An Introduction to Character Theory

J.R. McHugh

March 21, 2018

References

- *Abstract Algebra*, Third Edition. David S. Dummit and Richard M. Foote. 2004 John Wiley and Sons, Inc. (See chapters 18 and 19.)
- *Character Theory of Finite Groups*. I. Martin Isaacs. 1976 Academic Press.
- *A Course in Finite Group Representation Theory*. Peter Webb. 2016 Cambridge University Press. (A pre-publication version may be found at Peter Webb's site `http://www-users.math.umn.edu/~webb/`)

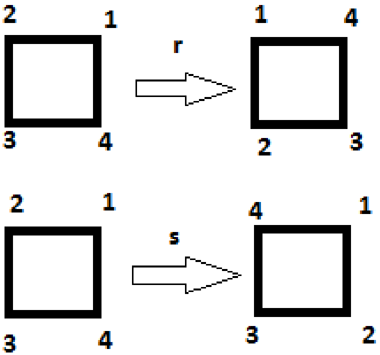
Motivation

Consider the set D_8 whose elements are the symmetries of a square.

Motivation

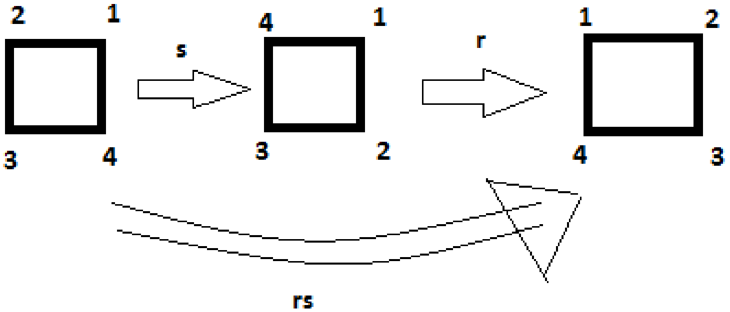
Consider the set D_8 whose elements are the symmetries of a square.

Two specific symmetries r and s in D_8 are described by the diagrams below:



We define a multiplication in the set D_8 by the rule: if x and y are symmetries then xy is the symmetry obtained by first performing y and then performing x.

For example, the symmetry rs is described by:



The multiplication in D_8 we have defined is associative and D_8 has an identity element 1 and inverses. In other words, the set D_8 together with our multiplication is a *group*.

The multiplication in D_8 we have defined is associative and D_8 has an identity element 1 and inverses. In other words, the set D_8 together with our multiplication is a *group*.

It is not difficult to see that every symmetry in D_8 is equal to a product of the form $r^i s^j$. We say that the group D_8 is *generated* by r and s.

The multiplication in D_8 we have defined is associative and D_8 has an identity element 1 and inverses. In other words, the set D_8 together with our multiplication is a *group*.

It is not difficult to see that every symmetry in D_8 is equal to a product of the form $r^i s^j$. We say that the group D_8 is *generated* by r and s.

The symmetries r and s satisfy $r^4 = 1$, $s^2 = 1$, and $srs = r^{-1}$.

It turns out that these equalities (called *relations*) completely determine how symmetries multiply together in D_8. We thus obtain a *presentation* for the group D_8:

$$D_8 = \langle r, s | r^4 = s^2 = 1, srs = r^{-1} \rangle.$$

This presentation allows us to define the group "abstractly," i.e., without any reference to the original square and its symmetries.

This presentation allows us to define the group "abstractly," i.e., without any reference to the original square and its symmetries.

Question

If we begin with the abstract definition of D_8 as a group, how can we recover the square-symmetry interpretation for its elements?

This presentation allows us to define the group "abstractly," i.e., without any reference to the original square and its symmetries.

Question

If we begin with the abstract definition of D_8 as a group, how can we recover the square-symmetry interpretation for its elements?

Here's one way. Begin by noting that a symmetry of the square permutes its vertices and is uniquely determined by how it permutes the vertices. We then have a one-to-one map

$$X : D_8 \to S_4.$$

(e.g., $X(r) = (1\,2\,3\,4)$ and $X(s) = (2\,4)$.) The map X is known as a *permutation representation* and is in fact a group homomorphism.

Another way is to use a *group action*.

Definition

Let G be a group and Ω a set. A *group action* of G on Ω is a map from $G \times \Omega$ to Ω written $g \cdot \omega$ for $g \in G$, $\omega \in \Omega$ that satisfies both $g \cdot (h \cdot \omega) = gh \cdot \omega$ and $1 \cdot \omega = \omega$ for all $g, h \in G$ and $\omega \in \Omega$.

Another way is to use a *group action*.

Definition

Let G be a group and Ω a set. A *group action* of G on Ω is a map from $G \times \Omega$ to Ω written $g \cdot \omega$ for $g \in G$, $\omega \in \Omega$ that satisfies both $g \cdot (h \cdot \omega) = gh \cdot \omega$ and $1 \cdot \omega = \omega$ for all $g, h \in G$ and $\omega \in \Omega$.

When a group action of G on Ω exists, we say G *acts on* Ω. For example, if V is a vector space over the field F then the multiplicative group $F^\times = F \setminus \{0\}$ acts on V since $c \cdot (d \cdot v) = cd \cdot v$ and $1 \cdot v = v$ for all $c, d \in F$ and $v \in V$ (these are axioms built into the definition of a vector space).

Another example: any group G acts on itself by left multiplication.

Let $X : D_8 \to S_4$ be the permutation representation of D_8 from before. We can define a group action of D_8 on $\Omega = \{1, 2, 3, 4\}$ by $g \cdot \omega = X(g)(\omega)$ for $g \in D_8$ and $\omega \in \Omega$. For example, $r \cdot 1 = 2$ and $s \cdot 2 = 4$.

