1

The Basics

1.1 Characters

The main subject of this book is complex characters of finite groups, so let us first establish our notation for them. We assume that the reader is familiar with the most basic facts about the characters which we are about to review. Our main source is the book by I. M. Isaacs (see [Is06]). If G is a finite group, then $\mathrm{Char}(G)$ is the set of **characters** of G, which are the traces of the complex **representations** (group homomorphisms)

$$\mathcal{X}\colon G \to \mathrm{GL}_n(\mathbb{C}).$$

If $\chi \in \mathrm{Char}(G)$ is the trace of the representation $\mathcal{X}$ – that is, if

$$\chi(g) = \mathrm{trace}(\mathcal{X}(g))$$

for $g \in G$ – then we say that $\mathcal{X}$ **affords** the character χ. Since $\mathcal{X}(1) = I_n$ is the identity matrix, we say that $n = \chi(1)$ is the **degree** of χ and of $\mathcal{X}$. If $M \in \mathrm{GL}_n(\mathbb{C})$, then the map

$$\mathcal{Y}\colon G \to \mathrm{GL}_n(\mathbb{C})$$

given by $\mathcal{Y}(g) = M^{-1}\mathcal{X}(g)M$ for $g \in G$, defines another representation of G which affords the same character χ (since similar matrices have the same trace), and we say that $\mathcal{X}$ and $\mathcal{Y}$ are **similar**. A striking fact is that two complex representations $\mathcal{X}$ and $\mathcal{Y}$ are similar if and only if they afford the same character. If $\mathcal{Y}$ and $\mathcal{Z}$ are representations of G, then the diagonal sum

$$\mathcal{D} = \begin{pmatrix} \mathcal{Y} & 0 \\ 0 & \mathcal{Z} \end{pmatrix}$$

defines another representation of G. It is clear that if $\mathcal{Y}$ and $\mathcal{Z}$ afford the characters α and β, then $\mathcal{D}$ affords the character $\alpha + \beta$. This proves that the sum of characters is a character. A complex representation $\mathcal{X}$ of G is **irreducible** if it is not similar to a representation of the form

$$\begin{pmatrix} \mathcal{Y} & 0 \\ 0 & \mathcal{Z} \end{pmatrix},$$

where $\mathcal{Y}$ and $\mathcal{Z}$ are representations of G. In this case, we say the character χ afforded by $\mathcal{X}$ is **irreducible**. We denote by $\mathrm{Irr}(G)$ the set of the irreducible characters of a finite group G.

If $\mathcal{X}$ is any complex representation of G, then $\mathcal{X}$ is similar to a diagonal sum of irreducible representations, and this implies that every $\chi \in \mathrm{Char}(G)$ is a non-negative integral linear combination of $\mathrm{Irr}(G)$.

The group homomorphism

$$1_G : G \to \mathbb{C}^\times$$

given by $1_G(g) = 1$ for all $g \in G$ affords the **trivial** or **principal** character 1_G, which is, of course, irreducible. In general, the group homomorphisms

$$\lambda : G \to \mathbb{C}^\times$$

are the irreducible representations (characters) of degree 1, and are very well understood. (In fact, from a historical point of view, these were the first characters that were discovered and used in number theory.) The (irreducible) characters of G of degree 1 are called the **linear** characters of G, and we shall denote them by $\mathrm{Lin}(G)$. It is straightforward to check that $\mathrm{Lin}(G)$ is a group with multiplication given by $(\lambda\nu)(g) = \lambda(g)\nu(g)$ for $g \in G$.

