Chapter 36

MSM4P4 Representation Theory

(36.1) Representations

Definition 1 *Let F be a field and let V be a vector space over F.*

1. *Define* $\mathrm{End}_F(V)$ *to be the set of all linear transformations $T\colon V \to V$ (endomorphisms of V).*
2. *Define* $\mathrm{GL}\,(,V)$ *to be the subset of* $\mathrm{End}_F(V)$ *consisting of the invertible transformations. This is a group under transformation composition.*
3. *Define* $\mathrm{GL}\,(n,F)$ *to be the group of $n \times n$ invertible matrices with elements from the field F.*

Clearly if V is of finite dimension n then $\mathrm{GL}\,(,V)$ and $\mathrm{GL}\,(n,F)$ are isomorphic. They are *not* equal as one is a set of functions whereas the other is a set of matrices. The isomorphism arrises because the linear transformation is determined by its effect on a basis of V, giving rise to a matrix. Note also that the representation in $\mathrm{GL}\,(n,\mathbb{C})$ is dependent on basis.

Definition 2 *Let G be a group, F be a field, and V be a vector space over F. A group homomorphism*

$$\sigma\colon G \to \mathrm{GL}\,(,V)$$

is a representation of G over F.

It is sometimes convenient to consider a representation as a group homomorphism from G to $\mathrm{GL}\,(n,F)$ rather than $\mathrm{GL}\,(,V)$. This causes no problem since in this case the representation is merely the composition of σ with the isomorphism between $\mathrm{GL}\,(,V)$ and $\mathrm{GL}\,(n,F)$.

Definition 3 *Let $\sigma\colon G \to H$ be a function and $g \in G$. The element of H obtained by applying σ to g is denoted $g\sigma$.*

Example 4 *Let G be the dihedral group of order n. So*

$$G = \left\langle x, y \mid x^2 = y^n = 1, x^{-1}yx = y^{-1} \right\rangle$$

Define

$$x\sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad y\sigma = \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & \sin\left(\frac{2\pi}{n}\right) \\ -\sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix}$$

As G is generated by x and y, σ extends to a representation of G over $\mathbb{R}$. Similarly one may define $\tau\colon G \to \mathrm{GL}\,(2,\mathbb{C})$ by

$$x\tau = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad y\tau = \begin{pmatrix} \omega & 0 \\ 0 & \overline{\omega} \end{pmatrix} \qquad \omega = \exp\left(\frac{2\pi i}{n}\right)$$

If σ is a representation of a group G over a field F then for each $g \in G$, $g\sigma$ is a linear transformation. Particular interest lies within groups whose linear transformations are closed on subspaces of a vector space over F: in a similar fashion to a normal subgroup or ideal.

Definition 5 *Let G be a group, F be a field, V be a vector space over F, and $\sigma\colon G \to \mathrm{GL}\,(,V)$ be a representation. Let W be a non-trivial proper subspace of V. If*

$$w(g\sigma) \in W \quad \forall g \in G \quad \forall w \in W$$

then W is called a G-invariant subspace of V.

In such a situation σ induces another representation $\tau\colon G \to \mathrm{GL}\,(,W)$ defined by $g\tau = g\sigma$ for all $g \in G$.

The matrix for a linear transformation is dependent on basis. Rather than use the standard basis, it can be convenient to find a basis for a G-invariant subspace W ($\dim W = m$ say) and extend this to a basis of V ($\dim V = n$ say). With vectors of V written as row vectors so that the transformation matrix acts on the right, the columns of the transformation matrix correspond to where the basis vectors are sent under the transformation. As the transformation is G-invariant it must therefore be of the form

$$g\sigma \dashrightarrow \begin{pmatrix} m \times m & 0 \\ * & (n-m) \times (n-m) \end{pmatrix}$$

The $m \times m$ sub-matrix is equal to $g\tau$; the representation restricted onto W. The zero sub-matrix indicates what happens to the basis vectors which extend the basis of W to one of V: the co-ordinates of the vector that are "unused" in W are sent to zero. The lower sub-matrices describe the transformation on $V \setminus W$.

Definition 6 *Let σ be a representation of a group G over a field F and let V be a vector space over F. If V has a G-invariant subspace then σ is called reducible. Otherwise σ is irreducible.*

Definition 7 *Let σ be a representation of a group G over a field F and let V be a vector space over F. If V has G-invariant subspaces U and W such that $V = U \oplus W$ then σ is said to be decomposable.*

Reducibility and decomposability are not the same thing, though often they do coincide. The following example illustrates the difference.

Example 8 *Let $G = \langle t \mid t^2 = 1 \rangle$, $F = \mathbb{Z}_2$, and $V = F^2$ with vectors written as row vectors. Define*

$$\sigma\colon G \to \mathrm{GL}\,(2,F) \quad \textit{by} \quad \sigma\colon t \mapsto \begin{cases} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \textit{if } t \neq 1 \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \textit{if } t = 1 \end{cases}$$

Let $W = \mathrm{Span}\,\{(1,1)\} = \{(1,1)\}$.

$$(1,1)\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = (1,1)$$

hence W is G-invariant and thus σ is reducible. Further to this, changing basis to $\{(1,1),(0,1)\}$;

$$\begin{pmatrix} 1 & 1 \end{pmatrix}(t\sigma) = (1,1) \qquad (0,1)(t\sigma) = (1,0) = (1,1) + (0,1)$$

therefore the transformation matrix for $t\sigma$ with respect to this basis is $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ which has the form described after Definition 5.

Suppose that $V = U \oplus W$ with U and W as proper, non-trivial subspaces which are both G-invariant. Then both U and W must have dimension 1 with respective bases $\{\mathbf{u}\}$ and $\{\mathbf{w}\}$ say. Therefore

$$\mathbf{u}(t\sigma) \in U \text{ so } \mathbf{u} = \lambda\mathbf{u} \text{ for some } \lambda \in F$$
$$\mathbf{w}(t\sigma) \in W \text{ so } \mathbf{w} = \mu\mathbf{w} \text{ for some } \mu \in F$$

Hence λ and μ are both eigenvectors of $t\sigma$. Now,

$$\begin{vmatrix} 0-x & 1 \\ 1 & 0-x \end{vmatrix} = x^2 - 1 = (x-1)^2$$

so the only eigenvalue of $t\sigma$ is 1 meaning that $\mu = 1 = \lambda$, and that if $\begin{pmatrix} a & b \end{pmatrix}$ is an eigenvector then

$$\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a & b \end{pmatrix}$$

Therefore $\begin{pmatrix} a & b \end{pmatrix} = \begin{pmatrix} b & a \end{pmatrix}$ and so the only eigenvector of $t\sigma$ is $\begin{pmatrix} 1 & 1 \end{pmatrix}$. As 2 distinct eigenvectors of $t\sigma$ cannot be found there cannot exist such U and W meaning that V is not decomposable.

(36.1.1) The Group Algebra

Definition 9 *Let V be a vector space over a field F. An algebra V is V extended by a multiplication operation $V \times V \to V$. This forms a ring.*

Note that an algebra is not exactly a ring, as unlike a ring it has a scalar multiplication operation defined on it and a field.

Definition 10 *Let F be a field and G be a finite group. The group algebra FG is the $|G|$-dimensional vector space over F that has basis G and multiplication on FG defined by*

$$\left(\sum_{g\in G} \alpha_g g\right)\left(\sum_{h\in G} \beta_h h\right) = \sum_{x\in G}\left(\sum_{\substack{(g,h)\in G\times H \\ x=gh}} \alpha_g \beta_h\right) x$$

Again, this is a ring. Note that addition is indeed associative since

$$\sum_{g\in G} \alpha_g g + \sum_{g\in G} \beta_g g = \sum_{g\in G} (\alpha_g + \beta_g) g = \sum_{g\in G} (\beta_g + \alpha_g) g = \sum_{g\in G} \beta_g g + \sum_{g\in G} \alpha_g$$

An algebra is different from a ring because it has a scalar multiplication with a field defined on it. A homomorphism between algebras must also preserve the structure relating to this scalar multiplication.

Definition 11 *An algebra homomorphism is a group homomorphism that is also a linear map.*

Definition 12 *Let R be a ring and V be a vector space. The R-module V is formed from V by defining an operation $\cdot\colon V \times R \to V$ which is associative, and distributive over vector addition.*

A module is therefore like a vector space with 2 scalar multiplications.

For the purposes of representation theory, complex group algebras will be of interest; that is, given a group G the algebra $\mathbb{C}G$ is examined.

Let V be an n-dimensional vector space over $\mathbb{C}$ and let σ be a representation of a group G in $\mathrm{GL}(n, \mathbb{C})$. Since $\mathbb{C}G$ is a ring $\mathbb{C}G$-modules may be formed, in this case by defining multiplication

$$\mathbf{v} \mapsto \mathbf{v}g = \mathbf{v}(g\sigma)$$

Many different $\mathbb{C}G$ modules may me formed, of different dimension, say.

Note that $\mathrm{End}_{\mathbb{C}}(V)$ is an algebra. It is a vector space, and a multiplication can be defined on it as function composition.

Lemma 13 *Let G be a finite group. If σ is a representation of G over a vector space V then σ can be extended to an algebra homomorphism between $\mathbb{C}G$ and $\mathrm{End}_{\mathbb{C}}(V)$.*

Proof. Let $\sigma\colon G \to \mathrm{GL}(, V)$ be a representation of G over a vector space V. Extend σ to an algebra homomorphism σ' by

$$\sigma'\colon \sum_{g\in G} \alpha_g g \mapsto \sum_{g\in G} \alpha_g (g\sigma)$$

then σ' is an algebra homomorphism of $\mathbb{C}G$ to $\mathrm{End}_{\mathbb{C}}(V)$. Now,

$$\left(\sum_{g\in G} \alpha_g g + \sum_{g\in G} \beta_g g\right)\sigma' = \sum_{g\in G} (\alpha_g + \beta_g)(g\sigma) = \sum_{g\in G} \alpha_g(g\sigma) + \sum_{g\in G} \beta_g(g\sigma)$$

A similar calculation can be performed for the multiplicative homomorphism property, showing that σ' is a ring homomorphism. Finally, for $\lambda \in \mathbb{C}$ it is clear that

$$\left(\lambda \sum_{g\in G} \alpha_g g\right)\sigma' = \lambda\left(\sum_{g\in G} \alpha_g g\right)\sigma'$$

so that σ' is a linear map and so is an algebra homomorphism, as required. □

Lemma 14 *If $\sigma\colon \mathbb{C}G \to \mathrm{End}_{\mathbb{C}}(V)$ is an algebra homomorphism then it restricts to a representation of G over $\mathrm{GL}(, V)$.*

Proof. For any $g \in G$,

$$(g\sigma)(g^{-1}\sigma) = (gg^{-1})\sigma = 1_G\sigma = \mathrm{id}_V$$

Hence the matrix $g\sigma$ has an inverse, namely $g^{-1}\sigma$ and so the image of G under σ is contained in $\mathrm{GL}(, V)$. Hence σ does indeed restrict to a group homomorphism of G to $\mathrm{GL}(, V)$. □

From the above 2 results the following equivalence has arisen.

- A matrix representation of G.
- A group homomorphism of G to $\mathrm{GL}(, V)$.
- An algebra homomorphism of $\mathbb{C}G$ to $\mathrm{End}_{\mathbb{C}}(V)$. Note that $\mathrm{End}_{\mathbb{C}}(V) = \mathrm{Hom}_{\mathbb{C}}(V) \cong M_n(\mathbb{C})$.
- V has the structure of a $\mathbb{C}G$ module.

The group algebra $\mathbb{C}G$ has itself the structure of a $\mathbb{C}G$ module.

Lemma 15 *The $\mathbb{C}G$-sub-modules of a vector space V are precisely the G invariant subspaces.*

Proof. If W is a G-invariant subspace of V then it is closed under the action of elements of G which defines the structure of a $\mathbb{C}G$-sub-module.

