Introduction to the character theory of finite groups

A.E. Zalesski

University of Brasilia, 5 – 8 February 2024

Section 1. **Main notions**

Fix a field F. If V is a vector space of finite dimension over F, we denote by $\operatorname{End} V$ (sometimes $\operatorname{End}_F V$) the set of all linear transformations $V \to V$ and by $GL(V)$ the subset of all invertible linear transformations. It is well known that $\operatorname{End} V$ is a ring and $GL(V)$ is a group.

Let $n = \dim V$. A choice of a basis in V identifies $\operatorname{End} V$ with the matrix ring $M(n, F)$ and $GL(V)$ with the group $GL(n, F)$ of all non-degenerate matrices with entries in F.

Definition 1. *Let S be a set.*
A **representation of S into** $\operatorname{End} V$ *is a mapping $\rho : S \to \operatorname{End} V$.*
If S is a group and ρ is a group homomorphism $S \to GL(V)$, one says that ρ is a **group representation.**
If S is a ring and $\rho : S \to \operatorname{End}(V)$ is a ring homomorphism, one says that ρ is a **ring representation.**
The dimension $\dim V$ *of V is called the* **dimension** *or the* **degree of** ρ*.*

In other words, ρ is a group representation if S is a group and $\rho(st) = \rho(s)\rho(t)$ for all $s, t \in S$ and $\rho(s^{-1}) = \rho(s)^{-1}$.
To specify F one says "F-representation".

Using $M(n, F)$ in place of $\operatorname{End} V$, one can similarly speaks on **matrix representations**. This sometimes is helpful as a matrix can be explicitly written.

Obviously, if T is a subset of S then $\rho|_T : T \to GL(V)$ is a representation of T. If H is a subgroup of a group G then
$\rho|_H \to GL(V)$ is a group representation of H.

Let W be a subspace of V.
If $\rho(s)W \subseteq W$ for all $s \in S$ then
W is called S-**stable** or S-invariant.

Definition 2. *Let $\rho : S \to \operatorname{End} V$ be a representation of a set S.*
One says that ρ is **reducible** *if there is an S-stable subspace W such that*
$0 \neq W \neq V$;
otherwise ρ is called **irreducible**.

Therefore, ρ is irreducible if $\rho(S)$ stabilizes no subspace of V except $\{0\}$ and V itself. Otherwise ρ is reducible.

Suppose that $\rho(S)W \subseteq W$. For $s \in S$ one can consider the linear transformation $\rho(s)|_W : W \to W$ obtained from $\rho(s)$ by the restriction of this transformation to W. Obviously, $s \to \rho(s)|_W$ defines a mapping $S \to \mathrm{End}\, W$.
If S is a group then the mapping $s \to \rho(s)|_W$ for $s \in S$ is a group representation $S \to GL(W)$.

If $0 \neq W \neq V$ then $\rho|_W$ is called a **subrepresentation** of ρ.

Matrix interpretation

Let ρ be a reducible matrix representation of S and V the underlying space of matrices in question. Then there is a basis of V under which ρ has a block-triangular shape with irreducible diagonal blocks, $\rho_1, \ldots, \rho_k$, say.

Indeed, there exists a string

$$0 = W_0 \subset W_1 \subset W_2 \subset ... \subset W_k = V$$

of subspaces of V, such that $W_{i-1} \subset W_i$ is a minimal $\rho(S)$-stable subspace of V that contains W_{i-1} for every $i = 1, ..., k$.
Then we can choose a basis B of V such that $B \cap W_i$ is a basis of W_i.

Next consider the matrices of $\rho(S)$ under this basis. Let $g \in S$. These are of shape

$$\rho(g) = \begin{pmatrix} \rho_1(g) & * & * & ... & * & * \\ 0 & \rho_2(g) & * & ... & * & * \\ ... & ... & ... & ... & ... & ... \\ 0 & 0 & ... & \rho_i(g) & * & * \\ ... & ... & ... & ... & ... & ... \\ 0 & 0 & 0 & ... & 0 & \rho_k(g) \end{pmatrix}$$

Suppose that $S = G$ is a group, and $g, g' \in G$. Then $\rho_i(gg') = \rho_i(g)\rho_i(g')$. This implies that each ρ_i is a representation of G. And ρ_i is irreducible as otherwise there would be a G-stable subspace W_i' such that $W_{i-1} \subset W_i' \subset W_i$.

The representations ρ_i are called **irreducible constituents of** ρ.

The following lemma provides a useful test for reducibility of a representation provided the ground field is algebraically closed.

Lemma 3. *Let F be an algebraically closed field and S a set. Let $\rho : S \to M(n, F)$ be a representation, and C an $(n \times n)$-matrix with entries in F. Suppose that C commutes with every matrix in $\rho(S)$.*
If C is non-scalar then ρ is reducible; equivalently, if ρ is irreducible then C is scalar.

Proof. Let $M(n, F)$ act naturally on a vector space $V = F^n$.
As F is algebraically closed, there exists a non-zero vector $v \in V$ such that $Cv = \lambda v$ with $\lambda \in F$. (This is a standard fact of linear algebra.) Then λ is called an *eigenvalue of C on V*.

Let $W = \{x \in V : Cx = \lambda x\}$. This is a subspace of V called the *eigenspace of* λ.

Then $W \neq 0$ as $0 \neq v \in W$, and $W \neq V$ as C is non-scalar.

Claim: W is S-stable.

Indeed, if $w \in W$ then $Cw \in W$ and $C\rho(s)w = \rho(s)Cw = \rho(s)\lambda w = \lambda\rho(s)w$.

As W consists of all vectors $v \in V$ such that $Cv = \lambda v$, we conclude that $\rho(s)w \in W$. So the result follows.

Corollary 4. *Assume that* G *is an abelian group and* F *is algebraically closed. Then every irreducible* F*-representation of* G *is* 1*-dimensional.*

This is true for S in place of G if all matrices of $\rho(S)$ commutes with each other.

Equivalent representations

Definition 5. *Let S be a set and $\rho : S \to GL(V)$, $\sigma : S \to GL(W)$ be two representations.*
One says that ρ is **equivalent** *to σ if there is a vector space isomorphism $E : V \to W$ such that for every $s \in S$ and $v \in V$ one has that*

$$E(\rho(s)v) = \sigma(s)(E(v)).$$

In other words, ρ, σ are equivalent if $\rho(s)v = (E^{-1}\sigma(s)E)v$ for all $v \in V$.

In matrix interpretation, representations $\rho : S \to GL(n, F)$, $\sigma : S \to GL(m, F)$ are equivalent if $m = n$ and there exists a non-degenerate matrix E such that $\rho(s) = E^{-1}\sigma(s)E$. In other words, ρ and σ are equivalent if there are bases in V and W relative to which the matrix of $\rho(s)$ coincides with the matrix of $\sigma(s)$ for every $s \in S$.