At this point, we do not even know if the set $\mathrm{Irr}(G)$ is finite or not. If $\mathrm{cf}(G)$ is the complex space of **class functions** $G \to \mathbb{C}$ (that is, the complex functions which are constant on the conjugacy classes of G), it is clear that every character χ is in $\mathrm{cf}(G)$, again because similar matrices have the same trace. If $\mathrm{Cl}(G)$ is the set of conjugacy classes of G, $K \in \mathrm{Cl}(G)$ and $\delta_K : G \to \mathbb{C}$ is the **characteristic function** on K (that takes the value 1 on the elements of K and 0 otherwise), then it is trivial to prove that the functions δ_K for $K \in \mathrm{Cl}(G)$ form a basis of $\mathrm{cf}(G)$. In particular, the dimension of $\mathrm{cf}(G)$ is $|\mathrm{Cl}(G)|$, the number of conjugacy classes of G. What is definitely nontrivial is to show that $\mathrm{Irr}(G)$ is a basis of $\mathrm{cf}(G)$. In particular, we have the fundamental equality

$$|\mathrm{Irr}(G)| = |\mathrm{Cl}(G)| .$$

Also, if $\chi \in \mathrm{Char}(G)$, and we write

$$\chi = n_1\chi_1 + \cdots + n_t\chi_t ,$$

where $\chi_i \in \mathrm{Irr}(G)$ and $n_i > 0$, then the set

$$\mathrm{Irr}(\chi) = \{\chi_1, \ldots, \chi_t\}$$

is uniquely determined by χ. We say that these are the **irreducible constituents** of χ. Also, the uniquely determined integer n_i is the **multiplicity** of χ_i in χ. We deduce that a character χ is irreducible if and only if it is not the sum of two characters.

Another fundamental consequence of the fact that $\mathrm{Irr}(G)$ is a basis of $\mathrm{cf}(G)$ is that the *character table* of G is an invertible matrix. If we arbitrarily order $\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_k\}$ and take representatives $g_j \in K_j$, where $\mathrm{Cl}(G) = \{K_1, \ldots, K_k\}$, then the square matrix

$$X(G) = (\chi_i(g_j))$$

is the **character table** of G. (Of course, the character table is only uniquely defined up to row and column permutations. It is customary to choose $\chi_1 = 1_G$ and $g_1 = 1$, and to order the characters by degrees, and the conjugacy classes by the orders of their elements.)

But more is going on. The complex space $\mathrm{cf}(G)$ is a *hermitian* space. If $\alpha, \beta \in \mathrm{cf}(G)$, then

$$[\alpha, \beta] = \frac{1}{|G|} \sum_{x \in G} \alpha(x)\overline{\beta(x)}$$

defines a hermitian inner product on $\mathrm{cf}(G)$. The following is often called the fundamental theorem of character theory, and we formally state it next.

Theorem 1.1 *Let G be a finite group. Then* $\mathrm{Irr}(G)$ *is an orthonormal basis of* $\mathrm{cf}(G)$ *with respect to the previous inner product.*

In particular, if $\psi \in \mathrm{Char}(G)$, then

$$\psi = \sum_{\chi \in \mathrm{Irr}(G)} [\psi, \chi]\chi \,.$$

Hence, ψ is irreducible if and only if $[\psi, \psi] = 1$. Also, $\alpha \in \mathrm{Irr}(G)$ is an irreducible constituent of ψ if and only if $[\psi, \alpha] \neq 0$, and $[\psi, \alpha]$ is the multiplicity of α in χ.

The fact that

$$[\chi, \psi] = \delta_{\chi,\psi}$$

for $\chi, \psi \in \mathrm{Irr}(G)$ is called the **first orthogonality relation**. (In this book, $\delta_{a,b}$ is the Kronecker delta symbol, which is 1 if $a = b$ and 0 otherwise.) From Theorem 1.1, it is not difficult to derive the following.

Theorem 1.2 (Second orthogonality relation) *Let G be a finite group and let $g, h \in G$. Then*

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(g)\overline{\chi(h)} = 0$$

if g and h are not conjugate in G. Otherwise, this sum is $|\mathbf{C}_G(g)|$.

The formula

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 = |G|$$

can therefore be viewed as a particular case of the second orthogonality relation. As we shall see, however, it has a deeper structural explanation. Notice that from this formula we can easily deduce that a finite group G is abelian if and only if all the irreducible characters of G are linear. Also, we see that the **regular character** of G, which is defined as

$$\rho_G = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi$$

has the value $|G|$ on the identity, and 0 elsewhere.

All the proofs of the results that we have mentioned so far can be found in Chapter 2 of [Is06], and in every textbook in character theory. The key object to prove all these results is the *complex group algebra* $\mathbb{C}G$, which we shall consider next.

