Z}_2 \oplus \mathbf{Z}_2$ have respective composition series

$$0 < \langle \bar{2} \rangle < \mathbf{Z}_4,$$

$$0 < \langle (\bar{0}, \bar{1}) \rangle < \mathbf{Z}_2 \oplus \mathbf{Z}_2$$

and hence they both have the two composition factors $\mathbf{Z}_2$, $\mathbf{Z}_2$. However, $\mathbf{Z}_4 \ncong \mathbf{Z}_2 \oplus \mathbf{Z}_2$ (since, for instance, $2x = 0$ for all $x \in \mathbf{Z}_2 \oplus \mathbf{Z}_2$, but not for $x = \bar{1} \in \mathbf{Z}_4$).

Suppose R has the property that every nonzero R-module has a composition series and hence composition factors (which is the case for our main object of study, $R = KG$, since we assume KG-modules to be finite-dimensional over K). In this case, one can determine all possible R-modules by first determining the simple ones and then determining all ways these simple modules can be "stacked" to form new modules. (This latter endeavor falls in the domain of "homological algebra." Given R-modules M and N, one studies the extension group $\mathrm{Ext}^1(N, M)$, which is an abelian group with the property that its elements are in one-to-one correspondence with the R-modules having a submodule isomorphic to M and corresponding factor module isomorphic to N. For the example above, we have $\mathrm{Ext}^1(\mathbf{Z}_2, \mathbf{Z}_2) \cong \mathbf{Z}_2 = \{\bar{0}, \bar{1}\}$. The element $\bar{1}$ corresponds to $\mathbf{Z}_4$ and the element $\bar{0}$ corresponds to $\mathbf{Z}_2 \oplus \mathbf{Z}_2$.)

Now suppose R has the property that every nonzero R-module is isomorphic to a direct sum of finitely many simple modules (which is the case for $R = KG$ when $\mathrm{char}\, K \nmid |G|$, as shown in the main result below). In this case, each nonzero module has a composition series and the composition factors are precisely the various simple modules appearing in the corresponding direct sum. Indeed, if $M = \bigoplus_{i=1}^{n} M_i$ with M_i simple, then viewing M_i as a submodule of M in the natural way and putting $N_i = \sum_{j \leq i} M_j$ we get a composition

series $0 = N_0 < N_1 < \cdots < N_n = M$ with $N_i/N_{i-1} \cong M_i$. Therefore, in this case a nonzero R-module is completely determined by its composition factors (implying that all R-modules are known once the simple ones have been determined, i.e., the "stacking problem" mentioned above is trivial). This observation points up the importance of the following result.

7.1 Maschke's Theorem. *If* $\operatorname{char} K \nmid |G|$, *then every* KG*-module is a direct sum of simple modules.*

Proof. Let M be a KG-module and let N be a submodule of M. By induction on $\dim_K M$, it suffices to show that N has a complement, i.e., that there exists $N' \leq M$ with $M = N \dot{+} N'$. For this, it is enough by Exercise 1 to find a KG-homomorphism $f : M \to N$ such that $f(n) = n$ for all $n \in N$.

Let $V \subseteq M$ be a vector space complement of N, so that $M = N \dot{+} V$ as vector spaces. Let $\pi : M \to N$ be the projection onto the first summand: $\pi(n + v) = n$ $(n \in N,\ v \in V)$.

Since $\operatorname{char} K \nmid |G|$, $|G|$ is nonzero when viewed as an element of K. Hence, it makes sense to define $f : M \to N$ by

$$f = \frac{1}{|G|} \sum_{a \in G} a^{-1} \pi a$$

(meaning $f = \frac{1}{|G|} \sum_{a \in G} \rho(a^{-1}) \circ \pi \circ \rho(a)$, where ρ is the representation afforded by M).

We will show that f is a homomorphism. First, f is clearly linear, so it is enough to show that $f(bm) = bf(m)$ for all $b \in G$, $m \in M$. We have

$$\begin{aligned} f(bm) &= \frac{1}{|G|} \sum_{a \in G} a^{-1} \pi a(bm) = \frac{1}{|G|} \sum_{a \in G} b(ab)^{-1} \pi (ab) m \\ &= b \frac{1}{|G|} \sum_{c \in G} c^{-1} \pi c m \\ &= bf(m), \end{aligned}$$

so f is a homomorphism, as desired.

Finally,

$$f(n) = \frac{1}{|G|} \sum_{a} a^{-1} \pi a n = \frac{1}{|G|} \sum_{a} a^{-1} \pi (an) = \frac{1}{|G|} \sum_{a} a^{-1} a n = n$$

and the proof is complete. $\square$

8 Characters

From now on, we restrict our attention to the field $K = \mathbf{C}$ so that both Schur's Lemma and Maschke's Theorem apply. (Actually, for fixed G we could choose any algebraically closed field of characteristic not dividing $|G|$ and get essentially the same theory.)

Let $A = [\alpha_{ij}]$ be an $n \times n$-matrix over $\mathbf{C}$. The **trace** of A is defined by $\operatorname{tr} A = \sum_{i=1}^{n} \alpha_{ii}$. We first establish some standard facts about the trace.

8.1 *For any $n \times n$-matrices A and B, we have $\operatorname{tr}(AB) = \operatorname{tr}(BA)$.*

PROOF. Let $A = [\alpha_{ij}]$ and $B = [\beta_{ij}]$ be $n \times n$-matrices. We have

$$\begin{aligned}\operatorname{tr}(AB) &= \operatorname{tr}\big[\sum_k \alpha_{ik}\beta_{kj}\big] = \sum_i \sum_k \alpha_{ik}\beta_{ki} = \sum_k \sum_i \beta_{ki}\alpha_{ik} \\ &= \operatorname{tr}\big[\sum_i \beta_{ki}\alpha_{il}\big] = \operatorname{tr}(BA). \quad \square\end{aligned}$$

8.2 *For $n \times n$-matrices A and C with C nonsingular, we have $\operatorname{tr}(C^{-1}AC) = \operatorname{tr} A$.*

PROOF. This follows directly from 8.1. $\square$

8.3 *If A is an $n \times n$-matrix, then $\operatorname{tr} A = \sum_{i=1}^{n} \lambda_i$, where the λ_i are the zeros of the polynomial $g(x) = \det(xI - A)$ repeated according to multiplicity.*

PROOF. Let $A = [\alpha_{ij}]$ be an $n \times n$-matrix. By definition,

$$g(x) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) b_{1\sigma(1)} \cdots b_{n\sigma(n)},$$

where $\operatorname{sgn}(\sigma)$ is 1 or -1 according as σ is even or odd, and $b_{ij} = \delta_{ij}x - \alpha_{ij}$. If $\sigma \neq 1$, then σ moves at least two numbers, whence $b_{1\sigma(1)} \cdots b_{n\sigma(n)}$ is of degree at most $n - 2$ in x. Thus,

$$g(x) = \prod_i b_{ii} + h_1(x) = \prod_i (x - a_{ii}) + h_1(x) = x^n - \sum_i a_{ii} x^{n-1} + h_2(x),$$

where $h_i(x)$ has degree at most $n - 2$. But we also have

$$g(x) = \prod_i (x - \lambda_i) = x^n - \sum_i \lambda_i x^{n-1} + h_3(x),$$

where $h_3(x)$ has degree at most $n-2$. Hence, $\operatorname{tr} A = \sum_i a_{ii} = \sum_i \lambda_i$, as desired. □

Remark. In the notation of 8.3, $v \mapsto Av$ defines a linear transformation from $\mathbf{C}^n$ to $\mathbf{C}^n$; the result says that $\operatorname{tr} A$ equals the sum of the eigenvalues (repeated according to multiplicity) of this linear transformation (in short, the eigenvalues of A). We also point out that 8.3 follows immediately from 8.2 and the theorem from linear algebra that says A is similar to a matrix in Jordan canonical form.

Now let V be a vector space over $\mathbf{C}$ and let $f : V \to V$ be a linear map. Define $\operatorname{tr} f = \operatorname{tr} A$, where A is the matrix of f relative to some basis B of V. By 8.2, $\operatorname{tr} f$ is well-defined, for if a different basis B' is chosen, then the matrix of f relative to B' is $C^{-1}AC$, where C is the change of basis matrix that changes B' coordinates to B coordinates.

Assume V is a $\mathbf{C}G$-module and let ρ be the representation it affords. The map $\chi : G \to \mathbf{C}$ defined by $\chi(a) = \operatorname{tr} \rho(a)$ is the **character of G afforded by** V (or by ρ).

8.4 *Let V_1 and V_2 be $\mathbf{C}G$-modules and let χ_1 and χ_2, respectively, be the characters they afford. Then*

(1) *$V_1 \oplus V_2$ affords the character $\chi_1 + \chi_2$,*
(2) *$V_1 \otimes V_2$ affords the character $\chi_1\chi_2$.*

Proof. (1) Let R_i be the matrix representation of G afforded by V_i relative to the basis B_i $(i = 1, 2)$. Then, viewing V_1 as a subspace of $V = V_1 \oplus V_2$ by identifying v_1 with $(v_1, 0)$, and similarly for V_2, we have that $B = B_1 \cup B_2$ is a basis for V. The matrix representation R of G afforded by V relative to B is easily seen to satisfy

$$R(a) = \begin{bmatrix} R_1(a) & 0 \\ 0 & R_2(a) \end{bmatrix}.$$

So if χ is the character afforded by V, then $\chi(a) = \operatorname{tr} R(a) = \operatorname{tr} R_1(a) + \operatorname{tr} R_2(a) = \chi_1(a) + \chi_2(a)$.

The proof of (2) is similar. □

Next, we assemble some standard facts about characters.

8.5 *Let V be a $\mathbf{C}G$-module and let χ be the character it affords.*

(1) *$\chi(e) = \dim_{\mathbf{C}} V$.*
(2) *For each $a \in G$, $\chi(a)$ is a sum of roots of unity.*
(3) *For each $a \in G$, $\chi(a^{-1}) = \overline{\chi(a)}$, where bar indicates complex conjugate ($\overline{a + bi} = a - bi$).*
(4) *For each $a, g \in G$, $\chi(g^{-1}ag) = \chi(a)$.*

Proof. (1) Let ρ be the representation afforded by V. We have $\chi(e) = \operatorname{tr} \rho(e) = \operatorname{tr} 1_V = \operatorname{tr} I_n = n$, where $n = \dim_{\mathbf{C}} V$.

(2) Let ρ be as above and let $a \in G$. If λ is an eigenvalue of $\rho(a)$, then for some $0 \neq v \in V$ we have $\rho(a)(v) = \lambda v$. Hence

$$\lambda^m v = \rho(a)^m(v) = \rho(a^m)(v) = \rho(e)(v) = v,$$

where m is the order of a. This implies $\lambda^m = 1$, so that λ is an mth root of unity. Finally, $\chi(a) = \operatorname{tr} \rho(a)$, which by 8.3 is the sum of the eigenvalues of $\rho(a)$ and hence a sum of roots of unity.

(3) Let $a \in G$. With ρ, λ, and v as above, we have

$$\rho(a^{-1})(v) = \rho(a)^{-1}(v) = \lambda^{-1}v.$$

Hence, λ is an eigenvalue of $\rho(a)$ if and only if λ^{-1} is an eigenvalue of $\rho(a^{-1})$. Furthermore, by the proof of (2), $|\lambda| = 1$, so the equation $\lambda\overline{\lambda} = |\lambda|^2 = 1$ gives $\lambda^{-1} = \overline{\lambda}$. As in 8.3, we have

$$\chi(a^{-1}) = \operatorname{tr} \rho(a^{-1}) = \sum_i \overline{\lambda_i} = \overline{\sum_i \lambda_i} = \overline{\operatorname{tr} \rho(a)} = \overline{\chi(a)}.$$

(4) Let $a, g \in G$ and let ρ be as above. Using 8.2, we have

$$\chi(g^{-1}ag) = \operatorname{tr} \rho(g^{-1}ag) = \operatorname{tr}\left[\rho(g)^{-1}\rho(a)\rho(g)\right] = \operatorname{tr}(C^{-1}AC) = \operatorname{tr} A = \operatorname{tr} \rho(a) = \chi(a),$$

where A and C are the matrices of $\rho(a)$ and $\rho(g)$, respectively, relative to some basis of V. $\square$

Exercise 4

Let U and V be $\mathbf{C}G$-modules and set $W = \operatorname{Hom}_{\mathbf{C}}(U, V)$ (= set of $\mathbf{C}$-linear maps from U to V). Since V is a vector space, W becomes a vector space in the natural way. We could also use the $\mathbf{C}G$ action on V to make W into a $\mathbf{C}G$-module, but instead we define $(af)(u) = a(f(a^{-1}u))$ ($a \in G$, $f \in W$, $u \in U$) and extend linearly to $\mathbf{C}G$.

(a) This operation makes W into a $\mathbf{C}G$-module. Verify only the following step: $(ab)f = a(bf)$ ($a, b \in G$, $f \in W$).

(b) Prove that $W \cong U^* \otimes V$ as $\mathbf{C}G$-modules.

(c) Explain how this construction generalizes the notion of a contragredient module (Section 3).

(d) Express the character afforded by W in terms of the characters afforded by U and V, respectively.

9 Orthogonality Relations

The set $\mathrm{Fun}(G, \mathbf{C})$ of all functions from G to $\mathbf{C}$ inherits from $\mathbf{C}$ the structure of vector space over $\mathbf{C}$. In this section we define an inner product on this space and show that the set of irreducible characters of G (i.e., those characters afforded by simple $\mathbf{C}G$-modules) forms an orthonormal set relative to this inner product.

The main lemma is the following result. Note that the characteristic of $\mathbf{C}$ being zero allows the division by $|G|$ in the statement of the result, and also notice that the fact $\mathbf{C}$ is algebraically closed (6.1) allows the use of Schur's lemma in the proof.

9.1 *Let V and V' be $\mathbf{C}G$-modules and let $f : V \to V'$ be a linear map. Set*

$$f^0 = \frac{1}{|G|} \sum_{a \in G} a^{-1} f a : V \to V'.$$

(1) *f^0 is a $\mathbf{C}G$-homomorphism.*
(2) *Assuming V and V' are simple, we have*

$$f^0 = \begin{cases} 0, & V' \ncong V, \\ \dfrac{\operatorname{tr} f}{n} 1_V, & V' = V, \end{cases}$$

where $n = \dim_{\mathbf{C}} V$.

Proof. (1) This proof is similar to that of Maschke's theorem (7.1).

(2) By part (1) and Schur's Lemma (6.2), if $V \ncong V'$, then $f^0 = 0$ and if $V' = V$, then $f^0 = \alpha 1_V$ for some $\alpha \in \mathbf{C}$. We have

$$\alpha \cdot n = \operatorname{tr} f^0 = \frac{1}{|G|} \sum_{a \in G} \operatorname{tr}(a^{-1} f a) = \frac{1}{|G|} \sum_{a \in G} \operatorname{tr} f = \operatorname{tr} f,$$

so $\alpha = (\operatorname{tr} f)/n$, as desired. □

Given two functions $\varphi, \psi : G \to \mathbf{C}$, set

$$\langle \varphi, \psi \rangle = \frac{1}{|G|} \sum_{a \in G} \varphi(a^{-1}) \psi(a).$$

9.2 *Let V and V' be simple $\mathbf{C}G$-modules and let $R = [\alpha_{ij}]$ and $R' = [\alpha'_{ij}]$, respectively, be the matrix representations they afford (relative to chosen bases). Then for all i, j, k, and l, we have*

$$\langle \alpha'_{ij}, \alpha_{kl} \rangle = \begin{cases} 0, & V' \ncong V, \\ \frac{1}{n}\delta_{il}\delta_{jk}, & V' = V. \end{cases}$$

PROOF. Let $n = \dim_{\mathbf{C}} V$ and $n' = \dim_{\mathbf{C}} V'$. Fix j and k and let C be the $n' \times n$-matrix defined by $C = [\delta_{xj}\delta_{yk}]_{xy}$, where the final subscripts indicate that the row index is x and the column index is y. Now C can be viewed as the matrix relative to the chosen bases of a linear transformation $f : V \to V'$. Therefore, 9.1 implies

$$\frac{1}{|G|}\sum_{a\in G} R'(a^{-1})CR(a) = \begin{cases} [0], & V' \ncong V, \\ \dfrac{\operatorname{tr} C}{n} I_n, & V' = V, \end{cases}$$

where I_n denotes the $n \times n$ identity matrix. The left hand side of this formula becomes

$$\frac{1}{|G|}\sum_{a\in G}\left[\sum_{x,y} \alpha'_{ix}(a^{-1})\delta_{xj}\delta_{yk}\alpha_{yl}(a)\right]_{il} = \left[\frac{1}{|G|}\sum_{a\in G}\alpha'_{ij}(a^{-1})\alpha_{kl}(a)\right]_{il} = \left[\langle \alpha'_{ij}, \alpha_{kl}\rangle\right]_{il}.$$

Since $\operatorname{tr} C = \sum_x \delta_{xj}\delta_{xk} = \delta_{jk}$, we have

$$\left[\langle \alpha'_{ij}, \alpha_{kl}\rangle\right]_{il} = \begin{cases} [0], & V' \ncong V, \\ \left[\frac{1}{n}\delta_{jk}\delta_{il}\right]_{il}, & V' = V. \end{cases}$$

An il-entry comparison finishes the proof. □

The set $\operatorname{Fun}(G, \mathbf{C})$ of functions from G to $\mathbf{C}$ is regarded as a vector space over $\mathbf{C}$ in the usual way. The pairing

$$(\varphi, \psi) = \frac{1}{|G|}\sum_{a\in G} \varphi(a)\overline{\psi(a)}$$

defines an "inner product" on $\operatorname{Fun}(G, \mathbf{C})$, meaning, for all $\varphi, \varphi', \psi, \psi' \in \operatorname{Fun}(G, \mathbf{C})$, $\alpha \in \mathbf{C}$,

(1) $(\varphi + \varphi', \psi) = (\varphi, \psi) + (\varphi', \psi)$
(2) $(\varphi, \psi + \psi') = (\varphi, \psi) + (\varphi, \psi')$
(3) $(\alpha\varphi, \psi) = \alpha(\varphi, \psi)$
(4) $(\varphi, \alpha\psi) = \overline{\alpha}(\varphi, \psi)$
(5) $(\varphi, \psi) = \overline{(\psi, \varphi)}$
(6) $(\varphi, \varphi) \geq 0$ with equality if and only if $\varphi = 0$.