Let $X : D_8 \to S_4$ be the permutation representation of D_8 from before. We can define a group action of D_8 on $\Omega = \{1, 2, 3, 4\}$ by $g \cdot \omega = X(g)(\omega)$ for $g \in D_8$ and $\omega \in \Omega$. For example, $r \cdot 1 = 2$ and $s \cdot 2 = 4$.

The fact that this defines an actual group action hinges on the fact that X is a homomorphism:

$$g \cdot (h \cdot \omega) = X(g)(X(h)(\omega)) = (X(g) \circ X(h))(\omega) = X(gh)(\omega) = gh \cdot \omega$$

and

$$1 \cdot \omega = X(1)(\omega) = \omega.$$

Let $X : D_8 \to S_4$ be the permutation representation of D_8 from before. We can define a group action of D_8 on $\Omega = \{1, 2, 3, 4\}$ by $g \cdot \omega = X(g)(\omega)$ for $g \in D_8$ and $\omega \in \Omega$. For example, $r \cdot 1 = 2$ and $s \cdot 2 = 4$.

The fact that this defines an actual group action hinges on the fact that X is a homomorphism:

$$g \cdot (h \cdot \omega) = X(g)(X(h)(\omega)) = (X(g) \circ X(h))(\omega) = X(gh)(\omega) = gh \cdot \omega$$

and

$$1 \cdot \omega = X(1)(\omega) = \omega.$$

We can interpret each element of D_8 as a symmetry of the square via this group action.

We can recover the permutation representation X from the action of D_8 on $\Omega = \{1, 2, 3, 4\}$.

The map from Ω to itself induced by left multiplication by an element $g \in D_8$ has a 2-sided inverse (can you guess what the inverse is?). In other words this map is a permutation, so we can treat it as an element of S_4.

We can recover the permutation representation X from the action of D_8 on $\Omega = \{1, 2, 3, 4\}$.

The map from Ω to itself induced by left multiplication by an element $g \in D_8$ has a 2-sided inverse (can you guess what the inverse is?). In other words this map is a permutation, so we can treat it as an element of S_4.

The map $X : D_8 \to S_4$ defined by $X(g) = (\omega \mapsto g \cdot \omega)$ is a homomorphism because

$$X(gh) = (\omega \mapsto gh \cdot \omega) = (\omega \mapsto g \cdot \omega) \circ (\omega \mapsto h \cdot \omega) = X(g)X(h).$$

Note that the middle equality above holds by the axiom $g \cdot (h \cdot \omega) = gh \cdot \omega$ required for a group action.

We can recover the permutation representation X from the action of D_8 on $\Omega = \{1, 2, 3, 4\}$.

The map from Ω to itself induced by left multiplication by an element $g \in D_8$ has a 2-sided inverse (can you guess what the inverse is?). In other words this map is a permutation, so we can treat it as an element of S_4.

The map $X : D_8 \to S_4$ defined by $X(g) = (\omega \mapsto g \cdot \omega)$ is a homomorphism because

$$X(gh) = (\omega \mapsto gh \cdot \omega) = (\omega \mapsto g \cdot \omega) \circ (\omega \mapsto h \cdot \omega) = X(g)X(h).$$

Note that the middle equality above holds by the axiom $g \cdot (h \cdot \omega) = gh \cdot \omega$ required for a group action.

The group D_8 is not special: in general, a group action determines a permutation representation and vice versa.

To recap what we have done: we began with a "concrete" group (D_8) with an action "built into" the group itself (the elements of D_8 were symmetries of a square). We then split the concrete group up into two components: an "abstract" group (D_8 defined by generators and relations, i.e., a set of symbols with multiplication) and a group action/permutation representation. What is the use of this latter perspective?

To recap what we have done: we began with a "concrete" group (D_8) with an action "built into" the group itself (the elements of D_8 were symmetries of a square). We then split the concrete group up into two components: an "abstract" group (D_8 defined by generators and relations, i.e., a set of symbols with multiplication) and a group action/permutation representation. What is the use of this latter perspective?

Cayley's Theorem

Every group is isomorphic to a subgroup of a symmetric group.

To recap what we have done: we began with a "concrete" group (D_8) with an action "built into" the group itself (the elements of D_8 were symmetries of a square). We then split the concrete group up into two components: an "abstract" group (D_8 defined by generators and relations, i.e., a set of symbols with multiplication) and a group action/permutation representation. What is the use of this latter perspective?

Cayley's Theorem

Every group is isomorphic to a subgroup of a symmetric group.

Sylow's Theorem

If G is a finite group of order $p^a m$ where p is a prime and p does not divide m, then G has a subgroup of order p^a.

To recap what we have done: we began with a "concrete" group (D_8) with an action "built into" the group itself (the elements of D_8 were symmetries of a square). We then split the concrete group up into two components: an "abstract" group (D_8 defined by generators and relations, i.e., a set of symbols with multiplication) and a group action/permutation representation. What is the use of this latter perspective?

Cayley's Theorem

Every group is isomorphic to a subgroup of a symmetric group.

Sylow's Theorem

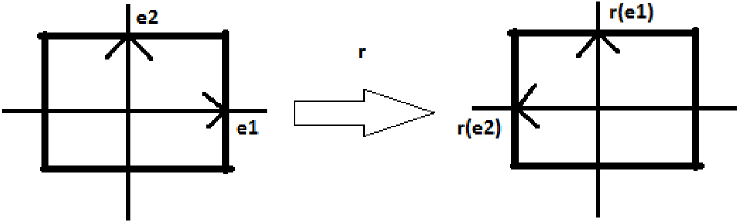
If G is a finite group of order $p^a m$ where p is a prime and p does not divide m, then G has a subgroup of order p^a.

