Groups and Representations

Contents

Chapter 1: Groups

1.1 Basic Definitions..........................................................3
1.2 Groups of Matrices..........................................................3
1.3 Cyclic Groups .................................................................4
1.4 Symmetric Groups and Alternating Groups..........................4
1.5 Dihedral Groups ..............................................................4
1.6 Homomorphism and isomorphisms. ......................................5

Chapter 2: Representations..................................................6

2.1 Representations of Cyclic Groups ......................................7

Chapter 3: Generators and Relations......................................10

3.1 Generating Sets ...............................................................10
3.2 Normal Subgroups ...........................................................10
3.3 Quotient Groups ..............................................................11
3.4 Free Groups .................................................................13
3.5 Presentations of Groups ...................................................17

Chapter 4: Modules..............................................................20

4.1 Group Actions .................................................................20
4.2 Representations afforded by $\mathbb{C}G$-modules .........................21
4.3 Submodules .................................................................22
4.4 Inner Products ...............................................................24

Chapter 5: Characters..........................................................27

5.1 Reminder on Conjugacy Classes .......................................28
5.2 Schur’s Lemma and Orthogonality .....................................30

Chapter 6: Regular Representations .......................................33

Chapter 7: Character Tables .................................................36

7.1 Definition and first Examples ..........................................36
7.2 Properties of Character Tables .........................................37
7.3 Characters and Normal Subgroups .....................................38
7.4 Linear Characters and the Derived Subgroup .........................40
7.5 More Examples ...............................................................41
Chapter 1: Groups

1.1 Basic Definitions

Group
A Group $G$ is a set $G$ together with a binary operation $\times: \times \rightarrow G$ mapping $(g, h) = gh$ such that the following conditions hold:

1. For any $a, b, c \in G, (ab)c = a(bc)$
2. There exists $1 \in G$ so that for all $a \in G, 1a = a1 = a$
3. For $a \in G$ there exists $a^{-1} \in G$ so that $aa^{-1} = a^{-1}a = 1$

Notation

- Let $G$ be a group. For $x \in G$ and $n \geq 0$ write $x^n$ instead of $\overbrace{xx \ldots xx}^n$ and $x^{-n} = (x^n)^{-1}$.
- The number of elements in $G$, denoted $\#G$ or $|G|$ is a number in $\mathbb{Z}_{\geq 0}$ and called the order of $G$.

Order of element
Let $x \in G$. Then the order of $x$ is the least positive integer $n > 0$ such that $x^n = 1$ or $n = \infty$ if no such integer $n$ exists.

Abelian Group
Two elements $x, y$ in a group $G$ are said to commute if $xy = yx$. A group $G$ is Abelian if for all $x, y \in G, xy = yx$.

Subgroup
A subgroup $H$ of a group $G$ is a non-empty subset $H \subseteq G$ such that the two following conditions hold:

1. $x, y \in H \Rightarrow xy \in H$
2. $x \in H \Rightarrow x^{-1} \in H$

If these conditions hold, write $H \leq G$. Note that $H$ is a group in its own right.

1.2 Groups of Matrices

Notation
Let $M(n, \mathbb{C}) = M_n(\mathbb{C}) :=$ set of $n \times n$ matrices with entries in $\mathbb{C}$. Two such matrices can be multiplied e.g.

$$
\begin{pmatrix}
a & b \\
c & d
\end{pmatrix}
\begin{pmatrix}
p & q \\
r & s
\end{pmatrix}
= 
\begin{pmatrix}
 ap + br & aq + bs \\
 cp + dr & cq + ds
\end{pmatrix}
$$

$A, B \in M(n, \mathbb{C})$ are called inverses of each other if $AB = BA = I_n$, the identity matrix.

Let $GL(n, \mathbb{C}) = GL_n(\mathbb{C})$ be the set of invertible elements of $M(n, \mathbb{C})$. This is a group under multiplication.
Fact: $GL(n, \mathbb{C}) = \{A \in M_n(\mathbb{C}): \det A \neq 0\}$. For $n \geq 2$, $GL(n, \mathbb{C})$ is not abelian while for $n = 1$ $GL(n, \mathbb{C}) \cong \mathbb{C}^*$.

1.3 Cyclic Groups

Cyclic Group

A group $G$ is said to be cyclic if there exists $g \in G$ such that $G = \{g^n: n \in \mathbb{Z}\}$. In this case $g$ is called a generator of $G$ (it may not be unique).

Proposition 8 (Classification of Cyclic Groups)

Let $G$ be a cyclic group with generator $g$. Then

a. If $\#G = \infty$ then $g^k = g^l \Rightarrow k = l$

b. If $\#G = n < \infty$. Then $g^0, g^1, ..., g^{n-1}$ are all the elements of $G$ with no repetitions.

In particular, two cyclic groups are isomorphic if and only if they have equal order.

Notation

Let the cyclic group of order $n$ (up to isomorphism) be denoted by $C_n, n \in \mathbb{Z} \cup \{\infty\}$.

1.4 Symmetric Groups and Alternating Groups

Permutation/Symmetric Group

A permutation of a set $A$ is a bijective map from $A$ to itself. The symmetric group $S_n$ is the set of permutations of $\{1, 2, ..., n\}$ with composition the binary operation.

If $a_1, ..., a_k \in \{1, ..., n\}$ are distinct then $(a_1, ..., a_k)$ or simply $(a_1 ... a_k)$ is defined to be the element $g \in S_n$ known as a $k$-cycle such that $g(a_i) = a_{i+1}$ for all $i$ (indices modulo $k$) and $g(x) = x$ whenever $x = \{1,2,...,n\} \setminus \{a_1,...,a_k\}$.

Alternating Group

For $n \geq 2$ the subgroup $A_n \leq S_n$ is the subgroup containing all 3-cycles. It is known as the alternating group and written $A_n$.

1.5 Dihedral Groups

The set of integers modulo $n$ is denoted $\mathbb{Z}/n$. It is a commutative ring.

Lemma 11

We define $D_{2n}$ to be the set of mappings from $\mathbb{Z}/n$ to itself of the form $x \rightarrow ax + b$ where $a \in \{-1,1\} \subseteq \mathbb{Z}/n$ and $b \in \mathbb{Z}/n$. Then $D_{2n}$ is a subgroup of the symmetric group on $\mathbb{Z}/n$ called the dihedral group.

Proof

It is clear that $D_{2n}$ is nonempty and $x \rightarrow ax + b$ is a map from $\mathbb{Z}/n$ to itself with inverse $y \rightarrow ay - ab$ hence every element of $D_{2n}$ is a permutation and thus $D_{2n} \subseteq S_n$. Let $p, q \in D_{2n}$ say $p(x) = ax + b$ and $q(x) = cx + d$ then $pq(x) = a(cx + d) + b = (ac)x + (ad + b)$ which is again of the required form so $pq \in D_{2n}$. Observe that $q = ax - ab \in D_{2n}$ and $pq(x) = a(ax - ab) + b = a^2x - a^2b + b = x$ so $q = p^{-1}$. Therefore $D_{2n} \leq S_n$. ■
Generating Elements of $D_{2n}$
We define $r, s \in D_{2n}$ to be the unique elements $r(x) = x + 1$ and $s(x) = -x$.

**Lemma 13**
We have $D_{2n} = \{r^k, sr^k : 0 \leq k \leq n\}$

**Proof**
Since $\#D_{2n} = 2n$ and $\#\{r^k, sr^k : 0 \leq k \leq n\} = 2n$ it is enough to prove only one inclusion.
Then observe that $r^b(x) = x + b$ and $sr^{-b}(x) = -x + b$ which are both elements of $D_{2n}$ for all $b \in \mathbb{Z}/n$ hence $\{r^k, sr^k : 0 \leq k \leq n\} \subseteq D_{2n}$. ■

We may refer to $r^k$ being a rotation and $sr^k$ being a reflection. Therefore every element of $D_{2n}$ is either a rotation or a reflection but not both.