(Note that some of these axioms are redundant. For instance, (2) follows from (1) and (5).)

9.3 *If χ and χ' are characters, then $(\chi, \chi') = \langle \chi, \chi' \rangle$.*

PROOF. By 8.5(3),

$$(\chi, \chi') = \frac{1}{|G|} \sum_{a \in G} \chi(a)\overline{\chi'(a)} = \frac{1}{|G|} \sum_{a} \chi(a)\chi'(a^{-1}) = \langle \chi, \chi' \rangle. \quad \square$$

9.4 *Let V and V' be simple $\mathbf{C}G$-modules affording the characters χ and χ', respectively. Then*

$$(\chi, \chi') = \begin{cases} 1, & V \cong V' \\ 0, & V \ncong V'. \end{cases}$$

PROOF. With the notation as in 9.2, we have

$$(\chi, \chi') = \langle \chi, \chi' \rangle = \langle \sum_i \alpha_{ii}, \sum_j \alpha'_{jj} \rangle = \sum_{i,j} \langle \alpha_{ii}, \alpha'_{jj} \rangle,$$

where we have used 9.3. First suppose $V \cong V'$. Then $\chi = \chi'$ (see Exercise 5 below), so we may assume $V = V'$. Then 9.2 implies that

$$(\chi, \chi') = \sum_{i,j} \frac{1}{n} \delta_{ij}\delta_{ij} = \sum_i \frac{1}{n} = 1.$$

Finally, if $V \ncong V'$, then 9.2 implies $\langle \alpha_{ii}, \alpha'_{jj} \rangle = 0$, so $(\chi, \chi') = 0$. $\square$

9.5 *Let $V_1, \ldots, V_t$ be pairwise nonisomorphic simple $\mathbf{C}G$-modules affording the characters $\chi_1, \ldots, \chi_t$, respectively, and let $m_1, \ldots, m_t \in \mathbf{N}$. Set $V = \bigoplus_i m_i V_i$, where $m_i V_i$ means $V_i \oplus \cdots \oplus V_i$ (m_i summands) and let χ be the character afforded by V. Then $m_i = (\chi, \chi_i)$ for all $1 \leq i \leq t$.*

PROOF. By 8.4, $\chi = \sum_j m_j \chi_j$, so $(\chi, \chi_i) = \sum_j m_j (\chi_j, \chi_i) = m_i$, by 9.4. $\square$

By Maschke's Theorem (Section 7), any $\mathbf{C}G$-module is isomorphic to a direct sum of simple modules. Moreover, according to 9.5, the number of times a given simple module appears is independent of the decomposition. (Actually, we already knew this from the Jordan-Hölder theorem. See the remarks in Section 7.)

9.6 *Let V and V' be $\mathbf{C}G$-modules affording the characters χ and χ', respectively. Then $\chi = \chi'$ if and only if $V \cong V'$.*

PROOF. The proof that $\chi = \chi'$ if $V \cong V'$ is Exercise 5 below.

Now assume that $\chi = \chi'$. We can write $V \cong \bigoplus_{i=1}^t m_i V_i$ and $V' \cong \bigoplus_{i=1}^t m'_i V_i$, where $V_1, \ldots, V_t$ are pairwise nonisomorphic simple modules and m_i and m'_i are nonnegative integers. If V_i affords the character χ_i, then using the fact that isomorphic $\mathbf{C}G$-modules

afford the same character (first part of this proof) and 9.5 we get $m_i = (\chi, \chi_i) = (\chi', \chi_i) = m_i'$ for all i. Therefore, $V \cong V'$. □

The character afforded by a simple module is called **irreducible**. We denote the set of all irreducible characters of G by $\mathrm{Irr}(G)$.

In the next result, we use the terminology that a subset X of $\mathrm{Fun}(G, \mathbf{C})$ is **orthonormal** if $(\varphi, \psi) = \delta_{\varphi\psi}$ for all $\varphi, \psi \in X$.

9.7 $\mathrm{Irr}(G)$ *is orthonormal.*

Proof. Use 9.4 and 9.6. □

9.8 *There are only finitely many pairwise nonisomorphic simple* $\mathbf{C}G$*-modules.*

Proof. First, $\mathrm{Irr}(G)$ is linearly independent. Indeed, if $\sum_i \alpha_i\chi_i = 0$ ($\alpha_i \in \mathbf{C}$, $\chi_i \in \mathrm{Irr}(G)$), then 9.7 implies $\alpha_j = (\sum \alpha_i\chi_i, \chi_j) = 0$ for each j. Also, if for $a \in G$ we define $f_a : G \to \mathbf{C}$ by $f_a(b) = \delta_{ab}$, then $\{f_a \mid a \in G\}$ clearly spans $\mathrm{Fun}(G, \mathbf{C})$. In particular, we have $|\mathrm{Irr}(G)| \leq \dim_{\mathbf{C}} \mathrm{Fun}(G, \mathbf{C}) \leq |G|$. □

Remark. Here is another proof of 9.8 not using character theory. Let S be a simple module and choose $0 \neq x \in S$. The map $\varphi : \mathbf{C}G \to S$ given by $\varphi(r) = rx$ is a $\mathbf{C}G$-epimorphism. Hence S is isomorphic to a quotient of the $\mathbf{C}G$-module $\mathbf{C}G$. Now $\mathbf{C}G$ is finite-dimensional ($\dim_{\mathbf{C}} \mathbf{C}G = |G|$), so $\mathbf{C}G$ has a composition series. Clearly, S is a composition factor of $\mathbf{C}G$. Since $\mathbf{C}G$ has only finitely many composition factors, the corollary follows.

Exercise 5

Let V and V' be isomorphic $\mathbf{C}G$-modules. Prove that the characters they afford are equal.

10 The Number of Simple Modules

In the last section, we found that there are only finitely many simple $\mathbf{C}G$-modules (up to isomorphism). In this section, we show that the number of simple modules is precisely the number of conjugacy classes of G.

Recall that $a, b \in G$ are **conjugate** if $b = g^{-1}ag$ for some $g \in G$. Conjugacy is an equivalence relation on G and hence the equivalence classes (called **conjugacy classes**) partition G. A function $f : G \to \mathbf{C}$ is a **class function** if it is constant on conjugacy classes, that is, $f(g^{-1}ag) = f(a)$ for all $a, g \in G$. Let $\mathrm{Cl}(G) \subseteq \mathrm{Fun}(G, \mathbf{C})$ be the set of all class functions on G. By 8.5(4), $\chi \in \mathrm{Cl}(G)$ for any character χ of G. In particular, $\mathrm{Irr}(G) \subseteq \mathrm{Cl}(G)$. By 9.7, $\mathrm{Irr}(G)$ is linearly independent. We wish to show that, in fact, $\mathrm{Irr}(G)$ is a basis for $\mathrm{Cl}(G)$. First, a lemma.

10.1 *Let V be a simple $\mathbf{C}G$-module affording the character χ. Let $f \in \mathrm{Cl}(G)$ and define $h = \sum_{a \in G} f(a)a : V \to V$. Then $h = \frac{|G|}{n}(f, \bar{\chi})1_V$, where $n = \dim_{\mathbf{C}} V$.*

Proof. We first show that h is a $\mathbf{C}G$-homomorphism. Since h is clearly linear, it suffices to show that $h(bv) = bh(v)$ for all $b \in G$, $v \in V$. We have

$$\begin{aligned} h(bv) &= \sum_{a \in G} f(a)a(bv) = \sum_{a} f(a)bb^{-1}abv \\ &= b\sum_{a} f(b^{-1}ab)b^{-1}abv = b\sum_{c \in G} f(c)cv = bh(v). \end{aligned}$$

By Schur's Lemma (6.2), we have $h = \alpha 1_V$ for some $\alpha \in \mathbf{C}$. But

$$\alpha n = \mathrm{tr}\, h = \sum_{a \in G} f(a)\chi(a) = |G|(f, \bar{\chi}),$$

so the result follows. □

10.2 $\mathrm{Irr}(G)$ *is a basis for* $\mathrm{Cl}(G)$.

Proof. By 9.7, it is enough to show that $\mathrm{Irr}(G)$ spans $\mathrm{Cl}(G)$, and for this, it suffices to show that the orthogonal complement of $\langle \mathrm{Irr}(G) \rangle$ is zero. So let $f \in \mathrm{Cl}(G)$ and assume $(\chi, f) = 0$ for all $\chi \in \mathrm{Irr}(G)$. Let $V = \mathbf{C}G$ and set $h = \sum_{a \in G} \overline{f(a)}a : V \to V$. If S is a simple submodule of V affording the character χ, then 10.1 says that the restriction of h to S equals $\frac{|G|}{n}(\bar{f}, \bar{\chi})1_S$, where $n = \dim_{\mathbf{C}} S$. Since $(\bar{f}, \bar{\chi}) = (\chi, f)$, this restriction is 0.

Now V is a direct sum of simple modules by Maschke's Theorem (7.1), so $h : V \to V$ is the zero map. Hence, $\sum_a \overline{f(a)}a = h(e) = 0$. This implies that $\bar{f}$ (and therefore f) is 0. $\square$

If C is a conjugacy class of G and $f \in \mathrm{Cl}(G)$, we define $f(C) := f(a)$, where a is any element of C. This notation is clearly well-defined. (We get agreement with the usual meaning of $f(C)$ as $\{f(a) \mid a \in C\}$ provided we are willing to identify the number $f(a) \in \mathbf{C}$ with the set $\{f(a)\}$.)

10.3 *The number of isomorphism classes of simple* $\mathbf{C}G$*-modules equals the number of conjugacy classes of* G*.*

Proof. Let $C_1, \ldots, C_t$ be the distinct conjugacy classes of G so that, in particular, $G = \dot{\cup}_i C_i$. For each i, let $f_i \in \mathrm{Cl}(G)$ be defined by $f_i(C_j) = \delta_{ij}$. Then $\{f_i \mid 1 \leq i \leq t\}$ is a basis for $\mathrm{Cl}(G)$. Indeed, if $\sum_i \alpha_i f_i = 0$ ($\alpha_i \in \mathbf{C}$), then $\alpha_j = \sum_i \alpha_i f_i(C_j) = 0$, so the set is linearly independent. Also, if $f \in \mathrm{Cl}(G)$, then $f = \sum_i f(C_i) f_i$, so the set spans. Now 9.6 implies that the number of isomorphism classes of simple $\mathbf{C}G$-modules is $|\mathrm{Irr}(G)|$, and then 10.2 implies $|\mathrm{Irr}(G)| = \dim_{\mathbf{C}} \mathrm{Cl}(G)$. By what we have just shown, $\dim_{\mathbf{C}} \mathrm{Cl}(G)$ is t, the number of conjugacy classes of G. $\square$

11 Further Orthogonality Relations

Let $C_1, \ldots, C_t$ be the distinct conjugacy classes of G and let $\chi_1, \ldots, \chi_t$ be the distinct irreducible characters of G (cf. 10.3).

11.1 $\sum_k \chi_k(C_i)\overline{\chi_k(C_j)} = \dfrac{|G|}{|C_j|}\delta_{ij}$.

PROOF. As in the proof of 10.3, for each $1 \leq j \leq t$, let $f_j \in \mathrm{Cl}(G)$ be given by $f_j(C_i) = \delta_{ij}$. By 10.2, $f_j = \sum_k \alpha_k \chi_k$ for some $\alpha_k \in \mathbf{C}$. Note that

$$\alpha_k = (\sum_i \alpha_i \chi_i, \chi_k) = (f_j, \chi_k) = \frac{1}{|G|}\sum_{a \in G} f_j(a)\overline{\chi_k(a)} = \frac{|C_j|}{|G|}\overline{\chi_k(C_j)},$$

so $f_j = \frac{|C_j|}{|G|}\sum_k \overline{\chi_k(C_j)}\chi_k$. Evaluation at C_i gives the result. □

If χ is a character of G afforded by the $\mathbf{C}G$-module V, then according to 8.5, $\chi(e) = \dim_{\mathbf{C}} V$. The number $\chi(e)$ is called the **degree** of χ. For each $1 \leq i \leq t$, set $n_i = \chi_i(e)$.

11.2 $\displaystyle\sum_{i=1}^{t} n_i^2 = |G|$.

PROOF. If $C_1 = \{e\}$, then

$$\sum_i n_i^2 = \sum_i \chi_i(e)\overline{\chi_i(e)} = \sum_i \chi_i(C_1)\overline{\chi_i(C_1)} = |G|,$$

the last equality from 11.1. □

11.3 *G is abelian if and only if every simple $\mathbf{C}G$-module is one-dimensional.*

PROOF. Assume G is abelian. Then every conjugacy class of G is a singleton, implying G has $|G|$ conjugacy classes. In view of 11.2, this implies $n_i = 1$ for all i. The converse is similar. □

Exercise 6

Prove that the number of irreducible characters of G of degree 1 equals the index in G of its commutator subgroup G'.

12 The Character Table

As in the last section, let $C_1, \ldots, C_t$ be the conjugacy classes of G and let $\chi_1, \ldots, \chi_t$ be the irreducible characters. We always assume that $C_1 = \{e\}$ and that χ_1 is the "trivial character" given by $\chi_1(a) = 1$ for all $a \in G$. (Let $V = \mathbf{C}$. The trivial homomorphism $\rho : G \to \mathrm{GL}(V)$ makes V into a $\mathbf{C}G$-module. This module is clearly simple since its dimension is 1. The character afforded by V is the trivial character as defined above.)

Set $\gamma_{ij} = \chi_i(C_j)$. The matrix $\Gamma = [\gamma_{ij}]$ is called the **character table** of G.

Example. Assume $G = \mathbf{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$. By 10.3 and 11.3, there are four irreducible characters, each of degree one. Now, a character of degree one is afforded by a representation $G \to \mathrm{GL}(\mathbf{C})$ and is therefore nothing more than a homomorphism $G \to \mathbf{C}^\times$. Moreover, the image of this homomorphism is contained in the set of fourth roots of unity which equals $\langle i \rangle = \{1, i, -1, -i\}$, where $i = \sqrt{-1}$. Therefore, the four irreducible characters are given by $\chi_k(\bar{j}) = i^{kj}$, $0 \le k \le 3$. The character table is as follows:

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
χ_0	1	1	1	1
χ_1	1	i	-1	$-i$
χ_2	1	-1	1	-1
χ_3	1	$-i$	-1	i

More generally, if $G = \langle a \rangle$ is cyclic of order n, then G has n irreducible characters, each of degree one, given by $\chi_i(a^j) = \omega^{ij}$ $(0 \le i, j < n)$, where $\omega = e^{2\pi i/n}$, and the character table of G is $[\gamma_{ij}] = [\omega^{ij}]$.

Remark. Of course, two isomorphic groups have the same character table (up to permutations of rows and columns). However, the converse does not hold. Indeed, we will see that the dihedral group D_4 and the quaternion group Q_8 have the same character table, but $D_4 \ncong Q_8$ (Exercise 10).

Set $c_i = |C_i|$. Here are the orthogonality relations from Sections 9 and 11 in the new notation.

12.1 (Orthogonality Relations)

I. $\sum_k c_k \gamma_{ik} \overline{\gamma_{jk}} = |G| \delta_{ij}$,

II. $\sum_k \gamma_{ki} \overline{\gamma_{kj}} = \dfrac{|G|}{c_j} \delta_{ij}$.

Example. To get a feel for the orthogonality relations, the reader could check to see that they hold for the character table of $\mathbf{Z}_4$ given in the example above. Here, we check the case of general cyclic G discussed at the end of that example:

I. We have $\sum_k c_k \gamma_{ik} \overline{\gamma_{jk}} = \sum_k \omega^{ik} \omega^{-jk} = \sum_k (\omega^{i-j})^k$. Now, in general, if $1 \neq \alpha \in \mathbf{C}$, then $1+\alpha+\alpha^2+\cdots+\alpha^{n-1} = \frac{1-\alpha^n}{1-\alpha}$, which can be checked by multiplying both sides by $1-\alpha$. Considering the cases $i = j$ and $i \neq j$ separately, we get $\sum_{k=0}^{n-1} (\omega^{i-j})^k = n\delta_{ij} = |G|\delta_{ij}$.