Both of these theorems are proved using the abstract theory of group actions.

Recall that the *general linear group of degree n over the field F* is the group $GL_n(F)$ of invertible $n \times n$ matrices with entries in the field F. If V is a vector space over F, the group $GL(V)$ is the group of nonsingular linear transformations of V.

Recall that the *general linear group of degree n over the field F* is the group $GL_n(F)$ of invertible $n \times n$ matrices with entries in the field F. If V is a vector space over F, the group $GL(V)$ is the group of nonsingular linear transformations of V.

If we embed the square at the center of a Cartesian coordinate system we can reinterpret the action of D_8 on the square via linear transformations:



In other words, the action of D_8 on the square can be thought of as a homomorphism $X : D_8 \to GL_2(\mathbb{R})$ with

$$X(r) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } X(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Representations

Definition

Let F be a field, V a vector space over F, and G a group. An *F-representation of G* is a homomorphism $X : G \to GL(V)$.

Representations

Definition

Let F be a field, V a vector space over F, and G a group. An *F-representation of G* is a homomorphism $X : G \to GL(V)$.

In case $\dim(V) = n < \infty$ we obtain an isomorphism $GL(V) \cong GL_n(F)$ after choosing a basis for V. A homomorphism $X : G \to GL_n(F)$ is sometimes called a *matrix representation*. The *degree* of the representation is n.

Just as for permutation representations, we may view a representation $X : G \to GL(V)$ as a description of an action of G on the vectors in V — simply define $g \cdot v = X(g)(v)$. The action of G on V satisfies, for all $g, h \in G$, $v, w \in V$, and $\lambda \in F$,

(1) $g \cdot (h \cdot v) = gh \cdot v$

(2) $1 \cdot v = v$

(3) $g \cdot (v + \lambda w) = g \cdot v + \lambda(g \cdot w)$.

An action of G on an F-vector space which satisfies all of the above is called a *linear action*.

Just as for permutation representations, we may view a representation $X : G \to GL(V)$ as a description of an action of G on the vectors in V — simply define $g \cdot v = X(g)(v)$. The action of G on V satisfies, for all $g, h \in G$, $v, w \in V$, and $\lambda \in F$,

(1) $g \cdot (h \cdot v) = gh \cdot v$

(2) $1 \cdot v = v$

(3) $g \cdot (v + \lambda w) = g \cdot v + \lambda(g \cdot w)$.

An action of G on an F-vector space which satisfies all of the above is called a *linear action*.

Given a linear action of G on V we may define a representation $X : G \to GL(V)$ by letting $X(g)$ denote the linear operator $v \mapsto g \cdot v$.

Some examples:

- We can create a homomorphism from any group G to $GL(V)$ by defining $X(g) = 1$ for all $g \in G$. This representation is called the *trivial representation*.

Some examples:

- We can create a homomorphism from any group G to $GL(V)$ by defining $X(g) = 1$ for all $g \in G$. This representation is called the *trivial representation*.
- Let $e_1, e_2, \ldots, e_n$ be a basis for the vector space V over F. Define an action of S_n on the basis vectors by $\sigma \cdot e_i = e_{\sigma(i)}$ for $\sigma \in S_n$. Extending the action linearly to all of V produces a linear action of S_n on V and thus a representation $X : S_n \to GL_n(F)$.

Some examples:

- We can create a homomorphism from any group G to $GL(V)$ by defining $X(g) = 1$ for all $g \in G$. This representation is called the *trivial representation*.
- Let $e_1, e_2, \ldots, e_n$ be a basis for the vector space V over F. Define an action of S_n on the basis vectors by $\sigma \cdot e_i = e_{\sigma(i)}$ for $\sigma \in S_n$. Extending the action linearly to all of V produces a linear action of S_n on V and thus a representation $X : S_n \to GL_n(F)$.
- If G is cyclic of order m with generator g, define $X : G \to GL_1(\mathbb{C})$ by $X(g^i) = (\xi^i)$ where ξ is a fixed mth root of unity.

Some examples:

- We can create a homomorphism from any group G to $GL(V)$ by defining $X(g) = 1$ for all $g \in G$. This representation is called the *trivial representation*.
- Let $e_1, e_2, \ldots, e_n$ be a basis for the vector space V over F. Define an action of S_n on the basis vectors by $\sigma \cdot e_i = e_{\sigma(i)}$ for $\sigma \in S_n$. Extending the action linearly to all of V produces a linear action of S_n on V and thus a representation $X : S_n \to GL_n(F)$.
- If G is cyclic of order m with generator g, define $X : G \to GL_1(\mathbb{C})$ by $X(g^i) = (\xi^i)$ where ξ is a fixed mth root of unity.
- Let G be a finite group and let N be a normal subgroup of G. Assume that N is isomorphic to a direct product of cyclic groups each of prime order p. Then N is a vector space over $\mathbb{F}_p$. There is a linear action of G on N induced by conjugation. In other words, conjugation by elements of G gives a representation $X : G \to GL(N) \cong GL_n(\mathbb{F}_p)$.

There is another way to interpret what a representation is.

Definition

Let F be a field and G a finite group. The *group algebra* FG is the F-vector space with basis G and multiplication defined by the linear extension of the multiplication in G.

There is another way to interpret what a representation is.

Definition

Let F be a field and G a finite group. The *group algebra* FG is the F-vector space with basis G and multiplication defined by the linear extension of the multiplication in G.