Conversely, if W is a $\mathbb{C}G$-sub-module then it is a subspace of V and is closed under the action of G i.e. is G-invariant. □

(36.1.2) Inner Products On Modules

Let G be a finite group and V be a $\mathbb{C}G$ module, so V is a vector space over $\mathbb{C}$ that has a multiplication with elements of G. An inner product may be defined on V, i.e. a function $V \times V \to \mathbb{C}$. Choosing a basis $\{\mathbf{v}_1, \mathbf{v}_n, \ldots, \mathbf{v}_n\}$,

$$\left\langle \sum_{i=1}^{n} \alpha_i \mathbf{v}_i, \sum_{i=1}^{n} \beta_i \mathbf{v}_i \right\rangle = \sum_{i=1}^{n} \alpha_i \overline{\beta}_i$$

The effect of multiplication by elements of G on this inner product is not clear. However, a 'nicer' inner product can be constructed:

$$\langle\langle \mathbf{v}, \mathbf{w} \rangle\rangle = \frac{1}{|G|} \sum_{g \in G} \langle \mathbf{v}g, \mathbf{w}g \rangle$$

This is indeed an inner product since

$$\begin{aligned} \langle\langle \alpha\mathbf{v}, \mathbf{w} \rangle\rangle &= \alpha \langle\langle \mathbf{v}, \mathbf{w} \rangle\rangle \\ \langle\langle \mathbf{v}, \beta\mathbf{w} \rangle\rangle &= \overline{\beta} \langle\langle \mathbf{v}, \mathbf{w} \rangle\rangle \\ \langle\langle \mathbf{v}, \mathbf{v} \rangle\rangle &\geqslant 0 \\ \langle\langle \mathbf{v}, \mathbf{v} \rangle\rangle &= 0 \Rightarrow \mathbf{v} = \mathbf{0} \end{aligned}$$

These properties are inherited directly from the inner produce $\langle \mathbf{v}, \mathbf{w} \rangle$. The merit of this new inner product is that it is G-invariant. Let $h \in G$ then

$$\begin{aligned} \langle\langle \mathbf{v}h, \mathbf{w}h \rangle\rangle &= \frac{1}{|G|} \sum_{g \in G} \langle (\mathbf{v}g)h, (\mathbf{w}g)h \rangle \\ &= \frac{1}{|G|} \sum_{g \in G} \langle \mathbf{v}(gh), \mathbf{w}(gh) \rangle \\ &= \frac{1}{|G|} \sum_{g \in G} \langle \mathbf{v}g, \mathbf{w}g \rangle \\ &= \langle\langle \mathbf{v}, \mathbf{w} \rangle\rangle \end{aligned}$$

(36.1.3) Maschke's Theorem

Theorem 16 (Maschke) *Let V be a finite dimensional $\mathbb{C}G$-module for a finite group G. If W is a $\mathbb{C}G$-sub-module then there exists another $\mathbb{C}G$-sub-module U such that $V = W \oplus U$.*

Proof. Let W be a $\mathbb{C}G$-sub-module (G invariant subspace) then with the inner product defined in Section 36.1.2 the orthogonal complement of W, $W^\perp$ may be formed, i.e.

$$W^\perp = \{\mathbf{v} \in V \mid \langle\langle \mathbf{v}, \mathbf{w} \rangle\rangle = 0 \quad \forall \mathbf{w} \in W\}$$

As a complex vector space, $V = W \oplus W^\perp$, so it is now sufficient to show that $W^\perp$ is a G-invariant subspace i.e. $\mathbb{C}G$-sub-module. Take $\mathbf{u} \in W$ then it must be shown that $\langle\langle \mathbf{u}g, \mathbf{w} \rangle\rangle = 0$ for all $\mathbf{w} \in W$ and $g \in G$, so that the action of G is closed on $W^\perp$.

$$\begin{aligned} \langle\langle \mathbf{u}g, \mathbf{w} \rangle\rangle &= \left\langle\left\langle \mathbf{u}g, \mathbf{w}(gg^{-1}) \right\rangle\right\rangle \\ &= \left\langle\left\langle \mathbf{u}g, (\mathbf{w}g)g^{-1} \right\rangle\right\rangle \quad \text{(module property)} \\ &= \left\langle\left\langle \mathbf{u}, \mathbf{w}g^{-1} \right\rangle\right\rangle \quad \text{(by } G\text{-invariance)} \end{aligned}$$

But as W is a $\mathbb{C}G$-submodule $\mathbf{w}g^{-1} \in W$ and thus this inner product is zero, meaning that $\mathbf{u}g$ is indeed in

$W^{\perp}$ which, thus, is a $\mathbb{C}G$-submodule. □

Corollary 17 *For vector spaces over $\mathbb{C}$ and for a finite group G, if V is reducible then V is decomposable.*

Proof. If V is reducible then it has a G-invariant subspace W. But then by Maschke's Theorem $V = W \oplus W^{\perp}$ and thus V is decomposable. □

Definition 18 *A matrix $M \in M_n(\mathbb{C})$ is unitary if $M^{-1} = \overline{M}^{\top}$ where $\overline{M}$ denotes the matrix obtained from M by replacing each element with its complex conjugate.*

The importance of unitary matrices is that the linear transformation is represents preserves the inner product with respect to which the chosen basis is orthonormal. By Gram-Schmidt an orthonormal basis can always be found and thus:

- For a finite-dimensional vector space V, a G-invariant inner product can always be constructed on V.
- An orthonormal basis with respect to the G-invariant inner product can be found for V (Gram-Schmidt).
- There is a representation $\sigma\colon G \to \mathrm{GL}(n, V)$ for which $g\sigma$ is always a unitary matrix. This happens because the inner product is G-invariant and the basis is orthonormal relative to the same inner product.
- Conversely if $\sigma\colon G \to \mathrm{GL}(n, V)$ and $g\sigma$ is always a unitary matrix then taking $V = \mathbb{C}^n$ with the usual inner product makes the inner product G-invariant.

The objective is to write any $\mathbb{C}G$-module as a direct sum of irreducible $\mathbb{C}G$-modules. Clearly Maschke's Theorem is important here. In fact the general result follows directly by induction on the dimension of V.

Theorem 19 *Let G be a finite group and V be a $\mathbb{C}G$-module. Then V can be expressed as a direct sum of irreducible $\mathbb{C}G$-modules.*

Proof. If $\dim V = 1$ then V is irreducible and there is nothing to show. Suppose that $\dim V > 1$, then if V is irreducible there is again nothing to show; suppose therefore that V is reducible. Then V has a proper non-trivial G-invariant subspace W say, but then by Maschke's Theorem $v = W \oplus W^{\perp}$. Furthermore $\dim W < \dim V$ and $\dim W^{\perp} < \dim V$ and thus by induction

$$W = U_1 \oplus U_2 \oplus \cdots \oplus U_k \quad \text{and} \quad W^{\perp} = U_1' \oplus U_2' \oplus \cdots \oplus U_l'$$

for irreducible $\mathbb{C}G$-modules U_i and U_j'. Hence

$$V = U_1 \oplus U_2 \oplus \cdots \oplus U_k \oplus U_1' \oplus U_2' \oplus \cdots \oplus U_l'$$

i.e. V is a direct sum of irreducible $\mathbb{C}G$-modules, as required. □

Thus the study of $\mathbb{C}G$-modules is reduced to the study of the irreducible ones.

(36.1.4) Schur's Lemma

Having reduced the area of interest to only irreducible $\mathbb{C}G$-modules, Schur's Lemma gives a property of them.

Lemma 20 (Schur) *The result may be stated in one of the following 3 (equivalent) forms. LEt G be a finite group,*

1. *(Complex Vector Space) Let $\sigma\colon G \to \mathrm{GL}\,(n,\mathbb{C})$ be an irreducible complex representation of G. Let $T \in M_n(\mathbb{C})$ be a matrix with the property $(g\sigma)T = T(g\sigma)$ for all $g \in G$. Then $T = \lambda I_n$ for some $\lambda \in \mathbb{C}$.*
2. *(General Vector Space) Let $\sigma\colon G \to \mathrm{GL}\,(,V)$ be an irreducible representation of G. If $T \in \mathrm{End}_{\mathbb{C}}(V)$ with $(g\sigma)T = T(g\sigma)$ for all $g \in G$, then $T = \lambda \mathrm{id}_V$ for some $\lambda \in \mathbb{C}$.*
3. *(Module Theoretic) If V is an irreducible $\mathbb{C}G$-module then $\mathrm{End}_{\mathbb{C}G}(V) = \mathbb{C}\mathrm{id}_V$ where*

$$\begin{aligned}\mathrm{End}_{\mathbb{C}}(V) &\stackrel{def}{=} \{T \in \mathrm{End}_{\mathbb{C}}(V) \mid (\mathbf{v}T)g = (\mathbf{v}G)T \quad \forall \mathbf{v} \in V \quad \forall g \in G\}\\ \mathbb{C}\mathrm{id}_V &\stackrel{def}{=} \{\lambda \mathrm{id}_V \mid \lambda \in \mathbb{C}\}\end{aligned}$$

Proof. The general vector space formulation is proven. Let $\sigma\colon G \to \mathrm{GL}\,(,V)$ be an irreducible representation of G and let $T \in \mathrm{End}_{\mathbb{C}}(V)$ with $(g\sigma)T = T(g\sigma)$ for all $g \in G$. As T is complex it has an eigenvalue, λ say. Let W be the λ eigenspace of T, that is

$$W = \ker(T - \lambda \mathrm{id}_V)$$

then $W \neq \{\mathbf{0}\}$. Now, $T(g\sigma) = (g\sigma)T$ and certainly $(g\sigma)\mathrm{id}_V = \mathrm{id}_V(g\sigma)$ so

$$\begin{aligned}(g\sigma)(T - \lambda \mathrm{id}_V) &= (T - \lambda \mathrm{id}_V)(g\sigma)\\ \text{so}\quad \mathbf{w}(g\sigma)(T - \lambda \mathrm{id}_V) &= \mathbf{w}(T - \lambda \mathrm{id}_V)(g\sigma)\\ &= \mathbf{0}(g\sigma)\\ &= \mathbf{0}\end{aligned}$$

Therefore $\mathbf{w}(g\sigma) \in W = \ker(T - \lambda \mathrm{id}_V)$ so W is a G-invariant subspace of V. But $W \neq \{\mathbf{0}\}$ and V is irreducible, therefore $V = W$ which means that $\mathbf{v}(T - \lambda \mathrm{id}_V) = \mathbf{0}$ for all $\mathbf{v} \in V$. Re-arranging, $T = \lambda \mathrm{id}_V$. □

(36.1.5) Orthogonality Relations

Let $\sigma\colon G \to \mathrm{GL}\,(n,\mathbb{C})$ and $\tau\colon G \to \mathrm{GL}\,(m,\mathbb{C})$ be irreducible representations and let $X \in M_{nm}(\mathbb{C})$. Define

$$Y = \sum_{g \in G} (g\sigma)^{-1} X (g\tau) \tag{21}$$

Lemma 22 *Where Y is defined as in Equation (21) $(h\sigma)^{-1}Y(h\tau) = Y$ for all $h \in G$.*

Proof. Choosing $h \in G$,

$$\begin{aligned}(h\sigma)^{-1}Y(h\tau) &= (h\sigma)^{-1}\left(\sum_{g \in G}(g\sigma)^{-1}X(g\tau)\right)(h\tau)\\ &= \sum_{g\in G}(h\sigma)^{-1}(g\sigma)^{-1}X(g\tau)(h\tau)\\ &= \sum_{g\in G}(gh)^{-1}\sigma X(gh)\tau\\ &= \sum_{g\in G}(g\sigma)^{-1}X(g\tau)\end{aligned}$$

with the last line following because for fixed $h \in G$, $\{gh \mid g \in G\} = G$. □

Corollary 23 *If $\sigma = \tau$ then $Y = \lambda I_n$.*

Proof. If $\sigma = \tau$ then Lemma 22 means that Y has the property $Y = (g\sigma)^{-1}Y(g\sigma)$ and so obeys the criteria of Schur's Lemma. Therefore $Y = \lambda I_n$ for some $\lambda \in \mathbb{C}$. □

Furthermore, since $\operatorname{tr} B^{-1}AB = \operatorname{tr} A$ for matrices A and B, in the above $\operatorname{tr} Y = |G| \operatorname{tr} X$ and thus $\lambda = \frac{|G|}{n} \operatorname{tr} X$.

Making particular choices for X yields results about G. These will be of use later.

Lemma 24 *Let $g\sigma = [a_{rs}(g)]$ and X_i have a single 1 in the ith diagonal position, and zero elsewhere. If Y_i is formed as in Equation (21) then*

$$(Y_i)_{pq} = \sum_{g\in G} a_{pi}(g^{-1})a_{iq}(g) = \begin{cases} 0 & \text{if } p \neq q \\ \frac{|G|}{n} & \text{if } p = q \end{cases}$$

Proof. With notation as described,

$$Y_i = \sum_{g\in G} [a_{rs}(g^{-1})] X_i [a_{rs}(g)]$$

with a little thought, this gives

$$(Y_i)_{pq} = \sum_{g\in G} \sum_{t=1}^{n} \left(\sum_{s=1}^{n} a_{ps}(g^{-1})(X_i)_{st} \right) a_{tq}(g) \tag{25}$$

But $(X_i)_{st} = 1$ only when $s = t = i$ and is zero otherwise, thus Equation (25) simplifies to

$$(Y_i)_{pq} = \sum_{g\in G} a_{pi}(g^{-1})a_{iq}(g)$$

But $Y_i = \frac{|G|}{n} I_n$ and hence the result. □

Lemma 26 *Let $g\sigma = [a_{rs}(g)]$ and X_{ij} have a single 1 in the (i, j) position ($i \neq j$) and zeros elsewhere. If Y_{ij} is formed as in Equation (21) then $Y_{ij} = [0]$, the null matrix and the pq entry is given by*

$$(Y_{ij})_{pq} = \sum_{g\in G} a_{pi}(g^{-1})a_{jq}(g)$$

Proof. By Corollary 23 Y_{ij} is a scalar matrix. Also, Y_{ij} must have the same trace as X_{ij}, which is 0. Hence Y_{ij} must be the null matrix. Now,

$$(Y_{ij})_{pq} = \sum_{g\in G} \sum_{t=1}^{n} \left(\sum_{s=1}^{n} a_{ps}(g^{-1})(X_{ij})_{st} \right) a_{tq}(g)$$

and $(X_{ij})_{st} = 1$ precisely when $s = i$ and $t = j$ giving

$$(Y_{ij})_{pq} = \sum_{g\in G} a_{pi}(g^{-1})a_{jq}(g)$$

□

Corollary 27 $\sum_{g\in G} a_{ii}(g^{-1})a_{jj}(g) = \frac{|G|}{n}\delta_{ij}$

Proof. Put $p = i$ and $q = j$

- For $i = j$, Lemma 24 shows the given sum to have value $\frac{|G|}{n}$.
- For $i \neq j$, Lemma 26 shows the given sum to have value 0.

Hence the result. □

(36.1.6) Characters

Definition 28 *Let V be the $\mathbb{C}G$-module associated with the representation $\sigma\colon G \to \mathrm{GL}\,(,V)$. The character of the representation σ, χ_V, is a function*

$$\chi_V : G \to \mathbb{C} \quad \textit{defined by} \quad \chi_V : g \mapsto \operatorname{tr} g\sigma$$

Noting that $\operatorname{tr} B^{-1}AB = \operatorname{tr} A$ reveals that χ_V is independent of basis, and that conjugate elements of G have the same character: χ is a "class function".