II. Similarly, $\sum_k \gamma_{ki} \overline{\gamma_{kj}} = \sum_k \omega^{ki} \omega^{-kj} = \sum_k (\omega^{i-j})^k = \frac{|G|}{c_j} \delta_{ij}$.

Example. Assume $G = S_3$, the symmetric group on three letters. First, in any symmetric group S_n, two elements are conjugate if and only if they have the same "cycle type," that is, when written as products of disjoint cycles, they have the same number of cycles of length 2, of length 3, etc. Indeed, if $\sigma, \tau \in S_n$ and $\sigma = (i_1, \ldots, i_s)$, then $\tau\sigma\tau^{-1} = (\tau(i_1), \ldots, \tau(i_s))$ [Hungerford, p. 51], so the statement follows.

Therefore, S_3 has three conjugacy classes: $C_1 = \{1\}$, $C_2 = \{(12), (13), (23)\}$, $C_3 = \{(123), (132)\}$. If χ_1, χ_2, χ_3 are the irreducible characters, then their degrees n_i satisfy $n_1^2 + n_2^2 + n_3^2 = |G| = 6$ by 11.2. Therefore, the degrees are $1, 1$ and 2 and we may assume the notation is chosen so that $n_1 = 1$, $n_2 = 1$, and $n_3 = 2$.

By convention, χ_1 is the trivial character ($\chi_1(a) = 1$ for all $a \in G$). Next, χ_2 is the "sign character" (available for any symmetric group) given by

$$\chi_2(a) = \begin{cases} 1, & \text{if } a \text{ is even,} \\ -1, & \text{if } a \text{ is odd.} \end{cases}$$

All we know about χ_3 so far is that $\chi_3(C_1) = 2$. We can use the orthogonality relations 12.1(II) to find the remaining values:

$$0 = \sum_k \gamma_{k1} \overline{\gamma_{k2}} = 1 - 1 + 2\chi_3(C_2),$$
$$0 = \sum_k \gamma_{k1} \overline{\gamma_{k3}} = 1 + 1 + 2\chi_3(C_3),$$

whence, $\chi_3(C_2) = 0$ and $\chi_3(C_3) = -1$. Therefore, the character table is as follows:

	C_1	C_2	C_3
χ_1	1	1	1
χ_3	1	-1	1
χ_3	2	0	-1

Incidentally, it can be shown that the irreducible character values of *any* symmetric group are always integers.

The statement of the orthogonality relations in 12.1 is probably the best suited for computations, but it lacks symmetry and simplicity. For this reason, the following might be of interest.

A complex $n \times n$-matrix is **unitary** if its conjugate transpose equals its inverse. This is the same as saying that the rows (respectively, columns) of the matrix form an orthonormal set with respect to the standard inner product on $\mathbf{C}^n$: $(\alpha_k) \cdot (\beta_k) = \sum_k \alpha_k \bar{\beta}_k$.

For $1 \le i, j \le t$ let $\gamma'_{ij} = \gamma_{ij}\sqrt{\frac{c_j}{|G|}}$ and put $\Gamma' = [\gamma'_{ij}]$.

12.2 Γ' *is unitary.*

Proof. Computing, we have

$$(\text{row } i) \cdot (\text{row } j) = \sum_k \gamma'_{ik}\overline{\gamma'_{jk}} = \frac{1}{|G|}\sum_k c_k \gamma_{ik}\overline{\gamma_{jk}} = \delta_{ij},$$

$$(\text{col } i) \cdot (\text{col } j) = \sum_k \gamma'_{ki}\overline{\gamma'_{kj}} = \frac{\sqrt{c_i c_j}}{|G|}\sum_k \gamma_{ki}\overline{\gamma_{kj}} = \delta_{ij}. \quad \square$$

13 Direct Products

One of the most powerful tools in finite group theory is induction (usually on the order of the group). So it makes sense to try to relate the representation theory of a group to that of its subgroups. This is what we will be doing in the next several sections.

This relationship is easiest to describe if the chosen subgroup has a complement, that is, if the group is the direct product of two subgroups.

Let G_1 and G_2 be finite groups and throughout this section assume $G = G_1 \times G_2 = \{(a_1, a_2) \mid a_i \in G_i\}$. If V_i is a $\mathbf{C}G_i$-module, then $V_1 \otimes V_2$ becomes a $\mathbf{C}G$-module by defining $(a_1, a_2)(v_1 \otimes v_2) = a_1 v_1 \otimes a_2 v_2$ and extending linearly.

Remark. This is different from the tensor product of modules we considered earlier, for in that case, V_1 and V_2 were both modules for the same algebra $\mathbf{C}H$ and $V_1 \otimes V_2$ became a $\mathbf{C}H$-module by defining $h(v_1 \otimes v_2) = hv_1 \otimes hv_2$. Here is the connection: This $\mathbf{C}H$-module $V_1 \otimes V_2$ corresponds to a representation that is really the composition $H \to H \times H \to \mathrm{GL}(V_1 \otimes V_2)$, where the first map is the diagonal map $h \mapsto (h, h)$ and the second is the representation afforded by the $\mathbf{C}(H \times H)$-module as described above.

13.1 *If χ_i is the character of G_i afforded by the $\mathbf{C}G_i$-module V_i $(i = 1, 2)$, then the map $(\chi_1, \chi_2) : G \to \mathbf{C}$ given by $(\chi_1, \chi_2)(a_1, a_2) = \chi_1(a_1)\chi_2(a_2)$ is the character of G afforded by $V_1 \otimes V_2$.*

Proof. The proof is similar to that of 8.4(ii). □

13.2 *If χ is a character of a finite group, then χ is irreducible if and only if $\|\chi\| = 1$ (where $\|\chi\| := (\chi, \chi)^{1/2}$).*

Proof. Let χ be a character of a finite group. Write $\chi = \sum_i n_i \chi_i$, where $\{\chi_i\}$ are the distinct irreducible characters of the group and the n_i are nonnegative integers. Then

$$\|\chi\|^2 = \sum_{i,j} n_i n_j (\chi_i, \chi_j) = \sum_i n_i^2.$$

The result follows. □

13.3 $\mathrm{Irr}(G) = \mathrm{Irr}(G_1) \times \mathrm{Irr}(G_2)$.

PROOF. Let $(\chi_1, \chi_2) \in \mathrm{Irr}(G_1) \times \mathrm{Irr}(G_2)$. Then

$$\begin{aligned}
\|(\chi_1, \chi_2)\|^2 &= \frac{1}{|G|} \sum_{(a_1,a_2)} (\chi_1, \chi_2)(a_1, a_2)\overline{(\chi_1, \chi_2)(a_1, a_2)} \\
&= \frac{1}{|G|} \sum_{(a_1,a_2)} \chi_1(a_1)\chi_2(a_2)\overline{\chi_1(a_1)}\,\overline{\chi_2(a_2)} \\
&= \frac{1}{|G_1|} \sum_{a_1} \chi_1(a_1)\overline{\chi_1(a_1)} \cdot \frac{1}{|G_2|} \sum_{a_2} \chi_2(a_2)\overline{\chi_2(a_2)} \\
&= \|\chi_1\|^2 \|\chi_2\|^2 \\
&= 1,
\end{aligned}$$

so $(\chi_1, \chi_2) \in \mathrm{Irr}(G)$ by 13.1 and 13.2. Therefore, $\mathrm{Irr}(G_1) \times \mathrm{Irr}(G_2) \subseteq \mathrm{Irr}(G)$.

To show equality, it is enough, according to 11.2, to show that the sum of the squares of the degrees of the various (χ_1, χ_2) is $|G|$. We have,

$$\sum_{(\chi_1,\chi_2)} [(\chi_1, \chi_2)(e_1, e_2)]^2 = \sum_{\chi_1} (\chi_1(e_1))^2 \cdot \sum_{\chi_2} (\chi_2(e_2))^2 = |G_1||G_2| = |G| \quad \square.$$

14 A More General Tensor Product

For the definition of an induced module in the next section, we need a generalization of the notion of tensor product of two vector spaces as introduced in Section 3. The construction requires no special properties of the field, so we again work with an arbitrary field K.

Let S be an algebra with identity over K. Let N be a left S-module and let M be a right S-module (so M is an abelian group equipped with a product $(m, s) \mapsto ms$ ($m \in M$, $s \in S$) satisfying the right-sided analogs of the four module axioms on p. 2). We denote this situation by ${}_SN$, M_S.

Recall that M and N are vector spaces over K. Let $\{m_i\}$ and $\{n_j\}$ be bases of M and N, respectively. Then, as in Section 3, $M \otimes N$ denotes the vector space over K with basis $\{m_i \otimes n_j\}$. Also as in that section, we put $m \otimes n = \sum_{i,j} \alpha_i \beta_j m_i \otimes n_j$ for arbitrary $m = \sum_i \alpha_i m_i \in M$ and $n = \sum_j \beta_j n_j \in N$. With this definition, it is easily checked that $m \otimes n$ is linear in each factor (meaning $(m+m') \otimes n = m \otimes n + m' \otimes n$, $(\alpha m) \otimes n = \alpha(m \otimes n)$, and similarly for the second factor).

The vector space $M \otimes N$ can be regarded as a device for changing bilinear maps into linear maps. Indeed, if V is a vector space over K and if $f : M \times N \to V$ is a bilinear map, then there is a unique linear map $\bar{f} : M \otimes N \to V$ satisfying $\bar{f}(m \otimes n) = f(m, n)$. (To see this, put $\bar{f}(m_i \otimes n_j) = f(m_i, n_j)$, extend this definition linearly to $M \otimes N$, and then show that the desired formula holds.)

Let W be the subspace of $M \otimes N$ generated by all vectors of the form $m \otimes sn - ms \otimes n$ with $m \in M$, $n \in N$, and $s \in S$ and define

$$M \otimes_S N = M \otimes N / W.$$

We denote the coset $m \otimes n + W$ by $m \otimes_S n$. Note that $m \otimes_S n$ is linear in each factor and that $m \otimes_S sn = ms \otimes_S n$ for all $m \in M$, $n \in N$, and $s \in S$.

14.1 *Let M_S, M'_S, ${}_SN$, ${}_SN'$ be S-modules as indicated. There are vector space isomorphisms as follows:*

(1) $(M \oplus M') \otimes_S N \cong (M \otimes_S N) \oplus (M' \otimes_S N)$,
(2) $M \otimes_S (N \oplus N') \cong (M \otimes_S N) \oplus (M \otimes_S N')$,
(3) $S \otimes_S N \cong N$,
(4) $M \otimes_S S \cong M$.

Proof. (1) One checks that the function $(M \oplus M') \times N \to (M \otimes_S N) \oplus (M' \otimes_S N)$ given by

$$((m, m'), n) \longmapsto (m \otimes_S n, m' \otimes_S n)$$

is bilinear. Therefore, according to the comments above, we get a unique linear map $\varphi : (M \oplus M') \otimes N \to (M \otimes_S N) \oplus (M' \otimes_S N)$ satisfying

$$\varphi((m, m') \otimes n) = (m \otimes_S n, m' \otimes_S n)$$

($m \in M$, $m' \in M'$, $n \in N$). In particular, this formula implies that for each $s \in S$

$$\varphi\big((m, m')s \otimes n - (m, m') \otimes sn\big) = 0,$$

so φ induces a well-defined linear map $\bar{\varphi} : (M \oplus M') \otimes_S N \to (M \otimes_S N) \oplus (M' \otimes_S N)$ satisfying

$$\bar{\varphi}((m, m') \otimes_S n) = (m \otimes_S n, m' \otimes_S n).$$

Similarly, we get a linear map $\bar{\psi} : (M \otimes_S N) \oplus (M' \otimes_S N) \to (M \oplus M') \otimes_S N$ satisfying

$$\bar{\psi}((m \otimes_S n, m' \otimes_S n')) = (m, 0) \otimes_S n + (0, m') \otimes_S n'.$$

One easily checks that $\bar{\psi}\bar{\varphi} = 1$ and $\bar{\varphi}\bar{\psi} = 1$. In particular, $\bar{\varphi}$ is an isomorphism. The proof of (2) is similar.

(3) Proceed as above to get linear maps $\bar{\varphi} : S \otimes_S N \to N$ and $\bar{\psi} : N \to S \otimes_S N$ satisfying $\bar{\varphi}(s \otimes_S n) = sn$ and $\bar{\psi}(n) = 1 \otimes_S n$, and then check that both compositions give the identity map. The proof of (4) is similar. □

Let R and S be algebras with identity over K. An (R, S)**-bimodule** is an abelian group M that is both a left R-module and a right S-module such that $(rm)s = r(ms)$ for all $r \in R$, $s \in S$, $m \in M$. To indicate such a bimodule, we write ${}_RM_S$.

Let ${}_RM_S$ and ${}_SN$ be modules as indicated. The vector space $M \otimes N$ becomes a left R-module if we define $r(m \otimes n) = (rm) \otimes n$. As before, let W be the subspace of $M \otimes N$ generated by all vectors of the form $m \otimes sn - ms \otimes n$ with $m \in M$, $n \in N$, $s \in S$. Then W is an R-submodule of $M \otimes N$ since, for $r \in R$, we have

$$r(m \otimes sn - ms \otimes n) = rm \otimes sn - r(ms) \otimes n = rm \otimes sn - (rm)s \otimes n \in W.$$

Therefore, $M \otimes_S N = M \otimes N/W$ becomes an R-module by defining $r(m \otimes_S n) = (rm) \otimes_S n$.

14.2 *Let L_R, ${}_RM_S$, ${}_SN$ be modules as indicated. Then $L \otimes_R (M \otimes_S N) \cong (L \otimes_R M) \otimes_S N$ as vector spaces.*

Proof. In general, if U, V, and W are vector spaces with $W < V$, then $U \otimes (V/W) \cong U \otimes V/U \otimes W$ by $u \otimes \overline{v} \leftrightarrow \overline{u \otimes v}$, where bars represent cosets.

There is a linear map $L \otimes (M \otimes N) \to (L \otimes_R M) \otimes_S N$ that sends $l \otimes (m \otimes n)$ to $(l \otimes_R m) \otimes_S n$. Indeed, if for fixed $l \in L$ we define $f_l : M \otimes N \to (L \otimes_R M) \otimes_S N$ by $f_l(m \otimes n) = (l \otimes_R m) \otimes_S n$, then we get a linear map $L \otimes (M \otimes N) \to (L \otimes_R M) \otimes_S N$ that sends $l \otimes x$ to $f_l(x)$ ($x \in M \otimes N$). Using the previous paragraph and then this map (together with the Fundamental Homomorphism Theorem), we get linear maps

$$L \otimes (M \otimes_S N) = L \otimes (M \otimes N/W) \cong L \otimes (M \otimes N)/L \otimes W \to (L \otimes_R M) \otimes_S N$$

(W as before the statement of this theorem) that sends $l \otimes (m \otimes_S n)$ to $(l \otimes_R m) \otimes_S n$. In turn, this composition induces a linear map

$$L \otimes_R (M \otimes_S N) \to (L \otimes_R M) \otimes_S N$$

that sends $l \otimes_R (m \otimes_S n)$ to $(l \otimes_R m) \otimes_S n$.

We get a similar map in the other direction and each composition gives the identity map. $\square$

Exercise 7

Let the notation be as at the first of this section. A linear map $f : M \otimes N \to V$ (V a vector space over K) is **middle linear** if $f(m \otimes sn) = f(ms \otimes n)$ for all $m \in M$, $n \in N$, $s \in S$. Let $\mathcal{C}$ be the category defined as follows: The objects are pairs (V, f) where V is a vector space over K and $f : M \otimes N \to V$ is a middle linear map; a morphism $(V, f) \to (V', f')$ is a linear map $\varphi : V \to V'$ such that $\varphi \circ f = f'$. Let $\pi : M \otimes N \to M \otimes_S N$ be the canonical epimorphism. Prove that $(M \otimes_S N, \pi)$ is a universal (=initial) object of $\mathcal{C}$ [Hungerford, p. 57].

15 Induced Modules

Let H be a subgroup of G. Then $\mathbf{C}H$ is a subalgebra of $\mathbf{C}G$. Moreover, $\mathbf{C}G$ is a $(\mathbf{C}G, \mathbf{C}H)$-bimodule. Therefore, if N is a $\mathbf{C}H$-module, we get a $\mathbf{C}G$-module

$$N^G := \mathbf{C}G \otimes_{\mathbf{C}H} N$$

called an **induced module**. In this section, we will study the structure of this module and relate the representation and character it affords to those afforded by N.

Fix a set $\{a_1, \ldots, a_r\}$ of representatives of the left cosets of H in G, so that $G = \dot\cup_i a_i H$. Below, we write $a \otimes n$ for the tensor $a \otimes_{\mathbf{C}H} n \in N^G$.