**1.6 Homomorphism and isomorphisms.**

**Homomorphism**
Let $G, H$ be groups. Then a function $f : G \to H$ such that $f(xy) = f(x)f(y)$ for all $x, y \in G$ is called a homomorphism.

**Isomorphism**
Let $G, H$ be groups. An isomorphism $G \to H$ is a bijective homomorphism. If there exists at least one isomorphism $G \to H$ we write $G \cong H$ and say that $G, H$ are isomorphic.

**Direct product of Groups**
Let $G, H$ be groups. The direct product $G \times H$ is the set of pairs $(g, h)$ where $g \in G$ and $h \in H$ and multiplication is defined component-wise: $(a, b)(c, d) = (ac, bd)$. It is easy to show that this makes $G \times H$ into a group.
Chapter 2: Representations

Representation
Let \( n \geq 0, G \) a group. A representation of \( G \) of dimension \( n \) is a homomorphism \( G \to GL(n, \mathbb{C}) \). Note that \( GL(0, \mathbb{C}) = \{1\} \)

Examples

a. Let \( f: G \to GL(n, \mathbb{C}) \) and set \( f(x) = I_n \) for all \( x \in G \). This is a representation; the \( n \)-dimensional trivial representation.

b. Let \( C_2 = \{1, g\} \) and \( f: C_2 \to GL(n, \mathbb{C}) \) be defined by \( f(g) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \). This is a representation.

Lemma 20
Let \( \rho: G \to GL(n, \mathbb{C}) \) be a representation and take \( T \in GL(n, \mathbb{C}) \) and define \( \sigma: G \to GL(n, \mathbb{C}) \) by \( \sigma(x) = T\rho(x)T^{-1} \). Then \( \sigma \) is also a representation.

Proof
Let \( x, y \in G \). Then \( \sigma(xy) = T\rho(xy)T^{-1} = T\rho(x)\rho(y)T^{-1} = T\rho(x)T^{-1}T\rho(y)T^{-1} = \sigma(x)\sigma(y) \).

Equivalent Representations
Two representations \( \rho, \sigma: G \to GL(n, \mathbb{C}) \) are equivalent if there exists \( T \in GL(n, \mathbb{C}) \) such that \( \sigma(x) = T\rho(x)T^{-1} \) for all \( x \in G \). Denote this as \( \sigma \sim \rho \)

Lemma 22
Equivalence of Representations is an equivalence relation.

Proof
Clearly \( \sigma \sim \sigma \) as \( \sigma(x) = Id\sigma(x)Td^{-1} \) for all \( \sigma \).

If \( \sigma \sim \rho \) then \( \sigma(x) = T\rho(x)T^{-1} \) so \( T^{-1}\sigma(x)T = \rho(x) \) \( \Rightarrow \) \( \rho \sim \sigma \)

If \( \sigma \sim \tau \) and \( \rho \sim \tau \) then \( \sigma(x) = T\rho(x)T^{-1} \) and \( \rho(x) = S\tau(x)S^{-1} \) hence \( \sigma(x) = TS\tau(x)S^{-1}T^{-1} = TS\tau(x)(TS)^{-1} \) \( \Rightarrow \) \( \sigma \sim \tau \)

Reminder on Set Theory
Let \( \sim \) be an equivalence relation on a set \( S \). An equivalence class with respect to \( \sim \) or a \( \sim \)-class is a subset of \( S \) of the form \( y/\sim := \{x \in S: x \sim y\} \) where \( y \in S \) and \( S \) is the disjoint union of all equivalence classes. Then \( S/\sim := \{\sim\text{-classes}\} \).

Notation
Let \( \text{Rep}_n(G) := \{n\text{-dimensional representations of } G\}/\sim \) and \( \text{Rep}(G) := \bigsqcup_{n \geq 0} \text{Rep}_n(G) \)

The main aim of this course is to analyse \( \text{Rep}(G) \) and later we will see that \( \#\text{Rep}_n(G) < \infty \) if \( |G| < \infty \).
2.1 Representations of Cyclic Groups

Lemma 23
Let $A$ and $B$ be two diagonal $n \times n$ matrices with elements on the diagonal denoted by $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ respectively. Then the following are equivalent:

1. There exists $T \in GL(n, \mathbb{C})$ so that $TAT^{-1} = B$
2. $\prod_{i=1}^n (x - a_i) = \prod_{i=1}^n (x - b_i)$
3. There exists a permutation $s \in S_n$ so that $b_i = a_{s(i)}$ for all $1 \leq i \leq n$.

Proof
[2 $\Rightarrow$ 3] If $\prod_{i=1}^n (x - a_i) = \prod_{i=1}^n (x - b_i)$ then the two polynomials are equal and hence have the same roots; i.e. $\{a_i\} = \{b_i\}$ up to reordering. Then simply choose a permutation $s \in S_n$ so that $a_i = b_{s(i)}$ for all $1 \leq i \leq n$.

[1 $\Rightarrow$ 2] If $TAT^{-1} = B$ then $A$ and $B$ have the same characteristic polynomial. As $A$ and $B$ are both diagonal, their characteristic polynomials are $\prod_{i=1}^n (x - a_i)$ and $\prod_{i=1}^n (x - b_i)$ respectively and so these are equal.

[3 $\Rightarrow$ 1] Let $\{e_1, \ldots, e_n\}$ be the standard basis of $\mathbb{C}^n$. Then $Ae_i = a_ie_i$ for all $1 \leq i \leq n$ because $A$ is diagonal. Similarly, as $B$ is diagonal, $Be_i = b_ie_i$ for $1 \leq i \leq n$. Then define $T$ to be the $n \times n$ invertible matrix representing the linear map $e_i \mapsto e_{s^{-1}(i)}$. Then observe that $TAT^{-1}(e_i) = T Ae_{s(i)} = T a_{s(i)} e_{s(i)} = a_{s(i)} e_i = b_{s(i)} e_i = Be_i$ for $1 \leq i \leq n$ hence $TAT^{-1} = B$. \(\blacksquare\)

Let $r \geq 1$ and define $C_r = \{1, \ldots, g^{r-1}\}$ for $g \in C_r$. We aim to list $Rep_n(C_r)$

Lemma 24
a. Let $A \in GL_n(\mathbb{C})$ with $A^r = 1$. Then there exists a unique representation $\rho_A$ of $C_r$ such that $\rho_A(g) = A$ and it satisfies $\rho_A(g^k) = A^k$ for all $k$.

b. Every representation of $C_r$ is of the form $\rho_A$ for some $A$.

c. $\rho_A \sim \rho_B$ if and only if $A, B$ are conjugate.

Proof
a. Since a homomorphism $C_r \to GL_n(\mathbb{C})$ is uniquely determined by its action on the generator $g$, the representation $\rho_A$ sending $\rho_A(g) = A$ is unique and $\rho_A(g^k) = A^k$ for all $k$.

b. Let $f$ be a representation of $C_r$; that is $f : C_r \to GL_n(\mathbb{C})$ is a homomorphism. Then $f(g) = B$ for some $B \in GL_n(\mathbb{C})$. As a homomorphism is uniquely determined by its action on $g$, we see that $f(g) = \rho_B(g) = B$ and $f(g^k) = \rho_B(g^k) = B^k$ for all $k$. Hence $f = \rho_B$.

c. Suppose $\rho_A \sim \rho_B$. Then for all $g^k \in C_r$, $\rho_A(g^k) = T \rho_B(g^k) T^{-1}$. In particular, $\rho_A(g) = T \rho_B(g) T^{-1} \Rightarrow A = T B T^{-1}$ and so $A$ and $B$ are conjugate.