1.2 Group Algebras

The foundations of character theory are ring-theoretical since they rely on the classification of certain algebras over the complex numbers (the *group algebras*). Since characters are often used to prove deep theorems on finite groups, there is a certain concern among group theorists whenever a purely group-theoretical result is proved using characters. In some sense, it is desirable that a theory solves the problems that it generates. However, there are many results in group theory for which there is no known character-free proof. The most famous is the Feit–Thompson theorem on the solvability of groups of odd order. But there are many others, such as the fact that a non-abelian simple group does not possess a nontrivial conjugacy class of prime power size. Some others, as Burnside's $p^a q^b$ theorem on the solvability of groups of order divisible by at most two primes, had taken many years to be proven by group-theoretical methods. Character theory started as a powerful tool to prove theorems on finite groups but it soon became a marvelous theory on its own.

Cambridge University Press
978-1-108-42844-6 — Character Theory and the McKay Conjecture
Gabriel Navarro
Excerpt
More Information

In this book, we shall sometimes need to work with other fields different from the complex numbers. Let F be a field, and let $\mathcal{A}$ be a ring (with 1) which is also a vector space of finite dimension over F. If

$$\lambda(ab) = a(\lambda b) = (\lambda a)b$$

for all $a, b \in \mathcal{A}$ and $\lambda \in F$, then we say that $\mathcal{A}$ is an F-**algebra**. The canonical example of an F-algebra to keep in mind is

$$\mathrm{Mat}_n(F)\,,$$

the algebra of $n \times n$ matrices over F. If $\mathcal{A}$ is an F-algebra, then

$$\mathbf{Z}(\mathcal{A}) = \{a \in \mathcal{A} \mid ab = ba \text{ for all } b \in \mathcal{A}\}$$

is also an F-algebra, which is called the **center** of $\mathcal{A}$. As is well known,

$$\mathbf{Z}(\mathrm{Mat}_n(F)) = \{\lambda I_n \mid \lambda \in F\}\,.$$

We can easily construct algebras by using direct sums. Recall that if $\mathcal{A}_i$ are F-algebras, then the vector space

$$\mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_k = \{(a_1, \ldots, a_k) \mid a_i \in \mathcal{A}_i\}$$

is an F-algebra with multiplication defined component-wise, and is called the **direct sum** of the algebras $\mathcal{A}_i$.

Our main interest here is the **group algebra**: if F is a field and G is a finite group, then

$$FG = \{\sum_{g \in G} a_g g \mid a_g \in F\}\,,$$

the F-vector space with basis G, is an F-algebra with multiplication defined by

$$\left(\sum_{g \in G} a_g g\right)\left(\sum_{g \in G} b_g g\right) = \sum_{g,h \in G} a_g b_h (gh)\,.$$

(In the same way, we can define the **group ring** RG for any commutative ring R.)

Since $z = \sum_{g \in G} a_g g \in \mathbf{Z}(FG)$ if and only if $z^y = z$ for all $y \in G$, we can easily check that the set of elements of the form

$$\hat{K} = \sum_{x \in K} x\,,$$

where $K \in \mathrm{Cl}(G)$, constitutes an F-basis of $\mathbf{Z}(FG)$. Hence

$$\dim_F(\mathbf{Z}(FG)) = |\mathrm{Cl}(G)|$$

Cambridge University Press
978-1-108-42844-6 — Character Theory and the McKay Conjecture
Gabriel Navarro
Excerpt
More Information

for any field F. We shall later use that if $K, L, M \in \mathrm{Cl}(G)$ and we fix $x_M \in M$ arbitrarily, then

$$\hat{K}\hat{L} = \sum_{M \in \mathrm{Cl}(G)} a_{KLM}\hat{M}\,,$$

where

$$a_{KLM} = |\{(x, y) \in K \times L \mid xy = x_M\}|.$$

Usually, an arbitrary algebra $\mathcal{A}$ is studied by analyzing the *algebra homomorphisms* $\mathcal{A} \to \mathrm{Mat}_n(F)$. Recall that an **algebra homomorphism** between two F-algebras $\mathcal{A}$ and $\mathcal{B}$ is an F-linear, multiplicative map

$$\tau : \mathcal{A} \to \mathcal{B}$$

with $\tau(1) = 1$. If τ is bijective, then $\mathcal{A}$ and $\mathcal{B}$ are **isomorphic**, which is written $\mathcal{A} \cong \mathcal{B}$.