Lemma 6. *(Schur's lemma) Let F be a field, $\rho : S \to \operatorname{End} V$, $\sigma : S \to \operatorname{End} W$ be irreducible representations of S. Let $C : V \to W$ be a linear mapping.*
Suppose that for every $s \in S$ and $v \in V$ one has $C(\rho(s)v) = \sigma(s)(C(v))$. Then either $C = 0$ or C is invertible. In the latter case ρ and σ are equivalent.

Proof. Let $V_1 = \ker C$ and $W_1 = CV$. Then V_1 is $\rho(G)$-stable and W_1 is $\tau(G)$-stable. Indeed, let $g \in G$. Then

$$C\rho(g)V_1 = \sigma(g)CV_1 = 0$$

and $\sigma(g)CV = C\rho(g)V = W_1$. Let $C \neq 0$. Then $W_1 \neq 0$ and $V_1 \neq V$. Then $W_1 = W$ as σ is irreducible. Hence C is surjective.

We have $V_1 = 0$ as ρ is irreducible. Hence C is injective. Therefore, C is bijective so C^{-1} exists. Then $C^{-1}\sigma(g)C = \rho(g)$ so ρ and σ are equivalent.

Section 2: **Averaging**

From now on G is a finite group. We denote by $|G|$ the order of G.

Let $\rho : G \to GL(V)$ be a representation of G. Define

$$V^G = \{v \in V : \; hv = v \; \text{ for all } \; h \in G.\}$$

The subspace V^G is often called the **fixed point subspace** of G in V, or the space of G-invariants in V.

Consider the mapping $\mu : V \to V$ defined for $v \in V$ as follows: $\mu(v) = \sum_{g \in G} \rho(g)v$.

Let $p \geq 0$ be the characteristic of the ground field F.

Lemma 7. (1) $\mu(V) \subseteq V^G$.

(2) *If* $|G|$ *is not a multiple of* $|p|$ *then* $\mu(V) = V^G$.

Proof. (1) Let $h \in G$. Then the mapping $G \to G$ defined by $g \to hg$ for $g \in G$ is bijective. Therefore,

$$\rho(h) \sum_{g \in G} \rho(g)v = \sum_{g \in G} \rho(hg)v = \sum_{g \in G} \rho(g)v.$$

(2) Take $v \in V^G$. Then $gv = v$ for every $g \in G$. So $\mu(v) = v + ... + v = |G| \cdot v$.

The right hand side is non-zero as $|G|$ is not a multiple of p. Then

$v = |G|^{-1}\mu(v) = \mu(|G|^{-1}v)$.

Let V, W be two vector spaces and let $\rho : G \to GL(V)$, $\sigma : G \to GL(W)$ be two representations of a finite group G.

For a linear mapping $T : V \to W$ we set

$$\tilde{T} = \sum_{g \in G} \rho(g) T \sigma(g^{-1}).$$

In matrix terms this can be expressed as follows.

Let $\rho : G \to GL(n, F), \sigma : G \to GL(m, F)$ be two matrix representations of G.

Let T be an $(n \times m)$-matrix. Then

$$\tilde{T} = \sum_{g \in G} \rho(g) T \sigma(g^{-1}).$$

If $M(n \times m, F)$ denote the set of all $(n \times m)$-matrices then $\tilde{T}$ is a linear transformation of the vector space $M(n \times m, F)$.

Theorem 8. *Let $h \in G$. Then*
$$\rho(h)\tilde{T} = \tilde{T}\sigma(h).$$

Proof. Let $h \in G$. As in Lemma 7,
$$\rho(h)\tilde{T} = \rho(h)\sum_{g\in G}\rho(g)T\sigma(g^{-1}) =$$
$$= \sum_{g\in G}\rho(hg)T\sigma(g^{-1}) =$$
$$= \sum_{g\in G}\rho(hg)T\sigma(g^{-1}h^{-1}h) =$$
$$= \sum_{g\in G}\rho(hg)T\sigma(g^{-1}h^{-1})\sigma(h) =$$
$$= \big(\sum_{g\in G}\rho(hg)T\sigma((hg)^{-1})\big)\sigma(h) =$$
$$= \big(\sum_{g\in G}\rho(g)T\sigma(g^{-1})\big)\sigma(h) = \tilde{T}\sigma(h).$$

This argument mimics the proof of Lemma 7.

Theorem 9. *Let $\rho : G \to GL(n, F)$ and $\sigma : G \to GL(m, F)$ be irreducible representations of a finite group G.*

(1) *If ρ and σ are not equivalent then $\tilde{T} = 0$ for any matrix $T \in M(n \times m, F)$.*

(2) *Suppose that F is algebraically closed. If $\rho = \sigma$ then $\tilde{T}$ is scalar. In addition, if $\tilde{T} = \lambda \cdot \mathrm{Id}$ then $n\lambda = |G| \cdot Trace\,(T)$.*

Proof. (1) follows from Theorem 8 and Schur's lemma 6.

(2) Similarly, the first assertion in (2) follows from Theorem 8 and Lemma 3.

To obtain the formula for λ, compute the trace of the both sides of the equality

$$\tilde{T} = \sum_{g \in G} \rho(g) T \rho(g^{-1}).$$

We have $n\lambda = |G| \cdot \mathrm{Trace}\,(T)$ as the trace of $\rho(g) T \rho(g^{-1})$ is equal to the trace of T.

Section 3: **Orthogonality relations**

Theorem 10. *Let* $\rho : G \to GL(n, F)$ *and* $\sigma : G \to GL(m, F)$ *be non-equivalent irreducible representations of* G, *and* $g \in G$. *Let*

$$\rho(g) = \begin{pmatrix} f_{11}(g) & \cdots & f_{1n}(g) \\ \cdots & \cdots & \cdots \\ f_{n1}(g) & \cdots & f_{nn}(g) \end{pmatrix}$$

and

$$\sigma(g) = \begin{pmatrix} t_{11}(g) & \cdots & t_{1m}(g) \\ \cdots & \cdots & \cdots \\ t_{m1}(g) & \cdots & t_{mm}(g) \end{pmatrix}.$$

Then

$$\sum_{g \in G} f_{ij}(g) t_{kl}(g^{-1}) = 0$$

for all choices i, j, k, l *where* $1 \leq i, j \leq n$, $1 \leq k, l \leq m$.

Proof. Let E_{jk} denote the $(n \times m)$-matrix with (j,k)-entry equal to 1 and 0 elsewhere. Here $1 \leq j \leq n$, $1 \leq k \leq m$.

$$\begin{pmatrix} 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 1_{jk} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Then the (i,k)-entry of $\rho(g)E_{jk}\sigma(g^{-1})$ equals $f_{ij}(g)t_{kl}(g^{-1})$.

Set

$$\tilde{E}_{jk} = \sum_{g \in G} \tau(g) E_{jk} \rho(g^{-1}).$$

By Theorem 8, $\tau(h)\tilde{E}_{jk} = \tilde{E}_{jk}\rho(h)$ for each $h \in G$.

By Lemma 6, $\tilde{E}_{jk}$ is the zero matrix so the (i, l)-entry of it is equal to 0.