Conversely, suppose $A$ and $B$ are conjugate, that is $A = T B T^{-1}$ for some $T \in GL_n(\mathbb{C})$. Then for all $k \in \mathbb{Z}$, $A^k = (T B T^{-1})^k = T B^k T^{-1}$ hence $\rho_A(g^k) = A^k = T B^k T^{-1} = T \rho_B(g^k) T^{-1}$ for all $k$ so $\rho_A \sim \rho_B$. \(\blacksquare\)
Lemma 25
Let $A \in GL(n, \mathbb{C})$ be a matrix of finite order. Then $A$ is diagonalisable.

Proof
Say that $A^r = 1$ for $r > 0$. We may suppose that $A$ is in Jordan Normal form. Note that 0 is not an eigenvalue of $A$ as $A^r = 1$. If $A$ is not diagonalisable, consider a Jordan Block

$J_i = \lambda_i \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$. This can be done because the eigenvalues $\lambda_i \neq 0$. By induction it is easy to prove that for all $k > 0 J_i^k$ is of the form

$J_i^k = \lambda_i^k \begin{pmatrix} 1 & k & * & * \\ 0 & 1 & k & * \\ 0 & 0 & 1 & k \\ 0 & 0 & 0 & 1 \end{pmatrix}$

Now $J_i^r = 1$ so the rows above the diagonal are $\lambda_i^r r = 0$. As $\lambda_i \neq 0$ and $r \neq 0$ this is a contradiction so $A$ is diagonalisable. ■

Put $\omega = \exp \left( \frac{2\pi i}{r} \right)$ so $\{1, \omega, \ldots, \omega^{r-1}\} = \{z \in \mathbb{C}: z^r = 1\}$. For $k = (k_0, \ldots, k_{r-1}) \in \mathbb{N}^r$ denote

$M(k) = \begin{pmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} & 0 & 0 & 0 \\ 0 & \begin{bmatrix} \omega & \omega \\ \omega & \omega \end{bmatrix} & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \begin{bmatrix} \ddots & \ddots & \ddots \\ \ddots & \ddots & \ddots \\ \omega^{r-1} & \omega^{r-1} & \omega^{r-1} \end{bmatrix} & 0 \end{pmatrix}.$

Note that $M(k)^r = 1$

Proposition 25 (Classification of Representations of $C_r$)
Let $D = D(n, r)$ be the set of $r$-tuples $(k_0, \ldots, k_{r-1}) \in \mathbb{N}^r$ such that $k_0 + \cdots + k_{r-1} = n$. Then there exists a bijection $f: D \to Rep_n(C_r)$ mapping $k \to \rho_{M(k)}/\sim$.

Proof

1. $f$ is well defined:
   Let $k = (k_0, \ldots, k_{r-1}) = (l_0, \ldots, l_{r-1}) = l$. Then $M(k) = M(l)$ so $\rho_{M(k)} \sim \rho_{M(l)}$.

2. $f$ is injective:
   Suppose $f(k) = f(l)$ so $\rho_{M(k)} \sim \rho_{M(l)}$. Then $M(k)$ and $M(l)$ are conjugate by Lemma 24 and so $M(k)$ and $M(l)$ have equal characteristic polynomials by Lemma 23. I.e. $\prod_{i=0}^{l} (x - \omega^i)^{k_i} = \prod_{i=0}^{r} (x - \omega^i)^{l_i}$. It therefore follows that $k_i = l_i$ for all $0 \leq i \leq r - 1$ and so $k = l$.

3. $f$ is surjective:
   By Lemma 24 every $n$-dimensional representation of $C_r$ is of the form $\rho_A$ where
$A^r = 1$ and $A \in GL(n, \mathbb{C})$. To prove $\rho_A/\sim$ is in the image of $f$, by Lemma 25, $A$ is diagonalisable so $A$ is conjugate to a diagonal matrix $B$. Also $B^r = 1$ so all diagonal entries of $B$ are powers of $\omega$. Say $\omega_i$ appears $k^i$ times for $0 \leq i \leq r - 1$ so $B$ is conjugate to $M(k)$ where $k = \sum_{i=0}^{r-1} k_i$ so $\rho_A \sim \rho_B \sim \rho_{M(k)}$ by Lemma 24. Hence $f(k) = \rho_{M(k)}/\sim$. 

**Example**

Let $r \geq 1$ and define $A \in GL(r, \mathbb{C})$ by $Ae_i = e_{i+1}$ with indices in $\mathbb{Z}/r$. Then $A^r = 1$ so there exists a unique representation $\rho_A$ of $C_r = \{1, g, ..., g^{r-1}\}$ (namely: $\rho_A(g^k) = A^k$ for all $k \in \mathbb{Z}$) what is $f^{-1}(\rho_A/\sim)$?

**Solution:**

Put $\omega = \exp\left(\frac{2\pi i}{r}\right)$ and $v_i = \sum_{j=1}^{r-1} \omega^{ij} e_j$ then $v_i$ is an eigenvector of $A$ because $A v_i = \sum_{j=0}^{r-1} \omega^{ij} e_{j+1} = \sum_{k=0}^{r-1} \omega^{i(k-1)} e_k = \omega^{-i} \sum_{k=0}^{r-1} \omega^{ik} e_k = \omega^{-i} v_i$ and so the eigenvalue is $\omega^{-i}$. So $A$ has $r$ distinct eigenvalues $\omega^{-i}$ with $0 \leq i \leq r - 1$ so all eigenvalues of $A$ are not repeated and because $A$ is $r \times r$ we have $f^{-1}\left(\frac{\rho_A}{\sim}\right) = (1, ..., 1) \in \mathbb{N}^r$ with $A = \rho_A(g)$.
Chapter 3: Generators and Relations

3.1 Generating Sets

Claim
For a group $G$, let $H_i \leq G$ where $i \in I$. Then $\bigcap_{i \in I} H_i \leq G$

Group generated by a subset
Let $A$ be a subset of a group $G$ then $\langle A \rangle := \bigcap_{A \subseteq H \leq G} H$ (this makes sense because $G \supseteq A$ and $G \leq G$).

Remarks:
1. By the claim $\langle A \rangle \leq G$. We say $A$ is a generating set for $\langle A \rangle$.
2. Every Group $G$ has a generating set as $G = \langle G \rangle$

Finitely Generated Group
A Group $G$ is finitely generated if there exists a finite set $\{a_1, \ldots, a_n\} \subseteq G$ such that $G = \langle a_1, \ldots, a_n \rangle$

Remark
$\langle A \rangle$ is the smallest subgroup of $G$ containing $A$.

Proposition 29
Let $A$ be a subset of a group $G$. Then $\langle A \rangle = \{a_1^{d_1} \ldots a_k^{d_k} : k \geq 0, a_i \in A \text{ for all } i \text{ and } d_i \in \{-1, 1\} \text{ for all } i\}$.

Proof
Let $B = RHS$. Observe that $B \subseteq \langle A \rangle$: Let $x, y \in B$ so $x = a_1^{d_1} \ldots a_k^{d_k}, y = b_1^{e_1} \ldots b_l^{e_l}$ then $xy^{-1} = a_1^{d_1} \ldots a_k^{d_k} b_1^{-e_1} \ldots b_l^{-e_l} \in B$.

Also observe that $\langle A \rangle \subseteq B$ by definition of $\langle A \rangle$.

Conversely, let $x \in B$ say $x = a_1^{d_1} \ldots a_k^{d_k}$ then $a_i \in A \subseteq \langle A \rangle$ and $\langle A \rangle \leq G$ so it is closed under group operations so $x \in \langle A \rangle$. Therefore $B \subseteq \langle A \rangle$. ■

Example
$D_{2n} = \langle r, s \rangle \langle r(x) = x + 1, s(x) = -x \rangle$ by an earlier example.

