Fix a basis (v_j) of E, (τ_j) the dual basis of E'.

By construction, $M(\rho)$ is spanned by the matrix-coefficients

$$f_{i,j} = f_{v_i, \tau_j} \qquad 1 \leq i, j \leq \dim \rho$$

The linear independence of matrix coefficients
$\Rightarrow$ this is a basis of $M(\rho)$
$\Rightarrow$ $\dim M(\rho) = (\dim \rho)^2$

The intertwining operator

$$\Phi = \bigoplus_i \Phi_{\tau_i} : \bigoplus_i \rho \longrightarrow M(\rho)$$

is surjective (since its image contains each basis vector $f_{i,j}$).

Both sides have the same dimension
$\Rightarrow$ Φ is an isomorphism.
$\Rightarrow$ $M(\rho) \simeq (\dim \rho)\rho$ as a representation of G.

Let us check (3).

Let $E \subset k^G$ be a subrepresentation of the regular representation which is isomorphic to ρ.

We would like to show that $E \subset M(\rho)$.

We check that $\forall f \in E$ which is a function on G is a matrix coefficient of E.

We define $\delta \in (k^G)'$, the linear form given by $\delta(f) = f(1) \quad \forall f \in k^G$.

Consider $\delta_E := \delta|_E \in E'$.

Then $\forall f \in E$, $\forall x \in G$, we have

$$\underbrace{\langle \delta_E, \rho_G(x) f \rangle}_{\text{as a function of } x, \text{ it is a matrix coefficient for } \rho, \text{ as } \rho_G \text{ on } E \text{ is isomorphic to } \rho.} = \rho_G(x) f(1) = f(x).$$

(ρ_G: the regular representation)

$\Rightarrow f \in M(\rho)$.

■

Recall

$$\sum_{\rho \in \hat{G}} (\dim \rho)^2 = |G|$$

A natural question:
What is the number of irreducible representations (up to isomorphism)?

Corollary 24 Let G be a finite group, k an algebraically closed field of characteristic not dividing $|G|$.
Then all irreducible finite-dimensional representations of G are of dimension 1 $\Leftrightarrow$ G is abelian.

In particular, if G is abelian, then $\exists$ $|G|$ non-isomorphic irreducible k-representations.

□ ($\Leftarrow$) see Corollary 20.

It is enough to check ($\Rightarrow$)

Observe that:

> 1-dimensional representations of G are in bijection with 1-dimensional representations of $\underbrace{G/[G,G]}_{G^{ab}}$

$[G,G]$ is the derived subgroup.

G^{ab} the abelianized group or the abelianization of G

This is because 1-dimensional representations are characters

$$G \longrightarrow GL_1(k) = k^\times, \quad k^\times \text{ is abelian}$$

($k^\times$: the multiplicative group of the field)

and there is a canonical bijection

$$\{G \to A\} \longleftrightarrow \{G/[G,G] \to A\}$$

homomorphisms — homomorphisms

$\forall$ group G and $\forall$ abelian group A.

Remark: In particular, if G is perfect, that is $G = [G,G]$, then any non-trivial representation of G, over any field k, has dimension at least 2.

E.g. $SL_d(k)$, $d \geq 2$ $k \neq \mathbb{F}_2$, $k \neq \mathbb{F}_3$

finite fields of 2 and 3 elements respectively.

Corollary 22 $\Rightarrow$ $|G| = |G/[G,G]|$

as both these cardinalities are equal to the number of irreducible k-representatic of G.

$\Rightarrow$ $[G,G] = 1$ $\Rightarrow$ G is abelian.

■

Exercise 25

Let G be a p-group acting on a finite set X with p not dividing $|X|$.

Show that this action has at least one fixed point.

Let $G = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \mid x, y, z \in \mathbb{F}_p \right\}$

$\mathbb{F}_p$: field of p elements

Let k be any field of characteristic p.

Show that any irreducible k-representation of G is trivial.

$\Rightarrow$ assumption on the characteristic of k in Corollary 24 is essential.

Theorem 26 Let G be a finite group, k an algebraically closed field of characteristic not dividing $|G|$.
Then the number $|\hat{G}|$ of isomorphism classes of irreducible k-representations of G is equal to the number of conjugacy classes of G.

Remarks

- Corollary 22, the decomposition of the regular representation, $\Longrightarrow$
  $\exists$ at most $|G|$ irreducible representations
- This upper bound is realized
  $\Longleftrightarrow$ G is abelian
- Theorem 26 (without proof) gives a more precise formula.
  This formula does not depend on the field k (assumed to satisfy the above hypothesis) $\rightsquigarrow$ bijections between the sets of irreducible characters for different fields $\rightsquigarrow$ Brauer's theory.

Representations as modules

Let R be a ring with identity.

Definition 27 An *R-module* is an abelian group M with a map

$$R \times M \longrightarrow M$$
$$(r, m) \longmapsto rm$$

such that

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

Examples

(1) A vector space E over a field k is a k-module

(2) Any ring R is a module over itself.