Theorem 29 (Test For Irreducibility) *If σ (or V) is irreducible then*

$$\sum_{g\in G} \chi_V(g^{-1})\chi_V(g) = |G|$$

Proof. Calculating as in Section 36.1.5,

$$\begin{aligned}
\sum_{g\in G} \chi_V(g^{-1})\chi_V(g) &= \sum_{g\in G} \operatorname{tr}(g^{-1}\sigma)\operatorname{tr} g\sigma \\
&= \sum_{g\in G}\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ii}(g^{-1})a_{jj}(g) \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{g\in G} a_{ii}(g^{-1})a_{jj}(g) \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n} \frac{|G|}{n}\delta_{ij} \quad \text{(by Corollary 27)} \\
&= |G|
\end{aligned}$$

□

This sum may be generalised to $\sum_{g\in G} \chi_V(g^{-1})\chi_W(g)$ for non-isomorphic $\mathbb{C}G$-modules V and W (whose associated representations are not equivalent).

Theorem 30 *If $V \ncong W$ are irreducible $\mathbb{C}G$-modules for a finite group G then*

$$\sum_{g\in G} \chi_V(G^{-1})\chi_W(g) = 0$$

Proof. By a general vector space argument, let $\sigma\colon G \to \mathrm{GL}\,(,V)$ and $\tau\colon G \to \mathrm{GL}\,(,W)$ are irreducible and not equivalent.

$$\mathrm{Hom}_{\mathbb{C}G}(V,W) = \{\phi \in \mathrm{Hom}_{\mathbb{C}}(V,W) \mid (\mathbf{v}g)\phi = (\mathbf{v}\phi)g \quad \forall \mathbf{v} \in V\ \forall g \in G\}$$

Let $\psi \in \mathrm{Hom}_{\mathbb{C}G}(V,W)$ then

- $\operatorname{Im}\psi$ is a submodule of W since certainly it is a subspace and, furthermore, if $\mathbf{w} = \mathbf{v}\psi$ then $\mathbf{w}g = (\mathbf{v}\psi)g = (\mathbf{v}g)\psi \in \operatorname{Im}\phi$.
- $\ker\psi$ is a submodule of V since certainly it is a subspace and, furthermore, if $\mathbf{v}\psi = \mathbf{0}$ then $(\mathbf{v}g)\psi = (\mathbf{v}\psi)g = \mathbf{0}g = \mathbf{0}$.

As V and W are irreducible, the only submodules are the improper and trivial ones.

- If $\operatorname{Im}\psi = W$ then $\ker\psi = \{\mathbf{0}\}$ and ψ is an isomorphism. But $V \ncong W$ and so this cannot be the case.
- If $\operatorname{Im}\psi = \{\mathbf{0}\}$ then $\ker\psi = V$ and ψ is the zero map.

Hence $\mathrm{Hom}_{\mathbb{C}G}(V, W) = \{0\}$. Letting V have dimension n and W have dimension m and choosing bases, $\mathrm{Hom}_{\mathbb{C}G}(\mathbb{C}^n, \mathbb{C}^m)$ consists only of the zero matrix. Let $g\sigma = (a_{ij}(g))$ and $g\tau = (b_{ij}(g))$ then for any $n \times m$ matrix X

$$\sum_{g \in G} (g\sigma)^{-1} X (g\tau) \in \mathrm{Hom}_{\mathbb{C}G}(\mathbb{C}^n, \mathbb{C}^m)$$

but this consists only of (0). Using X_{ij} as in Lemma 26 this yields

$$\begin{aligned}
\sum_{g \in G} a_{pi}(g^{-1}) b_{jq}(g) &= 0 \quad \forall i, j, p, q \\
\text{in particular } \sum_{g \in G} a_{ii}(g^{-1}) b_{jj}(g) &= 0 \\
&= \sum_{g \in G} \operatorname{tr}(g\sigma^{-1}) \operatorname{tr} g\tau \\
&= \sum_{g \in G} \chi_V(g^{-1}) \chi_W(g)
\end{aligned}$$ □

Thus the following result holds

$$\sum_{g \in G} \chi_V(g^{-1}) \chi_W(G) = \begin{cases} |G| & \text{if } V \cong W \\ 0 & \text{if } V \ncong W \end{cases} \tag{31}$$

It has already been noted that character is independent of basis by the property of traces that $\operatorname{tr} B^{-1}AB = \operatorname{tr} A$. Also by this relation, equivalent representations give rise to the same trace function.

Theorem 32 *There are at most m non-isomorphic irreducible $\mathbb{C}G$-modules, where G has m conjugacy classes.*

Proof. Let $G^{\mathbb{C}}$ be the vector space of functions $f\colon G \to \mathbb{C}$, then $G^{\mathbb{C}}$ is a $|G|$-dimensional vector space over $\mathbb{C}$ as, for example, a basis is

$$\{f_g \mid f_g(x) = 1 \iff x = g\}$$

This can be made into an inner product space by defining

$$\langle f_1, f_2 \rangle = \sum_{g \in G} f_1(g^{-1}) f_2(g)$$

Consider the subspace of class functions, i.e. those functions which are constant on the conjugacy classes of G. This subspace includes all the characters of G and if G has m conjugacy classes with representatives $x_1, x_2, \dots, x_m$ then it has basis

$$\{f_{x_i} \mid 1 \leqslant i \leqslant m\}$$

and thus is of dimension m. Now, all the irreducible characters of G are in the subspace of class functions, and for any two irreducible characters of non-isomorphic $\mathbb{C}G$-modules V and W, equation (31) gives $\langle \chi_V, \chi_W \rangle = 0$. But as this is in a space of dimension m there can be at most m different isomorphism types of $\mathbb{C}G$-module. □

Lemma 33 *Let $\{V_1, V_2, \dots, V_n\}$ be a full set of non-isomorphic irreducible $\mathbb{C}G$-modules with corresponding characters χ_i. If V is any $\mathbb{C}G$-module then where for $n \in \mathbb{N}$, $nV = \bigoplus_{i=1}^n V$,*

$$\begin{aligned}
V &= m_1 V_1 \oplus m_2 V_2 \oplus \cdots \oplus m_n V_n \\
\text{and } \chi_V &= m_1 \chi_1 + m_2 \chi_2 + \dots m_n \chi_n && (34) \\
\text{where } m_i &= \frac{1}{|G|} \sum_{g \in G} \chi_V(g^{-1}) \chi_i(g) && (35)
\end{aligned}$$

Proof. That V can be written as a direct sum of irreducible $\mathbb{C}G$-modules has already been shown in Theorem 19. Choose a basis for V by choosing a basis for V_1, extending to a basis of $V_1 \oplus V_1$ etc. will make the matrix of $g\sigma$ blockwise diagonal with ith block $g\sigma_i$. Hence Equation 34.

Now, to find the multiplicities, simply observe that

$$\begin{aligned}
\frac{1}{|G|}\sum_{g\in G}\chi_V(g^{-1})\chi_i(g) &= \frac{1}{|G|}\sum_{g\in G}\sum_{j=1}^{n} m_j\chi_j(g^{-1})\chi_i(g)\\
&= \frac{1}{|G|}\sum_{j=1}^{n} m_j\sum_{g\in G}\chi_j(g^{-1})\chi_i(g)\\
&= \frac{1}{|G|}\sum_{j=1}^{n} m_j\delta_{ij}\\
&= m_i
\end{aligned}$$

□

Theorem 36 *Let V and W be finite-dimensional $\mathbb{C}G$-modules for a finite group G. V and W are isomorphic if and only if they have the same character, i.e. $\chi_V = \chi_W$.*

Proof. ($\Rightarrow$) Let V and W be isomorphic and $\sigma\colon G \to \mathrm{GL}\,(,V)$ and $\tau\colon G \to \mathrm{GL}\,(,W)$ be representations. As V and W are isomorphic there exist bases $\mathcal{B}_V$ of V and $\mathcal{B}_W$ of W and an invertible matrix T such that

$$T^{-1}[g\sigma]_{\mathcal{B}_V}T = [g\tau]_{\mathcal{B}_W}$$

in which case $\operatorname{tr} g\sigma = \operatorname{tr} g\tau$ for all $g \in G$ meaning that V and W have the same character.

($\Leftarrow$) Let V and W be $\mathbb{C}G$-modules and $\chi_V = \chi_W$. Then by Lemma 33, χ_V determines the decomposition of V into irreducible modules, and ditto χ_W. But as the characters are equal the decompositions must be the same and thus $V \cong W$. □

This quite remarkable result shows that the traces of the matrices of a representation completely determines the isomorphism-type of its associated $\mathbb{C}G$-module.

Definition 37 *Let χ be the character of an irreducible $\mathbb{C}G$-module V. The degree of χ is the dimension of V.*

Note that for the representation σ, $1_G\sigma$ must be the identity, and so $\dim V = \chi(1_G)$.

Of particular interest is the regular representation: where V is the complex group algebra $\mathbb{C}G$. Defining the action of $\rho\colon G \to \mathrm{GL}\,(,\mathbb{C}G)$ as right multiplication by g so that

$$g \mapsto \sigma \quad \text{where} \quad \sigma\colon \mathbf{v} \mapsto \mathbf{v}g$$

then ρ acts to permute the elements of the basis of $\mathbb{C}G$. Thus when $\mathbf{v} \in \mathbb{C}G$,

$$\mathbf{v} = \sum_{x\in G}\lambda_x x \quad (\lambda_x \in \mathbb{C})$$

Now, multiplication by g causes a permutation of the basis, so when

$$\mathbf{v} = (\lambda_{x_1}, \lambda_{x_2}, \ldots, \lambda_{x_n})$$

the matrix for $g\rho$ is a permutation matrix. If $g = 1_G$ it is clear that $\operatorname{tr} g\rho = |G|$. If $g \neq 1_G$ then each element of G is sent to a *different* element (for if $gh = g$ then $h = 1_G$) and thus $\operatorname{tr} g\rho = 0$. That is

$$\chi_{\mathbb{C}G}(g) = \begin{cases} |G| & \text{if } g = 1_G \\ 0 & \text{otherwise} \end{cases}$$

Hence for the irreducible characters χ_i

$$\langle \chi_{\mathbb{C}G}, \chi_i \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_{\mathbb{C}G}(g^{-1})\chi_i(g) = \chi_i(1_g)$$

But now by Theorem **??** and Theorem 19

$$\mathbb{C}G = \bigoplus_{i=1}^{n} \chi_i(1_G) V_i$$

But $\chi_i(1_G) = \dim V_i$ (because for any representation σ, $1_g\sigma$ must be the identity matrix) and so

$$\dim \mathbb{C}G = |G| = \sum_{i=1}^{n} (\chi_i(1_G))^2 \tag{38}$$

(36.1.7) The Dual Representation

Definition 39 *Let $\sigma\colon G \to \mathrm{GL}(n, \mathbb{C})$ be a representation, then define the dual representation to be $\tau\colon G \to \mathrm{GL}(n, \mathbb{C})$ given by $g\tau = ((g\sigma)^{-1})^{\top}$.*

Let W be the $\mathbb{C}G$-module associated with a dual representation τ of a representation σ. Then

$$\chi_W(g) = \operatorname{tr}((g\sigma)^{-1})^{\top} = \operatorname{tr}(g\sigma)^{-1} = \chi_V(g^{-1})$$

where σ has $\mathbb{C}G$-module V. Now, $\chi_V(g)$ is the sum of the eigenvalues of $g\sigma$

Lemma 40 *Let G be a finite group and V be a $\mathbb{C}G$-module. For $g \in G$ of order n there is a basis $\mathcal{B}$ of V such that $[g]_{\mathcal{B}}$ is diagonal with entries the nth roots of unity.*

Proof. Since $g^n = 1$, $(g\sigma)^n = I$. But if λ is an eigenvalue of a matrix A then λ^r is an eigenvalue of A^r. The eigenvalues of I are just 1, so the eigenvalues of $g\sigma$ must be the nth roots of unity.

********* □

Theorem 41 *Let $\sigma\colon G \to \mathrm{GL}(n, \mathbb{C})$ be a representation, and $\tau\colon G \to \mathrm{GL}(n, \mathbb{C})$ be the dual representation. If V, W are the associated $\mathbb{C}G$-modules for σ, τ respectively then $\chi_W(g) = \overline{\chi_V(g)}$.*

Proof. If λ is an eigenvalue of $g\sigma$, then $(g\sigma)\mathbf{v} = \lambda\mathbf{v}$ so that $\frac{1}{\lambda}\mathbf{v} = (g\sigma)^{-1}\mathbf{v}$. Thus $\frac{1}{\lambda}$ is an eigenvalue of $(g\sigma)^{-1}$. But the eigenvalues of $g\sigma$ and $(g\sigma)^{\top}$ are the same, so since $g\tau = ((g\sigma)^{\top})^{-1}$, $g\tau$ must have the reciprocal eigenvalues to $g\sigma$. By Lemma 40 $\chi_V(g)$ is the sum of the nth roots of unity, and these are the eigenvalues of $g\sigma$. But for roots of unity the reciprocals are the complex conjugates, and since the conjugate of a sum is the sum of conjugates, $\chi_V(g) = \overline{\chi_W(g)}$. □

Corollary 42 $\chi_V(g^{-1}) = \overline{\chi_V(g)}$.