For example, a typical element in $\mathbb{Q}S_3$ may be written

$$a_1 1 + a_2(1\,2) + a_3(1\,3) + a_4(2\,3) + a_5(1\,2\,3) + a_6(1\,3\,2)$$

Where all $a \in \mathbb{Q}$. An example of multiplication in $\mathbb{Q}S_3$:

$$[3(1\,2) - \frac{2}{3}(1\,2\,3)] \cdot [-(1\,2)] = -3 \cdot 1 + \frac{2}{3}(1\,3).$$

FG has an identity element: $1_F 1_G$.

FG has an identity element: $1_F 1_G$.

We identify the elements $\lambda 1_G$ for $\lambda \in F$ with the field F. After making this identification we can say that $F \subseteq Z(FG)$.

Given an F-representation $X : G \to GL(V)$ of a finite group G we make V into a unital FG-module by defining

$$(\sum_{g \in G} a_g g) \cdot v = \sum_{g \in G} a_g X(g)(v).$$

Given an F-representation $X : G \to GL(V)$ of a finite group G we make V into a unital FG-module by defining

$$(\sum_{g \in G} a_g g) \cdot v = \sum_{g \in G} a_g X(g)(v).$$

Conversely, if V is a unital FG-module then V is in particular an F-vector space (since $F \subseteq FG$) and restricting the "action" of FG to the basis G gives a linear action of G on V. Hence we get a representation.

We think of a representation in 3 ways:

(1) a homomorphism from a group into the group of nonsingular linear transformations of a vector space (or the group of nonsingular matrices)

(2) a linear action of a group on a vector space

(3) a module over a group algebra.

Since these notions all coincide we call each of them a representation.

We think of a representation in 3 ways:

(1) a homomorphism from a group into the group of nonsingular linear transformations of a vector space (or the group of nonsingular matrices)

(2) a linear action of a group on a vector space

(3) a module over a group algebra.

Since these notions all coincide we call each of them a representation.

The third interpretation above provides a new example of a representation: the *regular representation* of G is FG considered as an FG-module (this is sometimes denoted ${}_{FG}FG$ to emphasize the left FG-module structure).

Definition

The F-representations X and Y of the finite group G are *equivalent* if the corresponding FG-modules are isomorphic.

Definition

The F-representations X and Y of the finite group G are *equivalent* if the corresponding FG-modules are isomorphic.

Exercise: If X and Y are equivalent F-representations of G, show that $T^{-1}XT = Y$ for some linear transformation T.

Definition

A representation $X : G \to GL(V)$ is *irreducible* if V is an irreducible FG-module (that is, the only FG-submodules of V are 0 and V).

Definition

A representation $X : G \to GL(V)$ is *irreducible* if V is an irreducible FG-module (that is, the only FG-submodules of V are 0 and V).

Note that an FG-submodule $W \subseteq V$ is just a subspace that is invariant under the action of the group elements: for all $g \in G$, $g \cdot W = W$.

Definition

A representation $X : G \to GL(V)$ is *irreducible* if V is an irreducible FG-module (that is, the only FG-submodules of V are 0 and V).

Note that an FG-submodule $W \subseteq V$ is just a subspace that is invariant under the action of the group elements: for all $g \in G$, $g \cdot W = W$.

The "square-symmetry" representation $X : D_8 \to GL_2(\mathbb{R})$ is irreducible: otherwise, $\mathbb{R}^2$ would have an $\mathbb{R}D_8$ submodule of $\mathbb{R}$-dimension 1. But lines in $\mathbb{R}^2$ are not left invariant by the "rotation element" $r \in D_8$.

Definition

A representation $X : G \to GL(V)$ is *indecomposable* if V is an indecomposable FG-module (that is, V cannot be written as a direct sum $V = U \oplus W$ of FG-submodules in a nontrivial way).

Definition

A representation $X : G \to GL(V)$ is *indecomposable* if V is an indecomposable FG-module (that is, V cannot be written as a direct sum $V = U \oplus W$ of FG-submodules in a nontrivial way).

Let $Z_2 = \langle z \rangle$ and define $X : Z_2 \to GL_2(\mathbb{F}_2)$ by $X(z) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Then X is a reducible, indecomposable representation: the subspace $\text{span}\{(1,0)\}$ is the only Z_2-invariant subspace of $\mathbb{F}_2^2$.

Maschke's Theorem

Let G be a finite group and F be a field whose characteristic does not divide the order of G. Let V be an FG-module and let U be an FG-submodule of V. Then there exists another FG-submodule W of V such that $V = U \oplus W$.

Maschke's Theorem

Let G be a finite group and F be a field whose characteristic does not divide the order of G. Let V be an FG-module and let U be an FG-submodule of V. Then there exists another FG-submodule W of V such that $V = U \oplus W$.

Proof: U is a subspace of the F-vector space V, so $V = U \oplus W_0$ for some subspace W_0.

Maschke's Theorem

Let G be a finite group and F be a field whose characteristic does not divide the order of G. Let V be an FG-module and let U be an FG-submodule of V. Then there exists another FG-submodule W of V such that $V = U \oplus W$.

Proof: U is a subspace of the F-vector space V, so $V = U \oplus W_0$ for some subspace W_0.But W_0 need not be G-invariant. To fix this, let $\pi_0 : V \to U$ be the projection map with kernel W_0 and define $\pi : V \to U$ by

$$\pi(v) = \frac{1}{|G|} \sum_{g \in G} g\pi_0(g^{-1}v).$$

Maschke's Theorem

Let G be a finite group and F be a field whose characteristic does not divide the order of G. Let V be an FG-module and let U be an FG-submodule of V. Then there exists another FG-submodule W of V such that $V = U \oplus W$.