(3) If R is any ring, then

$$\underbrace{R \times R \times \dots \times R}_{n \text{ times}}$$ is an R-module

(4) $\{n \times n$ matrices with entries in a ring $R\}$ is an R-module

(5) Let E be a vector space over a field k and $\mathrm{End}_k(E)$ be the ring of linear transformations from E to itself. Then E is an $\mathrm{End}_k(E)$-module, using

$$\tau \cdot v := \tau(v)$$

An R-module M "allows" addition of "vectors" and scalar multiplication. If we also have multiplication of "vectors" we obtain the notion of an R-algebra.

Definition 28 Let R be a commutative ring. An *algebra* A over R is an R-module that is also a ring and the ring and module operations are compatible:

$$r(xy) = (rx)y = x(ry) \quad \forall x, y \in A \ \forall r \in R$$

We will consider *unital* algebras, that is, with $1 \in A$.

We focus on *k-algebras*, that is, over the field.

Definition 29 A *representation* of a unital k-algebra A is an *algebra homomorphism*, that is a linear map preserving the multiplication and the multiplicative unit $1 \in A$:

$$\rho : A \longrightarrow End_k(E)$$

Remark: $End_k(E)$ is an example of an k-algebra

A representation of a unital k-algebra A defines a structure of an A-module on E by

$$a \cdot v := \rho(a) v$$

We focus on the case $A = k(G)$ the group algebra of G over k.

$k(G) :=$ the k-vector space with a basis $(e_g)_{g \in G}$

the product can be defined by

$$e_g \cdot e_h = e_{gh}$$

and extended by linearity;

Given $a, b \in k(G)$

$$a = \sum_{g \in G} \lambda_g e_g \quad , \quad b = \sum_{h \in G} \mu_h e_h$$

with only finitely many non-zero coefficients $\lambda_g \in k$, $\mu_h \in k$, the product $a \cdot b \in k(G)$ is given by

$$a \cdot b = \sum_{g \in G} \sum_{h \in G} \lambda_g \mu_h e_g e_h = \sum_{x \in G} \left(\sum_{gh = x} \lambda_g \mu_h \right) e_x$$

Representations of groups as modules over the group algebra

Theorem 30 Let G be a group and k be a field. If $\rho : G \longrightarrow GL(E)$ is a k-representation of E, then E has a structure of $k(G)$-module defined by extending ρ by linearity:

$$\left(\sum_{g \in G} \lambda_g e_g\right) \cdot v := \sum_{g \in G} \lambda_g \rho(g) v.$$

Conversely, any $k(G)$-module E inherits a representation of G by restricting "the multiplication by a" maps to the basis vectors e_g, that is, by defining

$$\rho(g) = \left(v \longmapsto e_g \cdot v\right).$$

Furthermore, a k-linear map

$\Phi : \rho_1 \longrightarrow \rho_2$ is a G-morphism

$\Longleftrightarrow$ Φ is $k(G)$-linear

□ The proof is straightforward.

■

Definition 31 Let M be an R-module.

(1) $N \subseteq M$ is an *R-submodule* if

a) N is a subgroup of M;

b) $rn \in N \quad \forall r \in R, \forall n \in N$

(2) Let M and M' be R-modules

$\varphi : M \to M'$ is an *R-homomorphism*

if a) $\varphi(m+n) = \varphi(m) + \varphi(n)$ $\quad \forall m, n \in M$

b) $\varphi(rm) = r\varphi(n)$ $\quad r \in R$

(3) An R-module M is *simple* if the only submodules of M are $\{0\}$ and M.

(4) An R-module M is *semisimple* if it is a direct sum of simple modules.

Examples 32

1) k is simple, viewed as a k-module.

2) $\underbrace{R \times R \times \dots \times R}_{n>1}$ is not simple as an R-module.

3) $M_n(k)$, $n>1$ is not simple as a k-module

It is simple as a ring: the only two-sided ideals are $\{0\}$ and $M_n(k)$.

4) $\underbrace{k \times k \times \dots \times k}_{n>1}$ is simple as an $M_n(k)$-module.

5) $M_n(k)$ is semisimple.

Thus, an $k(G)$-module is simple if and only if the corresponding representation is irreducible.

The trivial $k(G)$-module is a one-dimensional module over $k(G)$ which carries the trivial representation of G. This is k itself, where

$$\left(\sum_{g \in G} \lambda_g e_g\right) v = \left(\sum_{g \in G} \lambda_g\right) v \in k$$

Representation terminology	Module terminology
vector space over k with representation of G	$k(G)$-module
invariant subspace	submodule
irreducible representation	simple module
completely reducible representation	semisimple module
equivalent representations	isomorphic modules
G-equivariant linear transformations	module homomorphisms
the trivial representation	the trivial $k(G)$-module k

We can then rewrite fundamental results.

Schur's Lemma:

(1) Any non-zero homomorphism between simple R-modules is an isomorphism.