Proof. Observe that $g^{-1}\sigma = (g\sigma)^{-1}$ then apply Theorem 41. □

Note that if χ is an irreducible character then so is $\overline{\chi}$:

$$\begin{aligned}
\chi \text{ irreducible } &\Leftrightarrow \sum_{g\in G} \chi(g^{-1})\chi(g) = |G| \\
&\Leftrightarrow \sum_{g\in G} \overline{\chi(g)}\chi(g) = |G| \\
&\Leftrightarrow \sum_{g\in G} \overline{\overline{\chi(g)}\chi(g)} = |G| \\
&\Leftrightarrow \overline{\chi} \text{ irreducible}
\end{aligned}$$

(36.2) The Centre Of The Group Algebra

(36.2.1) Basis Of Class Sums

Consider the centre of the group algebra,

$$\begin{aligned}
Z(\mathbb{C}G) &= \{a \in \mathbb{C}G \mid ba = ab\ \forall b \in \mathbb{C}G\} \\
&= \{a \in \mathbb{C}G \mid ag = ga\ \forall g \in G\} \\
&= \{a \in \mathbb{C}G \mid g^{-1}ag\ \forall g \in G\}
\end{aligned}$$

Now, let $a \in \mathbb{C}G$ then

$$a = \sum_{x\in G} \alpha_x x \quad \text{and} \quad g^{-1}ag = \sum_{x\in G} \alpha_x g^{-1}xg$$

thus $a \in Z(\mathbb{C}G)$ if and only if $\alpha_x = \alpha_{g^{-1}xg}$ i.e. conjugate elements have the same coefficient. Thus if $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_r$ are the conjugacy classes of G, and $a \in Z(\mathbb{C}G)$ then

$$a = \sum_{i=1}^{r} \alpha_i \sum_{x\in\mathcal{C}_i} x$$

Hence the class sums $C_i = \sum_{x\in\mathcal{C}_i} x$ is a basis for $Z(\mathbb{C}G)$, which must therefore have dimension equal to the number of conjugacy classes of G.

(36.2.2) Basis Of Idempotents

Note that an idempotent element x has the property $x^2 = x$ while a nilpotent element has $x^n = 0$ for some $n \in \mathbb{N}$.

The aim of this section is to find a basis for the centre of the group algebra, this time consisting of idempotent elements. First of all, a general method is exhibited for finding such a basis.

Theorem 43 *Let A be a finite dimensional commutative algebra with a 1 over $\mathbb{C}$ and of dimension m. If A contains no non-zero nilpotent elements then*

$$A = A_1 \oplus A_2 \oplus \cdots \oplus A_m$$

for 1-dimensional algebras A_i with $a_i a_j = 0$ for all $a_i \in A_i$ and $a_j \in A_j$ when $i \neq j$.

Proof. Suppose $0 \neq e \in A$ and $e^2 = e$ i.e. e is idempotent. Now,

$$\begin{aligned}
ea_1 + ea_2 &= e(a_1 + a_2) & \qquad (ea_1)(ea_2) &= e^2(a_1a_2) \\
&\in A & &= e(a_1a_2) \in A
\end{aligned}$$

So eA is a subalgebra of A. Observing that $(1-e)^2 = 1-e$ so $1-e$ is also idempotent shows that $(1-e)A$ is also a subalgebra of A. Now, for any $a \in A$,

$$a = 1_A a = ea + (1-a)a \in eA \oplus (1-e)A$$

Further,

$$\begin{aligned} ea_1 &= (1-e)a_2 \\ \Rightarrow\ e^2 a_1 &= e(1-e)a_2 \\ \Rightarrow\ ea &= 0 \end{aligned} \qquad \begin{aligned} (ea_1)((1-e)a_2) &= e(1-e)a_1 a_2 \\ &= (e^2-e)a_1 a_2 \\ &= 0 \end{aligned}$$

so $(eA) \cap ((q-e)A) = \{0\}$ and $(eA)((1-e)A) = \{0\}$. Thus $A = eA \oplus (1-e)A$.

Now, if $A = X \oplus Y$ (with $xy = 0$ for all $x \in X$, $y \in Y$) then using induction on the dimension of A gives the required result. Thus assume that A cannot be written as a direct sum of subalgebras, then the above gives $e = 1$. To complete the proof it must be shown that $\dim_{\mathbb{C}} A = 1$.

For $b \in A$ consider

$$T_b \colon A \to A \quad \text{defined by} \quad T_b \colon a \mapsto ab$$

Let T_b have minimum polynomial

$$p(x) = \prod_{i=1}^{r} (x - \lambda_i)^{m_i}$$

then $p(T_b) = \prod_{i=1}^{r} (b - \lambda_i 1_A)^{m_i} = 0$ and is the polynomial of least degree with this property. (Note that using p in both occasions is a slight abuse of notation.) Thus $p(x) = 0 \Leftrightarrow p(b) = 0$. Now,

$$\prod_{i=1}^{r} (b - \lambda_i 1_A)^{m_i} = 0 \Rightarrow \left(\prod_{i=1}^{r} (b - \lambda_i 1_A) \right)^{\max_i m_i} = 0 \Rightarrow \prod_{i=1}^{r} (b - \lambda_i 1_A) = 0$$

because there are no nilpotent elements in A. As this is formed from the minimum polynomial r is minimal, so let

$$B_r = (b - \lambda_1 1_A)(b - \lambda_2 1_A) \dots (b - \lambda_{r-1} 1_A)$$

then by the minimality of r, $B_r \neq 0$. But $(b - \lambda_r 1_A) B_r = 0$. Note that cancellation cannot be used to deduce that $(b - \lambda_r 1_A) = 0$ because A is an algebra, not a field. Expanding this,

$$bB_r = \lambda_r B_r \tag{44}$$

Using this

$$\begin{aligned} B_r^2 &= (b - \lambda_1 1_A)(b - \lambda_2 1_A) \dots (b - \lambda_{r-1} 1_A) B_r \\ &= (b - \lambda_1 1_A)(b - \lambda_2 1_A) \dots (\lambda_r 1_A - \lambda_{r-1} 1_A) B_r \quad \text{by euquation (44)} \\ &\vdots \\ &= (\lambda_r 1_A - \lambda_1 1_A)(\lambda_r 1_A - \lambda_2 1_A) \dots (\lambda_r 1_A - \lambda_{r-1} 1_A) B_r \end{aligned}$$

Thus $B_r^2 = \mu_r B_r$ for some $\mu_r \in \mathbb{C}$. Thus $\frac{1}{\mu_r} B_r$ is idempotent and so must be equal to 1_A (from earlier). But $B_r(b - \lambda_r 1_A) = 0$ and therefore $b = \lambda_r 1_A$. As this holds for any $b \in A$, 1_A spans A, i.e. A is 1-dimensional.□

Corollary 45 *The algebra A has a basis of idempotent elements.*

Proof. Write $A = A_1 \oplus A_2 \oplus \cdots \oplus A_m$ where A_i is an algebra of dimension 1. Then

$$1_A = e_1 + e_2 + \cdots + e_m$$
$$1_A e_i = e_i^2$$

with the second line following because for a direct sum of algebras $e_i e_j = 0$ for $i \neq j$. But $1_A e_i = e_i$ and so A has a basis of idempotents,

$$\{e_1, e_2, \ldots, e_m\}$$ □

Having completed the general theory, it can now be applied to the centre of the group algebra.

Lemma 46 *For $a \in \mathbb{C}G$, let*

$$t \colon \mathbb{C}G \to \mathbb{C} \quad \textit{defined by} \quad t\left(\sum_{g \in G} \alpha_g g\right) = \alpha_{1_G}$$

Then $t(\alpha x) = 0$ for all $x \in G$ if and only if $a = 0$.

Proof. ($\Rightarrow$) Write $a = \sum_{y \in G} \alpha_y y$. But for each $y \in G$, $t(ay^{-1}) = 0$ and the coefficient of 1_G in ay^{-1} is the coefficient α_y of y in a. Thus $\alpha_y = 0$ for all $y \in G$, i.e. $a = 0$.

($\Leftarrow$) Obvious. □

Corollary 47 *$Z(\mathbb{C}G)$ contains no non-zero nilpotent elements.*

Proof. Suppose that $0 \neq z \in Z(\mathbb{C}G)$ and z is nilpotent so that $z^r = 0$ for some r. Hence

$$(zg)^n = z^n g^n = 0 g^n = 0$$

and so zg is nilpotent for all $g \in G$.
Hence where ρ is the regular representation, $\operatorname{tr}(zg)\rho = 0$ for all $g \in G$.
Hence $t(zg) = 0$ for all $g \in G$ and so by the preceding Lemma $z = 0$. Thus $Z(\mathbb{C}G)$ contains no nilpotent elements other than 0. □

Thus by Theorem 43 $Z(\mathbb{C}G)$ has a basis of idempotents.

(36.2.3) Number Of Irreducible Submodules

It has already been seen that there are at most m irreducible $\mathbb{C}G$-submodules where G has m conjugacy classes. The previous section provides the tools to show that there are also at least m.

Theorem 48 *There are at least m distinct non-isomorphic irreducible $\mathbb{C}G$-modules, where m is the number of conjugacy classes of G.*

Proof. Let $\{e_1, e_2, \ldots, e_,\}$ be a basis of idempotents for $Z = Z(\mathbb{C}G)$ with $1_{\mathbb{C}G} = e_1 + e_2 + \cdots + e_m$. Let V be an irreducible $\mathbb{C}G$-module, then $\mathbf{v}1_Z = \mathbf{v}$ for all $\mathbf{v} \in V$. Therefore $\exists i$ such that $\mathbf{v}e_i \neq \mathbf{0}$, so that $Ve_i \neq \{\mathbf{0}\}$. But $e_i \in Z$ so Ve_i is a submodule of V, and as is is not the trivial submodule, it must be the improper submodule, so $Ve_i = V$. Thus for each $\mathbf{v} \in V$, $\mathbf{v} = \mathbf{u}e_i$ for some $\mathbf{u} \in V$. But

$$\mathbf{v}e_i = (\mathbf{u}e_i)e_i = \mathbf{u}e_i^2 = \mathbf{u}e_i = \mathbf{v}$$

and so e_i acts like the identity on V. Similarly, for $j \neq i$, e_j acts like the zero on V.

As $\mathbb{C}G$ is itself a $\mathbb{C}G$-module, $\mathbb{C}Ge_i$ is a $\mathbb{C}G$-submodule for each i. Thus $\mathbb{C}Ge_i$ can be expressed as a direct sum of irreducible submodules, and so $\mathbb{C}Ge_i$ contains at least 1 irreducible submodule, V_i say. From above e_i acts like the identity on V_i and for any $j \neq i$, e_j acts like the zero.

But this can be done for each $1 \leqslant i \leqslant m$. For $i \neq j$ suppose that $V_i \cong V_j$. Then e_i acts like the identity on V_i but like the zero on V_j: a contradiction as any isomorphism must preserve the relationship of elements with all other elements. Thus there must be at least m non-isomorphic $\mathbb{C}G$-modules. □

Corollary 49 *$\mathbb{C}G$ has at exactly m non-isomorphic irreducible modules.*

Proof. By Theorem 32 there are at most m non-isomorphic irreducible $\mathbb{C}G$-modules, and by Theorem 48 there are at most that many. □

Further, if $\chi_1, \chi_2, \ldots, \chi_m$ are the characters of the m irreducible $\mathbb{C}G$-modules then

$$\frac{1}{|G|} \sum_{g \in G} \chi_i(g^{-1}) \chi_j(g) = \delta_{ij}$$

Also, if F is the complex vector space of class functions of G to $\mathbb{C}$, i.e. functions that are constant on the conjugacy classes of G, then F is of dimension m and F has an inner product

$$\langle f_1, f_2 \rangle = \frac{1}{|G|} \sum_{g \in G} f_1(g) f_2(g^{-1})$$

Hence the irreducible characters form an orthonormal basis of F.

Corollary 50 *Let $\theta \colon G \to \mathbb{C}$ be a class function, then θ has a unique expression of the form $\theta = \sum_{i=1}^{m} a_i \chi_i$ where $a_i = \langle \theta, \chi_i \rangle$. Furthermore, θ is a character of G if and only if $\langle \theta, \chi_i \rangle \in \mathbb{Z}_0^+$ for all i.*

(36.2.4) Changing Basis

Having found a basis of class sums and a basis of idempotents, it is of interest as to how to change between them. In particular two very useful orthogonality relations can be deduced in the process.

Theorem 51 $C_i = \displaystyle\sum_{j=1}^{m} \frac{[G : C_G(x_i)] \chi_j(x_i)}{\chi_j(1)} e_j$ *where $x_i \in \mathcal{C}_i$.*

Proof. Write $C_i = \sum_{j=1}^{m} \lambda_{ij} e_j$ then the task is to find the λ_{ij}. Let $V_1, V_2, \ldots, V_m$ be the irreducible $\mathbb{C}G$-submodules with corresponding characters $\chi_1, \chi_2, \ldots, \chi_m$. e_i acts like 1 on V_i and 0 on V_j $(i \neq j)$ so

$$\chi_i(e_i) = \chi_i(1) \qquad \chi_j(e_i) = 0$$

To find an expression for λ_{ik} consider $e_k C_i$, then

$$e_k C_i = C_i e_k = \sum_{j=1}^{m} \lambda_{ij} e_j e_k = \lambda_{ik} e_k$$

As e_k acts like 1 on V_k, $e_k C_i$ acts like C_i. Thus

$$\chi_k(C_i) = \chi_k(C_i e_k) = \chi_k(\lambda_{ik} e_k) = \lambda_{ik} \chi_k(e_k) = \lambda_{ik} \chi_k(1)$$

Choose $x_i \in \mathcal{C}_i$ then when $\sigma_k \colon G \to \mathrm{End}_{\mathbb{C}}(V_k)$ is a representation

$$\begin{aligned}\chi_k(C_i) &= \mathrm{tr}\left(\sum_{g\in G} g^{-1}x_i g\right)\sigma_k \\ &= [G : C_G(x_i)]\chi_k(x_i) \\ \text{hence} \quad \lambda_{ik} &= \frac{[G : C_G(x_i)]\chi_k(x_i)}{\chi_k(1)}\end{aligned}$$

and hence the result. $\square$

Theorem 52 $e_i = \sum_{j=1}^{m} \frac{\chi_i(1)\chi_i(x_j^{-1})}{|G|} C_j$ *where* $x_j \in \mathcal{C}_j$.