15.1 *Let the notation be as above.*

(1) $\dim_{\mathbf{C}} N^G = [G : H] \dim_{\mathbf{C}} N$,
(2) N^G *has basis* $\{a_i \otimes n_k\}$, *where* $\{n_k\}$ *is a basis for* N.

Proof. (1) First note that $\mathbf{C}G = \dot\sum_i a_i \mathbf{C}H$, since $G = \dot\cup_i a_i H$ and the subspace of $\mathbf{C}G$ generated by $a_i H$ is $a_i \mathbf{C}H$. Now each $a_i \mathbf{C}H$ is isomorphic to $\mathbf{C}H$ as right $\mathbf{C}H$-module, so we have $\mathbf{C}G \cong \bigoplus_{i=1}^r \mathbf{C}H$ as right $\mathbf{C}H$-modules. Using 14.1, we get vector space isomorphisms $N^G = \mathbf{C}G \otimes_{\mathbf{C}H} N \cong \bigoplus_i (\mathbf{C}H \otimes_{\mathbf{C}H} N) \cong \bigoplus_i N$. Hence $\dim_{\mathbf{C}} N^G = r \dim_{\mathbf{C}} N$, as desired.

(2) By part (1), it is enough to show that this set spans N^G. Let $a \in G$. Then $a = a_i h$ for some i and some $h \in H$. Hence, for any $n \in N$, we get

$$a \otimes n = a_i \otimes hn = a_i \otimes (\sum_k \alpha_k n_k) = \sum_k \alpha_k (a_i \otimes n_k),$$

where $hn = \sum_k \alpha_k n_k$. Since N^G is spanned by elements of the form $a \otimes n$, the proof is complete. □

15.2 *Let the notation be as above. Let R be the matrix representation of H afforded by N relative to the basis $\{n_1, \ldots, n_s\}$. For each $a \in G$ and $1 \le i, j \le r$, set $R_{ij}(a) = R(a_i^{-1} a a_j)$, where we define $R(g) := 0$ if $g \notin H$. Then $R^G := [R_{ij}]$ is the matrix representation of G afforded by the induced module N^G relative to the basis $\{a_i \otimes n_k\}$ (ordered lexicographically).*

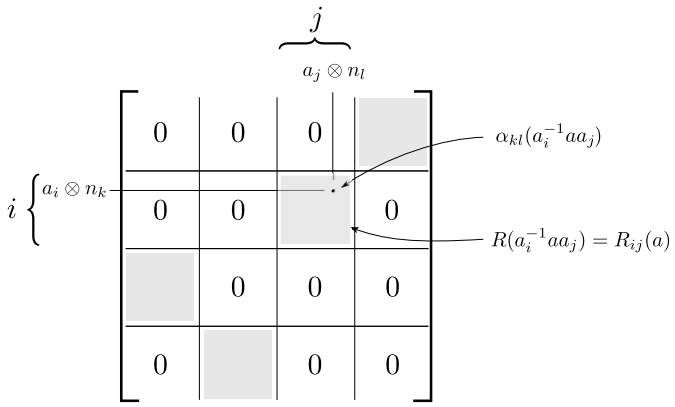
Proof. Write $R = [\alpha_{kl}]$ so that $hn_l = \sum_k \alpha_{kl}(h) n_k$ for each $h \in H$. Now let $a \in G$ and fix $1 \le j \le r$. Then $aa_j = a_i h$ for some uniquely determined $1 \le i \le r$ and $h \in H$.

Note that $h = a_i^{-1}aa_j$. Hence, for any $1 \le l \le s$ we have,

$$a(a_j \otimes n_l) = a_i h \otimes n_l = a_i \otimes hn_l = a_i \otimes (\sum_k \alpha_{kl}(h)n_k)$$
$$= \sum_k \alpha_{kl}(a_i^{-1}aa_j)a_i \otimes n_k.$$

Therefore, we have the following picture:

$R^G(a) \;=\;$



Note that if $i' \ne i$, then $a_{i'}^{-1}aa_j \notin H$ so that $R_{i'j}(a) = 0$. This proves the theorem. □

If the $\mathbf{C}H$-module N affords the character χ, then we write χ^G for the character afforded by the induced module N^G and call it an **induced character**.

15.3 *With the notation as above, we have*

$$\chi^G(a) = \frac{1}{|H|}\sum_{g\in G}\chi(g^{-1}ag),$$

where $\chi(b) := 0$ *if* $b \notin H$.

Proof. Using 15.2, we get

$$\chi^G(a) = \operatorname{tr} R^G(a) = \sum_i \operatorname{tr} R_{ii}(a) = \sum_i \operatorname{tr} R(a_i^{-1}aa_i) = \sum_i \chi(a_i^{-1}aa_i).$$

Now, if $h \in H$, then 8.5(4) says $\chi(a_i^{-1}aa_i) = \chi(h^{-1}a_i^{-1}aa_ih)$, so we have

$$\chi^G(a) = \frac{1}{|H|}\sum_{h\in H}\sum_i \chi\big((a_ih)^{-1}a(a_ih)\big) = \frac{1}{|H|}\sum_{g\in G}\chi(g^{-1}ag). \quad \square$$

15.4 (Additivity of Induction) *If N and N' are $\mathbf{C}H$-modules, then $(N \oplus N')^G \cong N^G \oplus {N'}^G$. In particular, if χ and χ' are characters of H, then $(\chi + \chi')^G = \chi^G + {\chi'}^G$.*

Proof. Using 14.1(2) we get a vector space isomorphism

$$(N \oplus N')^G = \mathbf{C}G \otimes_{\mathbf{C}H} (N \oplus N') \cong (\mathbf{C}G \otimes_{\mathbf{C}H} N) \oplus (\mathbf{C}G \otimes_{\mathbf{C}H} N') = N^G \oplus {N'}^G.$$

It is easy to check that this isomorphism is actually a $\mathbf{C}G$-isomorphism. The statement about characters now follows from 8.4(1) $\square$

15.5 (Transitivity of Induction) *If $H \leq J \leq G$ and N is a $\mathbf{C}H$-module, then $(N^J)^G \cong N^G$. In particular, if χ is a character of H, then $(\chi^J)^G = \chi^G$.*

Proof. We have by definition

$$(N^J)^G = \mathbf{C}G \otimes_{\mathbf{C}J} (\mathbf{C}J \otimes_{\mathbf{C}H} N).$$

By 14.2, the expression on the right is isomorphic as vector space to $(\mathbf{C}G \otimes_{\mathbf{C}J} \mathbf{C}J) \otimes_{\mathbf{C}H} N$, and the isomorphism in the proof of that result is easily seen to be a (left) $\mathbf{C}G$-isomorphism. In turn, the vector space isomorphism $\mathbf{C}G \otimes_{\mathbf{C}J} \mathbf{C}J \cong \mathbf{C}G$ of 14.1(4) is clearly an isomorphism of $(\mathbf{C}G, \mathbf{C}H)$-bimodules. Therefore,

$$(N^J)^G \cong (\mathbf{C}G \otimes_{\mathbf{C}J} \mathbf{C}J) \otimes_{\mathbf{C}H} N \cong \mathbf{C}G \otimes_{\mathbf{C}H} N = N^G. \quad \square$$

16 Frobenius Reciprocity

Let H be a subgroup of G, let M be a simple $\mathbf{C}G$-module and let N be a simple $\mathbf{C}H$-module. The module M viewed as a $\mathbf{C}H$-module (denoted M_H) might not be simple, but Maschke's Theorem (7.1) says it is at least isomorphic to a direct sum of simple modules. Similarly, N^G is isomorphic to a direct sum of simple modules. "Frobenius Reciprocity" states that the number of times N occurs as a direct summand of M_H is the same as the number of times M occurs as a direct summand of N^G. This can be proved by a straightforward character computation (see remark after 16.5), but we will give a more conceptual module-theoretic proof.

For the time being, let K be any field and let R be a K-algebra with identity. For (left) R-modules L and M, denote by $\mathrm{Hom}_R(L, M)$ the set of all R-homomorphisms from L to M. This set is a vector space over K with operations coming from those on M.

16.1 *Let L, L', M, and M' be R-modules. There are vector space isomorphisms as follows:*

(1) $\mathrm{Hom}_R(L \oplus L', M) \cong \mathrm{Hom}_R(L, M) \oplus \mathrm{Hom}_R(L', M)$,
(2) $\mathrm{Hom}_R(L, M \oplus M') \cong \mathrm{Hom}_R(L, M) \oplus \mathrm{Hom}_R(L, M')$,
(3) $\mathrm{Hom}_R(R, M) \cong M$.

Warning: In general, $\mathrm{Hom}_R(M, R) \ncong M$.

Proof. (1) The desired isomorphism is obtained by sending f to the pair $(f \circ \iota_L, f \circ \iota_{L'})$ $(= (f|_L, f|_{L'}))$, where ι_L (respectively, $\iota_{L'}$) is the usual injection.

(2) The desired isomorphism is obtained by sending f to the pair $(\pi_M \circ f, \pi_{M'} \circ f)$, where π_M (respectively, $\pi_{M'}$) is the usual projection.

(3) Here, define $\varphi : \mathrm{Hom}_R(R, M) \to M$ by $\varphi(f) = f(1)$. Clearly, φ is a monomorphism. For $m \in M$, define $f_m : R \to M$ by $f_m(r) = rm$. Then $f_m \in \mathrm{Hom}_R(R, M)$ and $\varphi(f_m) = m$, so φ is surjective. $\square$

Now let S be another K-algebra with identity and suppose we have modules ${}_RL_S$ and ${}_RM$ as indicated. Then $\mathrm{Hom}(L, M)$ (= space of K-linear maps from L to M) becomes an S-module if we define $(sf)(l) = f(ls)$ ($f \in \mathrm{Hom}(L, M)$, $s \in S$, $l \in L$). Moreover, $\mathrm{Hom}_R(L, M)$ is an S-submodule of $\mathrm{Hom}(L, M)$, for if $f \in \mathrm{Hom}_R(L, M)$, then

$$(sf)(rl) = f\big((rl)s\big) = f\big(r(ls)\big) = r\big(f(ls)\big) = r\big((sf)(l)\big).$$

Note the similarities between these homomorphism modules and the tensor products discussed earlier. Of course, there are the results 14.1 and 16.1. But also, $\mathrm{Hom}_R(L, M)$ is

an S-submodule of $\mathrm{Hom}(L, M)$ while, given modules ${}_RM_S$ and ${}_SN$ as indicated, $M \otimes_S N$ is a quotient of the R-module $M \otimes N$. Since submodules and quotients are dual concepts, this suggests the same of homomorphism modules and tensor products. The following theorem expresses an explicit relationship between these modules.

16.2 (Adjoint Associativity) *Let ${}_RL_S$, ${}_RM$, and ${}_SN$ be modules as indicated. There is a vector space isomorphism*

$$\mathrm{Hom}_R(L \otimes_S N, M) \cong \mathrm{Hom}_S(N, \mathrm{Hom}_R(L, M)).$$

Proof. See Exercise 8 below. □

We now return to a discussion of modules for group algebras over the field of complex numbers. Given $\mathbf{C}G$-modules M and M', we put

$$\iota_{\mathbf{C}G}(M, M') := \dim_{\mathbf{C}} \mathrm{Hom}_{\mathbf{C}G}(M, M')$$

and call this number the **intertwining number** of M and M'. According to 16.1, this number is "additive" in each component, meaning

$$\iota_{\mathbf{C}G}(M_1 \oplus M_2, M') = \iota_{\mathbf{C}G}(M_1, M') + \iota_{\mathbf{C}G}(M_2, M'),$$

and similarly in the second component.

16.3 *Let the notation be as above. If M and M' afford the characters χ and χ', respectively, then $\iota_{\mathbf{C}G}(M, M') = (\chi, \chi')$. In particular, if M' is simple, then $\iota_{\mathbf{C}G}(M, M')$ is the multiplicity of M' as a direct summand of M, and similarly, if M is simple, then $\iota_{\mathbf{C}G}(M, M')$ is the multiplicity of M as a direct summand of M'.*

Proof. By Maschke's Theorem (7.1) we can write $M \cong \bigoplus_i m_i M_i$ and $M' \cong \bigoplus_i m_i' M_i$ with the M_i pairwise nonisomorphic simple modules and the m_i and m_i' nonnegative integers. According to Schur's Lemma (6.2), we have

$$\mathrm{Hom}_{\mathbf{C}G}(M_i, M_j) \cong \begin{cases} \mathbf{C}, & i = j, \\ 0, & i \neq j, \end{cases}$$

so that $\iota_{\mathbf{C}G}(M_i, M_j) = \delta_{ij}$. Using the additivity in each component of the intertwining number, we obtain

$$\iota_{\mathbf{C}G}(M, M') = \sum_{i,j} m_i m_j' \iota_{\mathbf{C}G}(M_i, M_j) = \sum_i m_i m_i'.$$

On the other hand, if χ and χ' are the characters afforded by M and M', respectively, and χ_i is the (irreducible) character afforded by M_i, then 8.4 gives $\chi = \sum_i m_i \chi_i$ and $\chi' = \sum_i m_i' \chi_i$, so that

$$(\chi, \chi') = \sum_{i,j} m_i m_j' (\chi_i, \chi_j) = \sum_i m_i m_i',$$

where we have used 9.7. This gives the first statement. The second now follows from 9.5. □

16.4 (Frobenius Reciprocity for Modules) *Let H be a subgroup of G, let M be a simple $\mathbf{C}G$-module and let N be a simple $\mathbf{C}H$-module. The multiplicity of N as a direct summand of M_H equals the multiplicity of M as a direct summand of N^G.*

Proof. It is easy to see that the isomorphism $\mathrm{Hom}_{\mathbf{C}G}(\mathbf{C}G, M) \cong M$ of 16.1 is actually a $\mathbf{C}H$-isomorphism (viewing $\mathbf{C}G$ as a $(\mathbf{C}G, \mathbf{C}H)$-bimodule and hence $\mathrm{Hom}_{\mathbf{C}G}(\mathbf{C}G, M)$ as a $\mathbf{C}H$-module). Therefore, 16.2 gives $\mathrm{Hom}_{\mathbf{C}G}(N^G, M) \cong \mathrm{Hom}_{\mathbf{C}H}(N, M)$, so that $\iota_{\mathbf{C}G}(N^G, M) = \iota_{\mathbf{C}H}(N, M_H)$. The result now follows from 16.3. □

Given a class function χ on G and a subgroup H of G, we denote by χ_H the restriction of χ to H (manifestly a class function on H). If the $\mathbf{C}G$-module M affords the character χ, then the $\mathbf{C}H$-module M_H affords the character χ_H.

16.5 (Frobenius Reciprocity for Characters) *Let H be a subgroup of G, let χ be a character of G and let λ be a character of H. Then $(\lambda^G, \chi) = (\lambda, \chi_H)$.*

Proof. First note that restriction and induction of characters are both additive, that is, $(\chi+\chi')_H = \chi_H + \chi'_H$ (clearly) and $(\lambda+\lambda')^G = \lambda^G + \lambda'^G$ (by 15.3, for instance). Hence, we may assume that χ and λ are both irreducible. The result now follows from 16.4 and 9.5. □

Remark. Let H be a subgroup of G. For an arbitrary class function λ on H, we define a class function λ^G on G be means of

$$\lambda^G(a) = \frac{1}{|H|} \sum_{g \in G} \lambda^0(g^{-1}ag),$$

where

$$\lambda^0(b) = \begin{cases} \lambda(b), & b \in H, \\ 0, & b \notin H. \end{cases}$$

By 15.3, this notation agrees with the earlier notation in the case λ is a character.

Using 10.2 and 16.5, it is easy to show that the formula $(\lambda^G, \chi) = (\lambda, \chi_H)$ holds for arbitrary class functions $\chi \in \mathrm{Cl}(G)$, $\lambda \in \mathrm{Cl}(H)$. We also give a proof of this using the definitions alone. Computing, we have

$$\begin{aligned} (\lambda^G, \chi) &= \frac{1}{|G|} \sum_{a \in G} \lambda^G(a)\overline{\chi(a)} \\ &= \frac{1}{|G|} \sum_{a \in G} \frac{1}{|H|} \sum_{g \in G} \lambda^0(g^{-1}ag)\overline{\chi(a)} \\ &= \frac{1}{|H|}\frac{1}{|G|} \sum_{g \in G} \sum_{a \in G} \lambda^0(g^{-1}ag)\overline{\chi(g^{-1}ag)} \\ &= \frac{1}{|H|}\frac{1}{|G|} \sum_{g \in G} \sum_{b \in G} \lambda^0(b)\overline{\chi(b)} \end{aligned}$$

$$= \frac{1}{|H|} \sum_{b \in H} \lambda(b)\overline{\chi(b)}$$
$$= (\lambda, \chi_H),$$

where we have used that $\lambda^0(G\backslash H) = 0$ for the penultimate equality.

Exercise 8

Prove 16.2. (Hint: Define maps in both directions and show that the compositions are the respective identity maps. Do not bother to check linearity of the various maps involved. Note, however, that you need to check that your maps are well-defined in the sense that they map into the indicated spaces. Also, since $L \otimes_S N$ is a quotient space, you may need to check that your definitions are independent of the chosen coset representative.)