Therefore

$$\sum_{g \in G} f_{ij}(g) t_{kl}(g^{-1}) = 0.$$

As i, l and j, k are arbitrary, the formula holds for every choice of i, j, k, l.

Theorem 11. *(Orthogonality relations for the matrix entries of an irreducible representation)*

Let G be a group of finite order d and let $\rho : G \to GL(n, F)$ be an irreducible representation. For $g \in G$ we write

$$\rho(g) = \begin{pmatrix} f_{11}(g) & \cdots & f_{1n}(g) \\ \cdots & \cdots & \cdots \\ f_{n1}(g) & \cdots & f_{nn}(g) \end{pmatrix}.$$

Assume that F is an algebraically closed field either of characteristic 0 or of characteristic $p \neq 0$ coprime to d. Then

$$\sum_{g \in G} f_{ij}(g) f_{kl}(g^{-1}) = \begin{cases} 0 & if \ (i,j) \neq (l,k) \\ \frac{d}{n} & otherwise. \end{cases}$$

In addition, n is coprime to p.

Proof. For $1 \le i \le n$ let E_{jk} denote the $(n \times n)$-matrix with (j,k)-entry 1 and 0 elsewhere. Set

$$N = \tilde{E}_{jk} = \sum_{g \in G} \rho(g) E_{jk} \rho(g^{-1}).$$

By Theorem 8, $\rho(h)N = N\rho(h)$ for each $h \in G$. By Schur's lemma, $N = \lambda \cdot \mathrm{Id}$.

By Theorem 9, the trace of N is equal to $n\lambda = d \cdot \mathrm{Trace}\,(E_{jk})$, where $d = |G|$. Clearly, $\mathrm{Trace}\,(E_{jk}) = 0$ if $j \neq k$ and d otherwise. Therefore, if $j \neq k$ then

$$N_{il} = 0 = \textstyle\sum_{g \in G} f_{ij}(g) f_{kl}(g^{-1}).$$

Let $j = k$. Then $N_{il} = 0$ if $i \neq l$. Let $i = l$. Then $\mathrm{Trace}\,(E_{jk}) = 1$ and $n\lambda = d$. This is an equality in F, so $n \neq 0$ as an element in F. In particular, p does not divide n. Furthermore,
$\sum_{g \in G} f_{ij}(g) f_{ji}(g^{-1}) = N_{ii} = \lambda = d/n.$

Corollary 12. *Assume F, G to be as in Theorem* 11.
Let $\rho = \rho^{(1)}, \ldots, \rho^{(k)}$ be pairwise non-equivalent irreducible representations of G, and let $f_{ij}^{(l)}(g)$ be the (i,j)-entry function of $\rho^{(l)}$.

Then $f_{ij}^{(l)}(g)$ are linear independent as functions on G.

Proof. Suppose the contrary, that there are $c_{ij}^l \in F$ such that $\sum_{ijl} c_{ij}^l f_{ij}^l(g) = 0$, where at least one of the coefficients, say, $c_{i'j'}^{l'}$ is not 0. Then

$$0 = \sum_g (\sum_{ijl} c_{ij}^l f_{ij}^l(g) f_{j'i'}^{l'}(g^{-1})) =$$

$$= \sum_{ijl} c_{ij}^l (\sum_g f_{ij}^l(g) f_{j'i'}^{l'}(g^{-1})) = c_{i'j'}^{l'} d/n,$$

which is a contradiction.

Let $\mathcal{F}(G)$ denote the vector space of all functions on a finite group G.
Then $\dim \mathcal{F}(G) = |G|$. Therefore, the total number of the functions $f_{ij}^{(l)}(g)$ does not exceed $|G|$ as they are linear independent by Corollary 12.
The number of these functions is equal to

$$(\dim \rho_1)^2 + \cdots + (\dim \rho_l)^2.$$

It follows that

(*) the sum of squares of the dimensions of pairwise non-equivalent irreducible representations of G over a field F does not exceed $|G|$.

Section 4: **Characters of representations**

Definition 13. *Let* $\rho : G \to GL(n, F)$ *be a representation and let*

$$\rho(g) = \begin{pmatrix} f_{11}(g) & \cdots & f_{1n}(g) \\ \cdots & \cdots & \cdots \\ f_{n1}(g) & \cdots & f_{nn}(g) \end{pmatrix}.$$

The function $\chi : G \to F$ *defined by*

$$\chi(g) = f_{11}(g) + f_{22}(g) + \cdots + f_{nn}(g)$$

is called the **character of** ρ*.*

Note that $\chi(g)$ is the trace of the matrix $\rho(g)$.

Observe that characters are constant on the conjugacy classes of G.

Lemma 14. *The characters of equivalent representations coincide.*

Proof. If ρ, σ are equivalent representations then we can assume that

$\rho(G), \sigma(G) \in GL(n, F)$ and $\rho(g) = X\sigma(g)X^{-1}$

for some invertible matrix $X \in GL(n, F)$. It is well known that the traces of similar matrices coincide, whence the result.

(One can also argue as follows. If $\rho : G \to GL(V)$ and $\sigma : G \to GL(W)$ are equivalent then there are bases in V, W relative to which the matrices $\rho(g)$ and $\sigma(g)$ coincide for every $g \in G$.)

The term "irreducible character" means the character of an irreducible representation.

Note that the character theory is the same for arbitrary algebraically closed field F of characteristic 0, so one can choose $F = \mathbb{C}$ with no generality lost.

Orthogonality relations for irreducible characters

In this section and later G is a group of order d and F is an algebraically closed field of characteristic 0 or $p > 0$ coprime to d.

Let $\mathcal{F}(G)$ be the space of all functions $G \to F$. Functions on G that are constant on every conjugacy class of G are called *class functions*. They form a subspace of $\mathcal{F}(G)$; the dimension of it equals the number of conjugacy classes of G.
Given two functions $s, t \in \mathcal{F}(G)$, we set

$$\langle s, t \rangle = \frac{1}{d} \sum_{g \in G} s(g) t(g^{-1}).$$

This defines a mapping $\mathcal{F}(G) \times \mathcal{F}(G) \to F$ called the *inner product of the functions s and t*. Note that $\langle \cdot, \cdot \rangle$ is a bilinear form on $\mathcal{F}(G)$.

Theorem 15. *(Orthogonality relations for irreducible characters)*

Let χ, η *be irreducible characters of a finite group* G. *Let* d *be the order of* G. *Then*

$$\langle \chi, \eta \rangle = \frac{1}{d} \sum_{g \in G} \chi(g) \eta(g^{-1}) = \begin{cases} 0 & if\ \chi \neq \eta, \\ 1 & otherwise. \end{cases}$$

Proof. Let ρ, σ be representations whose characters are χ, η, respectively, and n, m their dimensions. Let f_{ij}, t_{kl} denote the matrix entry functions of ρ and σ, respectively. Then

$$\chi = f_{11} + f_{22} + \cdots + f_{nn},$$
$$\eta = t_{11} + t_{22} + \cdots + t_{mm}$$

so $\langle \chi, \eta \rangle = \sum_{ij} \langle f_{ii}, t_{jj} \rangle$.