Proof. Let $\chi_{\mathbb{C}G}$ be the character of the regular representation, then for a chosen class sum C_k

$$\chi_{\mathbb{C}G} = \begin{cases} |G| & \text{if } 1_G \in \mathcal{C}_k \\ 0 & \text{if } 1_g \notin \mathcal{C}_k \end{cases}$$

Hence

$$\begin{aligned}\chi_{\mathbb{C}G}(e_iC_k) &= |G| \times \text{coefficient of } 1_G \text{ in } e_iC_k \\ &= \frac{|G| \times \text{coefficient of } x_k^{-1} \text{ in } e_i}{[G : C_G(x_k)]}\end{aligned} \tag{53}$$

with the last line following because C_k is a sum of $[G : C_G(x_k)]$ elements, each of which must have the same coefficient. Now, also

$$\begin{aligned}\chi_{\mathbb{C}G}(e_iC_k) &= \sum_{j=1}^{m} \chi_j(1_G)\chi_i(e_iC_k) \\ &= \chi_i(1_G)\chi_i(C_k) \\ &= [G : C_G(x_k)]\chi_i(1_G)\chi_i(x_k)\end{aligned} \tag{54}$$

Hence equating equations (53) and (54) and rearranging,

$$\text{coefficient of } x_k^{-1} \text{ in } e_i = \frac{\chi_i(1_G)\chi_i(x_k)}{|G|}$$

and so

$$e_i = \sum_{j=1}^{m} \frac{\chi_i(1_G)\chi_i(x_j^{-1})}{|G|} C_j$$

$\square$

Two very useful orthogonality relations can now be deduced by substituting into one of the above two results using the other.

Theorem 55 (Row Orthogonality) $\frac{1}{|G|}\frac{\chi_i(1)}{\chi_k(1)}\sum_{i=1}^{m}[G : C_G(x_j)]\chi_i(x_j^{-1})\chi_k(x_j) = \delta_{ik}$

Proof. Substitute in Theorem 52 for C_j using Theorem 51 then

$$\begin{aligned} e_i &= \sum_{j=1}^{m} \frac{\chi_i(1)}{|G|} \chi_i(x_j^{-1}) \sum_{k=1}^{m} [g : C_G(x_j)] \frac{\chi_k(x_j)}{\chi_k(1)} e_k \\ &= \sum_{k=1}^{m} \left(\sum_{j=1}^{m} \frac{\chi_i(1)\chi_i(x_j^{-1})\chi_k(x_j)}{|C_G(x_j)|\chi_k(1)} \right) e_k \end{aligned}$$

But the e_i are linearly independent, hence

$$\begin{aligned} \delta_{ik} &= \sum_{j=1}^{m} \frac{\chi_i(1)\chi_i(x_j^{-1})\chi_k(x_j)}{|C_G(x_j)|\chi_k(1)} \\ &= \frac{1}{|G|} \frac{\chi_i(1)}{\chi_k(1)} \sum_{j=1}^{m} [G : C_G(x_j)] \chi_i(x_j^{-1}) \chi_k(x_j) \end{aligned}$$

□

Note that this result may be extended slightly. As any representative x_j of the conjugacy class $\mathcal{C}_j$ may be used and characters are class functions,

$$\sum_{j=1}^{m} [G : C_G(x_j)] \chi_i(x_j^{-1}) \chi_k(x_j) = \sum_{g \in G} \chi_i(g^{-1}) \chi_k(g)$$

By a similar process, another orthogonality relation can be found.

Theorem 56 (Column Orthogonality) $\displaystyle\sum_{j=1}^{m} \chi_j(g^{-1})\chi_j(h) = \begin{cases} |C_G(g)| & \text{if } g \text{ and } h \text{ are conjugate} \\ 0 & \text{otherwise} \end{cases}$

Proof. Substituting for e_j in Theorem 51 using Theorem 52 gives

$$\begin{aligned} C_i &= \sum_{j=1}^{m} \frac{[G : C_G(x_i)]\chi_j(x_i)}{\chi_j(1)} \sum_{k=1}^{m} \frac{\chi_j(1)\chi_j(x_k^{-1})}{|G|} C_k \\ &= \sum_{k=1}^{m} \left(\sum_{j=1}^{m} [G : C_G(x_j)] \frac{\chi_j(x_i)\chi_j(x_k^{-1})}{|G|} \right) \end{aligned}$$

But the C_i are linearly independent, hence

$$\delta_{ik} = \sum_{i=1}^{m} \frac{\chi_j(x_i)\chi_j(x_k^{-1})}{|C_G(x_j)|}$$

which re-arranges to give the required result. □

(36.2.5) The Feit-Higman Theorem

First of all a calculation.

$$\begin{aligned}
C_r C_s &= \left(\sum_{j=1}^{m} \frac{[G:C_G(x_r)]\chi_j(x_r)}{\chi_j(1)} e_j\right)\left(\sum_{k=1}^{m} \frac{[G:C_G(x_s)]\chi_k(x_s)}{\chi_k(1)} e_k\right)\\
&= \sum_{i=1}^{m} \frac{[G:C_G(x_r)]\chi_i(x_r)[G:C_G(x_s)]\chi_i(x_r)}{(\chi_i(1))^2} e_i\\
&= \sum_{i=1}^{m} \frac{[G:C_G(x_r)]\chi_i(x_r)[G:C_G(x_s)]\chi_i(x_r)}{(\chi_i(1))^2} \sum_{j=1}^{m} \frac{\chi_i(1)\chi_i(x_j^{-1})}{|G|} C_j\\
&= \sum_{j=1}^{m}\left(\sum_{i=1}^{m} \frac{[G:C_G(x_r)]\chi_i(x_r)[G:C_G(x_s)]\chi_i(x_r)\chi_i(x_j^{-1})}{|G|\chi_i(1)}\right) C_j
\end{aligned}$$

So the coefficient of C_j in $C_r C_s$ is

$$\frac{|G|}{|C_G(x_r)||C_G(x_s)|} \sum_{i=1}^{m} \frac{\chi_i(x_r)\chi_i(x_s)\chi_i(x_j^{-1})}{\chi_i(1)} \tag{57}$$

Note that this can be computed if the character table is known.

Theorem 58 (Feit-Higman) *Let G be a finite simple group containing an element t of order 2 and such that $|C_G(t)| = 4$. Then $G \cong A_5$.*

Proof. Let $1 = \chi_1, \chi_2, \ldots, \chi_m$ be the complex irreducible characters of G. so by Theorem 56 (column orthogonality)

$$1 + \sum_{i=2}^{m} (\chi_i(t))^2 = |C_G(t)| = 4$$

Hence without loss of generality

$$\chi_i(t) = \begin{cases} \pm 1 & \text{for } 2 \leqslant i \leqslant 4 \\ 0 & \text{for } i \geqslant 5 \end{cases}$$

Thus the following fragment of the character table has been deduced (where $\varepsilon_i = \pm 1$).

	1	t
χ_1	1	1
χ_2	x	ε_2
χ_3	y	ε_3
χ_4	z	ε_4
$\vdots$	$\vdots$	0

for $x, y, z \in \mathbb{N}$. Furthermore, by Theorem 56 (column orthogonality) again,

$$0 = \sum_{i=1}^{m} \chi_i(1)\chi_i(t) = 1 + x\varepsilon_2 + y\varepsilon_3 + z\varepsilon_4$$

which shows that the ε_i are not all of the same sign. Thus choose $\varepsilon_2 = 1$ and $\varepsilon_3 = -1$.

It can be shown that if t is an involution (*i.e.*, of order 2) then $\chi(1) - \chi(t) \equiv 0 \mod 4$. Using this:

$$x \equiv 1 \mod 4 \qquad y \equiv -1 \mod 4 \qquad z \equiv \varepsilon_4 \mod 4 \qquad \chi_i(1) \equiv 0 \mod 4 \; i \geqslant 5$$

Now, G is not of order 4 since neither $\mathbb{Z}_4$ nor V_4 (the 2 groups of order 4) is simple. Thus $C_G(t)$ is a proper subgroup of G. As G is simple $C_G(t) \ntrianglelefteq G$ and therefore G is not abelian because all subgroups of abelian groups are normal.

Let χ_i have associated representation $\sigma_i\colon G \to \mathrm{GL}(n, \mathbb{C})$. Suppose that $i > 1$ so that σ_i is not the trivial representation, then if $n = 1$ the Homomorphism Theorem gives $G \cong \operatorname{Im}\sigma_i \leqslant \mathbb{C}$. But $\mathbb{C}$ is abelian and G is not, so all the non-trivial characters must have order of at least 2.

Let C_r be the class sum for the conjugacy class of t then by Equation (57) the coefficient of C_r in C_rC_r is

$$\begin{aligned}
\frac{|G|}{16}\sum_{i=1}^{m}\frac{(\chi_i(t))^3}{\chi_i(1)} &= \frac{|G|}{16}\left(1+\frac{1}{x}-\frac{1}{x}+\frac{\varepsilon_4^3}{z}\right)\\
&\geqslant \frac{|G|}{16}\left(1+\frac{1}{x}-\frac{1}{x}-\frac{1}{z}\right)\\
&> \frac{|G|}{16}\frac{1}{3} = \frac{|G|}{48}
\end{aligned} \tag{59}$$

with the last line following because $y \geqslant 3$ and $z \geqslant 3$ and x can be large without bound.

As C_r is the class sum for $\mathrm{Cl}_G(t)$ the coefficient of C_r in C_rC_r is also the coefficient of t in C_rC_r when the class sums are expanded. As the coefficient of t in C_r is 1, the coefficient of t in C_rC_r must be the number of times t appears as a product of 2 of its conjugates, $t = t_1t_2$ say. Now,

$$\begin{aligned}
t^{-1} &= t_2^{-1}t_1^{-1}\\
&= t \text{ since } t \text{ is an involution}\\
\text{but then } t^{-1} &= t_2t_1\\
&= t
\end{aligned}$$

Hence $t_1, t_2 \in C_G(t)$. Now, if either of t_1 and t_2 are in fact t, then the other is 1_G.

$\boxed{t_1 \text{ and } t_2 \text{ are involutions}}$

Hence $t_1 \neq 1_G \neq t_2$ and so $t_1 \neq t \neq t_2$ and so $t_1, t_2 \in C_G(t) \setminus \{1_G, t\}$. But $|C_G(t)| = 4$ and there are at most 2 choices for t_1 as once t_1 is chosen t_2 can be determined. Hence the coefficient of t in C_rC_r is at most 2. Hence using equation (59)

$$2 > \frac{G}{48}$$

But

$$\begin{aligned}
|G| + |C_G(t)| &\equiv 0 \mod 16\\
|G| + 4 &\equiv 0 \mod 16\\
|G| &\equiv 12 \mod 16\\
|G| &\in \{12, 28, 44, 60, 76, 92\}
\end{aligned}$$

Now, for all of these possible orders other than 60 there exists a Sylow p-subgroup for prime p. For example $12 = 3.2^2$ giving $p = 3$, and $96 = 23.2^2$ giving $p = 23$. But any such subgroup is normal, and therefore the only possibility is $|G| = 60$. $\square$

(36.3) Groups & Their Characters

(36.3.1) Algebraic Integers & Burnside's Theorem

Let $T_r\colon Z(\mathbb{C}G) \to Z(\mathbb{C}G)$ be the linear transformation of right multiplication by C_r. Now,

$$\begin{aligned} C_r &= \sum_{i=1}^{m} [G : C_G(x_r)] \frac{\chi_i(x_r)}{\chi_i(1_G)} e_i \\ \text{so } C_r e_j &= \sum_{i=1}^{m} [G : C_G(x_r)] \frac{\chi_i(x_r)}{\chi_i(1_G)} e_i e_j \\ &= [G : C_G(x_r)] \frac{\chi_j(x_r)}{\chi_j(1_G)} e_i \end{aligned}$$

hence e_j is an eigenvector of T_r with eigenvalue

$$[G : C_G(x_r)] \frac{\chi_j(x_r)}{\chi_j(1_G)} \tag{60}$$

But the eigenvalues are the solutions to the characteristic polynomial of the matrix of T_r (with respect to the basis of class sums, say) and without loss of generality this polynomial may be assumed to be monic. Thus elements (of $\mathbb{C}$) of the form of equation (60) are the roots of such polynomials.

Definition 61 *A complex number α is said to be an algebraic integer if α is a root of some monic polynomial in $\mathbb{Z}[x]$.*

By Gauss' Lemma α is an algebraic integer if and only if the minimum polynomial of α over $\mathbb{Q}$ exists and is monic in $\mathbb{Z}[x]$.

Theorem 62 *The following results are available for algebraic integers.*

1. *$\alpha \in \mathbb{C}$ is an algebraic integer if and only if $\mathbb{Z}[\alpha]$ is finitely generated.*
2. *A rational algebraic integer is an integer.*

Proof. Omitted. □

By considering algebraic integers, some properties of characters can be found.

Lemma 63 *A rational algebraic integer is an integer.*

Proof. Let $\alpha \in \mathbb{Q}$ be a rational algebraic integer and have minimum polynomial $m(x)$ over $\mathbb{Z}$. Over $\mathbb{Q}$ the minimum polynomial of α is simply $x - \alpha$ and therefore (over $\mathbb{Q}$) $m(x) = (x - \alpha)p(x)$. By Gauss' Lemma m has the same factorisation in $\mathbb{Z}[x]$, and so $m(x) = x - \alpha$ *i.e.,* $\alpha \in \mathbb{Z}$. □

Corollary 64 *If G is a finite group and χ_i is an irreducible character of G then the order of χ_i, $\chi_i(1)$, divides $|G|$.*

Proof. Observe that

$$\begin{aligned} |G| &= \sum_{j=1}^{m} [G : C_G(x_j)] \chi_i(x_j) \chi_i(x_j^{-1}) \\ \frac{|G|}{\chi_i(1_G)} &= \sum_{j=1}^{m} \underbrace{[G : C_G(x_j)] \frac{\chi_i(x_j)}{\chi_i(1_G)}}_{\text{alg. int. by eq. (60)}} \quad \underbrace{\chi_j(x_j^{-1})}_{\text{sum of roots of unity}} \end{aligned}$$

But roots of unity are algebraic integers. Hence $\frac{|G|}{\chi_i(1_G)}$ is a sum of products of algebraic integers and so is an algebraic integer. Furthermore, $\frac{|G|}{\chi_i(1_G)} \in \mathbb{Q}$ and hence by Lemma 63 $\frac{|G|}{\chi_i(1_G)} \in \mathbb{Z}$ □

Following from this, let $\sigma\colon G \to \mathrm{GL}\,(n, \mathbb{C})$ be an irreducible representation with character χ. If $g \in G$ has order m then $\chi(g)$ is a sum of n mth roots of unity and hence by the triangle inequality $|\chi(g)| \leqslant \chi(1) = n$. Equality holds if and only if $\chi(g) = \omega\chi(1)$ where ω is an mth root of unity. In this case $g\sigma = \omega I_n \in Z(\mathrm{Im}\,\sigma)$.