3.2 Normal Subgroups

Notation
Let $A, B$ be subsets of a group $G$. Then $AB := \{ab : a \in A, b \in B\}$. For $a, b \in G$ $aB := \{a\}B, AB := A\{b\}$

Cosets
Let $H \leq G$. A left coset (respectively a right coset) of $G$ with respect to $H$ is a subset of $G$ of the form $Hx = \{hx : h \in H\}$ (Respectively $xH = \{xh : h \in H\}$) and $H \setminus G := \{Hx : x \in G\}$ (Respectively $G/H := \{xH : x \in G\}$)
Claim
Let $H \leq G$. Then:

a. $G = \bigsqcup_{H \trianglelefteq G} H \setminus G$

b. $\#(G/H) = \#(H \setminus G)$

From now on, $\#(G/H)$ will be denoted $[G: H]$ and called the index of $H$ in $G$.

Normal Subgroup
Let $H \leq G$. $H$ is a normal subgroup of $G$ if $Hg = gH$ for all $g \in G$ and denoted $H \trianglelefteq G$

Lemma
The following are equivalent:

1. $H$ is normal in $G$
2. $G/H = H \setminus G$
3. $G/H \subseteq H \setminus G$
4. $x^{-1}Hx = H$ for all $x \in G$

Example

a. $\{1, (12)\} \leq S_3$ but not a normal subgroup because $(23)(12)(23)^{-1} = (23)(12)(23) = (13) \neq (12)$
b. In an abelian group, every subgroup is normal.

Claim
Let $H_i \trianglerighteq G$ where $i \in I$. Then $\bigcap_{i \in I} H_i \trianglelefteq G$

Normal Closure
Let $A$ be a subset of a group $G$. Then $\langle A \rangle_G = \langle A \rangle := \cap_{A \in H \leq G} H$. It is a normal subgroup because of the Claim above. So $\langle A \rangle$ is the normal subgroup of $G$ generated by $A$ or the normal closure of $A$. In particular, a group is simple if it has no other normal subgroups but $\{1\}$ and itself.

3.3 Quotient Groups
Let $N \trianglelefteq G$. Then $G/N = N \setminus G$.

Claim
If $A, B \in G/N$ then $AB \in G/N$.

Proof
Say $A = xN$ and $B = yN$ for some $x, y \in G$. Then as $N$ is normal,

$$AB = (xN)(yN) = x(Ny)N = x(yn)N = xyN \in G/N$$

It is true that $G/N$, together with multiplication of cosets (defined above) makes $G/N$ into a group.

Examples:

a. $G/1 \cong G$
b. \( G/G \cong \{1\} \)

c. Let \( C_\infty = \langle g \rangle \) and \( N = \langle g^r \rangle \). Then \( N \trianglelefteq C_\infty \) and \( C_\infty/N \cong C_r \).

**Claim**

It is true that \( \langle r \rangle \trianglelefteq D_{2n} \).

**Proof**

We consider the sets of left cosets and right cosets. \( \{\langle r \rangle, \langle r \rangle s \} \) and \( \{\langle r \rangle, s \langle r \rangle \} \). As \( D_{2n} \) is the disjoint union of each of the elements of the sets, we observe that since \( \langle r \rangle = \langle r \rangle \), we must have \( \langle r \rangle s = s \langle r \rangle \). Therefore \( \langle r \rangle \) is normal. ■

**Kernel and Image**

Let \( f: G \to H \) be a homomorphism. Then the kernel of \( f \) denoted \( \ker f := \{ x \in G : f(x) = 1 \} \) and the image of \( f \) is \( \text{im}(f) := \{ f(x) : x \in G \} \). It is true that \( \ker f \trianglelefteq G \) and \( \text{im}(f) \leq H \).

**Proposition 38**

Let \( N \trianglelefteq G \). Then the natural map \( \pi: G \to G/N \) taking \( \pi(g) = gN \) is a surjective homomorphism with kernel \( N \).

**Proof**

\( \pi \) is surjective: take a coset \( gN \in G/N \). Then clearly \( \pi(g) = gN \).

\( \pi \) is a homomorphism:

Take \( x, y \in G \) then \( \pi(xy) = xyN = xNyN = \pi(x)\pi(y) \)

\( \ker \pi = N : \)

By definition \( \ker \pi = \{ g \in G : gN = N \} \) now \( gN = N \iff g \in N \) so \( \ker \pi = N \). ■

**Theorem 39 (First Isomorphism Theorem)**

Let \( f: G \to H \) be a homomorphism with kernel \( K \). Then there exists a unique isomorphism \( \mu: G/K \to \text{im}(f) \) so that \( f = \mu \circ \pi \). That is \( \mu(gK) = f(g) \)

**Proof**

Standard proof. ■

**Commutative Diagram**

The following diagram is said to commute if \( p = h \circ g \circ f \)

\[
\begin{array}{ccc}
A & \xrightarrow{f} & B \\
\downarrow{p} & & \downarrow{g} \\
C & \xleftarrow{h} & D
\end{array}
\]
3.4 Free Groups

The expression $G = \left\langle x, y \mid x^2, y^3, (xy)^3 \right\rangle$ determines $G$ uniquely; this is a presentation for $G$.

Alphabets and Letters

Let $A$ be a set, called an alphabet. Elements of $A$ are called letters (or generators).

Word of Length $k$, Length, Empty Word

A word of $A$ of length $k$ is a $k$-tuple of the form $\left( \frac{e_1}{a_1}, \ldots, \frac{e_k}{a_k} \right)$ where $a_i \in A$ and $e_i \in \{-1, 1\}$ for all $i$. We denote by $1$ the "empty word" which is the unique word of length 0. Denote by $L(u)$ the length of the word $u$.

An alternative notation is $a_1^{e_1} \ldots a_k^{e_k}$. Most people use this despite it causing confusion.

Multiplication of words

We multiply by a process called concatenation; the product of $\left( \frac{e_1}{a_1}, \ldots, \frac{e_k}{a_k} \right)$, $\left( \frac{d_1}{b_1}, \ldots, \frac{d_l}{b_l} \right)$ is simply $\left( \frac{e_1}{a_1}, \ldots, \frac{e_k}{a_k}, \frac{d_1}{b_1}, \ldots, \frac{d_l}{b_l} \right)$. Note in particular that $L(u, v) = L(u) + L(v)$. The inverse of $\left( \frac{e_1}{a_1}, \ldots, \frac{e_k}{a_k} \right)$ is defined to be $\left( \frac{-e_k}{a_k}, \ldots, \frac{-e_1}{a_1} \right)$.

Remark

The set $A^* = \{\text{words over } A\}$ is not a group because $uu^{-1} \neq 1$ in general, however multiplication of words is associative.

One-Step Reduction

a. Let $u, v \in A^*$ and $a \in A$. We say that $uv$ is a 1-step reduction of both $uav^{-1}$ and $ua^{-1}v$. We denote this by $uav^{-1}v \rightarrow uv$ and $ua^{-1}v \rightarrow uv$.

b. Let $\geq$ be the reflexive transitive closure of $\rightarrow$; equivalently $u \geq v$ if and only if there exists a sequence of 1-step reductions $u = w_0 \rightarrow w_1 \rightarrow \cdots \rightarrow w_k = v$.

c. Similar notions are $>, \leq, <$ in the usual way.

Ordering of a set

An ordering on a set $X$ is a relation $\leq$ such that:

1. Reflexivity: $x \leq x$ for all $x \in X$
2. Transitivity: $x \leq y$ and $y \leq z$ implies $x \leq z$
3. Antisymmetry: If $x \leq y$ and $y \leq x$ then $x = y$.