17 Clifford Theory

Clifford theory relates the representations of a group to those of a normal subgroup. The main theorem (17.3), due to Clifford, says that the restriction of a simple module to a normal subgroup is isomorphic to the direct sum of a full conjugacy class of simple modules (or possibly a direct sum of several copies of such).

We need some preliminaries. The first result gives a way to detect induced modules.

17.1 *Let H be a subgroup of G, let M be a $\mathbf{C}G$-module, and let L be a submodule of M_H. If $M = \dot{\sum}_{a\in A} aL$, where A is a set of representatives for the left cosets of H in G, then $M \cong L^G$.*

Proof. Assume the hypotheses. Define $\varphi : \mathbf{C}G \otimes L \to M$ by $s \otimes l \mapsto sl$ ($s \in \mathbf{C}G$, $l \in L$). This is a $\mathbf{C}G$-homomorphism; it is clearly surjective by our assumption on M. Note that

$$\varphi(s \otimes hl) = s(hl) = (sh)l = \varphi(sh \otimes l)$$

($s \in \mathbf{C}G$, $h \in H$, $l \in L$), so we get an induced $\mathbf{C}G$-epimorphism $\bar{\varphi} : L^G = \mathbf{C}G \otimes_{\mathbf{C}H} L \to M$. By 15.1, $\dim_{\mathbf{C}} L^G = [G : H] \dim_{\mathbf{C}} L$. This is also the dimension of M by our assumption, so $\bar{\varphi}$ is an isomorphism. □

Let M be a $\mathbf{C}G$-module and let L be a simple submodule of M. The submodule

$$\tilde{L} := \sum_{\substack{L' \le M \\ L' \cong L}} L' \le M$$

is called the **homogeneous component of M containing L.**

17.2 *Let the notation be as above.*

(1) *$\tilde{L} \cong \bigoplus_{i=1}^{t} L$ for some positive integer t.*

(2) *If L' is another simple submodule of M, then $\tilde{L}' = \tilde{L}$ if and only if $L' \cong L$.*

(3) *$M = \dot{\sum}_{N\in\mathcal{N}} N$, where $\mathcal{N}$ is the set of homogeneous components of M.*

Proof. (1) Let $\{L_1, \ldots, L_t\}$ be a collection of submodules of M with $L_i \cong L$ and $L_i \cap \sum_{j\neq i} L_j = \{0\}$ for each i. Since $\dim_{\mathbf{C}} \sum_i L_i = t \dim_{\mathbf{C}} L$, it is clear that there is a maximal such set, which we assume without loss of generality to be $\{L_1, \ldots, L_t\}$. Let L_{t+1} be a submodule of M with $L_{t+1} \cong L$. Then $L_{t+1} \subseteq \sum_{i=1}^{t} L_i$. Indeed, if this were not the case, then, since L_{t+1} is simple, we would have $L_{t+1} \cap \left(\sum_{i=1}^{t} L_i\right) = \{0\}$ and then

$L_i \cap \sum_{j\neq i} L_j = \{0\}$ for all $1 \leq i \leq t+1$, contradicting maximality of the set $\{L_1, \ldots, L_t\}$. It now follows that $\tilde{L} = \dot{\sum}_i L_i \cong \bigoplus_{i=1}^{t} L_i$.

(2) Let L' be another simple submodule of M and assume $\tilde{L'} = \tilde{L}$. By part (1), we have $\bigoplus_{i=1}^{t'} L' \cong \bigoplus_{i=1}^{t} L$ for some positive integers t and t'. Since the summands in a direct sum of simple modules are the composition factors of the sum, the uniqueness of composition factors guaranteed by the Jordan-Hölder Theorem implies $L' \cong L$. The converse is clear.

(3) By Maschke's Theorem, M is the internal direct sum of a collection of its simple submodules, and, since each simple submodule is contained in its own homogeneous component, we have $M = \sum_{N\in\mathcal{N}} N$. We just need to show that this sum is direct. Fix $N \in \mathcal{N}$. We have $N = \tilde{L}$ for some simple submodule L of M. By part (1), every composition factor, and hence every simple submodule, of N is isomorphic to L. On the other hand, if $N' \in \mathcal{N}$ and $N' \neq N$, then by parts (1) and (2), no composition factor of N' is isomorphic to L. Since the sum $\sum_{\substack{N'\in\mathcal{N}\\ N'\neq N}} N'$ is a homomorphic image of the direct sum $\bigoplus_{\substack{N'\in\mathcal{N}\\ N'\neq N}} N'$, it follows that it has no composition factor, and hence no submodule, isomorphic to L. Therefore,

$$N \cap \sum_{\substack{N'\in\mathcal{N}\\ N'\neq N}} N' = \{0\},$$

and the result follows. □

Let H be a subgroup of G and let $a \in G$. For $h \in H$ put ${}^a h = aha^{-1}$ and define ${}^a H = \{{}^a h \mid h \in H\} = aHa^{-1}$. Let L be a $\mathbf{C}H$-module. The **conjugate of L by a** is the $\mathbf{C}({}^a H)$-module ${}^a L$ that has as underlying vector space L and as action ${}^a h \cdot l = hl$ ($h \in H$, $l \in L$). It is easy to see that ${}^a L$ is simple if and only if L is simple. Note that if $H \lhd G$, then ${}^a L$ is a $\mathbf{C}H$-module.

17.3 (Clifford's Theorem for Modules) *Let M be a simple $\mathbf{C}G$-module, let $H \lhd G$, and let L be a simple submodule of M_H. Set $\tilde{H} = \{a \in G \mid a\tilde{L} = \tilde{L}\} \leq G$ and let A be a set of representatives for the left cosets of $\tilde{H}$ in G.*

(1) *$\{{}^a L\}_{a\in A}$ is a complete set of pairwise nonisomorphic conjugates of L.*
(2) *$M_H \cong t\left(\bigoplus_{a\in A} {}^a L\right)$, where t is the multiplicity of L as a summand of M_H.*
(3) *$\tilde{L}$ is a $\mathbf{C}\tilde{H}$-submodule of $M_{\tilde{H}}$. We have $\tilde{L}_H \cong \bigoplus_{i=1}^{t} L$ and $\tilde{L}^G \cong M$.*

Proof. Step 1: *For each $a \in G$, we have $aL \cong {}^a L$ as $\mathbf{C}H$-modules.* First note that $HaL = aa^{-1}HaL = aL$, so aL is indeed a $\mathbf{C}H$-module. Define $\varphi : {}^a L \to aL$ by $\varphi(l) = al$. This is clearly a vector space isomorphism. For $h \in H$, we have

$$\varphi(h \cdot l) = \varphi({}^a(a^{-1}ha) \cdot l) = \varphi(a^{-1}hal) = aa^{-1}hal = hal = h\varphi(l),$$

so φ is a $\mathbf{C}H$-isomorphism.

Step 2: *We have $M = \sum_{a\in G} aL$.* For each $b \in G$, we have $b\sum_a aL = \sum_a baL = \sum_a aL$, so $\sum_{a\in G} aL$ is a $\mathbf{C}G$-submodule of M. It contains $L = eL$ (assuming that $e \in A$, which we can do without loss of generality) and is hence nonzero. Since M is simple, the result follows.

Step 3: *For each $a \in G$, we have $a\tilde{L} = \widetilde{aL}$.* Let $a \in G$. By Step 1, aL is isomorphic to ${}^aL$ and is hence simple. Thus $\widetilde{aL}$ is defined. Now

$$a\tilde{L} = a \sum_{\substack{L' \le M_H \\ L' \cong L}} L' = \sum_{\substack{L' \le M_H \\ L' \cong L}} aL' \subseteq \sum_{\substack{L' \le M_H \\ L' \cong aL}} L' = \widetilde{aL},$$

so $a\tilde{L} \subseteq \widetilde{aL}$. This, in turn, implies

$$\widetilde{aL} = aa^{-1}\widetilde{aL} \subseteq \widetilde{aa^{-1}aL} = a\tilde{L}.$$

Step 4: $\widetilde{aL} = \widetilde{bL}$ *if and only if* $a\tilde{H} = b\tilde{H}$. Indeed,

$$\widetilde{aL} = \widetilde{bL} \iff a\tilde{L} = b\tilde{L} \iff b^{-1}a\tilde{L} = \tilde{L} \iff b^{-1}a \in \tilde{H} \iff a\tilde{H} = b\tilde{H},$$

the first equivalence from Step 3.

We are now in a position to prove the theorem. Using Step 1, 17.2(2), and Step 4, we find that ${}^aL \cong {}^bL$ if and only if $a\tilde{H} = b\tilde{H}$ $(a, b \in G)$. This proves (1).

Next, we prove (2). We have by Step 2 that

$$M = \sum_{a \in G} aL \subseteq \sum_{a \in G} \widetilde{aL} \subseteq M,$$

which forces $M = \sum_{a \in G} \widetilde{aL}$. In particular $\{\widetilde{aL} \mid a \in G\}$ is the complete set of components of M_H (see 17.2(3)). By Step 4, the modules $\widetilde{aL}$ $(a \in A)$ are the distinct components of M_H, so by 17.2(3), we have $M_H = \dot{\sum}_{a \in A} \widetilde{aL}$.

Let $a \in A$. According to 17.2(1), $\widetilde{aL} \cong \bigoplus_{i=1}^{t(a)} aL$ for some positive integer $t(a)$. Now, the map $x \mapsto ax$ defines a vector space automorphism of M. Hence (assuming without loss of generality that $e \in A$),

$$t(a) \dim_{\mathbf{C}} L = t(a) \dim_{\mathbf{C}} aL = \dim_{\mathbf{C}} \widetilde{aL} = \dim_{\mathbf{C}} a\tilde{L} = \dim_{\mathbf{C}} \tilde{L} = t(e) \dim_{\mathbf{C}} L.$$

We conclude that $t(a) = t(e) =: t$ for all $a \in A$. Therefore,

$$M_H = \dot{\sum}_{a \in A} \widetilde{aL} \cong \bigoplus_{a \in A} \bigoplus_{i=1}^{t(a)} aL \cong \bigoplus_{i=1}^{t} \bigoplus_{a \in A} {}^aL = t\left(\bigoplus_{a \in A} {}^aL\right).$$

Moreover, by part (1), t is precisely the multiplicity of L as a direct summand of M_H. This completes the proof of (2).

It remains to prove (3). First, by the definition of $\tilde{H}$, it is clear that $\tilde{L}$ is a $\mathbf{C}\tilde{H}$-submodule of $M_{\tilde{H}}$. By 17.2(1) and our definition of t, we have $\tilde{L}_H \cong \bigoplus_{i=1}^{t} L$. Finally, from the proof of part (2) together with Step 3 we get

$$M = \dot{\sum}_{a \in A} \widetilde{aL} = \dot{\sum}_{a \in A} a\tilde{L}.$$

Therefore, 17.1 implies $M \cong \tilde{L}^G$. $\square$

Let H be an arbitrary subgroup of G, let L be a $\mathbf{C}H$-module and let $a \in G$. If L affords the character λ, then the $\mathbf{C}({}^aH)$-module ${}^aL$ affords the **conjugate character** ${}^a\lambda$ of ${}^aH$ defined by ${}^a\lambda({}^ah) = \lambda(h)$.

We state the most frequently used portion of 17.3 in terms of characters.

17.4 (Clifford's Theorem for Characters) *Let $H \lhd G$, let $\chi \in \mathrm{Irr}(G)$, let $\lambda \in \mathrm{Irr}(H)$ and assume $t := (\chi_H, \lambda) \neq 0$. We have $\chi_H = t \sum_{a \in A} {}^a\lambda$, where $\{{}^a\lambda\}_{a \in A}$ is a complete set of distinct conjugates of λ.*

Exercise 9

A $\mathbf{C}G$-module is **faithful** if the representation it affords has trivial kernel (i.e., if the representation is injective). Prove that if there exists a simple faithful $\mathbf{C}G$-module, then the center of G is cyclic.

18 Mackey's Subgroup Theorem

Let X and Y be two subgroups of G. Given a $\mathbf{C}X$-module L, we can induce up to the group G and then restrict down to the subgroup Y to obtain the $\mathbf{C}Y$-module $(L^G)_Y$. The main result of this section, due to Mackey, expresses this new module in terms of modules obtained by taking conjugates of L, restricting them to certain subgroups of Y, and then inducing the resulting modules up to Y.

The constructions depend on the following notion from group theory. Given $a \in G$, the set

$$YaX = \{yax \,|\, y \in Y, x \in X\}$$

is called a (Y, X)**-double coset**. The main facts about double cosets are summarized in the next result.

18.1 *Let X and Y be two subgroups of G.*

(1) *The set of (Y, X)-double cosets partitions G.*
(2) *For each $a \in G$, the set YaX is a union of left cosets of X and is also a union of right cosets of Y.*
(3) *Let $a \in G$. If B is a set of representatives for the left cosets of ${}^aX \cap Y$ in Y, then Ba is a set of representatives for the left cosets of X in YaX.*

Proof. (1) Let YaX and $Ya'X$ be two (Y, X)-double cosets and suppose their intersection is nonempty. Then the intersection contains an element b, which can be written $b = yax$ and also $b = y'a'x'$ for some $y, y' \in Y$ and $x, x' \in X$. Then

$$YaX = YyaxX = Yy'a'x'X = Ya'X.$$

We conclude that the double cosets are pairwise disjoint. Finally, if $a \in G$, then $a = eae \in YaX$, so G is the union of the (Y, X)-double cosets.

(2) For each $a \in G$, we have $YaX = \cup_{y \in Y} yaX$ and $YaX = \cup_{x \in X} Yax$.

(3) Let B be a set of representatives for the left cosets of ${}^aX \cap Y$ in Y. We first show that $YaX = BaX$. Let $y \in Y$. Now y lies in some left coset of ${}^aX \cap Y$, so we have $b^{-1}y \in {}^aX \cap Y$ for some $b \in B$. In particular, $b^{-1}y = axa^{-1}$ for some $x \in X$. Then $yaX = yax^{-1}X = baX$. Thus $YaX = BaX$, as desired. Next, suppose $baX = b'aX$ for some $b, b' \in B$. Then

$$b'({}^aX \cap Y) = b'aXa^{-1} \cap Y = baXa^{-1} \cap Y = b({}^aX \cap Y),$$

so $b' = b$ (implying $b'a = ba$). This completes the proof. □

18.2 (Mackey's Subgroup Theorem) *Let X and Y be subgroups of G. If L is a $\mathbf{C}X$-module, then*

$$(L^G)_Y \cong \bigoplus_{a\in A} \left(({}^aL)_{{}^aX\cap Y}\right)^Y,$$

where A is a set of representatives for the (Y,X)-double cosets in G.

Proof. Let L be a $\mathbf{C}X$-module. Fix a (Y,X)-double coset D and let $W(D)$ be the subspace of $L^G = \mathbf{C}G\otimes_{\mathbf{C}X} L$ given by (writing $\otimes$ for $\otimes_{\mathbf{C}X}$)

$$W(D) = \sum_{c\in C} c\otimes L,$$

where C is a set of representatives for the left cosets of X in D (see 18.1(2)). This definition does not depend on the choice for C. Indeed, let C and C' be two sets of representatives for the left cosets of X in D. If $c'\in C'$, then $c' = cx$ for some $c\in C$ and $x\in X$, implying

$$c'\otimes L = cx\otimes L = c\otimes xL = c\otimes L.$$

This gives $\sum_{c'\in C'} c'\otimes L \subseteq \sum_{c\in C} c\otimes L$, and symmetry yields equality as desired.

Now $W(D)$ is a $\mathbf{C}Y$-submodule of $(L^G)_Y$. Indeed, if $y\in Y$ and C is as above, then for any $c\in C$, we have $yc = c'x$ for some $c'\in C$ and $x\in X$, so that

$$y(c\otimes L) = yc\otimes L = c'x\otimes L = c'\otimes xL = c'\otimes L,$$

and the claim follows.

Write $D = YaX$ and let B be a set of representatives for the left cosets of ${}^aX\cap Y$ in Y. By 18.1(3), $C := Ba$ is a set of representatives for the left cosets of X in YaX, so

$$W(D) = \dot{\sum}_{b\in B} ba\otimes L = \dot{\sum}_{b\in B} b(a\otimes L),$$

where we have used 15.1(2) to see that the sum is direct. Now the map $\varphi : {}^aL \to a\otimes L$ given by $\varphi(l) = a\otimes l$ is a $\mathbf{C}({}^aX)$-isomorphism. Indeed, it is clearly a vector space isomorphism, and we have

$$\varphi({}^ax\cdot l) = \varphi(xl) = a\otimes xl = ax\otimes l = {}^axa\otimes l = {}^ax\varphi(l)$$

($x\in X$, $l\in {}^aL$). In particular, $a\otimes L\cong {}^aL$ as $\mathbf{C}({}^aX\cap Y)$-modules. Therefore, by 17.1, we have $W(D)\cong \left(({}^aL)_{{}^aX\cap Y}\right)^Y$ as $\mathbf{C}Y$-modules.