Notice that in order to show that an F-linear map τ with $\tau(1) = 1$ is an algebra homomorphism, it is enough to check that it is multiplicative on some F-basis of $\mathcal{A}$. Hence, an algebra homomorphism

$$\mathcal{X} : FG \to \mathrm{Mat}_n(F)$$

is simply a group homomorphism $\mathcal{X} : G \to \mathrm{GL}_n(F)$ extended F-linearly.

At this point, the representation theory of finite groups splits into two different vast territories: when the characteristic of the field divides the order of the group and when it does not. This book is mainly about the latter situation. (In fact, most, but not all, of what we have to say here is about complex characters and characteristic zero fields.)

If F is any field of characteristic zero, then we can define F-representations of G, similarity and irreducibility of F-representations, and the F-characters of G, in the same way as we did for $\mathbb{C}$.

Theorem 1.3 (Wedderburn) *Let G be a finite group, and let F be an algebraically closed field of characteristic zero. Let k be the number of conjugacy classes of G.*

(a) There are exactly k irreducible non-similar F-representations $\{\mathcal{X}_1, \ldots, \mathcal{X}_k\}$ of G.
(b) If χ_i is the F-character afforded by $\mathcal{X}_i$, then $\{\chi_1, \ldots, \chi_k\}$ are F-linearly independent. Also, $\mathcal{X}_i(FG) = \mathrm{Mat}_{\chi_i(1)}(F)$.
(c) We have that

$$FG \cong \bigoplus_{i=1}^{k} \mathrm{Mat}_{\chi_i(1)}(F)\,.$$

Cambridge University Press
978-1-108-42844-6 — Character Theory and the McKay Conjecture
Gabriel Navarro
Excerpt
More Information

In particular,

$$|G| = \sum_{i=1}^{k} \chi_i(1)^2 .$$

An ingredient in the proof of Theorem 1.3 is Maschke's theorem, which asserts that the algebra FG is *semisimple*.

We shall use the following fact later in Chapter 3. Here $\overline{\mathbb{Q}}$ denotes the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.

Theorem 1.4 *Let G be a finite group, and let $\chi \in \mathrm{Irr}(G)$. Then there exists a representation*

$$\mathcal{X}\colon G \to \mathrm{GL}_n(\overline{\mathbb{Q}})$$

affording χ.

Proof Let k be the number of conjugacy classes of G. Let $F = \overline{\mathbb{Q}}$. By Theorem 1.3, let $\{\psi_1, \ldots, \psi_k\}$ be the set of irreducible F-characters of G. Now, each F-character is a complex character and therefore we can write

$$\psi_i = \sum_{j=1}^{k} a_{ij}\chi_j ,$$

where $\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_k\}$, and the a_{ij} are nonnegative integers. Since the F-irreducible characters $\{\psi_1, \ldots, \psi_k\}$ are F-linearly independent, we have that the matrix $(\psi_i(g_j))$ is invertible, where g_j are representatives of the conjugacy classes of G. In particular, $\{\psi_1, \ldots, \psi_k\}$ is a basis of $\mathrm{cf}(G)$, and the matrix (a_{ij}) is also invertible, because it is the matrix of a change of bases. In particular, it cannot have a column of zeros: given $1 \le s \le k$ there is i such that $a_{is} \neq 0$. Thus $\sum_{i=1}^{k}(a_{is})^2 \ge 1$ for all s. Now,

$$|G| = \sum_{i=1}^{k} \psi_i(1)^2 = \sum_{i=1}^{k}\left(\sum_{j=1}^{k} a_{ij}\chi_j(1)\right)^2 = \sum_{s,t=1}^{k} \chi_s(1)\chi_t(1)\left(\sum_{i=1}^{k} a_{is}a_{it}\right) .$$