Note that $u \rightarrow v$ implies $L(u) > L(v)$ so $u \geq v \Rightarrow L(u) \geq L(v)$ then $u \geq v \geq u \Rightarrow L(u) \geq L(v) \geq L(u)$ so $L(u) = L(v)$ and no letters are removed so $u = v$. Therefore the relation $\geq$ defined by 1-step reduction is an ordering on $A^*$. 
Total Ordering
A total-ordering on a set $X$ is an ordering $\leq$ on $X$ which additionally satisfies:

4. For any $x, y \in X$ either $x \leq y$ or $y \leq x$.

Reduced Word
We call $u \in A^*$ a reduced word if $\nexists v \in A^*$ with $u \rightarrow v$. The set of reduced words in $A^*$ is denoted by $F(A)$.
Equivalently, $u \in F(A) \iff u$ is neither of the form $xaxa^{-1}y$ nor $xa^{-1}ya$ for $x, y \in A^*$ and $a \in A$.

Lower Bound/Reduced Lower Bound
In an ordered set $(X, \leq)$ if $x \leq y$ then we say that $x$ is a lower bound of $y$. So a reduced lower bound (RLB) of $u \in A^*$ is any reduced $v \in F(A)$ such that $u \geq v$.

Example
Let $a, b, c, d \in A$ be distinct letters. Then $w := aabb^{-1}a^{-1}cdd^{-1}b \rightarrow aaaa^{-1}cdd^{-1}b \rightarrow acdd^{-1}b \rightarrow acab$ so $acb$ is an RLB of $w$.

Lemma
Let $u \in A^*$. Then $u$ has a unique RLB denoted $R(u)$.

Proof
Existence:
Take $u \in A^*$ then consider the set $V = \{v \in A^* \text{ such that } v \leq u\}$ as $u \in V, V \neq \emptyset$. Choose an element $v \in V$ of least length $L(v)$. This is possible because $L(v) \in \mathbb{N}$ by the Well-Ordering Principle. Then $v$ is an RLB, because otherwise there exists $w \in V$ with $w < v$ so $L(w) < L(v)$ contradicting the minimality of $L(v)$.

Uniqueness:
We apply induction on $L(u)$. It is clear if $L(u) \leq 1$ (since then every word is a RLB of itself).

Let $L(u) > 1$. Assume all shorter words have a unique lower bound. Let $v, w$ be RBs of $u$.
We will prove that $v = w$.
By definition, there exist $v_1, w_1$ such that $u \rightarrow v_1 \geq v$ and $u \rightarrow w_1 \geq w$. We may assume $u \neq v$ and $u \neq w$ since otherwise we are done.

Say there is overlap if some letter in $u$ is removed in both arrows $u \rightarrow v_1$ and $u \rightarrow w_1$.
Assume there is no overlap; then there exist $p, q, r, s, t \in A^*$ with $u = pqrst \rightarrow prst = v_1$ and
$u = pqrst \rightarrow pqrt = w_1$ then $v_1 \rightarrow prt$ and $w_1 \rightarrow prt$. Denote $\geq = \rightarrow$ then we have the

diagram
Let $x$ be a RLB of $prt$. Now, $v, x$ are both RLBs of $v_1$; hence by induction hypothesis $v = x$ as $L(v_1) < L(u)$. Similarly $w, x$ are both RLBs of $w_1$ hence by induction hypothesis $w = x$ as $L(w_1) < L(u)$. Therefore $w = x = v$.

If there is overlap, assume $v \neq w$. Then there exists $a \in A \cup A^{-1}$ and $p, q \in A^*$ such that $u = paa^{-1}aq \rightarrow v_1 = paq$ and $u = paa^{-1}aq \rightarrow w_1 = paq$ so $v_1 = w_1$. As $v, w$ are RLBs of $v_1$, by the induction hypothesis $v = w$ as $L(v_1) \leq L(u)$. As required. ■

Exercise
Let $u, v \in A^*$. Then $R(R(u)v) = R(1v) = R(u1v)$ where $R(u)$ is the unique RLB of $u$.

Reduced concatenation
Let $u, v \in F(A)$. Then define the binary operation $*: F(A) \times F(A) \rightarrow F(A)$ by $u \ast v := R(uv)$

Example
$$aab \ast b^{-1}a^{-1}cdd^{-1}b = R(aabb^{-1}a^{-1}cdd^{-1}b) = R(aaa^{-1}cb) = acb$$

Theorem 49
The set of reduced words on an alphabet $A$ equipped with $\ast, (F(A), \ast)$ is a group.

Proof
1. $1 \ast u = u \ast 1 = u$ for all $u \in F(A)$
2. $u \ast u^{-1} = 1$ (in the middle there are one-step reductions until everything cancels and you get 1. Likewise for $u^{-1} \ast u = 1$.
3. For associativity, let $u, v, w \in F(A)$. Then $u \ast (v \ast w) = R(u(v \ast w)) = R(uR(vw)) = R(uvw) = R(R(uvw)) = R((u \ast v) \ast w) = (u \ast v) \ast w$. ■

Example 51
a. $F(\emptyset) = 1$

b. Claim

Proof
$F(\{a\})$ consists purely of powers of $a$ hence generated by $a$ so cyclic. Moreover for all $n \geq 0$ $a \ldots a \in F(\{a\})$ are all distinct so $\#F(\{a\}) = \infty$

More precisely define a map $\phi: F(\{a\}) \rightarrow \mathbb{Z}$ by $a^n \rightarrow n$. Then $\phi(a^n a^m) = \phi(a^{n+m}) = n + m = \phi(a^n) + \phi(a^m)$ so $\phi$ is a homomorphism. We can define $\phi^{-1}$ as $n \rightarrow a^n$ so $\phi$ is an isomorphism. ■
Claim

\[ F(A) \cong F(B) \iff |A| = |B| \]

Proof

[\leq] If \(|A| = |B|\) then there exists a bijection \(\phi: A \to B\). We then extend this bijection \(\phi\) into an isomorphism of the Free Groups by defining \(\phi(ab) = \phi(a)\phi(b)\).

[\geq] Since \(F(A) \cong F(B)\) there exists an isomorphism \(\phi\) which in particular is a bijection. Restricting this isomorphism to the set \(A \subset F(A)\) defines a bijection from \(A\) to some subset \(B'\) of \(F(B)\). As \(\phi\) is an isomorphism on the free groups, the set \(B'\) is a generating set for \(F(B)\) so \(|A| = |B'| = |B|\) as required.

In conclusion the free group \(F(a_1, \ldots, a_n)\) depends up to isomorphism only on \(n\), so we can denote by \(F_n\) the free group with \(n\) generators, or free group of rank \(n\).

Unproved Theorem
Every subgroup of a free group is again isomorphic to a free group.

Exercise
Let \(G, H\) be groups, \(G = \langle A \rangle\) and \(f: A \to H\) a map. Then there is at most one homomorphism \(g: G \to H\) extending \(f\); that is \(g(a) = f(a)\) for all \(a \in A\).

Solution
Define \(g(a) = f(a)\) for all \(a \in A\).

Take \(x \in G\). Then \(x = a_1^{e_1} a_2^{e_2} \cdots a_k^{e_k}\) for some \(a_i \in A\) and \(e_i \in \{-1,1\}\). Then define \(g(x) = f(a_1)^{e_1} f(a_2)^{e_2} \cdots f(a_k)^{e_k}\) clearly \(g\) is a homomorphism so \(g\) is determined uniquely.

Theorem 52 (Universal Property of Free Groups)

Let \(A\) be a set. Define \(F := F(A)\), the free group of \(A\). In particular, \(A \subset F\). Let \(F'\) be a group and \(r': A \to F'\) be a function. Then there exists a unique homomorphism \(s: F \to F'\) such that \(s(a) = r'(a)\) for all \(a \in A\).

Proof

Uniqueness:
This follows from the Previous Exercise.