If ρ, σ are not equivalent then $\langle f_{ii}, t_{jj} \rangle = 0$ by Theorem 10 and the result follows.

If ρ, σ are equivalent then we can assume that $\rho = \sigma$ (see Lemma 14). Then n is coprime to p and

$$\langle f_{ii}, f_{jj} \rangle = \begin{cases} 0 & if\ i \neq j \\ 1/n & if\ i = j, \end{cases}$$

by Theorem 11. So

$$\langle \chi, \eta \rangle = \sum_i^n \langle f_{ii}, f_{ii} \rangle = 1.$$

Theorem 16. *Let* $\chi_1, \ldots, \chi_k$ *be the characters of non-equivalent irreducible representations of* G. *Then* $\chi_1, \ldots, \chi_k$ *are linear independent functions on* G.

Proof. Suppose the contrary, that $f = a_1\chi_1 + \cdots + a_k\chi_k = 0$ for some $a_1, \ldots, a_k \in F$ and $a_i \neq 0$ for some i with $1 \leq i \leq k$. Then

$$0 = \langle f, \chi_i \rangle = \langle \chi_i, \chi_i \rangle = a_i \neq 0,$$

by Theorem 15. This is a contradiction.

Observation: The character of a reducible representation ρ is the sum of the characters of the irreducible constituents of ρ.

This is clear from a matrix shape of a reducible representation. Indeed, we have seen that a reducible representation can be written in a matrix interpretation as

$$\rho(g) = \begin{pmatrix} \rho_1(g) & * & * & ... & * & * \\ 0 & \rho_2(g) & * & ... & * & * \\ ... & ... & ... & ... & ... & ... \\ 0 & 0 & ... & \rho_i(g) & * & * \\ ... & ... & ... & ... & ... & ... \\ 0 & 0 & 0 & ... & 0 & \rho_k(g) \end{pmatrix}$$

So the trace of $\rho(g)$ is the sum of the traces of $\rho_1(g), \ldots, \rho_k(g)$.

Let σ be some irreducible representation of G.
The number m of terms in the set $\rho_1, \ldots, \rho_k$ that are equivalent to σ is called the **multiplicity of σ in ρ**.
If none of $\rho_1, \ldots, \rho_k$ is equivalent to σ, one says that the multiplicity of σ in ρ is 0.

Lemma 17. *Suppose that F is of characteristic 0. Let ρ, σ be representations of G and let χ, ν be their characters. Suppose that τ is irreducible. Then the multiplicity of σ in ρ is equal to $\langle \chi, \nu \rangle$.*

Proof. ρ can be transformed to a block-triangular shape with irreducible diagonal constituents, $\rho_1, \ldots, \rho_k$, say. Then
$\chi = \chi_1 + \cdots + \chi_k$ where χ_j is the character of ρ_j for $j = 1, \ldots, k$.
Equivalent representations have the same characters. Therefore, if m constituents are equivalent to σ then $\chi = m\nu +$ the characters χ_j of the constituents that are not equivalent to σ. By Theorem 15,

$$\langle \chi, \nu \rangle = \sum_j \langle \chi_j, \nu \rangle = m.$$

If F is of characteristic $p > 0$ then $\langle \chi, \nu \rangle$ cannot be interpreted as the multiplicity of σ in ρ which is a natural number.

Section 5: **Properties of characters**

Regular representation

We need the notion of a regular character. For this consider the permutation representation π of G on itself, given by

$$\pi(g) : h \to gh \ (h \in G).$$

Let V be a vector space with basis b_h $(h \in G)$ on which g acts by sending b_h to b_{gh}. Then the representation $\rho_{\text{reg}} : G \to GL(V)$ given by $b_h \to b_{gh}$ is called the **regular representation** of G.

We denote by χ_{reg} the character of ρ_{reg}.

The matrices of ρ_{reg} permute the basis elements b_h of V, and if $g \neq 1$ then $gb_h \neq b_h$ for every b_h as $gh \neq h$, and hence $gb_h = b_{gh} \neq b_h$.

In this basis the matrices of $\rho_{reg}(G)$ are so called *permutational matrices.* Their entries are $0, 1$, and every row and every column has exactly one entry equal to 1.

Lemma 18. *Let $g \in G$. Then*

$$\chi_{\mathrm{reg}}(g) = \begin{cases} |G| & if\ g = 1 \\ 0 & otherwise. \end{cases}$$

Thus, χ_{reg} vanishes on $G \setminus 1$.

Theorem 19. *Let F be an algebraically closed field of characteristic* 0.
Then every irreducible representation ρ of G is a constituent of the regular representation ρ_{reg} of G; the multiplicity of ρ in ρ_{reg} is equal to $\dim \rho$.

Proof. Let χ be the character of ρ and $d = |G|$. Then

$$\langle \chi_{\mathrm{reg}}, \chi \rangle = \frac{1}{d} \sum_{g \in G} \chi_{\mathrm{reg}}(g) \chi(g) =$$

$$= \frac{1}{d}\, \chi_{\mathrm{reg}}(1) \chi(1) = \chi(1),$$

and the result follows.

Theorem 20. *Let F be an an algebraically closed field of characteristic* 0*. Let* $m_1, \ldots, m_k$ *be the dimensions of the irreducible representations* $\rho_1, \ldots, \rho_k$ *of* G*. Then*

$$m_1^2 + \cdots + m_k^2 = |G|.$$

Proof. As $|G|$ is the dimension of the regular representation of G, we have $|G| = m_1^2 + \cdots + m_k^2$.

Irreducible character basis in the space of class functions

Let F be an algebraically closed field of characteristic 0, and let $\mathcal{F}(G)$ be the set of all functions $G \to F$.
Recall that $\mathcal{F}(G)$ is a vector space over F.

Let $\rho^1, \ldots, \rho^k$ be a maximal set of irreducible representations of G such that ρ^i and ρ^j are non-equivalent for $i \neq j$.
Let $m_1, \ldots, m_k$ be their dimensions.

Theorem 21. *The matrix entry functions ρ^l_{ij} $(1 \leq i, j \leq m_l,\ l = 1, \ldots, k)$ of these representations constitute a basis in $\mathcal{F}(G)$.*

Proof. By Corollary 12, the matrix entries of $\rho_1, \ldots, \rho_k$ are linear independent functions on G. The number of these is equal to $m_1^2 + \cdots + m_k^2 = d$ where $d = |G|$ (see Theorem 20). As $\dim \mathcal{F}(G) = d$, the claim follows.

The number of irreducible characters

Lemma 22. *Let $\rho, \tau : G \to GL_n(F)$ be equivalent irreducible representations of G. Then each $\tau_{ij}(g)$ is a linear combination of $\rho_{kl}(g)$ for $1 \leq i, j, k, l \leq n$. In other words, the subspaces spanned by $\rho_{ij}(g)$ and by $\tau_{ij}(g)$ coincide.*

Proof. As ρ and τ are equivalent, there is a non-degenerate matrix A such that $\rho(g) = A\tau(g)A^{-1}$. So the claim follows.