Since

$$\sum_{s=1}^{k} \chi_s(1)^2 \left(\sum_{i=1}^{k}(a_{is})^2\right) \ge |G| ,$$

we deduce that

$$\sum_{i=1}^{k} a_{is}a_{it} = \delta_{s,t} .$$

Hence, for each index s there exists a unique j such that $a_{js} \neq 0$, and in fact $a_{js} = 1$. Thus $\psi_j = \chi_s \in \mathrm{Irr}(G)$. This easily implies that $\mathrm{Irr}(G) = \{\psi_1, \ldots, \psi_k\}$. □

Complex group algebras are not fully understood without the **central primitive idempotents**, which are defined as the elements

$$e_\chi = \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g^{-1}) g \in \mathbf{Z}(\mathbb{C}G)$$

for $\chi \in \mathrm{Irr}(G)$.

Theorem 1.5 *Let G be a finite group. We have that*

$$e_\chi e_\psi = \delta_{\chi,\psi} e_\chi$$

for $\chi, \psi \in \mathrm{Irr}(G)$. In particular, $\{e_\chi \mid \chi \in \mathrm{Irr}(G)\}$ is a basis of $\mathbf{Z}(\mathbb{C}G)$.

Corollary 1.6 (Generalized orthogonality relations) *Let G be a finite group and let $g, h \in G$. Let $\chi, \psi \in \mathrm{Irr}(G)$. Then*

$$\frac{1}{|G|} \sum_{g \in G} \chi(gh)\psi(g^{-1}) = \delta_{\chi,\psi} \frac{\chi(h)}{\chi(1)} .$$

Proof The coefficient of h^{-1} in $e_\chi e_\psi$ is

$$\left(\frac{\chi(1)\psi(1)}{|G|^2}\right) \sum_{\substack{x,y \in G \\ xy = h^{-1}}} \chi(x^{-1})\psi(y^{-1}) = \left(\frac{\chi(1)\psi(1)}{|G|^2}\right) \sum_{g \in G} \chi(gh)\psi(g^{-1}) ,$$

by writing $g = y$. By Theorem 1.5, this equals

$$\delta_{\chi,\psi} \frac{\chi(1)}{|G|} \chi(h) ,$$

and the result easily follows. □

From Theorem 1.5, we can easily deduce that $e_\chi \mathbb{C}G$ is an algebra (with identity e_χ) which is isomorphic to $\mathrm{Mat}_{\chi(1)}(\mathbb{C})$. We shall not need this fact, however.

We end this section on group algebras with a quite elementary and useful result.

Theorem 1.7 (Schur's lemma) *Suppose that* $\mathcal{X}\colon G \to \mathrm{GL}_n(\mathbb{C})$ *is an irreducible representation of* G*. If* $M \in \mathrm{Mat}_n(\mathbb{C})$ *is such that* $M\mathcal{X}(g) = \mathcal{X}(g)M$ *for all* $g \in G$*, then* $M = \lambda I_n$ *for some* $\lambda \in \mathbb{C}$.

Proof See Lemma 2.25 of [Is06]. □

All the results that we have mentioned in this section are contained in Chapters 1 and 2 of [Is06]. (The statement that we have used for Theorem 1.3 can also be found in Chapter 1 of [Na98], for example.)

1.3 Character Values, Kernel, Center, and Determinant

Suppose that $\chi \in \mathrm{Char}(G)$ is afforded by the representation $\mathcal{X}$ of degree n. If $g \in G$, then the matrix $\mathcal{X}(g)$ is similar to a diagonal matrix $\mathrm{diag}(\epsilon_1, \ldots, \epsilon_n)$, where $\epsilon_j^{o(g)} = 1$, by elementary linear algebra. (We use $o(g)$ to denote the order of the element g.) Hence