Existence:
Define \(s: A' \to F'\) by mapping \(a\) to \(r'(a)\) for all \(a \in A\); that is
\[ s(a_1^{d_1} \cdots a_k^{d_k}) := r'(a_1)^{d_1} \cdots r'(a_k)^{d_k} \]
Clearly \(s(a) = r'(a)\) for all \(a \in A\). To prove \(s: F(A) \to F'\) is a homomorphism, let \(u \to v\) say \(u = paa^{-1}q\) and \(v = pq\) and \(a \in A \cup A^{-1}\). Then
So $s(u) = s(pa^{-1}q) = s(p)r'(a)r'^{-1}s(q) = s(p)s(q) = s(pq) = s(v)$
So $s(u) = s(v)$ whenever $u \to v$. By induction, $s(u) = s(R(u))$ so for all $u, v \in F(A)$,
$s(u \ast v) = s(R(uv)) = s(uv) = s(u)s(v)$. ■

**Remark**

$F(A)$ can be characterised by the universal property.

We never need reduced words again.

### 3.5 Presentations of Groups

#### Group Presentation

a. A group presentation is a pair $(A, R)$ where $A$ is a set and $R \subset F(A)$.

b. For any group presentation $(A, R)$ we associate a group $\langle A| R \rangle := F(A)/\langle \langle R \rangle \rangle$

We say that this group (or any isomorphic group) is presented by this group presentation $(A, R)$

c. We allow various ways of writing down relations. For example $xyx^{-1}y^{-1}$, $xy = yx$, $xyx^{-1}y^{-1} = 1$ are all equivalent.

There is a natural map $\phi: A \to \langle A| R \rangle$ taking $\phi(a) = a(\langle R \rangle)$. Often we identify $\phi$ with the identity map. Watch out for confusion if $\phi$ is not injective.

Also one simply writes down a word in $A$ and considers it an element of $\langle A| R \rangle$.

**Corollary 55**

Let $G$ be a group then:

a. There exists a surjective homomorphism from some free group to $G$.

b. There is a a presentation for $G$.

**Proof**

a. Let $A$ be a generating set of $G$ (if necessary we can take $A = G$)

Then let $F(A)$ be the free group generated by $A$. By the Universal Property of Free groups there exists a unique homomorphism $s:F(A) \to G$ such that $s(a) = a$ for all $a \in A$. Then the image of $s$ contains $A$ hence contains $\langle A \rangle = G$ because $\text{im}(s) \leq G$.

b. Put $R = \ker s$. Then $\langle \langle R \rangle \rangle = R$ because the kernel of a homomorphism is a normal subgroup. Then using the first isomorphism theorem on $s$ from part a,

$$\langle A| R \rangle := \frac{F(A)}{\langle \langle R \rangle \rangle} = \frac{F(A)}{R} = \frac{F(A)}{\ker s} \cong \text{im}(s) = G \ ■$$

**Finitely Presented**

A group is finitely presented if it has a presentation $(A, R)$ where $A$ is a finite set and $R$ is a finite subset of $F(A)$.

**Example 56**

For $1 \leq r < \infty$ we have $C_r \cong \langle a| a^r \rangle$
Proof
\( F(a) \cong C_\infty \) as we saw before. Take \( \phi: \{a\} \to C_r \) map \( a \to 1 \). Then \( \langle \langle a^r \rangle \rangle = \langle a^r \rangle = \ker \phi \) because \( C_\infty \) is abelian, and \( \phi \) is surjective so \( \langle \langle a^r \rangle \rangle = \frac{F(a)}{\langle a^r \rangle} \cong C_r \) by the first isomorphism theorem. \( \blacksquare \)

Satisfying Relations
Let \( (A, R) \) be a presentation, \( H \) a group and \( g: A \to H \) a map. We say that \( g \) satisfies \( R \) if \( g(a_1)^{d_1} \cdots g(a_n)^{d_n} = 1 \) whenever \( a_1^{d_1} \cdots a_n^{d_n} \in R \).

Theorem 60 (Universal Property for group presentations)
Let \( (A, R) \) be a presentation, \( H \) a group \( g: A \to H \) a map. The following are equivalent:

1. There exists a homomorphism \( f: \langle \langle a^r \rangle \rangle \to H \) such that \( f(a) = g(a) \) for all \( a \in A \)
2. \( g \) satisfies \( R \)

Moreover, if these conditions hold, then the homomorphism \( f \) is unique.

Proof
Non-examinable. \( \blacksquare \)

Example 62
Prove \( D_{2n} \cong \langle x, y | x^n, y^2, (xy)^2 \rangle \)

Proof
Let \( G = \langle x, y | x^n, y^2, (xy)^2 \rangle \). Then recall that \( D_{2n} \) is (by definition) generated by the functions \( r, s \) where \( r(x) = x + 1 \mod n \), \( s(x) = -x \). Then observe that \( r, s \) satisfy the relations \( x^n, y^2, (xy)^2 \) by taking \( x = r \) and \( y = s \). For example \( (rs)^2 = rsr(s(x)) = rsr(-x) = rs(1-x) = r(x-1) = x \) so \( (rs)^2 = 1 \).
Similarly \( r^n = r \cdots r(x) = x + n = x \).

By Theorem 60, there is a unique homomorphism \( f: G \to D_{2n} \) mapping \( f(x) = r \) and \( f(y) = s \). Note that \( f \) is surjective because \( \text{im}(f) \leq D_{2n} \) and \( \text{im}(f) \) contains \( r, s \) and \( D_{2n} \) is generated by \( r, s \) by an earlier example.

Let \( g \in G \) can be written as a word in \( x \) and \( y \). Say \( g = x^{k_1}y^{l_1} \cdots x^{k_m}y^{l_m} \). We may assume without loss of generality that no exponents in the middle are 0. Using the fact that \( y^2 = 1 \) and \( (xy)^2 = 1 \) we find
\[
  yx = x^{-1}y, \quad y^{-1}x = x^{-1}y^{-1}, \quad yx^{-1} = xy, \quad y^{-1}x^{-1} = xy^{-1}
\]
Using this we can “push” all the \( y \)’s to the right in an expression for \( g \) so \( g \) is of the form \( x^ky^l \) for \( k, l \in \mathbb{Z} \). Using that \( x^n = 1 \) and \( y^2 = 1 \) \( G = \{x^ky^l | 0 \leq k \leq n, 0 \leq l < 2 \} \) so \( |G| \leq 2n = |D_{2n}| \). \( \blacksquare \)

Example
Prove there is a unique presentation \( \rho: D_8 \to GL(2, \mathbb{C}) \) such that \( \rho(r) = A \) and \( \rho(s) = B \) where \( A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \), \( B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \)

Solution
We apply Theorem 60. From the above example we know \( D_8 = \langle x, y | x^4, y^2, (xy)^2 \rangle \). We need
to prove that $A, B$ satisfy the relations. Observe $A^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = B^2$ and $(AB)^2 = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ so $A, B$ satisfy the relations. ■

For $p, q, r \geq 2$ the triangle group is $T(p, q, r) = \langle x, y | x^p, y^q, (xy)^r \rangle$. It can be shown that:

1. $T(p, q, r)$ is finite $\iff \frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1$
2. $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} = 1 \iff [T(p, q, r) : \mathbb{Z}^2] < \infty$

**Examples:**

$T(n, 2, 2) \cong D_{2n}, T(2,3,3) \cong A_4$ this is an exercise on sheet 2, $T(2,3,5) \cong A_5$
Chapter 4: Modules

We assume now on that all vector spaces are over \( \mathbb{C} \).