Proof: U is a subspace of the F-vector space V, so $V = U \oplus W_0$ for some subspace W_0.But W_0 need not be G-invariant. To fix this, let $\pi_0 : V \to U$ be the projection map with kernel W_0 and define $\pi : V \to U$ by

$$\pi(v) = \frac{1}{|G|} \sum_{g \in G} g\pi_0(g^{-1}v).$$

Since $g\pi_0 g^{-1}$ is a linear transformation, π is as well.

Maschke's Theorem

Let G be a finite group and F be a field whose characteristic does not divide the order of G. Let V be an FG-module and let U be an FG-submodule of V. Then there exists another FG-submodule W of V such that $V = U \oplus W$.

Proof: U is a subspace of the F-vector space V, so $V = U \oplus W_0$ for some subspace W_0.But W_0 need not be G-invariant. To fix this, let $\pi_0 : V \to U$ be the projection map with kernel W_0 and define $\pi : V \to U$ by

$$\pi(v) = \frac{1}{|G|} \sum_{g \in G} g\pi_0(g^{-1}v).$$

Since $g\pi_0 g^{-1}$ is a linear transformation, π is as well.If $h \in G$ then

$$\pi(hv) = \frac{1}{|G|} \sum_{g \in G} g\pi_0(g^{-1}hv) = \frac{1}{|G|} \sum_{g \in G} hh^{-1}g\pi_0((h^{-1}g)^{-1}v) = h\pi(v).$$

So π is an FG-module homomorphism. Thus $W = \ker \pi$ is an FG-submodule of V.

So π is an FG-module homomorphism. Thus $W = \ker \pi$ is an FG-submodule of V.If $u \in U$ then

$$\pi(u) = \frac{1}{|G|} \sum_{g \in G} g \pi_0(g^{-1} u) = \frac{1}{|G|} \sum_{g \in G} u = u.$$

So π is an FG-module homomorphism. Thus $W = \ker \pi$ is an FG-submodule of V.If $u \in U$ then

$$\pi(u) = \frac{1}{|G|} \sum_{g \in G} g\pi_0(g^{-1}u) = \frac{1}{|G|} \sum_{g \in G} u = u.$$

It follows that if $u \in U \cap W$ then $0 = \pi(u) = u$, i.e., $U \cap W = 0$.

So π is an FG-module homomorphism. Thus $W = \ker \pi$ is an FG-submodule of V.If $u \in U$ then

$$\pi(u) = \frac{1}{|G|} \sum_{g \in G} g\pi_0(g^{-1}u) = \frac{1}{|G|} \sum_{g \in G} u = u.$$

It follows that if $u \in U \cap W$ then $0 = \pi(u) = u$, i.e., $U \cap W = 0$.If $v \in V$ then $\pi(v) \in U$ and $v - \pi(v) \in W$ since $\pi(v - \pi(v)) = \pi(v) - \pi(\pi(v)) = 0$. Thus $v = \pi(v) + (v - \pi(v)) \in U + W$ and $V = U \oplus W$. $\square$

Wedderburn's Theorem

Let R be a ring with $1 \neq 0$. The following are equivalent:

(1) Every R-module is injective.

(2) Every R-module is a direct sum of irreducible submodules.

(3) R is isomorphic to a direct product of finitely many matrix rings with entries in division rings.

Wedderburn's Theorem

Let R be a ring with $1 \neq 0$. The following are equivalent:

(1) Every R-module is injective.

(2) Every R-module is a direct sum of irreducible submodules.

(3) R is isomorphic to a direct product of finitely many matrix rings with entries in division rings.

Let F be a field whose characteristic does not divide $|G|$. Then FG satisfies (1). By (2), to understand all FG-modules, it is enough to understand the *irreducible* ones!

Wedderburn's Theorem

Let R be a ring with $1 \neq 0$. The following are equivalent:

(1) Every R-module is injective.

(2) Every R-module is a direct sum of irreducible submodules.

(3) R is isomorphic to a direct product of finitely many matrix rings with entries in division rings.

Let F be a field whose characteristic does not divide $|G|$. Then FG satisfies (1). By (2), to understand all FG-modules, it is enough to understand the *irreducible* ones!

The matrix ring $M_n(D)$ over the division ring D has a unique isomorphism class of irreducible (left) modules. In essence, the only irreducible $M_n(D)$-module is D^n. It then follows directly from (3) above that FG has only *finitely many* irreducible modules!

If we choose our field F to be $\mathbb{C}$ then the division rings that appear in Wedderburn's Theorem all become $\mathbb{C}$. That is, for G a finite group,

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

and $\mathbb{C}G$ has exactly r distinct isomorphism types of irreducible modules with complex dimensions $n_1, n_2, \ldots, n_r$.

If we choose our field F to be $\mathbb{C}$ then the division rings that appear in Wedderburn's Theorem all become $\mathbb{C}$. That is, for G a finite group,

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

and $\mathbb{C}G$ has exactly r distinct isomorphism types of irreducible modules with complex dimensions $n_1, n_2, \ldots, n_r$.

Note that

$$|G| = \dim_{\mathbb{C}}(\mathbb{C}G) = \sum_{i=1}^{r} \dim(M_{n_i}(\mathbb{C})) = \sum_{i=1}^{r} n_i^2.$$

It can be shown that each n_i divides $|G|$.

If we choose our field F to be $\mathbb{C}$ then the division rings that appear in Wedderburn's Theorem all become $\mathbb{C}$. That is, for G a finite group,

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

and $\mathbb{C}G$ has exactly r distinct isomorphism types of irreducible modules with complex dimensions $n_1, n_2, \ldots, n_r$.

Note that

$$|G| = \dim_{\mathbb{C}}(\mathbb{C}G) = \sum_{i=1}^{r} \dim(M_{n_i}(\mathbb{C})) = \sum_{i=1}^{r} n_i^2.$$

It can be shown that each n_i divides $|G|$.