$$\chi(g) = \epsilon_1 + \cdots + \epsilon_n,$$

and $\chi(g)$ is an algebraic integer in the cyclotomic field $\mathbb{Q}_{o(g)}$. (In this book, $\mathbb{Q}_m$ will represent the field $\mathbb{Q}(\xi)$, where $\xi \in \mathbb{C}$ is a primitive mth root of unity. An **algebraic integer** is a root of any monic polynomial in $\mathbb{Z}[x]$, and the set $\mathbf{R}$ of algebraic integers forms a ring in $\mathbb{C}$, by elementary number theory. It is also a well-known elementary fact that $\mathbf{R} \cap \mathbb{Q} = \mathbb{Z}$.) We deduce that $\mathcal{X}(g^{-1})$ is similar to $\mathrm{diag}(\bar{\epsilon}_1, \ldots, \bar{\epsilon}_n)$ and

$$\chi(g^{-1}) = \overline{\chi(g)},$$

where here $\bar{\epsilon}$ is the complex conjugate of $\epsilon \in \mathbb{C}$. Furthermore, if we define $\bar{\mathcal{X}}(g) = \overline{\mathcal{X}(g)}$ (the matrix in which we complex-conjugate every entry), then we see that $\bar{\mathcal{X}}$ is a representation affording the character

$$\bar{\chi}(g) = \overline{\chi(g)}.$$

Furthermore, $[\bar{\chi}, \bar{\chi}] = [\chi, \chi]$, and therefore $\bar{\chi} \in \mathrm{Irr}(G)$ if and only if $\chi \in \mathrm{Irr}(G)$. The character $\bar{\chi}$ is the **complex conjugate** of χ.

Notice that if $\chi(1) = 1$, then $\chi(g)$ is a root of unity for every $g \in G$, and in particular $\chi(g) \neq 0$ for all $g \in G$. (The converse of this is true, and it is a theorem of Burnside, which we shall consider later.)

Since $|\epsilon_j| = 1$, by using the triangle inequality for complex numbers we have that

$$|\chi(g)| \leq \chi(1)\,.$$

(The well-known triangle inequality asserts that if $\alpha_i \in \mathbb{C}$, then

$$|\alpha_1 + \cdots + \alpha_n| \leq |\alpha_1| + \cdots + |\alpha_n|\,,$$

with equality if and only if there are nonnegative real numbers λ_i and some $\alpha \in \mathbb{C}$ such that $\alpha_i = \lambda_i \alpha$ for all i.) Using again the triangle inequality, we also deduce that $|\chi(g)| = \chi(1)$ if and only if $\mathcal{X}(g)$ is a scalar matrix, and that $\chi(g) = \chi(1)$ if and only if $\mathcal{X}(g) = I_n$. Hence the subgroup $\ker(\mathcal{X})$ is uniquely determined by the character χ that it affords. This subgroup, denoted by $\ker(\chi)$, is the **kernel** of the character χ. The same happens with the subgroup $\mathbf{Z}(\chi) = \{g \in G \mid \mathcal{X}(g) \text{ is scalar}\}$, which is called the **center** of the character χ. A character χ is **faithful** if $\ker(\chi) = 1$. Notice that

$$\bigcap_{\chi \in \mathrm{Irr}(G)} \ker(\chi) = 1$$

by the second orthogonality relation.

Since the determinant map

$$\det\colon \mathrm{GL}_n(\mathbb{C}) \to \mathbb{C}^{\times}$$

is a group homomorphism, we have that χ has associated a linear character $\det(\chi)$ given by

$$\det(\chi)(g) = \det(\mathcal{X}(g))\,.$$

Notice that, again, $\det(\chi)$ only depends on χ, since two representations affording χ are similar. We write $o(\chi)$ to denote the order of $\det(\chi)$ in the group $\mathrm{Lin}(G)$. This is called the **determinantal order** of χ.

1.4 More Algebraic Integers

If $\chi \in \mathrm{Irr}(G)$ and $g \in G$, we already know that $\chi(g) \in \mathbf{R}$. But there are some other algebraic integers associated with χ of the utmost importance. In order to introduce them, we need to come back, again, to representations. If $\mathcal{X}$ affords $\chi \in \mathrm{Irr}(G)$, let us extend $\mathcal{X}$ linearly to a homomorphism of algebras

$$\mathcal{X}\colon \mathbb{C}G \to \mathrm{Mat}_n(\mathbb{C})\,.$$