Theorem 65 (Burnside) *Let G be a finite simple group and let $x \in G \setminus \{1_G\}$. Then $[G : C_G(x)] = |\mathrm{Cl}_G\,(x)\,|$ is not a power of a prime.*

Proof. Suppose that $[G : C_G(x)] = p^r$.

Let $\chi_1, \chi_2, \ldots, \chi_m$ be the irreducible complex characters of G with χ_1 being the trivial character. Then by Theorem 56 (column orthogonality)

$$\begin{aligned} & 1 + \sum_{i=2}^{m} \chi_i(1_G)\chi_i(x) = 0 \\ \Rightarrow \quad & \sum_{i=2}^{m} \chi_i(1_G)\chi_i(x) = -1 \\ \Rightarrow \quad & \sum_{i=2}^{m} \frac{\chi_i(1_G)\chi_i(x)}{p} = \frac{-1}{p} \notin \mathbb{Z} \end{aligned}$$

hence $\exists i$, $2 \leqslant i \leqslant m$ such that $\frac{\chi_i(1_G)\chi_i(x)}{p}$ is not an algebraic integer. Therefore

- $p \nmid \chi_i(1_G)$.
- $\chi_i(x) \neq 0$. If it were equal to 0 then $\frac{\chi_i(1_G)\chi_i(x)}{p} = 0$ which is an algebraic integer.

Since $[G : C_G(x)] = p^r$ the highest common factor of this and $\chi_i(1_G)$ is 1, so there exists integers a and b such that

$$a[G : C_G(x)] + b\chi_i(1_G) = 1$$
$$a\frac{[G : C_G(x)]\chi_i(x)}{\chi_i(1_G)} + b\chi_i(x) = \frac{\chi_i(x)}{\chi_i(1_G)}$$

but both terms on the left hand side are algebraic integers, and therefore so is the right hand side. Let

$$M = \{m \in \mathbb{Z} \mid 1 \leqslant m \leqslant o(x), \gcd\,(m, o(x)) = 1\}$$

then for $m \in$M $\langle x \rangle = \langle x^m \rangle$ and $C_G(x) = C_G(x^m)$. Applying the same argument as above,

$$\frac{\chi_i(x^m)}{\chi_i(1_G)} \text{ is an algebraic integer } \forall m \in M$$

Now, let $i > 1$ and let σ_i be the representation that gives character χ_i. Now, $\ker \sigma_i \trianglelefteq G$ and G is simple. Since σ_i is not the trivial character this gives $G \cong G\sigma_i = \mathrm{Im}\,\sigma_i$. But then $G\sigma_i$ is simple too, and therefore its centre is trivial. Hence for no $g \in G$ is $g\sigma_i$ a scalar matrix and so by the comments preceding Theorem 65

$$|\chi_i(x)| < |\chi_i(1_G)| \;\Rightarrow\; \left|\frac{\chi_i(x)}{\chi_i(1_G)}\right| < 1 \tag{66}$$

and of course the same holds for x^m for all $m \in M$. Consider the polynomial

$$\prod_{m \in M} t - \frac{\chi_i(x^m)}{\chi_i(1_G)} \in \mathbb{C}[t] \tag{67}$$

By the above calculations all the coefficients of this polynomial are algebraic integers.

Let $s = o(x)$ and $\omega = \exp \frac{2\pi i}{s}$. $\chi_i(x)$ is a sum of powers of ω which are the eigenvalues of the matrix $x\sigma_i$. But for any matrix X, if λ is an eigenvalue of X then λ^m is an eigenvalue of X^m and hence

$$\text{if } \chi_i(x) = \omega_1 + \omega_2 + \cdots + \omega_n$$
$$\text{then } \chi_i(x^m) = \omega_1^m + \omega_2^m + \cdots + \omega_n^m$$

Now, Galois group of the field extension $\mathbb{Q}(\omega) : \mathbb{Q}$ consists of all automorphisms of the form $\tau_m : \omega \mapsto \omega^m$ where $m \in M$ and thus

$$\tau_m \left(\frac{\chi_i(x)}{\chi_i(1_G)} \right) = \frac{\chi_i(x^m)}{\chi_i(1_G)}$$

But the factors of the polynomial given in equation (67) remain the same (only re-ordered) under such automorphisms, and thus the coefficients of this polynomial are invariant under the action of this Galois group. But the Galois group has fixed field $\mathbb{Q}$ and therefore the coefficients lie in $\mathbb{Q}$. But each is a product of algebraic integers and so is an algebraic integer. Therefore all the coefficients lie in $\mathbb{A}$. In particular the constant term is

$$\pm \prod_{m \in M} \frac{\chi_i(x^m)}{\chi_i(1_G)} \in \mathbb{Z}$$

and by equation (66) each term is strictly less than 1. Therefore the whole product is less than 1, and so must be zero. Hence $\exists m \in M$ such that $\chi_i(x^m) = 0$. But then using the Galois group, $\chi_i(x^m) = 0$ for all $m \in M$. In particular $\chi_i(x) = 0$ which contradicts the choice of i. □

Corollary 68 *Let G be a finite non-Abelian group with $|G| = p^a q^b$ where $p, q \in \mathbb{Z}$ are prime and $a, b \in \mathbb{N} \cup \{0\}$. Then G is not simple, and G is solvable.*

Proof. Let $x_1, x_2, \ldots, x_n$ be representatives of the conjugacy classes of G with $x_1 = 1_G$. Suppose G is simple, then $|\mathrm{Cl}_G(x_1)| = [G : C_G(x_1)] = 1$ and so

$$|G| = 1 + \sum_{i=1}^{n} [G : C_G(x_i)] \tag{69}$$

Without loss of generality, $b > 0$ so then $q \mid |G|$ and $q \neq 1$. But then by equation (69) $\exists i$ such that $q \nmid [G : C_G(x_i)]$. But the size of each conjugacy class must divide $|G|$ (Orbit-Stabiliser Theorem) hence

$$[G : C_G(x_i)] \mid |G| \;\Rightarrow\; [G : C_G(x_i)] \mid p^a \;\Rightarrow\; [G : C_G(x_i)] \mid p^r \text{ for some } r \leqslant a$$

But this contradicts Theorem 65 and therefore G cannot be simple.

To show that G is solvable, proceed by induction on $a + b$. If $a + b \leqslant 1$ then the result follows since G is either trivial or a p-group. If $a + b \geqslant 2$ then by above G has a non-trivial proper normal subgroup H, and $|H| = p^r q^s$ where $r + s < a + b$ and therefore H is solvable with composition series

$$\{1_G\} = G_0, G_1, \ldots, G_n = H$$

say. Similarly by induction $\frac{G}{H}$ is solvable with series

$$\{1_G\} = \frac{G_n}{H}, \frac{G_{n+1}}{H}, \ldots, \frac{G_m}{H} = \frac{G}{H}$$

say. Hence

$$\{1_G\} = G_1, G_2, \ldots, G_m = H$$

is a composition series for G *i.e.,* G is solvable. □

(36.3.2) Characters Of Abelian Groups

Theorem 70 *If G is a finite Abelian group then G is isomorphic to a direct product of cyclic groups.*

Proof. Omitted. □

To this end it is useful to work out the irreducible characters of a direct product of groups.

Theorem 71 *If $G = A \times B$, $\chi_1, \chi_2, \ldots, \chi_l$ are the irreducible characters of A, and $\mu_1, \mu_2, \ldots, \mu_m$ are the irreducible characters of B then*

$$\{\chi_i \mu_j \mid 1 \leqslant i \leqslant l, 1 \leqslant j \leqslant m\}$$

are the irreducible characters of G.

Proof. First of all, observe that each χ_i may be considered as a character of G with B in its kernel. Similarly for μ_j so that the product $\chi_i\mu_j$ is

$$\chi_i\mu_j((a,b)) = \chi_i(a)\mu_j(b)$$

which is indeed a character of G. Taking the inner product of this character with itself,

$$\begin{aligned}
\frac{1}{|G|}\sum_{g\in G}|\chi_i\mu_j(g)|^2 &= \frac{1}{|A||B|}\sum_{a\in A}\sum_{b\in B}|\chi_i(a)|^2|\mu_j(b)|^2 \\
&= \left(\frac{1}{|A|}\sum_{a\in A}|\chi_i(a)|^2\right)\left(\frac{1}{|B|}\sum_{b\in B}|\mu_j(b)|^2\right) \\
&= 1
\end{aligned}$$

Also,

$$\begin{aligned}
\left\langle \chi_i\mu_j, \chi_r\mu_s \right\rangle &= \frac{1}{|G|}\sum_{g\in G}\chi_i\mu_j(g^{-1})\chi_r\mu_s(g) \\
&= \frac{1}{|A||B|}\sum_{a\in A}\sum_{b\in B}\chi_i(a^{-1})\mu_j(b^{-1})\chi_r(a)\mu_s(b) \\
&= \left(\frac{1}{|A|}\sum_{a\in A}\chi_i(a^{-1})\chi_r(a)\right)\left(\frac{1}{|B|}\sum_{b\in B}\mu_j(b^{-1})\mu_s(b)\right) \\
&= \langle \chi_i, \chi_r\rangle \left\langle \mu_j, \mu_s\right\rangle \\
&= \begin{cases} 1 & \text{if } i = r \text{ and } j = s \\ 0 & \text{otherwise} \end{cases}
\end{aligned}$$

therefore the products $\chi_i\mu_j$ give lm distinct. But since $G = A \times B$ G must have lm conjugacy classes, and therefore these are a full set of irreducible characters of G. □

Let G be a finite Abelian group, then by Theorem 70 $G \cong C_1 \times C_2 \times \ldots C_s$ where C_i is cyclic of order n_i.

Let ω_i be a primitive n_ith root of unity and let $C_i = \langle c_i \rangle$, then for $0 \leqslant j \leqslant n_i - 1$ define the character $\mu_j^{(i)}$ by

$$\mu_j^{(i)}(c_i) = \omega_i^j$$

since c_i generates C_i and the representation is 1-dimensional this extends to give a proper definition of a character, and indeed of the representation. Since C_i is Abelian each element is in a conjugacy class of its own and hence there are n_i conjugacy classes. By calculating the appropriate inner products, the n_i

characters $\mu_j^{(i)}$ are the irreducible characters of C_i. Hence by Theorem 71 the irreducible characters of G are precisely

$$\{\mu_{j_1}^{(1)}\mu_{j_2}^{(2)}\ldots\mu_{j_s}^{(s)} \mid 0 \leqslant j_1 \leqslant n_1 - 1, 0 \leqslant j_2 \leqslant n_2 - 1, \ldots, 0 \leqslant j_s \leqslant n_s - 1\}$$

(36.3.3) Frobenius' Theorem

The statement of Frobenius' Theorem is quite straight forward, indeed the result itself is easy to understand. Unfortunately the proof is a mammoth task.

Theorem 72 (Frobenius) *Let G be a finite group and $H \leqslant G$ with the property that $H \cap (g^{-1}Hg) = \{1_G\}$ for all $g \in G \setminus H$. Then there exists a normal subgroup of G, K say, such that $G = HK$ and $H \cap K = \{1_G\}$.*

Note that $K \setminus \{1_G\} = \{x \in G \mid \text{no conjugate of } x \text{ lies in } H\}$.

Proof. Let $h_1, h_2, \ldots, h_m$ be representatives of the distinct conjugacy classes of H with $h_1 = 1_G$. Let $\mu_1, \mu_2, \ldots, \mu_m$ be the irreducible characters of H with μ_1 being the trivial character. Now some preliminaries.

- Choose h_i for $2 \leqslant i \leqslant m$ and let $c \in C_G(h_i)$. Then $h_i \in H$ and $h_i = c^{-1}h_ic \in c^{-1}Hc$ and therefore $H \cap (c^{-1}Hc) \neq \{1_G\}$. Hence by hypothesis $c \in H$ and so $C_G(h_i) \subseteq H$. But the reverse inclusion holds, trivially, and thus
$$C_G(h_i) = C_H(h_i) \quad \forall h \in H \setminus \{1_G\} \tag{73}$$
- Certainly the h_i are not H-conjugate, but suppose that $\exists g \in G$ such that $h_j = g^{-1}h_ig$. Then $h_j \in H \cap (g^{-1}Hg)$ and so by hypothesis $g \in H$ which is a contradiction. Hence
$$\text{If } 2 \leqslant i, j, \leqslant m \text{ then } h_i \text{ and } h_j \text{ are not } G\text{-conjugate} \tag{74}$$
- Next the number of elements of G that aren't conjugate to any element of H other than the identity are counted. Well, clearly 1 element of G is conjugate to $1_G \in H$, namely 1_G. Consider now an element of G that is G-conjugate to a non-identity element of H. By (74) such an element must be G-conjugate to precisely one of $h_2, h_3, \ldots, h_m$, h_i say. But by (73) h_i has $[G : G_G(h_i)] = [G : G_H(h_i)]$ conjugates in G. But
$$[G : H][H : C_H(h_i)] = [G : C_H(h_i)]$$
and therefore the number of elements of G that are conjugate to a non-identity element of H is
$$\begin{aligned}[G : H]\sum_{i=2}^{m}[H : C_H(h_i)] &= [G : H]\left(-1 + \sum_{i=1}^{m}[H : C_H(h_i)]\right) \\ &= [G : H](|H| - 1) \\ &= |G| - [G : H]\end{aligned}$$
This gives
$$\begin{aligned}&\text{Exactly } [G : H] - 1 \text{ elements of } G \text{ are not conjugate to any element of } H \setminus \{1_G\}. \\ &\text{Equivalently, if } K = \{x \in G \mid x = 1_G \text{ or no conjugate of } x \text{ lies in } H\} \text{ then } |K| = [G : H]\end{aligned} \tag{75}$$

Furthermore, K has the property $K \cap H = \{1_G\}$

$\boxed{\text{and therefore } |HK| = |H||K| = |H|[G : H] = |G| \text{ and therefore } G = HK}$

It remains to be shown that $K \trianglelefteq G$. For $2 \leqslant i \leqslant m$ define the class function

$$\mu_i^*(g) = \begin{cases} \mu_i(g) & \text{if } g \text{ is } G\text{-conjugate to some } h \in H \setminus \{1_G\} \\ \mu_i(1_G) & \text{if no conjugate of } g \text{ lies in } H \text{ or if } g = 1_G \end{cases}$$

then by equation (74) this is a well defined function.