Finally, 15.1(2) and 18.1(1) imply $L^G = \dot{\sum}_D W(D)$, where the sum is over all (Y,X)-double cosets D in G, whence

$$(L^G)_Y \cong \bigoplus_{a\in A} \left(({}^aL)_{{}^aX\cap Y}\right)^Y,$$

where A is a set of representatives for the (Y,X)-double cosets in G. This completes the proof. □

We record a useful special case of 18.2.

18.3 *If $H \lhd G$ and L is a $\mathbf{C}H$-module, then*

$$(L^G)_H \cong \bigoplus_{a \in A} {}^aL,$$

where A is a set of representatives for the (left) cosets of H in G.

PROOF. Assume the hypotheses and let A be as stated. For each $a \in A$, we have $HaH = aHH = aH$, so that A is also a set of representatives for the (H, H)-double cosets in G. Also, for each $a \in A$, we have

$$(({}^aL)_{{}^aH \cap H})^H = (({}^aL)_H)^H \cong {}^aL.$$

The result now follows from 18.2. □

Remark. One can also prove 18.3 quite easily without using Mackey's Subgroup Theorem. With the notation as in the statement, it is easy to see that for each $a \in A$, the subspace $a \otimes L$ of L^G is actually a $\mathbf{C}H$-submodule. Moreover, by essentially the same argument as that in the proof of 17.3, Step 1, we have $a \otimes L \cong {}^aL$ $(a \in A)$ as $\mathbf{C}H$-modules. Therefore,

$$(L^G)_H = \dot{\sum}_{a \in A} a \otimes L \cong \bigoplus_{a \in A} {}^aL,$$

as desired.

19 Quotients

In the last few sections, we have been studying the relationship between the representations of a group and those of its subgroups. We see in the next theorem that the relationship between the representations of a group and those of a *quotient* of the group is much easier to describe.

Let H be a normal subgroup of G. Put $\bar{G} = G/H$ and let $\pi : G \to \bar{G}$ denote the canonical epimorphism ($\pi(a) = aH$).

19.1 *The assignment $\rho \mapsto \rho \circ \pi$ defines a bijection between the set of representations of $\bar{G}$ and the set of those representations of G with kernel containing H. Moreover, this map sends each irreducible representation to an irreducible representation.*

Proof. If $\rho : \bar{G} \to \mathrm{GL}(V)$ is a representation, then $\rho \circ \pi : G \to \mathrm{GL}(V)$ is a representation with kernel containing H, so the map is well-defined.

Let $\varphi : G \to \mathrm{GL}(V)$ be a representation with kernel containing H. By the main lemma to the First Isomorphism Theorem (see [Hungerford, Theorem 5.6, p. 43]), there exists a unique homomorphism $\bar{\varphi} : \bar{G} \to \mathrm{GL}(V)$ such that $\bar{\varphi} \circ \pi = \varphi$, that is, such that $\bar{\varphi} \mapsto \varphi$. This shows that the map is bijective.

Finally, if $\rho : \bar{G} \to \mathrm{GL}(V)$ is a representation and $W \leq V$ satisfies $\big((\rho \circ \pi)(G)\big)W \subseteq W$, then $\big(\rho(\bar{G})\big)W \subseteq W$. Therefore, the last statement follows. $\square$

20 Example: The Dihedral Group

In this section, we use some of the theory we have developed to compute the character table of the dihedral group.

Fix a positive integer m and let $G = D_m$, the dihedral group of degree m. Thus G is the group of symmetries of a regular m-gon. Since there are m orientations of the m-gon without flipping it over, as well as m orientations after flipping it over, it is clear that G has order $2m$.

Position the m-gon in such a way that one of the vertices is at the top. Label the vertices $1, 2, \ldots, m$ starting with 1 at the top and proceeding clockwise. Any orientation of the m-gon gives rise to a permutation of the vertices, which can be viewed, relative to the labeling system just described, as an element of the symmetric group S_m. In this way, we consider G to be a subgroup of S_m. The clockwise rotation of the m-gon through an angle of $2\pi/m$ radians is given by

$$a = \begin{pmatrix} 1 & 2 & \cdots & m-1 & m \\ 2 & 3 & \cdots & m & 1 \end{pmatrix}.$$

The flip of the m-gon about the vertical line through the top vertex is given by

$$b = \begin{pmatrix} 1 & 2 & 3 & \cdots & m-1 & m \\ 1 & m & m-1 & \cdots & 3 & 2 \end{pmatrix}.$$

Since any symmetry of the m-gon produced by rotation is a power of a, it follows that $G = \langle a, b \rangle$. It is easy to check that $a^m = 1 = b^2$, and that $a^i b = ba^{-i}$ for all i. In particular, $G = \{a^i, ba^i \mid 0 \leq i < m\}$.

Set $H = \langle a \rangle$. Then H is a cyclic group of order m. According to the first example of Section 12, H has precisely m irreducible characters λ_j $(0 \leq j < m)$ given by $\lambda_j(a^i) = \omega^{ij}$, where $\omega = e^{2\pi i/m}$.

Fix $0 \leq j < m$. Now H is a normal subgroup of G since, for instance, its index in G is two. Therefore, 18.3 applies to give

$$({\lambda_j}^G)_H = \lambda_j + {}^b\lambda_j,$$

where ${}^b\lambda_j$ denotes the conjugate by b of the character λ_j as defined in Section 17. For each $h \in H$, we have

$${}^b\lambda_j(h) = {}^b\lambda_j\big({}^b(b^{-1}hb)\big) = \lambda_j(b^{-1}hb) = \lambda_j(h^{-1}) = \overline{\lambda_j(h)},$$

whence ${}^b\lambda_j = \overline{\lambda_j}$. Then, by Frobenius Reciprocity (16.5), we get

$$({\lambda_j}^G, {\lambda_j}^G) = (\lambda_j, ({\lambda_j}^G)_H) = (\lambda_j, \lambda_j + \overline{\lambda_j}) = 1 + (\lambda_j, \overline{\lambda_j}).$$

Hence, ${\lambda_j}^G$ is irreducible if and only if $\lambda_j \neq \overline{\lambda}_j$ (see 13.2).

The even m case. By the previous paragraph, ${\lambda_j}^G$ is irreducible if $1 \leq j < m/2$. This gives $m/2-1$ distinct irreducible characters of G, each of degree two. Since the sum of the squares of the degrees of the irreducible characters equals the order of the group (11.2), we see that we have not yet found all of the irreducible characters.

Set $K = \langle a^2 \rangle$. Then K is a normal subgroup of G. Indeed, it is clear that $a^{-1}Ka = K$ and since $a^i b = ba^{-i}$, we have $b^{-1}Kb = K$. Since a and b generate G, the claim follows. The group $\bar{G} := G/K$ has order four and it contains two elements of order two, namely $\bar{a}$ and $\bar{b}$. Hence we obtain an isomorphism $\bar{G} \to \mathbf{Z}_2 \oplus \mathbf{Z}_2$ by mapping $\bar{a} \mapsto (1,0)$ and $\bar{b} \mapsto (0,1)$. Denoting by σ the nontrivial character of $\mathbf{Z}_2$ (i.e., $\sigma(0) = 1$, $\sigma(1) = -1$), we have from 13.3 the following character table of $\mathbf{Z}_2 \oplus \mathbf{Z}_2$:

	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
1	1	1	1	1
$(\sigma,1)$	1	-1	1	-1
$(1,\sigma)$	1	1	-1	-1
(σ,σ)	1	-1	-1	1

According to 19.1, the compositions of these characters with the canonical map $G \to \bar{G} \cong \mathbf{Z}_2 \oplus \mathbf{Z}_2$, yield four characters of G, each of degree one, which we denote by ψ_i, $0 \leq i \leq 3$, respectively. Checking the sum of the squares of the degrees we see that these characters complete the list. There are thus $m/2+3$ irreducible characters of G and the character table is as follows ($1 \leq j < m/2$):

	a^i	ba^i
$\psi_0 = 1$	1	1
ψ_1	$(-1)^i$	$(-1)^i$
ψ_2	1	-1
ψ_3	$(-1)^i$	$(-1)^{i+1}$
${\lambda_j}^G$	$2\cos\frac{2\pi ij}{m}$	0

To get the last line, note that

$${\lambda_j}^G(a^i) = \lambda_j(a^i) + \overline{\lambda_j(a^i)} = \omega^{ij} + \omega^{-ij} = 2\,\mathrm{Re}(\omega^{ij}) = 2\cos(2\pi ij/m),$$

and that for $x \in G \backslash H$,

$${\lambda_j}^G(x) = \frac{1}{|H|} \sum_{g \in G} \lambda_j^0(g^{-1}xg) = 0$$

by 15.3, where we have used the definition of λ_j^0 and the fact that $g^{-1}xg \notin H$ for each $g \in G$ since H is normal.

Finally, one checks that G has $m/2+3$ conjugacy classes, namely,

$$\begin{aligned}
&\{1\},\\
&\{a^i, a^{m-i}\} \quad (1 \le i < m/2),\\
&\{a^{m/2}\},\\
&\{ba^{2k} \mid 0 \le k < m/2\},\\
&\{ba^{2k+1} \mid 0 \le k < m/2\}.
\end{aligned}$$

Therefore, the number of irreducible characters equals the number of conjugacy classes as expected (see 10.3).

The odd m case. In this case, ${\lambda_j}^G$, $1 \le j \le (m-1)/2$, are irreducible and distinct. This yields $(m-1)/2$ irreducible characters of degree two. Also, G/H is isomorphic to $\mathbf{Z}_2$, so, arguing as above, we obtain two characters of degree one. Summing the squares of the degrees, we get $2m = |G|$, so these are all of the irreducible characters of G. Thus, there are $(m+3)/2$ irreducible characters and the character table is as follows ($1 \le j \le (m-1)/2$):

	a^i	ba^i
$\psi_0 = 1$	1	1
ψ_1	1	-1
${\lambda_j}^G$	$2\cos\frac{2\pi ij}{m}$	0

There are $(m+3)/2$ conjugacy classes, namely,

$$\begin{aligned}
&\{1\},\\
&\{a^i, a^{m-i}\} \quad (1 \le i \le (m-1)/2),\\
&\{ba^i \mid 0 \le i < m\}.
\end{aligned}$$

Exercise 10

Let Q_8 be the subgroup of $\mathrm{GL}_2(\mathbf{C})$ generated by $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$. Show that Q_8 and D_4 have the same character table, yet $Q_8 \ncong D_4$. (Hint: First check that $A^4 = I = B^4$ and that $BA = A^3B$.)

21 The Structure of the Group Algebra

According to Maschke's Theorem (7.1), the group algebra $\mathbf{C}G$ is semisimple. (See Hungerford, Theorem 3.7 (i $\Leftrightarrow$ v), p. 439. Note that $\mathbf{C}G$ is left Artinian. Indeed, its left ideals are vector subspaces and, since $\mathbf{C}G$ is finite-dimensional, any chain of left ideals must terminate.) Therefore, the Artin-Wedderburn Theorem (Hungerford, Theorem 5.4, p. 452) says that $\mathbf{C}G$ is isomorphic to a direct sum of matrix algebras with the entries of each matrix algebra coming from a division algebra over $\mathbf{C}$. In this section, we give an elementary proof of this special case of the Artin-Wedderburn Theorem using the representation theory we have developed.

Let $\chi_1, \ldots, \chi_t$ be the irreducible characters of G. For $1 \le i \le t$, let $R_i : G \to \mathrm{GL}_{n_i}(\mathbf{C})$ be a matrix representation of G affording χ_i and note that $n_i = \chi_i(e)$. We extend R_i linearly to an algebra homomorphism $\mathbf{C}G \to \mathrm{Mat}_{n_i}(\mathbf{C})$, which we continue to denote by R_i.

Set $R = (R_i) : \mathbf{C}G \to \bigoplus_i \mathrm{Mat}_{n_i}(\mathbf{C})$. So for $x \in \mathbf{C}G$, we have $R(x) = \big(R_i(x)\big) = \big(R_1(x), \ldots, R_t(x)\big)$. This is an algebra homomorphism, where the codomain is viewed as an algebra under componentwise multiplication.

Let $n = \sum_i n_i$. The set of all diagonal block matrices, with blocks of sizes $n_1, n_2, \ldots, n_t$, respectively, is a subalgebra of $\mathrm{Mat}_n(\mathbf{C})$. It is easy to see that this subalgebra is isomorphic to $\bigoplus_i \mathrm{Mat}_{n_i}(\mathbf{C})$. We use this isomorphism to identify these two algebras. In particular, for any $x \in \mathbf{C}G$, we view $R(x)$ as the diagonal block matrix with blocks $R_1(x), R_2(x), \ldots, R_t(x)$, respectively.

21.1 *The map $R : \mathbf{C}G \to \bigoplus_i \mathrm{Mat}_{n_i}(\mathbf{C})$ is an algebra isomorphism.*

Proof. It was observed above that R is an algebra homomorphism. The dimension of both algebras is $|G| = \sum_i n_i^2$ (see 11.2), so it suffices to show that R is injective. For this, it is enough to find a map $S : \bigoplus_i \mathrm{Mat}_{n_i}(\mathbf{C}) \to \mathbf{C}G$ such that $S \circ R = 1$. Set $S((D_i)) = \sum_{a \in G} \beta_a a$, where

$$\beta_a = \frac{1}{|G|} \sum_i n_i \operatorname{tr}\big(R_i(a^{-1}) D_i\big).$$

If $x = \sum_{a \in G} \alpha_a a \in \mathbf{C}G$, then $(S \circ R)(x) = S\big((R_i(x))\big) = \sum_{a \in G} \beta_a a$, where

$$\beta_a = \frac{1}{|G|} \sum_i n_i \operatorname{tr}\left(R_i(a^{-1}) R_i\left(\sum_{b \in G} \alpha_b b\right)\right)$$

$$
\begin{aligned}
&= \frac{1}{|G|} \sum_i n_i \sum_{b \in G} \alpha_b \operatorname{tr}\big(R_i(a^{-1}b)\big) \\
&= \frac{1}{|G|} \sum_{b \in G} \alpha_b \sum_i \chi_i(e)\overline{\chi_i(b^{-1}a)} \\
&= \frac{1}{|G|} \sum_{b \in G} \alpha_b |G| \delta_{ab} \\
&= \alpha_a,
\end{aligned}
$$

using 11.1 for the next to the last equality. □

There are several obvious structural features of $\bigoplus_i \operatorname{Mat}_{n_i}(\mathbf{C})$, which carry over to $\mathbf{C}G$ thanks to 21.1. We point out a few of these features next.

Set $B = \bigoplus_i \operatorname{Mat}_{n_i}(\mathbf{C})$. For each $1 \le i \le t$, set

$$B_i = (0, \dots, 0, \overset{i}{\operatorname{Mat}_{n_i}}(\mathbf{C}), 0, \dots, 0)$$

and put $A_i = R^{-1}(B_i)$.

21.2 *Let the notation be as above.*

(1) *Each A_i is an ideal of $\mathbf{C}G$ and $\mathbf{C}G = \dot{\sum}_i A_i$.*
(2) *Let L_i be a simple $\mathbf{C}G$-module affording χ_i. Then A_i is a direct sum of n_i left ideals, each $\mathbf{C}G$-isomorphic to L_i. In particular, $\mathbf{C}G \cong \bigoplus_i n_i L_i$ as $\mathbf{C}G$-modules.*
(3) *Let $e_i = \frac{n_i}{|G|} \sum_{a \in G} \chi_i(a^{-1})a$. Then e_i is a multiplicative identity of A_i and $\sum_i e_i = 1 \in \mathbf{C}G$.*

Proof. (1) Clearly each B_i is an ideal of B and $B = \dot{\sum}_i B_i$, so the statement follows from 21.1.

(2) For each $1 \le j \le n_i$, let B_{ij} be the subspace of B consisting of those matrices having nonzero entries confined to the jth column of the ith block. In particular, $B_{ij} \subseteq B_i$. Clearly, B_{ij} is a left ideal of B and $B_i = \dot{\sum}_j B_{ij}$. Therefore, each $A_{ij} := R^{-1}(B_{ij})$ is a left ideal of $\mathbf{C}G$ and $A_i = \dot{\sum}_j A_{ij}$.

We claim that $A_{ij} \cong L_i$ as $\mathbf{C}G$-modules. To prove this, it suffices to show that $B_{ij} \cong L_i$, where the B-module B_{ij} is viewed as a $\mathbf{C}G$-module via R. Now L_i can be identified with $\mathbf{C}^{n_i}$ (= space of n_i-dimensional column vectors over $\mathbf{C}$), which is a $\mathbf{C}G$-module with multiplication $xl = R_i(x)l$ ($x \in \mathbf{C}G$, $l \in \mathbf{C}^{n_i}$), the product on the right being matrix multiplication. Let $\varphi : L_i = \mathbf{C}^{n_i} \to B_{ij}$ be the natural map. Then

$$\varphi(xl) = \varphi\big(R_i(x)l\big) = \big(0, \dots, 0, \overset{(i,j)}{R_i(x)l}, 0, \dots, 0\big) = R(x)\varphi(l) = x\varphi(l)$$

($x \in \mathbf{C}G$, $l \in L_i$), where the superscript (i,j) signifies the jth column of the ith block. Therefore, φ is a $\mathbf{C}G$-isomorphism.