Keep F to be an algebraically closed field of characteristic 0.

Lemma 23. *Let $\rho^{(1)}, \dots, \rho^{(k)}$ be a maximal set of irreducible representations of G such that $\rho^{(i)}$ and $\rho^{(j)}$ are non-equivalent for $i \neq j$.*
Let $\mathcal{F}_i(G)$ denote the F-span of $\rho^{(i)}_{kl}(g)$ in $\mathcal{F}(G)$ (where $1 \leq k, l \leq \dim \rho^{(i)}$). Then

$$\mathcal{F}(G) = \mathcal{F}_1(G) \oplus \cdots \oplus \mathcal{F}_k(G)$$

(the direct sum of subspaces).

Moreover, if $f(g) \in \mathcal{F}_i(G)$ and $h \in G$ then $f(hgh^{-1}) \in \mathcal{F}_i(G)$.

Proof. The first claim follows from Theorem 21 as functions $\rho^{(i)}_{kl}(g)$ are linear independent.

The second one follows from Lemma 22. Indeed,

$$f(hgh^{-1}) = \sum_{kl} c_{kl}^{(i)} \rho_{kl}^{(i)}(hgh^{-1}) =$$

$$= \sum_{kl} c_{kl}^{(i)} (\rho^{(i)}(hgh^{-1}))_{kl} =$$

$$= \sum_{kl} c_{kl}^{(i)} (\rho^{(i)}(h)\rho^{(i)}(g)(\rho^{(i)}(h)^{-1}))_{kl}.$$

As h is fixed here, the mapping

$$g \to (\rho^{(i)}(h)\rho^{(i)}(g)(\rho^{(i)}(h)^{-1}))$$

is a representation of G equivalent to $\rho^{(i)}$, whence the claim.

Lemma 24. *Let $f \in \mathcal{F}(G)$ be a class function. Express $f = \sum f_i$ where $f_i \in \mathcal{F}_i(G)$* (see Lemma 23). *Then each f_i is a class function.*

Proof. Let $h \in G$. As f is a class function, $f(g) = f(hgh^{-1})$. So

$$0 = f(g) - f(hgh^{-1}) = \sum_i (f_i(g) - f_i(hgh^{-1})).$$

Set $f_i' = f_i(g) - f_i(hgh^{-1})$. By Lemma 23, $f_i' \in \mathcal{F}_i(G)$ whence $f_i' = 0$ as $\mathcal{F}(G)$ is the direct sum of $\mathcal{F}_i(G)$ $(1 \le i \le k)$. Hence $f(g) = f(hgh^{-1})$ for any $h \in G$, that is, $f_i(g)$ is a class function.

Let $f_{11}(x)$, $f_{12}(x), \ldots, f_{nn}(x)$ denote the entries of a matrix $x \in M(n, \mathbb{C})$. We wish to view f_{ij} as a mapping $M(n, F) \to F$ which corresponds $f_{ij}(x)$ to every matrix x.

If $\rho : G \to GL(n, F)$ is a representation then $f_{ij}(g)$ can be viewed as the composition of the mappings $\rho : G \to GL(n, F)$ and $x \to f_{ij}(x)$. The advantage of this viewpoint is that for $g, g' \in G$ the expression $f_{ij}(\rho(g) + \rho(g'))$ is not meaningless.

In Lemma 25 we shall use a particular case of Theorem 9 which states that $\tilde{T} = \frac{|G|}{n}\text{TraceT} \cdot \text{Id}$, where T is a matrix and $\tilde{T}$ is $\sum_{h \in G} \rho(h) T \rho(h^{-1})$. For $T = \rho(g)$ we have $\tilde{T} = \frac{|G|}{n}\chi(g) \cdot \text{Id}$ where χ is the character of ρ.

Lemma 25. *Let $\rho : G \to GL(n, F)$ be an irreducible representation with entry functions $f_{11}(g), f_{12}(g), \ldots, f_{nn}(g)$.*
Let α be a class function on G such that $\alpha = \sum_{i,j} c_{ij} f_{ij}(g)$ with $c_{ij} \in F$.
Then $\alpha(g) = c\chi_\rho(g)$ for some $c \in F$, where χ_ρ is the character of ρ.

Proof. Compute $\frac{1}{|G|}\sum_{h\in G}\alpha(hgh^{-1})$ for $h \in G$. Clearly, it is equal to $\alpha(g)$ as α is a conjugacy class function. So

$$\alpha(g) = \frac{1}{|G|}\sum_{h\in G}\sum_{i,j} c_{ij} f_{ij}(hgh^{-1}) =$$

$$= \frac{1}{|G|}\sum_{h\in G}\sum_{i,j} c_{ij}(\rho(hgh^{-1}))_{ij}$$

$$= \frac{1}{|G|}\sum_{i,j} c_{ij}(\sum_{h\in G}\rho(hgh^{-1}))_{ij}.$$

The internal sum $\sum_{h\in G}\rho(hgh^{-1})$ is a matrix T_g, say, which commute with every $\rho(t)$ for $t \in G$ (Theorem 8). As ρ is irreducible, by Schur's Lemma T_g is scalar, say, $T_g = \lambda(g) \cdot \mathrm{Id}$. Therefore, $(T_g)_{ij} = 0$ if $i \neq j$ while $(T_g)_{ii} = \lambda(g)$.

Hence

$$\sum_{ij} c_{ij}(\sum_{h\in G}\rho(hgh^{-1}))_{ij} =$$

$$= \sum_{ij} c_{ij}(\sum_{h\in G}\rho(h)\rho(g)\rho(h^{-1}))_{ij} =$$

$$= \sum_{i} c_{ii}\lambda(g) = \lambda(g)\cdot\sum_{i} c_{ii}.$$

We use an abbreviature "tr" for "trace". Let $d = |G|$. Observe that

$$tr(T_g) = n\lambda(g) = \textstyle\sum_{h\in G} tr(\rho(hgh^{-1})) = d\cdot\chi(g)$$

(Theorem 9). Therefore,

$$\alpha(g) = \frac{1}{d}(\sum_{i} c_{ii})\cdot\frac{d}{n}\chi(g) = \frac{1}{|n|}(\sum_{i} c_{ii})\cdot\chi(g)$$

as desired.

Theorem 26. *The characters of non-equivalent irreducible representations of G form a basis in the vector space of class functions.*

Proof. Let f be a class function. By Theorem 21 and Lemma 24, $f = \sum f_i$ where $f_i \in \mathcal{F}_i(G)$. By Lemma 25, $f_i(g) = c_i\chi_i(g)$ where χ_i is the character of ρ_i and $c \in \mathbb{C}$. Therefore, $f = \sum_i c_i\chi_i$. Thus, the space of class functions is spanned by the irreducible characters. So the result follows as the irreducible characters are linear independent.