Also note that $\dim_{\mathbb{C}}(Z(\mathbb{C}G)) = r$. It is not hard to show that a basis for $Z(\mathbb{C}G)$ is given by "class sums" $\sum_{g \in \mathcal{K}} g$ where $\mathcal{K}$ is a G-conjugacy class. It follows that r is the number of conjugacy classes of elements of G.

If A is an abelian group then A has $|A|$ conjugacy classes. Under the notation of the previous frame we have $r = |A|$ and this forces each $n_i = 1$. Thus all irreducible $\mathbb{C}A$-modules have dimension 1.

If G is non-abelian then $r < |G|$. Thus some $n_i > 1$. We have observed that a group G is abelian if and only if all irreducible $\mathbb{C}G$-modules have dimension 1 over $\mathbb{C}$.

Characters

We want to get our hands on the irreducible $\mathbb{C}$-representations of G. The problem is that, while there are only finitely many (up to equivalence), their degrees can be massive. For example, the monster group M is a simple group of order

$$\begin{aligned} |M| = {} & 808,017,424,794,512,875,886,459, \\ & 904,961,710,757,005,754,368,000,000,000. \end{aligned}$$

(According to Wikipedia, the order of M is approximately 808 sexdecillion.)

Characters

We want to get our hands on the irreducible $\mathbb{C}$-representations of G. The problem is that, while there are only finitely many (up to equivalence), their degrees can be massive. For example, the monster group M is a simple group of order

$$
\begin{aligned}
|M| = {} & 808,017,424,794,512,875,886,459, \\
& 904,961,710,757,005,754,368,000,000,000.
\end{aligned}
$$

(According to Wikipedia, the order of M is approximately 808 sexdecillion.) The smallest nontrivial irreducible representation of M

(famously) has degree $196,883$. A square matrix of order $196,883$ has $38,762,915,689$ entries.

Observe that if $X : G \to GL_n(\mathbb{C})$ is a representation and $g \in G$ has order k, then $X(g)^k = 1$. In other words the minimal polynomial of $X(g)$ divides $x^k - 1$, hence $X(g)$ is diagonalizable. This suggests studying the eigenvalues of $X(g)$ for the various elements of G and leads to the following definition:

Definition

If $X : G \to GL_n(\mathbb{C})$ is a representation of a finite group G, the *character of G afforded by X* is the function $\chi(g) = \mathrm{trace}(X(g))$.

Observe that if $X : G \to GL_n(\mathbb{C})$ is a representation and $g \in G$ has order k, then $X(g)^k = 1$. In other words the minimal polynomial of $X(g)$ divides $x^k - 1$, hence $X(g)$ is diagonalizable. This suggests studying the eigenvalues of $X(g)$ for the various elements of G and leads to the following definition:

Definition

If $X : G \to GL_n(\mathbb{C})$ is a representation of a finite group G, the *character of G afforded by X* is the function $\chi(g) = \mathrm{trace}(X(g))$.

So $\chi(g)$ is the sum of the eigenvalues of $X(g)$. In particular χ is a function from G to $\mathbb{C}$. In general, χ is not a group homomorphism.

Observe that if $X : G \to GL_n(\mathbb{C})$ is a representation and $g \in G$ has order k, then $X(g)^k = 1$. In other words the minimal polynomial of $X(g)$ divides $x^k - 1$, hence $X(g)$ is diagonalizable. This suggests studying the eigenvalues of $X(g)$ for the various elements of G and leads to the following definition:

Definition

If $X : G \to GL_n(\mathbb{C})$ is a representation of a finite group G, the *character of G afforded by X* is the function $\chi(g) = \text{trace}(X(g))$.

So $\chi(g)$ is the sum of the eigenvalues of $X(g)$. In particular χ is a function from G to $\mathbb{C}$. In general, χ is not a group homomorphism.

Note that $\chi(1) = \text{trace}(X(1)) = \text{trace}(I) = n$, the degree of the representation X.

Some examples:

- The character χ of the trivial representation $X : G \to GL_1(\mathbb{C})$ is just the constant function 1 on G: $\chi(g) = 1$ for all $g \in G$. This character is called the *principal character of* G.

Some examples:

- The character χ of the trivial representation $X : G \to GL_1(\mathbb{C})$ is just the constant function 1 on G: $\chi(g) = 1$ for all $g \in G$. This character is called the *principal character of* G.
- Let G act on $\{1, 2, \ldots, n\}$ and let V be a $\mathbb{C}$-space with basis $e_1, e_2, \ldots, e_n$. Let G act on the basis vectors by $g \cdot e_i = e_{g \cdot i}$ and extend the action linearly to all of V. Then V is a $\mathbb{C}G$-module with associated homomorphism $X : G \to GL(V)$. The matrix $X(g)$ with respect to the basis $e_1, e_2, \ldots, e_n$ has a 1 in position i, j if and only if $g \cdot j = i$ and zeros elsewhere. In particular, there will be a 1 in position i, i if $g \cdot i = i$ and a 0 otherwise. This shows that, if χ is the character afforded by X, then

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

Some examples:

- The character χ of the trivial representation $X : G \to GL_1(\mathbb{C})$ is just the constant function 1 on G: $\chi(g) = 1$ for all $g \in G$. This character is called the *principal character of* G.
- Let G act on $\{1, 2, \ldots, n\}$ and let V be a $\mathbb{C}$-space with basis $e_1, e_2, \ldots, e_n$. Let G act on the basis vectors by $g \cdot e_i = e_{g \cdot i}$ and extend the action linearly to all of V. Then V is a $\mathbb{C}G$-module with associated homomorphism $X : G \to GL(V)$. The matrix $X(g)$ with respect to the basis $e_1, e_2, \ldots, e_n$ has a 1 in position i, j if and only if $g \cdot j = i$ and zeros elsewhere. In particular, there will be a 1 in position i, i if $g \cdot i = i$ and a 0 otherwise. This shows that, if χ is the character afforded by X, then

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

- If ρ is the character of the regular representation of G then $\rho(1) = |G|$ and $\rho(g) = 0$ for all $g \neq 1$.