Finally,

$$\mathbf{C}G = \dot{\sum_i} A_i = \dot{\sum_{i,j}} A_{ij} \cong \bigoplus_i n_i L_i.$$

(3) Let $E_i = (0, \ldots, 0, I_{n_i}, 0, \ldots, 0) \in B$. Then, with notation as in the proof of 21.1, we have

$$R^{-1}(E_i) = S(E_i) = \frac{n_i}{|G|} \sum_{a \in G} \chi_i(a^{-1})a = e_i.$$

Therefore, by 21.1 it suffices to show that E_i is a multiplicative identity of B_i and that $\sum_i E_i = I$, both of which are clear. $\square$

22 The Center of the Group Algebra

In the last section, we saw that many structural properties of the group algebra $\mathbf{C}G$ become transparent once it is identified with a direct sum of matrix algebras. Here, we continue using this technique to study the center of $\mathbf{C}G$. (The **center** $Z(R)$ of a ring R is the set of those elements of R that commute with all other elements: $Z(R) := \{z \in R \mid zr = rz \text{ for all } r \in R\}$.)

22.1 *Let n be a positive integer. The center of $\mathrm{Mat}_n(\mathbf{C})$ is the set $\{\alpha I \mid \alpha \in \mathbf{C}\}$ of all scalar matrices.*

Proof. First, the set of scalar matrices is clearly contained in the center of $\mathrm{Mat}_n(\mathbf{C})$. Now, let $[\alpha_{ij}]$ be in the center of $\mathrm{Mat}_n(\mathbf{C})$ and let $E_{kl} = [e_{ij}]$ be the $n \times n$-matrix with 1 in the (k,l)-position and zeros elsewhere. Since $[\alpha_{ij}]E_{kl} = E_{kl}[\alpha_{ij}]$, we have for all $1 \leq i,k,l \leq n$

$$\alpha_{ik} = \sum_j \alpha_{ij} e_{jl} = \sum_j e_{ij}\alpha_{jl} = \alpha_{ll}\delta_{ik}.$$

For $i \neq k$, we have $\alpha_{ik} = 0$, while, for any $1 \leq i,l \leq n$, we have $\alpha_{ii} = \alpha_{ll}$. $\square$

Remark. This result also follows from Schur's Lemma (6.2). (Actually, for this we require the G in the statement of Schur's Lemma to have infinite order. Defining a representation of an infinite G just like we did for finite G, it is easily checked that representations still correspond to $\mathbf{C}G$-modules where now $\mathbf{C}G$ consists of only *finite* linear combinations of group elements. The proof of Schur's Lemma is seen to be valid in this setting.) Set $G = \mathrm{GL}_n(\mathbf{C})$ and $V = \mathbf{C}^n$. We view V as a $\mathbf{C}G$-module via matrix multiplication. It is easy to see that V is simple as such. Let A be in the center of $\mathrm{Mat}_n(\mathbf{C})$ and let $f : V \to V$ be multiplication by A. Then for all $a \in G$, $v \in V$ we have $f(av) = Aav = aAv = af(v)$, so f is a $\mathbf{C}G$-homomorphism. By Schur's Lemma, $f = \alpha 1_V$ for some $\alpha \in \mathbf{C}$, whence $A = \alpha I$.

Let the notation be as in Section 21. According to 21.1, $R : \mathbf{C}G \to \bigoplus_{i=1}^t \mathrm{Mat}_{n_i}(\mathbf{C})$ is an algebra isomorphism. Therefore, R maps the center $Z = Z(\mathbf{C}G)$ of $\mathbf{C}G$ isomorphically onto the center of $\bigoplus_i \mathrm{Mat}_{n_i}(\mathbf{C})$, which, by 22.1, is $\dot{\sum}_i \mathbf{C}E_i$, where $E_i = (0,\ldots,0,I_{n_i},0,\ldots,0)$. Therefore, if $z \in Z$, then $R(z) = \sum_i \omega_i(z)E_i$ for unique $\omega_i(z) \in \mathbf{C}$. This defines for each $1 \leq i \leq t$ a map $\omega_i : Z \to \mathbf{C}$. Clearly, each ω_i is an algebra homomorphism.

22.2 *If $z = \sum_{a\in G} \alpha_a a \in Z$, then for each $1 \le i \le t$ we have*

$$\omega_i(z) = \frac{1}{n_i} \sum_{a\in G} \alpha_a \chi_i(a).$$

PROOF. Let $1 \le i \le t$. The given formula for ω_i is linear in z, so it suffices to check its validity on a basis for Z. Since $\{E_i \mid 1 \le i \le t\}$ is clearly a basis for the center of $\bigoplus_i \mathrm{Mat}_{n_i}(\mathbf{C})$, the set $\{e_i \mid 1 \le i \le t\}$ is a basis for Z, where $e_i = S(E_i) = \frac{n_i}{|G|} \sum_a \chi_i(a^{-1})a$ (S as in the proof of 21.1). For each $1 \le j \le t$, we have

$$\omega_i(e_j) = \delta_{ij} = \frac{1}{|G|} \sum_a \chi_j(a^{-1})\chi_i(a) = \frac{1}{n_i} \sum_a \frac{n_j}{|G|} \chi_j(a^{-1})\chi_i(a).$$

This completes the proof. □

Let $C_1, \ldots, C_t$ be the conjugacy classes of G (there are t such by 10.3) and for each $1 \le i \le t$, set $s_i = \sum_{c\in C_i} c$.

22.3 *With notation as above, $\{s_i \mid 1 \le i \le t\}$ is a basis for Z.*

PROOF. Since the sets C_i ($1 \le i \le t$) are pairwise disjoint, $\{s_i\}$ is linearly independent. Therefore, it remains to show that this set spans Z.

Let $x = \sum_{a\in G} \alpha_a a \in \mathbf{C}G$. We have

$$\begin{aligned}
x \in Z &\iff g^{-1}xg = x \quad \text{for all } g \in G \\
&\iff \sum_{a\in G} \alpha_a g^{-1}ag = \sum_{a\in G} \alpha_a a \quad \text{for all } g \in G \\
&\iff \sum_{a\in G} \alpha_{gag^{-1}} a = \sum_{a\in G} \alpha_a a \quad \text{for all } g \in G \\
&\iff \alpha_{gag^{-1}} = \alpha_a \quad \text{for all } a, g \in G.
\end{aligned}$$

In other words, x is in Z if and only if the function $a \mapsto \alpha_a$ is constant on conjugacy classes (i.e., is a class function). In particular, each s_i is in Z so the span of $\{s_i\}$ is contained in Z. On the other hand, suppose $x \in Z$. Then for each $1 \le i \le t$, we get a well-defined complex number β_i by setting $\beta_i = \alpha_c$ for any $c \in C_i$. Then

$$x = \sum_{a\in G} \alpha_a a = \sum_{i=1}^{t} \sum_{c\in C_i} \alpha_c c = \sum_{i=1}^{t} \beta_i \sum_{c\in C_i} c = \sum_{i=1}^{t} \beta_i s_i,$$

so that $\{s_i\}$ spans Z, as desired. □

Remark. The proof of 22.2 shows that $\{e_i \mid 1 \le i \le t\}$ is a basis of Z. This, together with 22.3 provides another proof of 10.3.

23 Some Algebraic Number Theory

We need some standard results from algebraic number theory in order to utilize some of the more subtle properties of characters.

The first result is a statement about **Z**-modules. Since "**Z**-module" is the same as "abelian group," it could be recast as a statement about abelian groups as well.

23.1 *Any submodule of a finitely generated* **Z***-module is finitely generated.*

PROOF. Let A be a finitely generated **Z**-module and let H be a submodule of A. We have $A = \langle a_1, \ldots, a_n \rangle = \sum_i \mathbf{Z}a_i$ for some $a_i \in A$. We proceed by induction on n. If $n = 1$, then A is cyclic, so that H is cyclic as well and hence finitely generated. Now assume $n > 1$. Let

$$I = \{z_1 \in \mathbf{Z} \mid h = z_1a_1 + \cdots + z_na_n \text{ for some } h \in H \text{ and some } z_2, \ldots, z_n \in \mathbf{Z}\}.$$

Clearly I is an ideal of **Z**, so $I = (z)$ for some $z \in \mathbf{Z}$. Since $z \in I$, we have $h_0 = za_1 + z_2a_2 + \cdots + z_na_n$ for some $h_0 \in H$ and some $z_2, \ldots, z_n \in \mathbf{Z}$. Let $A_1 = \sum_{i>1} \mathbf{Z}a_i$ and put $H_1 = H \cap A_1$. By the induction hypothesis, $H_1 = \sum_{i=1}^{m} \mathbf{Z}h_i$ for some m and some $h_i \in H$. But then, $H = \mathbf{Z}h_0 + \sum_{i=1}^{m} \mathbf{Z}h_i$. Indeed, if $h \in H$, then we have $h = z_1za_1 + z_2a_2 + \cdots + z_na_n$ for some $z_i \in \mathbf{Z}$, so $h - z_1h_0 \in H_1$. Thus H equals $\langle h_0, \ldots, h_m \rangle$ and is hence finitely generated. □

Let R be a commutative ring with identity. An element α of R is **integral** over **Z** if $f(\alpha) = 0$ for some monic $f \in \mathbf{Z}[x]$ (i.e., for some $f \in \mathbf{Z}[x]$ of the form $f(x) = x^n + z_{n-1}x^{n-1} + \cdots + z_1x + z_0$).

Let S be a subring of R and let X be a subset of R. The subring of R generated by the set $S \cup X$ is denoted $S[X]$. We write $\mathbf{Z}[X]$ to mean $(\mathbf{Z}\cdot 1_R)[X]$. Suppose $X = \{\alpha_1, \ldots, \alpha_n\}$. We write $S[\alpha_1, \ldots, \alpha_n]$ for $S[X]$. We have $S[\alpha_1, \ldots, \alpha_n] = \{g(\alpha_1, \ldots, \alpha_n) \mid g \in S[x_1, \ldots, x_n]\}$. Indeed, the set on the right is contained in every subring of R containing $S \cup \{\alpha_1, \ldots, \alpha_n\}$ and it is a subring of R since it is the image of the evaluation map $S[x_1, \ldots, x_n] \to R$ obtained by replacing the x_i in a polynomial with the α_i. Finally, it is an easy exercise to show that $S[\alpha_1, \ldots, \alpha_n] = S[\alpha_1, \ldots, \alpha_{n-1}][\alpha_n]$.

23.2 *Let $\alpha \in R$. The following are equivalent:*

(1) *α is integral over* **Z***,*
(2) **Z**$[\alpha]$ *is finitely generated as* **Z***-module,*
(3) **Z**$[\alpha]$ *is contained in a finitely generated* **Z***-submodule of R.*

PROOF. (1⇒2) Assume α is integral over $\mathbf{Z}$. We have $f(\alpha) = 0$ for some monic $f \in \mathbf{Z}[x]$ of degree, say, n. We claim that $\mathbf{Z}[\alpha] = \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle$. Since $\mathbf{Z}[\alpha] = \{g(\alpha) \,|\, g \in \mathbf{Z}[x]\}$, it is enough to show that $\alpha^m \in \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle$ for each $m \geq 0$. We proceed by induction on m. The case $m \leq n-1$ is clear so assume $m \geq n$. We have

$$\begin{aligned} 0 = \alpha^{m-n} f(\alpha) &= \alpha^{m-n}(\alpha^n + z_{n-1}\alpha^{n-1} + \cdots + z_1\alpha + z_0) \\ &= \alpha^m + z_{n-1}\alpha^{m-1} + \cdots + z_1\alpha^{m-n+1} + z_0\alpha^{m-n}, \end{aligned}$$

where $f(x) = x^n + z_{n-1}x^{n-1} + \cdots + z_1x_1 + z_0$. So

$$\alpha^m = -z_{n-1}\alpha^{m-1} - \cdots - z_1\alpha^{m-n+1} - z_0\alpha^{m-n} \in \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle$$

by the induction hypothesis.

(2⇒1) Assume $\mathbf{Z}[\alpha]$ is finitely generated as $\mathbf{Z}$-module. Then $\mathbf{Z}[\alpha] = \langle y_1, \ldots, y_s \rangle$ for some $y_i \in \mathbf{Z}[\alpha]$. In turn, for each $1 \leq i \leq s$, we have $y_i = f_i(\alpha)$ for some $f_i \in \mathbf{Z}[x]$. Choose a positive integer n with $n > \deg f_i$ for all i. Then $\alpha^n = \sum_i z_i y_i = \sum_i z_i f_i(\alpha)$ for some $z_i \in \mathbf{Z}$. Hence α is a zero of the monic polynomial $x^n - \sum_i z_i f_i(x)$.

(2⇒3) This is trivial.

(3⇒2) This follows directly from 23.1. □

Set $\mathcal{O}(R) = \{\alpha \in R \,|\, \alpha \text{ is integral over } \mathbf{Z}\}$.

23.3 *$\mathcal{O}(R)$ is a subring of R.*

PROOF. Clearly $0 \in \mathcal{O}(R)$. Let $\alpha, \beta \in \mathcal{O}(R)$. By 23.2, $\mathbf{Z}[\alpha]$ and $\mathbf{Z}[\beta]$ are both finitely generated $\mathbf{Z}$-modules, say $\mathbf{Z}[\alpha] = \langle \alpha_1, \ldots, \alpha_m \rangle$ and $\mathbf{Z}[\beta] = \langle \beta_1, \ldots, \beta_n \rangle$. Then

$$\mathbf{Z}[\alpha, \beta] = \mathbf{Z}[\alpha][\beta] = \left(\sum_i \mathbf{Z}\alpha_i \right)[\beta] = \sum_i \mathbf{Z}[\beta]\alpha_i = \sum_{i,j} \mathbf{Z}\beta_j\alpha_i,$$

so that $\mathbf{Z}[\alpha, \beta]$ is a finitely generated $\mathbf{Z}$-module. The subrings $\mathbf{Z}[\alpha + \beta]$, $\mathbf{Z}[-\alpha]$, and $\mathbf{Z}[\alpha\beta]$ are contained in $\mathbf{Z}[\alpha, \beta]$, so 23.2(1⇔3) implies that $\alpha + \beta$, $-\alpha$, and $\alpha\beta$ are in $\mathcal{O}(R)$. This shows that $\mathcal{O}(R)$ is a subring of R, as desired. □

Put $\mathcal{O} = \mathcal{O}(\mathbf{C})$. The elements of $\mathcal{O}$ are called **algebraic integers**.

23.4 *We have $\mathcal{O} \cap \mathbf{Q} = \mathbf{Z}$.*

PROOF. It is clear that $\mathcal{O} \cap \mathbf{Q}$ contains the set $\mathbf{Z}$. Now let $\alpha \in \mathcal{O} \cap \mathbf{Q}$. Then we can write $\alpha = p/q$ with p and q relatively prime integers, and with q positive. Since $\alpha \in \mathcal{O}$, we have $f(\alpha) = 0$ for some $f(x) = x^n + z_{n-1}x^{n-1} + \cdots + z_1x + z_0 \in \mathbf{Z}[x]$. Hence,

$$p^n + z_{n-1}p^{n-1}q + z_{n-2}p^{n-2}q^2 + \cdots + z_1pq^{n-1} + z_0q^n = 0.$$

This shows that any prime divisor of q must also be a divisor of p. But p and q are relatively prime, so it follows that $q = 1$, whence $\alpha = p \in \mathbf{Z}$. □

Remark. The elements of $\mathcal{O}$ are often referred to as just "integers." The elements of $\mathbf{Z}$ are then called "rational integers," the terminology being justified by 23.4.

24 Character Degrees and the Group Order

The results from algebraic number theory obtained in the last section will be applied here to show that the degree of any irreducible character of G divides the order of G.

Recall that $\mathcal{O} = \mathcal{O}(\mathbf{C})$ denotes the ring of (algebraic) integers.

24.1 *If χ is a character of G, then $\chi(a)$ is an element of $\mathcal{O}$ for each $a \in G$.*

PROOF. First note that each root of unity lies in $\mathcal{O}$ as it is a zero of the monic polynomial $x^n - 1$ for some n. If χ is a character of G, then for each $a \in G$, $\chi(a)$ is a sum of roots of unity, by 8.5(2), and hence lies in $\mathcal{O}$. □

As earlier, we use Z to denote the center of the group algebra $\mathbf{C}G$, we let $\chi_1, \ldots, \chi_t$ be the distinct irreducible characters of G, and we put $n_i = \chi_i(e)$ $(1 \leq i \leq t)$.

24.2 *Let $x = \sum_{a \in G} \alpha_a a \in Z$ and assume $\alpha_a \in \mathcal{O}$ for each a. Then $x \in \mathcal{O}(Z)$. In particular, $\frac{1}{n_i} \sum_a \alpha_a \chi_i(a) \in \mathcal{O}$ for each $1 \leq i \leq t$.*

PROOF. For each $1 \leq i \leq t$, 22.2 gives $\omega_i(x) = \frac{1}{n_i} \sum_a \alpha_a \chi_i(a)$. Therefore, since a ring homomorphism preserves integral elements, the second statement follows from the first.