The following fact is another arithmetic property of irreducible characters which is valid for arbitarary finite group.

Corollary 27. *The number of irreducible characters of G is equal to the number of conjugacy classes in G.*

Character values

Observation. Let χ be a character of a finite group G, $n = \chi(1)$ and $g \in G$. Then $\chi(g)$ is a sum of n $|g|$-roots of unity.

Proof. Let H be the cyclic group generated by g, so $|H| = |g|$. Let ρ be a representation afforded by χ, and let τ be the restriction of ρ to H. Then τ is a representation of a cyclic group H.
To prove the observation, we can include the ground field F to an algebraically closed field and assume F algebraically closed. So τ can be assumed to have an upper triangle form

$$\tau(g) = \begin{pmatrix} \tau_1(g) & * & * & ... & * & * \\ 0 & \tau_2(g) & * & ... & * & * \\ ... & ... & ... & ... & ... & ... \\ 0 & 0 & ... & \tau_i(g) & * & * \\ ... & ... & ... & ... & ... & ... \\ 0 & 0 & 0 & ... & 0 & \tau_k(g) \end{pmatrix}$$

where $\tau_1, \ldots, \tau_k$ are irreducible constituents of τ. As H is abelian, every irreducible representation of H is one dimensional. In particular, $\dim \tau_1 = ... = \dim \tau_k = 1$. Then we conclude that it suffices to prove the observation for a one dimensional representation.

Consider $\tau_1 : H \to GL_1(F)$. If $|g| = m$, say, then $\tau_1(g^m) = \tau_1(1) = 1$ and $\tau_1(g^m) = \tau_1(g)^m$ as τ_1 is group homomorphism. Hence $\tau_1(g)^m = 1$. So $\tau_1(g)$ is an m-root of unity. This completes the proof.

Recall that the fact that every irreducible representation of an abelian group is one dimensional is true for infinite abelian group as well, and it is also true when S consists of pairwise commuting matrices. Therefore, a well known theorem of linear algebra saying that every matrix over an algebraically closed field is similar to an upper triangular matrix follows from Schur's lemma.

Character table

Let G be a finite group of order d. If one fixes an ordering of the group elements as, say, $g_1, \dots, g_d$, then a character χ of G can be viewed simply as a row of the values $\chi(g_1), \dots, \chi(g_d)$. However, there could be a lot of repetitions in this row as characters are constant on the conjugacy classes.

Let $C_1, \dots, C_k$ be the conjugacy classes of G. We can write $\chi(C_1), \dots, \chi(C_k)$ instead of $\chi(g_1), \dots, \chi(g_k)$, where $\chi(C_i) = \chi(g)$ for $g \in C_i$.

Let $\chi_1, \dots, \chi_k$ be the distinct irreducible characters of G.

In both the cases k is the same as the number of irreducible characters equals the number of conjugacy classes of G.

We can build a matrix $\mathbf{X}(G)$ with entris $\chi_i(C_j)$ with $1 \leq i, j \leq k$. This matrix is called the **character table** of G.

The character table depends on ordering both of the conjugacy classes and of the irreducible characters.

There is no canonical ordering except that the first row is reserved for the trivial character and the first column for the character values at the group identity.

$$\mathbf{X}(G) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \chi_2(1) & \chi_2(g_2) & \cdots & \chi_2(g_k) \\ \cdots & \cdots & \cdots & \cdots \\ \chi_k(1) & \chi_k(g_2) & \cdots & \chi_k(g_k) \end{pmatrix}.$$

To perform a computation of the inner product of two characters χ, χ' in a simpler way, one needs to hold in mind the size d_i of each conjugacy class C_i, $i = 1, \ldots, k$.

$$\langle \chi, \chi' \rangle = \sum_{g \in G} \chi(g)\chi'(g^{-1}) =$$

$$= \sum_{i=1}^{k} d_i \chi(g_i)\chi'(g_i^{-1})$$

where $g_i \in C_i$.

Sometimes one adds to the character table some extra rows or columns in which some additional information is recorded. The row $d_1, \ldots, d_k$ of the class sizes is one of the most useful.

There is a large format book with title "Atlas of finite group" which contains near 100 character tables for most important finite groups. The largest character table exposed there consists of 247 rows and columns.

Example. Let $G = S_3$ be the symmetric group. There are 3 conjugacy classes C_1, C_2, C_3 and 3 irreducible characters χ_1, χ_2, χ_3. According to the above convention, C_1 is the class of the identity element, and χ_1 is the trivial character. Then

$$\mathbf{X}(G) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 2 & 0 & -1 \end{pmatrix}.$$

The character table with extra information is often given as follows (where the first row records the sizes of C_i:

	1	3	2
	C_1	C_2	C_3
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Here is more complex example for $G = S_5$, the symmetric group of 5 letters. This group has 7 conjugacy classes, so the table is a (7×7)-matrix.

1	1	1	1	1	1	1
1	-1	1	1	-1	-1	1
4	2	0	1	-1	0	-1
4	-2	0	1	1	0	-1
5	-1	1	-1	-1	-1	0
5	1	1	-1	1	-1	0
6	0	-2	0	0	0	1

To this, one can add a row with the order of elements in each of 7 conjgacy classes of S_5; these are $1, 2, 3, 4, 5, 6, 10$; and the sizes d_i of them which are $1, 10, 15, 20, 20, 30, 24$. In an additional column one can record the lable (or the number) of a character, say, $\chi_1, \cdots, \chi_7$.

Let

$$D = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & d_k \end{pmatrix}$$

be the diagonal matrix with $d_1, \ldots, d_k$ at the diagonal. (Recall that these are the sizes of the conjugacy classes.) In addition, define $\mathbf{X}(G)^*$ to be the matrix with (i, j)-entries $\chi_j(g_i^{-1})$). In other words,

$$\mathbf{X}(G)^* = \begin{pmatrix} 1 & \chi_2(1) & \chi_2(1) & \cdots & \chi_k(1) \\ 1 & \chi_2(g_2^{-1}) & \chi_3(g_2^{-1}) & \cdots & \chi_k(g_2^{-1}) \\ \cdots & \cdots & \cdots & \cdots & \\ 1 & \chi_2(g_k^{-1}) & \chi_3(g_k^{-1}) & \cdots & \chi_k(g_k^{-1}) \end{pmatrix}.$$

Then the orthogonal relations for irreducible characters can be converted to the matrix form as follows:

$$\mathbf{X}(G)D\mathbf{X}(G)^* = |G| \cdot \mathrm{Id}\,.$$

It follows that the matrix $\mathbf{X}(G)$ is non-degenerate hence invertible. Therefore,

$$\mathbf{X}(G)^*\mathbf{X}(G) = |G| \cdot D^{-1},$$

which is called the
second orthogonality relations
for the irreducible characters. Observe that the right hand side matrix is diagonal with diagonal entries $c_i = d/d_i$ for $i = 1, \dots, k$.