We adopt module-theoretic terminology to describe characters. For example, if the representation X is irreducible we say that the afforded character χ is irreducible and vice versa.

We adopt module-theoretic terminology to describe characters. For example, if the representation X is irreducible we say that the afforded character χ is irreducible and vice versa.

If Q is an $n \times n$ matrix and P is an invertible $n \times n$ matrix then

$$\mathrm{trace}(P^{-1}QP) = \mathrm{trace}(Q).$$

It follows immediately that *equivalent representations afford the same character*.

We adopt module-theoretic terminology to describe characters. For example, if the representation X is irreducible we say that the afforded character χ is irreducible and vice versa.

If Q is an $n \times n$ matrix and P is an invertible $n \times n$ matrix then

$$\operatorname{trace}(P^{-1}QP) = \operatorname{trace}(Q).$$

It follows immediately that *equivalent representations afford the same character*.

Note also that if $g, h \in G$ and X is a representation affording the character χ then

$$\begin{aligned}\chi(h^{-1}gh) = \operatorname{trace}(X(h^{-1}gh)) &= \operatorname{trace}(X(h)^{-1}X(g)X(h)) \\ &= \operatorname{trace}(X(g)) = \chi(g)\end{aligned}$$

so characters are constant on conjugacy classes.

If V is a (finite-dimensional) $\mathbb{C}G$-module by Wedderburn's Theorem we have

$$V = U_1 \oplus U_2 \oplus \cdots \oplus U_s$$

for some irreducible submodules U_i of V. Let χ be the character afforded by V and ψ_i the character afforded by U_i. Each element $g \in G$ then acts on V as a block-diagonal matrix with blocks corresponding to the modules U_i. It follows that

$$\chi = \psi_1 + \psi_2 + \cdots + \psi_s.$$

If V is a (finite-dimensional) $\mathbb{C}G$-module by Wedderburn's Theorem we have

$$V = U_1 \oplus U_2 \oplus \cdots \oplus U_s$$

for some irreducible submodules U_i of V. Let χ be the character afforded by V and ψ_i the character afforded by U_i. Each element $g \in G$ then acts on V as a block-diagonal matrix with blocks corresponding to the modules U_i. It follows that

$$\chi = \psi_1 + \psi_2 + \cdots + \psi_s.$$

It is not difficult to show that the irreducible characters of a group G are linearly independent. It follows that *two $\mathbb{C}$-representations are equivalent if and only if they afford the same character.*

If V is a (finite-dimensional) $\mathbb{C}G$-module by Wedderburn's Theorem we have

$$V = U_1 \oplus U_2 \oplus \cdots \oplus U_s$$

for some irreducible submodules U_i of V. Let χ be the character afforded by V and ψ_i the character afforded by U_i. Each element $g \in G$ then acts on V as a block-diagonal matrix with blocks corresponding to the modules U_i. It follows that

$$\chi = \psi_1 + \psi_2 + \cdots + \psi_s.$$

It is not difficult to show that the irreducible characters of a group G are linearly independent. It follows that *two $\mathbb{C}$-representations are equivalent if and only if they afford the same character*.

This observation reduces the problem of studying equivalence classes of irreducible representations to the study of irreducible characters.

Definition

Let G be a finite group with r conjugacy classes. The *character table* of G is an $r \times r$ table whose columns are indexed by the conjugacy classes of G, whose rows are indexed by the irreducible characters of G, and whose entry in row $(\chi, \mathcal{K})$ is $\chi(g)$, g an element of the conjugacy class $\mathcal{K}$.

Definition

Let G be a finite group with r conjugacy classes. The *character table* of G is an $r \times r$ table whose columns are indexed by the conjugacy classes of G, whose rows are indexed by the irreducible characters of G, and whose entry in row $(\chi, \mathcal{K})$ is $\chi(g)$, g an element of the conjugacy class $\mathcal{K}$.

For example, let $Z_2 = \langle z \rangle$. We have already observed that Z_2 has the trivial representation and the representation $X : Z_2 \to GL_1(\mathbb{C})$ defined by $X(z) = (-1)$. These representations are clearly inequivalent and since $|Z_2| = 2$ these are the only irreducible representations of Z_2. The character table of Z_2 is

	1	z
χ_1	1	1
χ_2	1	-1

One helpful observation in the determination of the character table of a group G is that if ρ denotes the character of the regular representation of G then

$$\rho = \sum_{\chi \text{ irreducible}} \chi(1)\chi.$$

This follows from the Wedderburn decomposition of $\mathbb{C}G$.

Let's see how this can be used by constructing the character table of S_3. The conjugacy classes of S_3 are represented by 1, $(1\,2)$, and $(1\,2\,3)$. Thus S_3 has 3 irreducible characters.

	1	$(1\,2)$	$(1\,2\,3)$
χ_1			
χ_2			
χ_3			

	1	$(1\,2)$	$(1\,2\,3)$
χ_1			
χ_2			
χ_3			

Any group has the principal character, and the group S_3 has the *sign homomorphism* which assigns 1 or -1 to a permutation depending on its cycle type. This can be viewed as a homomorphism from S_3 to $GL_1(\mathbb{C})$ so we have

	1	(1 2)	(1 2 3)
χ_1	1	1	1
χ_2	1	-1	1
χ_3			

	1	(1 2)	(1 2 3)
χ_1	1	1	1
χ_2	1	-1	1
χ_3			

Now the equality $\rho = \chi_1 + \chi_2 + \chi_3(1)\chi_3$ allows us to fill in the final row:

$$6 = \rho(1) = \chi_1(1) + \chi_2(1) + \chi_3(1)^2 = 2 + \chi_3(1)^2,$$

thus $\chi_3(1) = 2$.