Let $\chi_1, \chi_2, \ldots, \chi_l$ be the irreducible characters of G, and define $\mu_1^* = \chi_1$. It is now shown that the μ_i^* are the irreducible characters of G.

- As the μ_i^* are class functions of G, they can be expressed as a linear combination of the characters. It is now shown that the coefficients are integers. Well,

$$\left\langle \mu_i^*, \chi_j \right\rangle = \left\langle \mu_i^* - \mu_i^*(1_G)\chi_i, \chi_j \right\rangle + \underbrace{\mu_i^*(1_G)}_{\in \mathbb{Z}} \underbrace{\left\langle \chi_1, \chi_j \right\rangle}_{=\delta_{ij}}$$

Hence it suffices to show that the first term on the right is an integer.

$$\begin{aligned} \left\langle \mu_i^* - \mu_i^*(1_G)\chi_i, \chi_j \right\rangle &= \frac{1}{|G|} \sum_{g \in G} (\mu_i^*(g) - \mu_i^*(1_G))\overline{\chi_j(g)} \qquad \text{but } \mu_i^*(g) - \mu_i^*(1_G) \text{ is zero on } K text, and so \\ &= \frac{1}{|G|} \sum_{r=2}^{k} [G : C_G(x_r)](\mu_i^*(x_r) - \mu_i^*(1_G))\overline{\chi_j(x_r)} \end{aligned}$$

where x_r is G-conjugate to an element of H and x_s is not conjugate to an element of the same G-conjugacy class of x_r for $r \neq s$.

$$\begin{aligned} &= \frac{1}{|G|} \sum_{r=2}^{k} [G : C_G(x_r)](\mu_i(x_r) - \mu_i(1_G))\overline{\chi_j(x_r)} \\ &= \frac{1}{|G|} \sum_{r=2}^{k} [G : C_H(x_r)](\mu_i(x_r) - \mu_i(1_G))\overline{\chi_j(x_r)} \qquad \text{by equation (73)} \\ &= \frac{1}{|H|} \sum_{r=2}^{k} [H : C_H(x_r)](\mu_i(x_r) - \mu_i(1_G))\overline{\chi_j(x_r)} \\ &= \frac{1}{|H|} \sum_{h \in H} (\mu_i(h) - \mu_i(1_G))\overline{\chi_j(h)} \\ &= \left\langle \mu_i - \mu_i(1_G)\mu_1, \operatorname{Res}_H^G \left(\chi_j\right) \right\rangle_H \end{aligned}$$

Now, the first term in the inner product is an integer combination of the irreducible characters of H. The second term is a character of H

$\boxed{\text{and therefore is an } \mathbb{N}\text{-combination of irreducible characters of } H.}$

Thus

$$\left\langle \mu_i - \mu_i(1_G)\mu_1, \operatorname{Res}_H^G \left(\chi_j\right) \right\rangle_H \in \mathbb{Z}$$

and hence it has been shown that

$$\mu_i^* = \sum_{j=1}^{l} z_j \chi_j \text{ where } z_j \in \mathbb{Z} \tag{76}$$

- The objective is to show that the μ_i^* are irreducible, so the following inner product is calculated.

$$\begin{aligned}
\langle \mu_i^*, \mu_i^* \rangle_G &= \frac{1}{|G|} \sum_{g \in G} |\mu_i^*(g)|^2 \\
&= \frac{1}{g} \left(\sum_{g \in K} (\mu_i(1_G))^2 + \sum_{r=2}^{k} [G : C_G(x_r)] \, |\mu_i(x_r)|^2 \right) \\
&= \frac{1}{|G|} [G : H] \, (\mu_i(1_G))^2 + \frac{1}{|G|} \sum_{r=2}^{k} [G : C_H(x_r)] \, |\mu_i(x_r)|^2 \qquad \text{by equations (73) and (75)} \\
&= \frac{1}{|H|} \, (\mu_i(1_G))^2 + \frac{1}{|H|} \sum_{r=2}^{k} [H : C_H(x_r)] \, |\mu_i(x_r)|^2 \\
&+ \frac{1}{|H|} \sum_{h \in H} |\mu_i(h)|^2 \\
&= \langle \mu_i, \mu_i \rangle_H \\
&= 1
\end{aligned}$$

Hence

$$\langle \mu_i^*, \mu_i^* \rangle_G = 1 \tag{77}$$

From equations (76) and (77)

$$\sum_{j=1}^{l} z_j^2 = 1$$

and therefore there is exactly one value of j for which $z_j^2 = 1$, and all the other z_j are zero. For this j, $\mu_i^* = \pm\chi_j$. But $\mu_i^*(1_G) > 0$ and $\chi_j(1_G) > 0$, therefore $\mu_i^* = \chi_j$. Hence the μ_i^* are the irreducible characters of G. Let

$$L = \bigcap_{i=1}^{l} \ker \mu_i^* \quad \text{where} \quad \ker \chi = \{g \in G \mid \chi(g) = \chi(1_G)\} = \ker \sigma$$

then $K \subseteq L$ since $\mu_i^*(g) = \mu_i(1_G)$ for all $g \in K$. But L is an intersection of normal subgroups of G and so $L \trianglelefteq G$.

Now, consider $h \in H \cap L$. Then since $h \in L$, $\mu_i^*(h) = \mu_i^*(1_G)$. Furthermore, since $h \in H$ this gives $\mu_i(g) = \mu_i(1_G)$ and therefore

$$\sum_{i=1}^{m} \mu_i(1_G)\mu_i(h) = \sum_{i=1}^{m} \mu_i(1_G)\mu_i(1_G) = |H| > 0$$

and thus by Theorem 56 (column orthogonality) h is conjugate to 1_G. Therefore $h = 1_G$ and so $H \cap L = \{1_G\}$. Hence

$$L \cong \frac{L}{L \cap H} \cong \frac{LH}{H} \leqslant \frac{G}{H}$$

Hence $|L| \leqslant \left|\frac{G}{H}\right| = [G : H] = |K|$ and therefore since $K \subseteq L$, $K = L \trianglelefteq G$. □

Not surprisingly, Frobenius' Theorem has a number of uses.

Example 78 *Let G be a finite group of order pq where p and q are prime. Then all Sylow p- and q-subgroups are normal.*

Proof. Solution Assume that $p > q$, let P be a Sylow p-subgroup, and let Q be a Sylow q-subgroup. Consider $N_G(Q)$. If $N_G(Q) = G$ then $Q \trianglelefteq G$ and there is nothing more to show. Assume that $N_G(Q) \neq G$. Now,

$$p = [G : Q] = [G : N_G(Q)][N_G(Q) : Q]$$

Since $N_G(Q) \neq G$, $[G : N_G(Q)] > 1$. But p is prime and therefore $[G : N_G(Q)] = p$. But then $[N_G(Q) : Q] = 1$ and so $N_G(Q) = Q$.

Now, for all $g \in G \setminus Q$, $g^{-1}Qg \neq Q$. But Q has prime order and therefore $Q \cap (g^{-1}Qg) = \{1_G\}$. Hence by Frobenius' Theorem there exists $K \trianglelefteq G$ with $K \cap Q = \{1_G\}$ and $G = KQ$. By equation (75) $|K| = [G : Q] = p$ and so K is a Sylow p-subgroup. But all Sylow p-subgroups are conjugate, and so K is the only one. □

(36.3.4) Induced Modules And Characters

Let $H \leqslant G$. From a representation of H it is possible to construct a representation of G. Let $[G : H] = n$ then the class equation for G is

$$G = Hx_1 \cup Hx_2 \cup \cdots \cup Hx_n$$

where x_i is a representative of the ith conjugacy class of H and $x_1 = 1_G$. Note that this is a disjoint union. Now, for each i and $g \in G$ there is a unique value j such that $Hx_ig = Hx_j$ *i.e.*, $x_igx_j^{-1} \in H$.

Let $\sigma\colon H \to \mathrm{GL}\,(m, \mathbb{C})$ be a representation of H. Construct the function $\tau\colon G \to \mathrm{GL}\,(mn, \mathbb{C})$ as follows. For $g \in G$ let $g\tau$ be an $n \times n$ array of $m \times m$ blocks where the (i, j) block is given by

$$(g\tau)_{ij} = (x_ig\dot{x}_j^{-1}\sigma) \begin{cases} x_igx_j^{-1}\sigma & \text{if } x_igx_j^{-1} \in H \\ (0)_{m\times m} & \text{otherwise} \end{cases}$$

Theorem 79 *The function $\tau\colon G \to \mathrm{GL}\,(mn, \mathbb{C})$ defined in equation (**??**) is a representation of G.*

Proof. Let $a, b \in G$ and let $a\tau$ have (i, j) block A_{ij}, which is an $m \times m$ matrix. Similarly let the (i, l) block of $b\tau$ be B_{ij}. Then $(a\tau)(b\tau)$ has (i, j) block C_{ij}, again an $m \times m$ matrix, where

$$\begin{aligned} C_{ij} &= \sum_{k=1}^{n} A_{ik}B_{kj} \\ &= \sum_{k=1}^{n} (x_ia\dot{x}_k^{-1}\sigma)(x_kb\dot{x}_j^{-1}\sigma) \\ &= \begin{cases} (x_iax_k^{-1}\sigma)(x_kbx_j^{-1}\sigma) & \text{if } x_iax_k^{-1} \in H \text{ and } x_kbx_j^{-1} \in H \\ (0)_{m\times m} & \text{otherwise} \end{cases} \end{aligned}$$

But since σ is a homomorphism,

$$(x_iax_k^{-1}\sigma)(x_kbx_j^{-1}\sigma) = x_iabx_j^{-1}\sigma$$

and thus $C_{ij} = (x_iab\dot{x}_j^{-1}\sigma)$ which is the (i, j) block of $(ab)\tau$.

Now, for any i $\exists!k$ such that $x_iax_k^{-1} \in H$, and for that k $\exists!j$ such that $x_kbx_j^{-1} \in H$. Hence for this unique k,

$$C_{ij} = \sum_{l=1}^{n} A_{il}B_{lj} = A_{ik}B_{kj}$$

and $C_{il} = (0)_{m\times m}$ for all $l \neq j$.

***** □

The representation τ is called the representation induced from H to G of σ, $\mathrm{Ind}_H^G(\sigma)$. Let W be the $\mathbb{C}H$-

module for σ. Then where

$$H = Hx_1 \cup Hx_2 \cup \cdots \cup Hx_n$$

form $V = (W \otimes x_1) \oplus (W \otimes x_@) \oplus \cdots \oplus (W \otimes x_n)$

where as vector spaces $W \otimes x_i \cong W$ with $\mathbf{w} \otimes x_i \mapsto \mathbf{w}$. Now, given any $g \in G$ and $1 \leqslant i \leqslant n$ there exists a unique value of j such that $x_i g x_j^{-1} \in H$ and hence g induces a linear transformation from $W \otimes x_i$ to $W \otimes x_j$ via

$$(\mathbf{w} \otimes x_i)g = \mathbf{w} x_i g x_j^{-1} \otimes x_j$$

Besides an induced representation and module, there is of course an induced character. In the $mn \times mn$ matrix $g\tau$ it is only the n diagonal $m \times m$ blocks that will contribute to the character. Suppose that σ gives character χ, then

$$\begin{aligned} \operatorname{tr} g\tau &= \sum_{i=1}^{n} \operatorname{tr} x_i g \dot{x}_i^{-1} \sigma \\ &= \sum_{i=1}^{n} \dot{\chi}(x_i g x_i^{-1}) \end{aligned}$$

$$\text{where } \dot{\chi}(x_i g x_i^{-1}) = \begin{cases} \chi(x_i g x_i^{-1}) & \text{if } x_i g x_i^{-1} \in H \\ 0 & \text{otherwise} \end{cases}$$

Theorem 80 (Frobenius Reciprocity) *Let $H \leqslant G$, let α be a class function of H, and let β be a class function of G. Then*

$$\left\langle \operatorname{Ind}_H^G(\alpha), \beta \right\rangle_G = \left\langle \alpha, \operatorname{Res}_H^G(\beta) \right\rangle_H$$

Proof. Let $G = \bigcup_{i=1}^n Hx_i$ then

$$\begin{aligned} \left\langle \operatorname{Ind}_H^G(\alpha), \beta \right\rangle_G &= \frac{1}{|G|} \sum_{g \in G} \operatorname{Ind}_H^G(\alpha)(g)\overline{\beta(g)} \\ &= \frac{1}{|G|} \sum_{g \in G} \overline{\beta(g)} \sum_{i=1}^{n} \dot{\alpha}(x_i g x_i^{-1}) \\ &= \frac{1}{|G|} \sum_{g \in G} \sum_{i=1}^{n} \dot{\alpha}(x_i g x_i^{-1})\overline{\beta(x_i g x_i^{-1})} \end{aligned}$$