The second orthogonality relations can be expressed as follows:

$$\sum_{i=1}^{k} \chi_i(g^{-1})\chi_i(h) = \begin{cases} c_i & if\ g, h \in C_i \\ 0 & otherwise. \end{cases}$$

This can be viewed as relations between the columns of matrix $\mathbf{X}(G)$.

The numbers c_i are the orders of certain subgroups of G. Namely, set
$C_G(g) = \{x \in G : xg = gx\}$.
This is a subgroup called the **centralizer of g in G**.

Observe that the conjugacy classes are the orbits of G in its conjugacy action on itself.

Indeed, for $x \in G$ define a permutation $\alpha(x) : G \to G$ by $\alpha(x)g = xgx^{-1}$. Then the action in question is the homomorphism $x \to \alpha(x)$.
As $xg = gx$ is equivalent to $xgx^{-1} = g$, the group $C_G(g)$ is the stabilizer of g in G under the conjugation action. It follows that $d_i \cdot |C_G(g_i)| = |G|$ for any $g_i \in C_i$ so $|C_G(g)| = d/d_i = c_i$.

Product of conjugacy classes

Recall that a polynomial with leading coefficient equal to 1 is called **monic**.

Definition 28. *A complex number is called an* **algebraic integers** *is it is a root of a monic polynomial with integer coefficients.*

Below $\mathbb{Z}$ denote the ring of integers, and $\mathbb{C}$ the complex number field.

Lemma 29. *Let* $a, b_1, \ldots, b_m \in \mathbb{C}$ *be non-zero integers. Suppose that*

$$ab_i = \sum_{v=1}^{m} z_{ij} b_j$$

for each $i = 1, \ldots, m$ *and for some* $z_{ij} \in \mathbb{Z}$*. Then* a *is an algebraic integer.*

Proof. Set $M = (z_{ij})$ so M is a $(m \times m)$-matrix. Denote by B the column vector with coordinates $b_1, \ldots, b_m$.
The equalities in the lemma can be expressed as $(a \cdot \mathrm{Id}_m - M)B = 0$ where Id_m stands for the identity $(m \times m)$-matrix.
It is known from linear algebra that this is only possible if $\det(a \cdot \mathrm{Id}_m - M) = 0$.
It follows that a is a root of the characteristic polynomial of M which is obviously monic and with coefficients in $\mathbb{Z}$.

Lemma 30. *Let $r, t \in \mathbb{C}$ be two algebraic integers. Let $r^n \in \sum_{i=0}^{n-1} \mathbb{Z}\, r^i$ and $t^m \in \sum_{i=0}^{m-1} \mathbb{Z}\, t^j$. Then*

$$K := \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \mathbb{Z}\, r^i t^j$$

is a subring of $\mathbb{C}$, and K consists of algebraic integers.

Proof. It is quite clear that one has only to check that $rK \subseteq$ and $tK \subseteq K$ which is obvious. It follows that from Lemma 29 that K consists of algebraic integers (choose $\{r^i t^j\}_{0\leq i<n, 0\leq j<m}$ for $b_1, \ldots, b_k$ and $a \in K$).

Theorem 31. *Algebraic integers form a subring of* $\mathbb{C}$*.*

Proof. Let r, t be algebraic integers. Let n, m, K be as in Lemma 29, in particular, K is a subring of $\mathbb{C}$ and $r, t \in K$. As $-r, r+t, rt \in K$, the result follows.

Lemma 32. *Let χ be a character of a finite group G. Then the values $\chi(g)$ are algebraic integers for every $g \in G$.*

Proof. We already know that $\chi(g)$ is a sum of $|g|$-roots of unity. As algebraic integers form a ring, the lemma follows.

Lemma 33. *Let $\mathbb{Q}$ denote the set of rational numbers. Then algebraic integers in $\mathbb{Q}$ are ordinary integers.*

Proof. Let $q \in \mathbb{Q}$ be an algebraic integer. Write $q = l/m$ where l, m are ordinary integers coprime to each other. Suppose $m \neq \pm 1$. As $q^n = z_{n-1}q^{n-1} + \cdots + z_1 q + z_0$ for some n and integers $z_{n-1}, \ldots, z_0$, it follows that $\frac{l^n}{m} = z_{n-1}l^{n-1} + \cdots + m^{n-2}z_1 l + m^{n-1}z_0$. Then the right hand side is an integer and the left hand side is not.
This is a contradiction.

Let $C_1, \ldots, C_k$ be the conjugacy classes of G. For classes C_i, C_j and $g \in G$ denote by $C_{ij}(g)$ the set of all pairs (x, y) such that $x \in C_i, y \in C_j$ and $xy = g$.

Let $m_{ij}(g)$ be the number of elements in $C_{ij}(g)$. Then the function $g \to m_{ij}(g)$ is constant on the conjugacy classes.

Indeed, if $g' = hgh^{-1}$ then $C_{ij}(g')$ consists of (hxh^{-1}, hyh^{-1}), and the mapping $(x, y) \to (hxh^{-1}, hyh^{-1})$ yields a bijection between $C_{ij}(g)$ and $C_{ij}(g')$. Therefore, one can replace $m_{ij}(g)$ by m_{ij}^l as the former number depends on C_l rather than on $g \in C_l$. (One can think of m_{ij}^l as the multiplicity of C_l in C_iC_j.)

Lemma 34. *Let F be an algebraically closed field. Let ρ be an irreducible representation of G of dimension n. For $g_i \in C_i$ set $\Theta_i = \sum_{x \in C_i} \rho(x)$.*

(1) $\Theta_i = \theta_i \cdot \mathrm{Id}$ *where* $\theta_i = \frac{d_i \chi(g_i)}{n}$.

(2) $\Theta_i \Theta_j = \sum_{l=1}^{k} m_{ij}^{l} \Theta_l$ *and*

$$\theta_i \theta_j = \sum_{l=1}^{k} m_{ij}^{l} \theta_l.$$

(3) *Suppose that F is of characteristic 0. Then $\theta_1, \ldots, \theta_k$ are algebraic integers.*

Proof. Set $c_i = |C_G(g)|$ and $d_i = |C_i|$ for $g \in C_i$, so $c_i d_i = |G|$.

(1) Let $T = \rho(g)$ and $\tilde{T} = \sum_{h \in G} \rho(h)\rho(g)\rho(h)^{-1} = \sum_{h \in G} \rho(hgh^{-1})$. Let $g \in C_i$. Then $\tilde{T} = c_i \Theta_i$. By Theorem 9, $\tilde{T} = \frac{|G| \cdot \chi(g)}{n} \cdot \mathrm{Id}$. As $d_i = |G|/c_i$, the result follows.

(2) $\Theta_i\Theta_j = \sum_{x\in C_i, y\in C_j} \rho(x)\rho(y) =$
$= \sum_{x\in C_i, y\in C_j} \rho(xy) = \sum_l m_{ij}^l \sum_{g\in C_l} \rho(g)$
$= \sum_l m_{ij}^l \Theta_l$.

(3) This follows from Lemma 29 if one takes $\theta_i = a$ and $\theta_1 = b_1, \ldots, \theta_k = b_k$.