By 22.3, x is a linear combination of class sums: $x = \sum_{i=1}^{t} \beta_i s_i$, where $s_i = \sum_{c \in C_i} c$. Since the conjugacy classes are mutually disjoint, linear independence of the group elements allows us to conclude that for each i, $\beta_i = \alpha_c$ for every $c \in C_i$. In particular, each β_i is in $\mathcal{O}$. Recall that we view $\mathbf{C}$ as a subring of $\mathbf{C}G$ by identifying $\alpha \leftrightarrow \alpha e$. With this identification we clearly have $\mathcal{O} \subseteq \mathcal{O}(Z)$ so that each β_i is in $\mathcal{O}(Z)$. Therefore, in order to establish our claim that x is in $\mathcal{O}(Z)$ it is enough, by the closure properties of the subring $\mathcal{O}(Z)$, to show that each s_i is in $\mathcal{O}(Z)$.

Fix $1 \leq j, k \leq t$. As $s_j s_k$ is in Z, 22.3 gives $s_j s_k = \sum_l \gamma_l s_l$ for some $\gamma_l \in \mathbf{C}$. On the other hand, $s_j s_k$ is clearly a $\mathbf{Z}$-linear combination of group elements. Using the linear independence of the group elements and arguing as above, we find that each γ_l is in $\mathbf{Z}$.

The preceding paragraph shows that $\sum_j \mathbf{Z} s_j$ is a subring of Z. Since this subring is finitely generated as $\mathbf{Z}$-module and since it contains each $\mathbf{Z}[s_i]$, we have from 23.2(3⇒1) that s_i is in $\mathcal{O}(Z)$ for each i. This completes the proof. □

24.3 *The degree of any irreducible character of G divides the order of G.*

PROOF. Fix $1 \leq i \leq t$ and let

$$x = \sum_{a \in G} \chi_i(a^{-1}) a = \sum_{a \in G} \overline{\chi_i(a)} a.$$

Since χ_i is a class function (8.5(4)), we have $x \in Z$ by 22.3 (or its proof). Also, $\chi_i(a^{-1}) \in \mathcal{O}$ for each $a \in G$ by 24.1. Therefore, using the orthogonality relation 9.4 and then 24.2 and 23.4 in succession, we obtain

$$\frac{|G|}{n_i} = \frac{1}{n_i} \sum_{a \in G} \chi_i(a^{-1})\chi_i(a) \in \mathcal{O} \cap \mathbf{Q} = \mathbf{Z}.$$

(We have to look back to the fraction $|G|/n_i$ to see why the second member lies in $\mathbf{Q}$ as well.) Therefore, n_i divides $|G|$, as desired. $\square$

25 Burnside's Theorem on Solvability

The group G is **solvable** if all its composition factors are abelian (so called for the connection with solvability by radicals of polynomials via Galois Theory). Burnside's Theorem states that if the order of G is divisible by at most two prime numbers, then G is solvable. The original proof, which we present here, uses character theory. Fairly recently a character-free proof has been found, but the original proof is much shorter. We begin by reviewing some results from basic algebra.

If $\alpha \in \mathbf{C}$, then $\mathbf{Q}(\alpha)$ denotes the subfield of $\mathbf{C}$ generated by $\mathbf{Q} \cup \alpha$.

25.1 *Let $\alpha \in \mathcal{O}$ and let $f_\alpha \in \mathbf{Q}[x]$ be a monic polynomial of minimal degree such that $f_\alpha(\alpha) = 0$.*

(1) *If $g \in \mathbf{Q}[x]$ and $g(\alpha) = 0$, then f_α divides g. In particular, f_α is the unique irreducible monic polynomial in $\mathbf{Q}[x]$ for which $f_\alpha(\alpha) = 0$.*

(2) *We have $f_\alpha(x) = \prod_i (x - \alpha_i)$ with $\alpha_1 (= \alpha), \alpha_2 \ldots, \alpha_n$ distinct elements of $\mathcal{O}$. In particular, $N(\alpha) := \prod_i \alpha_i$ is an integer and $N(\alpha) \neq 0$ if $\alpha \neq 0$.*

(3) *For each $1 \leq i \leq n$, there exists a field isomorphism $\sigma_i : \mathbf{Q}(\alpha) \to \mathbf{Q}(\alpha_i)$ such that $\sigma_i(\alpha) = \alpha_i$.*

Remark. f_α is called the **minimal polynomial** of α and $N(\alpha)$ is called the **norm** of α.

Proof. (1) First, since α is in $\mathcal{O}$, it is a zero of a monic polynomial in $\mathbf{Z}[x] \subseteq \mathbf{Q}[x]$, so f_α is defined. Let $g \in \mathbf{Q}[x]$ and assume that $g(\alpha) = 0$. By the division algorithm, there exist $q, r \in \mathbf{Q}[x]$ with $\deg r < \deg f_\alpha$ such that $g = qf_\alpha + r$. Hence $r(\alpha) = g(\alpha) - q(\alpha) f_\alpha(\alpha) = 0$. If $r \neq 0$, then we can divide r by its leading coefficient to get a monic polynomial of degree less than the degree of f_α having α as a zero, a contradiction. So $r = 0$ and $g = qf_a$. Therefore, $f_\alpha | g$.

Suppose f_α has a factorization $f_\alpha = gh$ with $\deg g, \deg h < \deg f_\alpha$. We have $g(\alpha)h(\alpha) = f_\alpha(\alpha) = 0$ so that $g(\alpha) = 0$ or $h(\alpha) = 0$. In either case, we get a contradiction to the choice of f_α (after dividing by leading coefficients to make the polynomials monic if necessary). Therefore, f_α is irreducible.

Let $g \in \mathbf{Q}[x]$ be an irreducible monic polynomial such that $g(\alpha) = 0$. By the first statement, f_α divides g and, since g is irreducible, we have $g = \beta f_\alpha$ for some $\beta \in \mathbf{Q}$. But g and f_a are monic, so $\beta = 1$ and $g = f_\alpha$. This proves the uniqueness statement.

(2) Since $\mathbf{C}$ is algebraically closed, $f_\alpha(x) = \prod_i (x - \alpha_i)$ for some $\alpha_i \in \mathbf{C}$. Now $f(\alpha) = 0$ for some monic $f \in \mathbf{Z}[x]$ and part (1) implies $f_\alpha | f$. Since $f_\alpha(\alpha_i) = 0$ we also have

$f(\alpha_i) = 0$, so each α_i is in $\mathcal{O}$.

Suppose the α_i are not all distinct, so that $f_\alpha(x) = (x-\alpha_i)^2 g(x)$ for some $g \in \mathbf{C}[x]$ and some i. Then $f'_\alpha(x) = (x-\alpha_i)^2 g'(x) + 2(x-\alpha_i)g(x)$ implying $f'_\alpha(\alpha_i) = 0$. Now $f_\alpha(\alpha_i) = 0$ so part (1) gives $f_{\alpha_i} = f_\alpha$, implying $\deg f'_\alpha < \deg f_\alpha = \deg f_{\alpha_i}$ contrary to the definition of f_{α_i}. Hence $\alpha_1, \ldots, \alpha_n$ are distinct.

Note that $f_\alpha(x) = \prod_i (x - \alpha_i) = x^n + \cdots \pm N(\alpha)$, so $N(\alpha) \in \mathbf{Q}$. But also, $N(\alpha) \in \mathcal{O}$ since each $\alpha_i \in \mathcal{O}$ and $\mathcal{O}$ is a subring of $\mathbf{C}$. Hence $N(\alpha) \in \mathbf{Q} \cap \mathcal{O} = \mathbf{Z}$ by 23.4.

Finally, assume $N(\alpha) = 0$. Then $\alpha_i = 0$ for some i so that $f_\alpha(x) = f_{\alpha_i}(x) = x$ giving $\alpha = f_\alpha(\alpha) = 0$.

(3) By evaluating polynomials at α_i we obtain a ring epimorphism $\mathbf{Q}[x] \to \mathbf{Q}[\alpha_i]$. The kernel of this map is (f_{α_i}) which is maximal since f_{α_i} is irreducible. Therefore, $\mathbf{Q}[\alpha_i] \cong \mathbf{Q}[x]/(f_{\alpha_i})$ is a field. In particular, $\mathbf{Q}[\alpha_i] = \mathbf{Q}(\alpha_i)$. Now $f_{\alpha_i} = f_\alpha$, so we get isomorphisms $\mathbf{Q}(\alpha) \to \mathbf{Q}[x]/(f_\alpha) \to \mathbf{Q}(\alpha_i)$ the composition of which sends α to α_i. □

Next, we record a fact about roots of unity.

25.2 *Let $\omega_1, \omega_2, \ldots, \omega_n \in \mathbf{C}$ be roots of unity. We have $|\omega_1 + \omega_2 + \cdots + \omega_n| \le n$ with equality if and only if $\omega_1 = \omega_2 = \cdots = \omega_n$.*

Proof. An elementary result from complex analysis states that if α and β are complex numbers, then $|\alpha+\beta| \le |\alpha|+|\beta|$ ("triangle inequality") with equality if and only if $\beta = r\alpha$ for some $r \ge 0$. We now prove the claim by induction on n. The case $n = 1$ is trivial. Assume $n > 1$. By the triangle inequality and then the induction hypothesis, we have $|\omega_1 + \cdots + \omega_n| \le |\omega_1 + \cdots + \omega_{n-1}| + |\omega_n| \le (n-1) + 1 = n$. Suppose we have equality: $|\omega_1 + \cdots + \omega_n| = n$. Then $|\omega_1 + \cdots + \omega_{n-1}| = n - 1$ so the induction hypothesis gives $\omega_1 = \omega_2 = \cdots = \omega_{n-1}$. Also, the equality $|\omega_1 + \cdots + \omega_n| = |\omega_1 + \cdots + \omega_{n-1}| + |\omega_n|$ implies $\omega_n = r(\omega_1 + \cdots + \omega_{n-1}) = r(n-1)\omega_1$ for some $r \ge 0$. Taking moduli gives $r(n-1) = 1$ so that $\omega_n = \omega_1$. The converse is obvious. □

In the proof of the next lemma we will need some results from linear algebra. Let $A \in \mathrm{Mat}_n(\mathbf{C})$. Recall that $f_A(x) = \det(xI - A)$ is the **characteristic polynomial** of A. The Cayley-Hamilton theorem states that $f_A(A) = 0$ if we view $f_A \in (\mathrm{Mat}_n(\mathbf{C}))[x]$ by identifying $\alpha \in \mathbf{C}$ with αI. Let $m_A \in \mathbf{C}[x]$ be the monic polynomial of least degree for which $m_A(A) = 0$. Using arguments similar to those in the proof of 25.1 we find that m_A is uniquely determined and if $g(A) = 0$ for some $g \in \mathbf{C}[x]$, then $m_A | g$. (However, m_A is *not* irreducible, in general.) m_A is called the *minimum polynomial* of A.

25.3 *Let $R : G \to \mathrm{GL}_n(\mathbf{C})$ be a matrix representation affording the character χ and let $a \in G$. Then $|\chi(a)| \le n$ with equality if and only if $R(a) \in \mathbf{C}^\times \cdot I$.*

Proof. Set $A = R(a)$. The eigenvalues $\omega_1, \omega_2, \ldots, \omega_n$ of A are roots of unity and $\chi(a) = \sum_i \omega_i$, so 25.2 gives $|\chi(a)| \le n$.

For the second part, the implication ($\Leftarrow$) is clear, so assume $|\chi(a)| = n$. Then $\omega_1 = \omega_2 = \cdots = \omega_n =: \omega$ using 25.2 again. Hence, $f_A(x) = (x-\omega)^n$. By the Cayley-Hamilton theorem, $f_A(A) = 0$. But also, $g(A) = 0$ where $g(x) = x^{|G|} - 1$, so $m_A | f_A$ and $m_A | g$. Since g has no multiple zeros, neither does m_A, whence $m_A = x - \omega$. Therefore, $A - \omega I = m_A(A) = 0$ and $A = \omega I \in \mathbf{C}^\times \cdot I$. □

25.4 (Burnside's Theorem) *If $|G| = p^x q^y$ with p and q prime, then G is solvable.*

Proof. Suppose the theorem is false and assume G is a counterexample of minimal order.

Step 1: *G is simple and nonabelian, and $x, y > 0$.*

Let H be a normal subgroup of G with $H \neq \{e\}$. By Lagrange's Theorem, both H and G/H have order of the form $p^r q^s$. Suppose $H \neq G$. Then $|H|, |G/H| < |G|$ so by the choice of G, H and G/H are both solvable. But a composition series for H can be completed to a composition series for G by using the correspondence theorem to draw back a composition series for G/H to G. This implies that G is solvable, a contradiction. Whence, $H = G$ and G is simple.

Since any abelian group is solvable, G is nonabelian. Finally, assume that $y = 0$. Then G is a p-group. By Sylow's theorem, G possesses a subnormal series with successive quotients isomorphic to $\mathbf{Z}_p$, implying that G is solvable. This contradiction implies that $y > 0$. Similarly, $x > 0$.

Step 2: *G contains a conjugacy class of order q^d for some $d > 0$.*

Let P be a Sylow p-subgroup of G, so $|P| = p^x > 1$ by Step 1. Since the center of a nontrivial finite p-group is nontrivial, there exists $e \neq a \in Z(P)$. Let $\bar{a}$ denote the conjugacy class of a so that $|\bar{a}| = [G : C_G(a)]$, where $C_G(a) = \{g \in G \mid ga = ag\}$. Now $C_G(a) \supseteq P$ and $C_G(a) \neq G$ (for otherwise $a \in Z(G)$ so that $\{e\} \neq Z(G) \triangleleft G$ contradicting simplicity of G if $Z(G)$ is proper or the fact that G is nonabelian if $Z(G) = G$). We have $p^x q^y = |G| = [G : C_G(a)]|C_G(a)|$ and since $p^x \mid |C_G(a)|$ and $[G : C_G(a)] \neq 1$, the result follows.

Step 3: *Let C_i be a conjugacy class of order q^d ($d \neq 0$) as in Step 2. Then $\chi_j(C_i) \neq 0$ for some $j > 1$ such that $q \nmid n_j$.*

By an orthogonality relation (11.1), we have

$$0 = \sum_j \chi_j(C_i)\overline{\chi_j(C_1)} = 1 + \sum_{j>1} n_j \chi_j(C_i).$$

Therefore, if the statement is not true, we have $1 \in q\mathcal{O}$, whence, $q^{-1} \in \mathcal{O} \cap \mathbf{Q} = \mathbf{Z}$, a contradiction.

Step 4: $\chi_j(C_i)/n_j \in \mathcal{O}$.

First, putting $x = s_i = \sum_{c \in C_i} c$ in 24.2, we get $|C_i|\chi_j(C_i)/n_j \in \mathcal{O}$. Now, $|C_i| = q^d$ and $q \nmid n_j$, so there exist integers r and s such that $r|C_i| + sn_j = 1$. Hence,

$$\chi_j(C_i)/n_j = r|C_i|\chi_j(C_i)/n_j + s\chi_j(C_i) \in \mathcal{O}.$$

Step 5: $|\chi_j(C_i)| = n_j$.

Set $\beta = \chi_j(C_i)$. By 25.3, $|\beta| \leq n_j$. Assume $|\beta| < n_j$. Then $|\alpha| < 1$, where $\alpha = \beta/n_j$. By Step 4, $\alpha \in \mathcal{O}$, so 25.1 applies. In the notation of that result, we have for each $1 \leq l \leq n$, $\alpha_l = \sigma_l(\alpha) = \sigma_l(\beta/n_j) = \sigma_l(\beta)/n_j$. Now β is a sum of n_j roots of unity not all of which are equal (since $|\beta| < n_j$) so the same is true of $\sigma_l(\beta)$ since σ_l is a field isomorphism. Therefore, $|\alpha_l| = |\sigma_l(\beta)|/n_j < 1$. Hence, $|N(\alpha)| = |\prod_l \alpha_l| < 1$. But $0 \neq N(\alpha) \in \mathbf{Z}$, so this is a contradiction. Thus, $|\beta| = n_j$, as desired.

Now we can complete the proof of the theorem. Let R be a matrix representation affording χ_j and set $H = R^{-1}(\mathbf{C}^\times \cdot I) \triangleleft G$. By 25.3 and Step 5, $H \neq \{e\}$ (in fact, H contains C_i). By simplicity of G, $H = G$, implying $R(G) \subseteq \mathbf{C}^\times \cdot I$. But since R is irreducible, this implies $n_j = 1$ (see Section 5), that is, χ_j is a character of degree 1 other than the trivial character ($j > 1$). So G has at least two irreducible characters of degree 1. By Exercise 6, $[G : G'] \geq 2$. Now $G' \triangleleft G$, so this implies $G' = \{e\}$, whence G is abelian, contrary to Step 1. Therefore, the original assumption that there exists a counterexample to the theorem is false. This completes the proof. $\square$