4.1 Group Actions

Action of a Group on a Vector Space

Let \( V \) be a vector space and \( G \) a group. An action of \( G \) on \( V \) is a map \( G \times V \rightarrow V \) mapping \((g, v) \rightarrow gv\) such that:

1. For all \( g \in G \) the map \( V \rightarrow V \) mapping \( v \rightarrow gv \) is linear; that is \( \forall \lambda \in \mathbb{C}, \ u, v \in V \)
   \[ g(u + v) = g(u) + g(v) \text{ and } g(\lambda v) = \lambda g(v) \]
   Equivalently, \( g(au + bv) = ag(u) + bg(v) \) for all \( a, b \in \mathbb{C} \) and \( u, v \in V \)
2. \( g(hu) = gh(u) \) for all \( h, g \in G, u \in V \)
3. \( 1_G(u) = u \) for all \( u \in V \)

Example 65

Let \( r \geq 1 \), \( C_r = \langle g^r \rangle \). Let \( V \) be a vector space with basis \( \{ v_i; v_i \in \mathbb{Z}/r\mathbb{Z} \} \) so \( \dim V = r \)
Define \( C_r \times V \rightarrow V \) mapping \( (g^k, v_i) \rightarrow g^k v_i = v_{i+k} \) on basis vectors and extend \( v \rightarrow g^k v \) by linear maps.

Claim

This is an action

Proof

Condition 3 is trivial. Condition 1 is true by hypothesis.
As to 2: \( g^k(g^l v_i) = g^k(v_{i+l}) = v_{i+l+k} = g^{k+l}(v_i) = g^k g^l(v_i) \) holds for the basis vectors. But both sides of \( g(h(u)) = gh(u) \) are linear functions of these basis elements; if they agree on the basis elements then they agree on the entire vector space. \( \blacksquare \)

\( \mathbb{C}G \)-module

Let \( G \) be a group. A \( \mathbb{C}G \)-module is a vector space together with a \( G \)-action on it.

Remark

The ring \( \mathbb{C}G \) is called the group algebra such that \( \mathbb{C}G \)-modules as we define them are the “same” as modules over \( \mathbb{C}G \) in the sense of ring theory. Hence \( \mathbb{C}G \) has no meaning for this course, but \( \mathbb{C}G \)-modules do have meaning.

\( \mathbb{C}G \)-Homomorphism

Let \( V, W \) be \( \mathbb{C}G \)-modules. A \( \mathbb{C}G \) homomorphism is a linear map \( f: V \rightarrow W \) such that \( g(f(v)) = f(g(v)) \) for all \( g \in G \) and \( v \in V \)

Example 69

Let \( G = C_2 = \{ 1, g \} \) take \( V = \mathbb{C}^2 \) and \( W = \mathbb{C} \). Make \( V, W \) into \( \mathbb{C}G \)-modules by \( g(x, y) = (y, x) \) and \( g(x) = -x \). It is clear that this makes \( V \) and \( W \) into \( \mathbb{C}G \)-modules. Define \( f: V \rightarrow W \) by \( f(x, y) = x - y \). This is a \( \mathbb{C}G \)-homomorphism because
\[
g(f(x, y)) = g(x - y) = y - x = f(y, x) = f(g(x, y))
\]
4.2 Representations afforded by \( \mathbb{C}G \)-modules

**Reminder From Linear Algebra**

Let \( V \) be a vector space with basis \( A = (v_1, ..., v_m) \) and \( W \) a vector space with basis \( B = (w_1, ..., w_n) \). To a linear map \( f: W \to V \) as associate a matrix \( \langle A, f, B \rangle = (c_{ij}) \) by \( f(w_i) = \sum c_{ij}v_j \). Then \( f \to \langle A, f, B \rangle \) is a bijection from \( \text{Hom}(V, W) := \{ \text{linear maps } W \to V \} \) to \( M_{m \times n}(\mathbb{C}) \) and:

1. \( \langle A, f, B \rangle \langle B, g, C \rangle = \langle A, f \circ g, C \rangle \) whenever this makes sense
2. If \( A \) is the standard basis of \( \mathbb{C}^n \) and \( f: \mathbb{C}^n \to \mathbb{C}^n \) then \( f(v) = \langle A, f, A \rangle \cdot v \) (the \( \cdot \) here represented matrix multiplication).

**Notation**

If \( V \) is a \( \mathbb{C}G \)-module and \( g \in G, x \in V \) then \( t^V = t_g: V \to V \) is the linear map defined by \( t_g(x) = g(x) \) for all \( x \in V \).

**Summary:** \( \mathbb{C}G \)-modules and representations are the same thing.

**Lemma 71**

Let \( V \) be a \( \mathbb{C}G \)-module with basis \( A \). Define \( \rho: G \to GL(n, \mathbb{C}) \) (where \( n = \dim V < \infty \)) by \( \rho(x) = \langle A, t^V_x , A \rangle \). Then \( \rho \) is a representation of \( G \).

**Proof**

Firstly \( t_g t_h = t_{gh} \) for all \( g, h \in \mathbb{C} \) because:

\[
t_g t_h(x) = t_g(h \cdot x) = g \cdot (h \cdot x) = gh \cdot x = t_{gh}(x) \quad \forall x \in V
\]

Also \( \rho(g) \rho(h) = \rho(gh) \) for all \( g, h \in G \) because:

\[
\rho(g) \rho(h) = \langle A, t_g, A \rangle \langle A, t_h, A \rangle = \langle A, t_g t_h, A \rangle = \langle A, t_{gh}, A \rangle = \rho(gh)
\]

Next, we use that \( 1x = x \) for all \( x \in V \). Then

\( t_1 = id_V \) so \( \rho(1) = I_n \) so for all \( g \in G, \rho(g) \rho(g^{-1}) = \rho(gg^{-1}) = \rho(1) = I_n \) so for all \( g \in G, \rho(g) \) is invertible with inverse \( \rho(g)^{-1} = \rho(g^{-1}) \).

**Representation afforded by \( (V, A) \)**

Given a (finite dimensional) vector space \( V \) with basis \( A \) and \( \dim V = n \). The representation in Lemma 71 \( \rho: G \to GL(n, \mathbb{C}) \) defined by mapping \( \rho(x) = \langle A, t^V_x , A \rangle \) is the representation afforded by \( (V, A) \).

**Lemma 73**

Every representation is afforded by some pair \( (V, A) \) where \( V \) is a \( \mathbb{C}G \)-module and \( A \) is a basis.

**Proof**

Let \( \rho: G \to GL(n, \mathbb{C}) \) a representation. Put \( V = \mathbb{C}^n \). For \( g \in G \) and \( x \in \mathbb{C}^n \), define \( g \cdot x = \rho(g) \cdot x \) where \( \rho(g) \in GL(n, \mathbb{C}) \subset \mathbb{C}^n \).

**Claim**

This is an action of \( G \) on \( \mathbb{C}^n \).
Proof
For all \( x \in V, g \cdot (h \cdot x) := g(\rho(h) \cdot x) = \rho(g)\rho(h) \cdot x = \rho(gh)x = (gh) \cdot x \) and \( 1_G x = \rho(1) \cdot x = l_n \cdot x = x \). □

So \( V = \mathbb{C}^n \) is now a \( CG \)-module. Let \( A \) be the standard basis of \( \mathbb{C}^n = V \). Then by Lemma 71, \((V, A)\) gives rise to some representation \( \sigma \) where \( \sigma(g) = (A, t^V_g, A) \). Then \( \rho(g) \cdot x = g x = t_g(x) \) so \( \rho(g) = (A, t_g, A) = \sigma(g) \). So \( \rho \) is afforded by \((V, A)\). □

Lemma 74
The representations afforded by \((V, A)\) and \((V, B)\) are equivalent.

Proof
Let \( \rho \) and \( \sigma \) be the representations afforded by \((V, A)\) and \((V, B)\) respectively. Put \( T = \langle A, id_V, B \rangle \), the matrix of the identity with respect to \( A \) and \( B \). For all \( g, h \in G \) we have
\[
T \sigma(g) T^{-1} = (A, id_V, B)(B, t_g, B)(B, id_V, A) = (A, t_g, A) = \rho(g)
\]
Hence \( \rho \) and \( \sigma \) are equivalent. □

Lemma 75
The representations afforded by \((V, A)\) and \((W, B)\) are equivalent if and only if \( V \cong W \).