Now, for fixed $h \in H$, hx_i is another coset representative of Hx_i *i.e.*, $Hx_i = Hhx_i$ and so

$$= \frac{1}{|G|} \sum_{g \in G} \sum_{i=1}^{n} \dot{\alpha}(hx_i g x_i^{-1} h^{-1})\overline{\beta(hx_i g x_i^{-1} h^{-1})}$$

But this can be done for all $h \in H$, so adding these together,

$$\begin{aligned} |H| \left\langle \operatorname{Ind}_H^G(\alpha), \beta \right\rangle_G &= \frac{1}{|G|} \sum_{h \in H} \sum_{g \in G} \sum_{i=1}^{n} \dot{\alpha}(hx_i g x_i^{-1} h^{-1})\overline{\beta(hx_i g x_i^{-1} h^{-1})} \\ &= \frac{1}{|G|} \sum_{g \in G} \sum_{h \in H} \sum_{i=1}^{n} \dot{\alpha}(hx_i g x_i^{-1} h^{-1})\overline{\beta(hx_i g x_i^{-1} h^{-1})} \end{aligned}$$

But over all $h \in H$ the product hx_i takes on all values in Hx_i. Then summing over $1 \leqslant i \leqslant n$, hx_i takes all values of G, and hence

$$
\begin{aligned}
&= \frac{1}{|G|} \sum_{g \in G} \sum_{y \in G} \dot{\alpha}(ygy^{-1})\overline{\beta(ygy^{-1})} \\
&= \frac{1}{|G|} \sum_{\substack{(g,y) \in G \times G \\ ygy^{-1} \in H}} \alpha(ygy^{-1})\overline{\beta(ygy^{-1})}
\end{aligned}
$$

Consider the ordered pairs over which this summation is taken. g must be G-conjugate to some $h \in H$, so $ygy^{-1} = h$ say. Hence for this h there are $[G : C_G(h)]$ choices for g. For each such g there is at least 1 choice for y, but if y_1 and y_2 both meet the criteria then

$$y_1 g y_1^{-1} = y_2 g y_2^{-1} \Leftrightarrow y_2^{-1} y_1 \in C_G(g)$$

Since g is conjugate to h, $C_G(g) = C_G(h)$ and so the are $|C_G(h)|$ possible choices for y. Hence there are $|C_G(h)|[G : C_G(h)] = |G|$ ordered pairs such that for chosen $h \in H$, $ygy^{-1} = h$. Hence

$$\frac{1}{|G|} \sum_{\substack{(g,y) \in G \times G \\ ygy^{-1} \in H}} \alpha(ygy^{-1})\overline{\beta(ygy^{-1})} = \sum_{h \in H} \alpha(h)\overline{\beta(h)} \qquad = |H| \left\langle \alpha, \mathrm{Res}_H^G(\beta) \right\rangle_H$$

as required. □

(36.4) Clifford Theory

Continuing the theme of induction from a subgroup, attention is turned to induction from a normal subgroup. In particular the modules are examined.

Let G be a group and $H \leqslant G$. Let V be a $\mathbb{C}G$-module and let W be a $\mathbb{C}H$-module. Now, as sets $V = \mathrm{Res}_H^G(V)$ but the same is not true for W and $\mathrm{Ind}_H^G(W)$. Referring to Section 36.3.4 W embeds natrularry in $\mathrm{Ind}_H^G(W)$ in a way which defines a $\mathbb{C}H$-homomorphism $i \colon W \to \mathrm{Ind}_H^G(W)$. The following situation arrises

$$
\begin{tikzcd}
\mathrm{Ind}_H^G(W) \arrow[rr, "\mathbb{C}G\text{-homomorphisms}"] & & V \\
W \arrow[u, "i"] \arrow[rr, "\mathbb{C}H\text{-homomorphisms}"] & & \mathrm{Res}_H^G(V) \arrow[u, "\text{identity}"']
\end{tikzcd}
$$

Theorem 81 *Let G be a group and $H \leqslant G$. Let V be a $\mathbb{C}G$-module and W be a $\mathbb{C}H$-module. If $\theta \colon W \to \mathrm{Res}_H^G(V)$ is a $\mathbb{C}H$-homomorphism and i is the canonical inclusion of W into $\mathrm{Ind}_H^G(W)$ then there exists a unique $\mathbb{C}G$-homomoprhism $F_\theta \colon \mathrm{Ind}_H^G(W) \to V$ such that $F \circ i = \theta$.*

That is to say, the requirement $F_\theta \circ i = \theta$ defines F_θ uniquely.

Proof. Define a map

$$\mathrm{Hom}_{\mathbb{C}G}\left(\mathrm{Ind}_H^G(W), V\right) \to \mathrm{Hom}_{\mathbb{C}H}\left(W, \mathrm{Res}_H^G(V)\right) \quad \text{by} \quad F \mapsto F \circ i \tag{82}$$

Trivially this is 1-to-1. Now let χ be a character of W and ψ be a character of V. Hence by Theorem 80 (Frobenius Reciprocity)

$$\dim \mathrm{Hom}_{\mathbb{C}G}\left(\mathrm{Ind}_H^G(W), V\right) = \left\langle \mathrm{Ind}_H^G(\chi), \psi \right\rangle_G = \left\langle \chi, \mathrm{Res}_H^G(\psi) \right\rangle_H = \dim \mathrm{Hom}_{\mathbb{C}H}\left(W, \mathrm{Res}_H^G(V)\right)$$

Hence the map defined in equation (82) is also onto. Hence if θ is any $\mathbb{C}H$-homomorphism there must exist a unique $\mathbb{C}G$-homomorphism F_θ such that $F_\theta \circ i = \theta$. □

Definition 83 *Let G be a group, $H \leqslant G$, and W be a $\mathbb{C}H$-module. A module induced from H is a pair (X, i) where X is a $\mathbb{C}G$-module and $i\colon W \to X$ is the inclusion function with the property described in Theorem 81.*

Theorem 84 *Let G be a group and $H \leqslant G$. If (X, i) and (Y, j) are both $\mathbb{C}G$-modules that are induced from the same $\mathbb{C}H$-module, W, then $X \cong Y$.*

Simply put, $\mathrm{Ind}_H^G(W)$ is unique up to isomorphism.

Proof. Now, in the definition of induced module replace V with X or Y to get

$$\begin{array}{ccc} X & \xrightarrow{F_X} & Y \\ i\big\uparrow & & \big\uparrow \\ W & \xrightarrow{j} & \mathrm{Res}_H^G(Y) \end{array} \qquad\qquad \begin{array}{ccc} Y & \xrightarrow{F_Y} & X \\ j\big\uparrow & & \big\uparrow \\ W & \xrightarrow{i} & \mathrm{Res}_H^G(X) \end{array}$$

Hence $F_X \circ i = j$ and $F_Y \circ j = i$ and these functions are unique. But then

$$j = F_X \circ i = F_X \circ F_Y \circ j$$

and hence $F_X \circ F_Y\colon X \to X$ is the identity on X. Similarly $F_Y \circ F_X$ is the identity on Y. Hence F_X and F_Y are mutual inverses and so define an isomorphism $X \cong Y$. □

Definition 85 *Let G be a group, $H \trianglelefteq G$, and let L be a $\mathbb{C}H$-module. For any $g \in G$ define $L^{(g)}$ to be the $\mathbb{C}H$-module which is equal to L as a vector space bu has action with H defined by*

$$h * \mathbf{l} = (g^{-1}hg)\mathbf{l}$$

Theorem 86 *Let G be a group and $H \trianglelefteq G$. Let M be a $\mathbb{C}G$-module and let L be a $\mathbb{C}H$-submodule of M. Then for any $g \in G$, gL is also a $\mathbb{C}H$-submodule of M and $gL \cong L^{(g)}$.*

Proof. The action of g on L is that of a linear transformation. The image of this must also be a vector space, and a subspace of M. Hence gL is a subspace of M. To show that gL is also a $\mathbb{C}H$-submodule of M let $h \in H$ and $g\mathbf{l} \in gL$. Then

$$h(g\mathbf{l}) = g(g^{-1}hg)\mathbf{l} \in gL$$

because $h \in H \trianglelefteq G$. Now for the isomorphism, define a function

$$\phi\colon gL \to L^{(g)} \quad \text{by} \quad \phi\colon \mathbf{x} \mapsto g^{-1}\mathbf{x}$$

By definition this is a linear map, and trivially it is 1-to-1. Let $g\mathbf{l} \in gL$ then $\phi(g\mathbf{l}) = g^{-1}g\mathbf{l} = \mathbf{l}$ and so ϕ is onto.

To complete the proof, ϕ needs to be shown to be a $\mathbb{C}H$-homomorphism,

$$\begin{aligned} \phi(h(g\mathbf{l})) &= g^{-1}(hg\mathbf{l}) \\ &= (g^{-1}hg)(g^{-1}g)\mathbf{l} \\ &= h * g^{-1}g\mathbf{l} \\ &= h * \phi(g\mathbf{l}) \end{aligned}$$

Hence ϕ preserves the action of h, and thus together with its status as a linear map, this defines ϕ as a $\mathbb{C}H$-homomorphism, as required. □

Note that in particular this theorem can be used when $L = \mathrm{Res}_H^G(M)$ for some $\mathbb{C}G$-module M.

Theorem 87 (Clifford) *Let G be a group and $N \trianglelefteq G$. Let V be an irreducible $\mathbb{C}G$-module. Then $\mathrm{Res}_N^G(V)$ is a direct sum of conjugate irreducible $\mathbb{C}N$-modules.*

Proof. Choose any irreducible $\mathbb{C}N$-module $W \leqslant \mathrm{Res}_N^G(V)$, then for any $g \in G$ the $\mathbb{C}N$-module gW is also irreducible (by Theorem 86 it is isomorphic to a module that is equal to W as a vector space) and so

$$V \geqslant \sum_{g \in G} gW$$

is a non-trivial $\mathbb{C}G$-submodule of V. Since V is irreducible this means that

$$V = \sum_{g \in G} gW = \bigoplus_{g \in X} gW \quad \text{for some } X \subseteq G$$

Note that a sum can be made direct by removing appropriate summands. □

Definition 88 *Let G be a group and let V be a $\mathbb{C}G$-module. Let L be an irreducible $\mathbb{C}G$-module, then define the L-homogeneous component of V to be*

$$V^{(L)} = \sum_{\substack{X \leqslant V \\ X \cong L}} X$$

where "$X \leqslant V$" means that X is a $\mathbb{C}G$-submodule of V.

Theorem 89 *Let G be a group, V be a $\mathbb{C}G$-module, and $N \trianglelefteq G$. Then G acts on the set of homogeneous components of V.*

Proof. Let W be an irreducible $\mathbb{C}N$-module and let L be the W-homogeneous component of $\mathrm{Res}_N^G(V)$, so

$$L = \sum_{\substack{X \leqslant \mathrm{Res}_N^G(V) \\ X \cong W}} X$$

Now, $gX \cong X^{(g)}$ and since $N \trianglelefteq G$ this is again a $\mathbb{C}N$-module. Since V is a $\mathbb{C}G$-module it is closed under the action of G and as a set $\mathrm{Res}_N^G(V) = V$, therefore $gX \subseteq \mathrm{Res}_N^G(V)$ and from the previous sentence is a $\mathbb{C}N$-submodule. Hence the following calculation is justified:

$$gL = \sum_{\substack{X \leqslant \mathrm{Res}_N^G(V) \\ X \cong W}} gX = \sum_{\substack{Y \leqslant \mathrm{Res}_N^G(V) \\ Y \cong W^{(g)}}} Y$$

So gL is the $W^{(g)}$ homogeneous component of V. □

Corollary 90 *Let V be any $\mathbb{C}G$-module and let $N \trianglelefteq G$.In the decomposition of $\mathrm{Res}_N^G(V)$ into irreducible $\mathbb{C}N$-modules, conjugate irreducible $\mathbb{C}N$-modules appear with the same multiplicity.*

Proof. By Theorem 19 (Maschke's Theorem) write $V = m_1V_1 \oplus m_2V_2 \oplus \cdots \oplus m_nV_n$ for irreducible $\mathbb{C}G$-modules V_i. By Theorem 87,

$$\mathrm{Res}_N^G(V_i) = \bigoplus_{g \in X \subseteq G} gW$$

for some irreducible $\mathbb{C}N$-module W which depends on i (as does X). □

Definition 91 *Let G be a group, $N \trianglelefteq G$, and W be an irreducible $\mathbb{C}N$-module. The inertia group of G is the stabiliser of the action of G on the conjugates of W* i.e., $\{g \in G \mid W^{(g)} \cong W\}$.

Definition 92 *Let G be a group, $N \trianglelefteq G$, and V be an irreducible $\mathbb{C}G$-module. V lies over the irreducible $\mathbb{C}N$-module W if and only if*

$$\mathrm{Hom}_{\mathbb{C}N}\left(W, \mathrm{Res}_N^G\left(V\right)\right) \neq \{0\}$$

Note that by Frobenius reciprocity $\mathrm{Hom}_{\mathbb{C}N}\left(W, \mathrm{Res}_N^G\left(V\right)\right) = \mathrm{Hom}_{\mathbb{C}G}\left(\mathrm{Ind}_N^G\left(W\right), V\right)$.

Theorem 93 *Let G be a group, $N \trianglelefteq G$, and W be an irreducible $\mathbb{C}N$-module. Let H be the inertia group for W, then there is a bijection between $\mathbb{C}H$-modules lying over W and irreducible $\mathbb{C}G$-modules lying over W.*