Theorem 35. *The dimension of every irreducible representation of G divides $|G|$.*

Proof. Let ρ be an irreducible representation of G, χ character of ρ and $n = \dim\rho$. By orthogonality relations $\langle\chi,\chi\rangle = 1$ whence $|G| = \sum_{g\in G} \chi(g)\chi(g^{-1}) = \sum d_i\chi(g_i)\chi(g_i^{-1})$. Dividing the both sides by n, we get

$$\sum \frac{d_i\chi(g_i)}{n}\chi(g_i^{-1}) = \frac{|G|}{n}.$$

The right hand side is a rational number. As algebraic integers form a ring, the left hand side is an algebraic integer. Hence it is an ordinary integer.

Maschke's theorem

The method of averaging is used for proving another important result of representation theory of finite groups.

Theorem 36. (Maschke's theorem) *Let $G \subset GL(n, F)$ be a finite group of order d. Suppose that characteristic of F is either 0 or coprime to d.*
Then every G-stable subspace has a G-stable complement.

Proof. Let W be a G-stable subspace of $V = F^n$. If $k = \dim W$, we can choose a basis $b_1, \ldots, b_n$ of V such that $b_1, \ldots, b_k \in W$. Under this basis the matrices of G are of shape $\begin{pmatrix} g_{11} & g_{12} \\ 0 & g_{22} \end{pmatrix}$ which entries are submatrices of an appropriate size.

Set $P = \begin{pmatrix} \mathrm{Id} & 0 \\ 0 & 0 \end{pmatrix}$ and $\tilde{P} = \sum_{g \in G} gPg^{-1}$. Observe that $gPg^{-1} = \begin{pmatrix} \mathrm{Id} & * \\ 0 & 0 \end{pmatrix}$ with some matrix at the $*$-position. Therefore, $\tilde{P} = \begin{pmatrix} d \cdot \mathrm{Id} & Y \\ 0 & 0 \end{pmatrix}$ for some matrix Y and $d \neq 0$ by determinant reason. As the inverse of $M = \begin{pmatrix} \mathrm{Id} & Y \\ 0 & \mathrm{Id} \end{pmatrix}$ is equal to $\begin{pmatrix} \mathrm{Id} & -Y \\ 0 & \mathrm{Id} \end{pmatrix}$, one has

$$M\tilde{P}M^{-1} = N =: \begin{pmatrix} d \cdot \mathrm{Id} & 0 \\ 0 & 0 \end{pmatrix}.$$

By Lemma 8, $g\tilde{P} = \tilde{P}g$ for every $g \in G$. Therefore, the matrices of MGM^{-1} commute with N.

A straightforward computations shows that every matrix commuting with N is of shape $\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$ hence stabilizes the space U of vectors with first d coordinates equal to 0. So MGM^{-1} stabilizes U. Clearly, U is a complement to W, and so is MU. As MGM^{-1} stabilizes MU, we have obtains a G-stable complement of W.

Remark. Let $\tilde{P}_1 = \tilde{P} - d \cdot \mathrm{Id}$. One can observe that $MU = (\tilde{P} - d \cdot \mathrm{Id})V$. Therefore, one can find the G-stable complement to W to be the space $(\tilde{P} - d \cdot \mathrm{Id})V$.

Permutation representations

Let Ω be a finite set of n elements which we identify with the set $\{1, \ldots, n\}$. Let S_n denote the group of all permutations of Ω.

Let $P_n \subset GL(n, F)$ denote the group of all permutation matrices. We assume that P_n acts in F^n by permuting the standard basis elements $b_1, \ldots, b_n$. We identify S_n with P_n by obvious way. Namely, given $s \in S_n$, we identify it with the matrix $x \in P_n$ sending each b_i to $b_{s(i)}$.

Definition 37. *Let G be a group. A homomorphism $\rho : G \to P_n$ is called a permutation representation of G.*

Thus, $\rho(G)$ is a subgroup of $P_n \subset GL(n, F)$. Permutation representations constitute an important class of matrix representations of groups.

Example. Let $G = \{1, g, g^2\}$ be a group of order 3 so $g^3 = 1$. Set $\rho(1) = \mathrm{Id}$,

$$\rho(g) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},\ \rho(g^2) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Then ρ is a permutation representation of G.

Exercise. Let $|G| = 2$. Show that there are exactly 4 permutation representations $G \to P_3$. Show that three of them are equivalent to each other.

If H is a subgroup of G, one can decompose G as a union of the cosets

$$G = H \cup g_2 H \cup \cdots \cup g_m H.$$

The left multiplication permutes the cosets. Therefore, the set of the cosets can be taken as a permutation set for G to obtain a permutation representation.

It is easy to compute the character of a permutation representation in terms of the action of G on $\Omega = \{1, \dots, n\}$.

Theorem 38. *Let* $\rho : G \to P_n$ *be a permutation representation and let* χ *be the character of* ρ*. Let* $g \in G$*.*
Then $\chi(g)$ *is equal to the number of points* $i \in \Omega$ *fixed by* g*.*

Proof. The diagonal entries of $\rho(g)_{ii}$ are non-zero if and only if $\rho(g)b_i = b_i$.

Lemma 39. *Let a finite group G act by permutations on finite set Ω partitioning it in k orbits. For $g \in G$ let $|\Omega^g|$ denote the number of elements of Ω fixed by g. Then $\sum_{g \in G} |\Omega^g| = k \cdot |G|$.*

Proof. It suffices to prove the lemma for $k = 1$.
Compute the number m of pairs (g, ω) : $g\omega = \omega$ in two ways.
On one hand $m = \sum_{g \in G} |\Omega^g|$.
On the other hand, $m = \sum_{\omega \in \Omega} |G_\omega|$, where $G_\omega = \{g \in G : g\omega = \omega\}$. The latter number is equal to $|G|$ as $|G| = |\Omega| \cdot |G_\omega|$ for each $\omega \in \Omega$. Hence $\sum_{\omega \in O} |G_\omega| = |G|$, and the result follows.

Theorem 40. *Let $\rho : G \to P_n$ be a permutation representation. Then the multiplicity of 1_G in ρ is equal to the number of the orbits of G on Ω.*

Proof. Let χ_1 denote the character of the trivial representation of G. Compute the inner product $\langle \chi, \chi_1 \rangle$, where χ is the character of ρ.

$$\langle \chi, \chi_1 \rangle = \frac{1}{|G|} \sum \chi(g).$$

By Theorem 38, $\chi(g) = |\Omega^g|$ where $\Omega = \{1, \ldots, n\}$. In addition, $\sum_{g \in G} |\Omega^g| = k \cdot |G|$ by Lemma 39 where k is the number of the orbits. Hence $\langle \chi, \chi_1 \rangle = k$, as stated.

Handbooks for further reading

W. Feit, The characters of finite groups, 1967 (or later editions)

I.M. Isaacs, Character theory of finite groups, 1976 (or later editions)

G. James and M. Liebeck, Representation and characters of groups, 2001.