(2) If simple R-modules M and N are isomorphic, then
$\mathrm{Hom}_R(M,N) \simeq \mathrm{Hom}_R(M,M) = \mathrm{End}_R(M)$
is a division ring.

If k is algebraically closed, and
M is a finite dimensional simple R-module
then $\mathrm{End}_R(M) = \{\lambda I : \lambda \in k\} \simeq k$.

...

Maschke's Theorem

If $|G|$ is not divisible
by the characteristic of k, then
every $k(G)$-module is semisimple.

Conversely, ...

Permutation representations

$\forall$ group G, $G \leq \mathrm{Sym}(X)$

↑ the group of all bijections of some set X

Indeed, $X := G$ and $g \longmapsto \tau_g \in \mathrm{Sym}(G)$, where $\tau_g(h) := gh$.

More generally, consider any action $G \curvearrowright X$, that is any homomorphism

$$\begin{cases} G \longrightarrow \mathrm{Sym}(X) \\ g \longmapsto (x \longmapsto g \cdot x) \end{cases}$$

Even if X is not a vector space we can "linearize" it. Given a field k, we consider

$k(X) = \{$ the k-vector space with a basis $(e_x)_{x \in X}\}$

and define

$$\rho : G \longrightarrow GL(k(X))$$
$$g \longmapsto \rho(g), \quad \rho(g) e_x := e_{g \cdot x}$$

ρ is indeed a representation, $\dim \rho = |X|$

It is called the permutation representation.

Examples 33

1) The representation π defined on $k(G)$ is the permutation representation associated to the left-action of G on itself by multiplication.

2) $H \leq G$ a subgroup of finite index
$X = G/H$ the finite set of right cosets of G modulo H.
$G \curvearrowright X$: $g \cdot (xH) = gxH \in G/H$

the corresponding permutation representation ρ is isomorphic to the induced representation

$$\mathrm{Ind}_H^G(\mathbb{1})$$

Indeed, the space for this representation is

$$F = \{ f : G \to k \mid f(hg) = f(g) \ \forall h \in H \}$$

with the action $G \curvearrowright F$ by the regular representation.

Basis of $F = \{ f_x := $ characteristic functions of the left coset $Hx \}$

$$g \cdot f_x := f_{xg^{-1}}$$

$\Rightarrow$ $f_x \longmapsto e_{x^{-1}}$ gives an intertwiner $F \to k(X)$.

A permutation representation is never irreducible if X is finite, $|X| \neq 1$:

$\sum_{x \in X} e_x \in k(X)$ is an invariant vector.

The character χ of the permutation representation ρ on X, $|X| < \infty$ is given by

$$\chi_\rho(g) = |\{x \in X \mid \rho(g)x = x\}|$$

By definition, $\chi_\rho(g) = \operatorname{tr} \rho(g)$

The trace of a (permutation) matrix is the number of non-zero diagonal ~~ma~~ entries (which are equal to 1).

This corresponds to $x \in X$ such that $e_x = \rho(1) \cdot x = \rho(g)x = e_{gx}$ $\Rightarrow$ to the fixed points of g.

This character is called the permutation character of $G \curvearrowright X$.

The module corresponding to a permutation representation is called a permutation module.

Theorem 34 Let χ be the permutation character of $G \curvearrowright X$. Then

$$\frac{1}{|G|} \sum_{g \in G} \chi(g) \text{ is}$$

the number of orbits of X. [Here G and X are finite.]

□ Let us count the set

$$\{(g,x) \in G \times X \mid g \cdot x = x\}$$

in two different ways.

The cardinality of this set is equal to

$$\sum_{g \in G} |\{x \in X \mid g \cdot x = x\}| = \sum_{g \in G} \chi(g).$$

On the other hand, it equals

$$\sum_{x \in X} |\{g \in G \mid gx = x\}| = \sum_{x \in X} |\mathrm{Stab}_G(x)|,$$

where $\mathrm{Stab}_G(x)$ is the isotropy subgroup of x of $G \curvearrowright X$.

Let $O_1, \ldots, O_k$ be the distinct orbits of $G \curvearrowright X$.

We know a bijection

$$x \in O_i \leftrightarrow G/\mathrm{Stab}_G(x)$$

$$\Rightarrow |O_i| = |G/\mathrm{Stab}_G(x)| \quad \text{and}$$

$$|O_i| = |G| / |\mathrm{Stab}_G(x)|$$

Thus, $|Stab_G(x)|$ has a constant value

$= |G|/|O_i|$ on the orbit.

$$\Rightarrow \sum_{g \in G} \chi(g) = \sum_{i=1}^{k} \sum_{x \in O_i} |Stab_G(x)| =$$

$$= \sum_{i=1}^{k} \sum_{x \in O_i} \frac{|G|}{|O_i|} = k|G|$$

$$\Rightarrow \frac{1}{|G|} \sum_{g \in G} \chi(g) = k \text{ the number of orbits.}$$

■