$0 = \rho((1\,2)) = \chi_1((1\,2)) + \chi_2((1\,2)) + \chi_3(1)\chi_3((1\,2)) = 1 + (-1) + 2\chi_3((1\,2))$,

thus $\chi_3((1\,2)) = 0$. Similarly, $\chi_3((1\,2\,3)) = -1$.

The character table of S_3 is

	1	$(1\,2)$	$(1\,2\,3)$
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

The character table of S_3 is

	1	(1 2)	(1 2 3)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Let π be the permutation character afforded by the representation of S_3 on a vector space of dimension 3 (so S_3 permutes the basis vectors around just as it permutes the numbers 1,2,3 around). We know that $\pi(g)$ is the number of fixed points of g on $\{1, 2, 3\}$. So $\pi(1) = 3$, $\pi((1\,2)) = 1$, and $\pi((1\,2\,3)) = 0$. One can see immediately that a decomposition of π is

$$\pi = \chi_1 + \chi_3.$$

Lots of information about a group G can be obtained by studying the character table of G. We have already seen, for example, that a group G is abelian if and only if all of its irreducible character degrees are 1.

Lots of information about a group G can be obtained by studying the character table of G. We have already seen, for example, that a group G is abelian if and only if all of its irreducible character degrees are 1.

Let X be a representation that affords the character χ of G. Since X is a group homomorphism, $\ker(X)$ is a normal subgroup of G. Now $g \in \ker(X)$ if and only if $X(g)$ is the identity matrix, which holds if and only if $\chi(g) = \chi(1)$. Thus

$$\ker(\chi) = \{g \in G : \chi(g) = \chi(1)\}$$

is a normal subgroup of G. It is not hard to show that every normal subgroup of G is an intersection of subgroups of the form $\ker(\chi)$ for χ an irreducible character of G. It follows that given the character table of a group G, one can find *all* normal subgroups of G.

Lots of information about a group G can be obtained by studying the character table of G. We have already seen, for example, that a group G is abelian if and only if all of its irreducible character degrees are 1.

Let X be a representation that affords the character χ of G. Since X is a group homomorphism, $\ker(X)$ is a normal subgroup of G. Now $g \in \ker(X)$ if and only if $X(g)$ is the identity matrix, which holds if and only if $\chi(g) = \chi(1)$. Thus

$$\ker(\chi) = \{g \in G : \chi(g) = \chi(1)\}$$

is a normal subgroup of G. It is not hard to show that every normal subgroup of G is an intersection of subgroups of the form $\ker(\chi)$ for χ an irreducible character of G. It follows that given the character table of a group G, one can find *all* normal subgroups of G.

In particular, G is simple if and only if $\chi(g) = \chi(1)$ implies $g = 1$ for all irreducible characters χ of G.

The character table of G tells you...

- the order of G
- the number of conjugacy classes of G
- whether or not G is abelian, nilpotent, solvable, or simple
- $Z(G)$
- $|G : G'|$, the index of the commutator subgroup
- information about representations over fields of prime characteristic

The character table of G does *not* tell you the isomorphism type of G.
The character tables of D_8 and Q_8 are identical but $D_8 \ncong Q_8$.

Two of the main tools in constructing a character table are...

- The Hermitian inner product $(\chi, \psi) = \dfrac{1}{|G|} \sum_{g \in G} \chi(g)\psi(g^{-1})$ for characters χ and ψ of G. This inner product satisfies $(\chi, \psi) = \delta_{\chi\psi}$ for irreducible characters χ, ψ of G and allows one to perform fast decompositions of reducible characters.

Two of the main tools in constructing a character table are...

- The Hermitian inner product $(\chi, \psi) = \frac{1}{|G|} \sum_{g \in G} \chi(g)\psi(g^{-1})$ for characters χ and ψ of G. This inner product satisfies $(\chi, \psi) = \delta_{\chi\psi}$ for irreducible characters χ, ψ of G and allows one to perform fast decompositions of reducible characters.
- Induction: If $H \leq G$ and V is a $\mathbb{C}H$-module, then $\mathbb{C}G \otimes_{\mathbb{C}H} V$ is a $\mathbb{C}G$ module. This tool allows one to build characters of groups using characters of subgroups.

Character theory is a wonderful tool for proving theorems about groups. For example...

Burnside's $p^a q^b$ Theorem

A group of order $p^a q^b$ where p, q are primes is necessarily solvable.

Character theory is a wonderful tool for proving theorems about groups. For example...

Burnside's $p^a q^b$ Theorem

A group of order $p^a q^b$ where p, q are primes is necessarily solvable.

P. Hall

If for all primes p dividing $|G|$ a Sylow p-subgroup of G has a complement, then G is solvable.

Character theory is a wonderful tool for proving theorems about groups. For example...

Burnside's $p^a q^b$ Theorem

A group of order $p^a q^b$ where p, q are primes is necessarily solvable.

P. Hall

If for all primes p dividing $|G|$ a Sylow p-subgroup of G has a complement, then G is solvable.

Frobenius

Let G be a finite group and H be a nontrivial proper subgroup of G such that $H \cap H^g = 1$ for all $g \in G \setminus H$. Then there exists a normal subgroup N of G such that $NH = G$ and $N \cap H = 1$.