Proof
[⇒] Let \( \rho \) be the representation afforded by \((V, A)\) and \( \sigma \) by \((W, B)\). We know they are equivalent so there exists \( T \in GL(n, \mathbb{C}) \) so that \( \sigma(g) = T \rho(g) T^{-1} \) for all \( g \in G \). Hence there exists a linear map \( f: V \to W \) such that \( T = (B, f, A) \). Note that \( f \) is bijective since \( T \) is invertible. Then for all \( g \in G \)
\[
\langle B, t^W_g, B \rangle = \sigma(g) = T \rho(g) T^{-1} = \langle B, f, A \rangle (A, t^V_g, A)(A, f^{-1}, B) = \langle B, f t^V_g f^{-1}, B \rangle
\]
That is \( t^W_g f = f t^V_g \). Thus \( g(fv) = f(gv) \) for all \( v \in V \). This shows that \( f \) is a homomorphism of \( CG \)-modules. It is an isomorphism because \( f \) is bijective.

[⇐] Let \( f: V \to W \) be the isomorphism of \( CG \)-modules. Then \( g(fv) = f(gv) \) for all \( v \in V \) and \( g \in G \) so \( t^W_g f = f t^V_g \) so let \( T \) be the invertible matrix corresponding to its linear map. Then
\[
\sigma(g) = \langle B, t^W_g, B \rangle = \langle B, f t^V_g f^{-1}, B \rangle = \langle B, f, A \rangle (A, t^V_g, A)(A, f^{-1}, B) = T \rho(g) T^{-1}
\]
Hence \( \sigma \) and \( \rho \) are equivalent. □

Intertwiner
\( T \) is an intertwiner from \( \sigma \) to \( \rho \) if \( \rho(x) T = T \sigma(x) \) for all \( x \in G \).

4.3 Submodules
Submodules
A submodule of a \( CG \)-module \( V \) is a subspace \( W \subset V \) such that \( gW \subset W \) for all \( g \in G \).

Example
Let \( C_\infty = \langle g \rangle \) act on \( \mathbb{C}^2 \) by the formula \( g(x, y) = (x + y, y) \). Then we claim \( \mathbb{C} \cdot (1, 0) \) is the only 1-dimensional submodule of \( \mathbb{C}^2 \).
Observe \( g(1,0) = (1,0) \) so it is indeed a submodule. Consider any 1-dimensional submodule of the form \( \mathbb{C}(a, 1) \). Then \( g(a, 1) = (a + 1,1) \) which is not in \( \mathbb{C} \cdot (a, 1) \) so we get a contradiction.

**Simple Submodule**

A \( \mathbb{C}G \)-module \( V \) is said to be simple if it has no submodules other than 0 and itself.

**Example**

In particular, every 1-dimensional \( \mathbb{C}G \)-module is simple.

**Internal Direct sums**

Let \( V \) be a vector space and \( X, Y \subset V \) subspaces. We say \( V \) is an internal direct sum \( X \oplus Y = V \) if the following equivalent properties hold:

1. Every element of \( V \) can be written uniquely as \( x + y \) where \( x \in X \) and \( y \in Y \)
2. \( X \cap Y = 0 \) and \( X + Y := \{ x + y : x \in X, y \in Y \} = V \)
3. There exists a basis \( A \) of \( X \) and a basis \( B \) of \( Y \) such that \( A \cap B = \emptyset \) and \( A \cup B \) is a basis of \( V \)

Furthermore, if \( \dim V < \infty \) then the following two properties are also equivalent:

4. \( X \cap Y = 0 \) and \( \dim V = \dim X + \dim Y \)
5. \( X + Y = V \) and \( \dim V = \dim X + \dim Y \)

**External Direct Sums**

The External Direct Sum of \( X \) and \( Y \) is the set

\[
X \times Y = \left( X \times \{0\} \right) \oplus \left( Y \times \{0\} \right)
\]

In practice we assume any two vector spaces \( X \) and \( Y \) have a direct sum \( X \oplus Y \).

**Diagonal Sum/ Irreducible Representations**

1. Let \( \rho: G \to GL(n, \mathbb{C}) \) and \( \sigma: G \to GL(m, \mathbb{C}) \) be representations. The diagonal sum \( \rho \oplus \sigma \) is the \( (m + n) \) dimensional representation defined by

\[
(\rho \oplus \sigma)(x) = \begin{pmatrix} \rho(x) & 0 \\ 0 & \sigma(x) \end{pmatrix}
\]

2. A representation \( \rho: G \to GL(n, \mathbb{C}) \) is said to be irreducible if it is not equivalent to any representation of the form:

\[
\sigma(x) = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}^{k} \begin{pmatrix} * & * \\ k & l \end{pmatrix} \text{ for some } k, l > 0, \text{ for all } x
\]

**Claim**

The representation afforded by \((V, A)\) is a diagonal sum of two representations of dimension >0 if and only if there exist non-zero submodules \( X, Y \subset V \) such that \( V = X \oplus Y \)

**Corollary**

The representation afforded by \((V, A)\) is irreducible if and only if \( V \) is simple.
**Dictionary**

<table>
<thead>
<tr>
<th><strong>CG-module</strong></th>
<th>Representation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CG-homomorphism</strong></td>
<td>Intertwiner</td>
</tr>
<tr>
<td><strong>Simple</strong></td>
<td>Irreducible</td>
</tr>
<tr>
<td><strong>Direct Sum</strong></td>
<td>Diagonal Sum</td>
</tr>
</tbody>
</table>

**Theorem 81 (Maschke)**
Let $G$ be a finite group, $V$ a finite dimensional $\mathbb{C}G$-module. For every submodule $W \subset V$ there exists a submodule $X \subset V$ such that $V = W \oplus X$.

In order to prove Maschke’s Theorem we need to digress into Inner Products. The proof will be given later.

**4.4 Inner Products**

**Inner Product**
An Inner Product or IP on a vector space $V$ is a map $V \times V \to \mathbb{C}$ mapping $(v, w) \to \langle v, w \rangle$ such that:

1. **Bilinearity**: $\langle au + bv, w \rangle = a \langle u, w \rangle + b \langle v, w \rangle$ for all $a, b \in \mathbb{C}$ and $u, v, w \in V$.
2. **Hermitian**: $\langle v, w \rangle = \overline{\langle w, v \rangle}$
3. **Positive Definite**: $\langle v, v \rangle > 0$ for all $v \in V \setminus \{0\}$

**Remarks:**
- By 2, $\langle v, v \rangle = \overline{\langle v, v \rangle}$ so $\langle v, v \rangle \in \mathbb{R}$ so the third condition makes sense.
- $\langle u, av + bw \rangle = a \langle u, v \rangle + b \langle u, w \rangle$ is a consequence of 1 and 2

**Claim**
Every finite dimensional vector space has an IP.

**Proof**
Let $e_1, ..., e_n$ be a basis and put 

$$\langle \sum_i a_i e_i, \sum_i b_i e_i \rangle = \sum_i a_i \overline{b_i}$$

It is then clear that this defines an inner product. ■

Conversely, every IP on a finite dimensional vector space is of this form; we won’t need this or prove it.

**Orthogonal Complement**
Let $V$ be a vector space with an inner product $\langle , \rangle$ and a subspace $W \subset V$. The orthogonal complement of $W$ is $W^\perp := \{ x \in V : \langle x, y \rangle = 0 \text{ for all } y \in W \}$

Note that $W^\perp \subset W$ is a subspace.
Lemma 85
Let $V$ be a finite dimensional vector space with an inner product $\langle , \rangle$ and let $W$ be any subspace. Then $V = W \oplus W^\perp$.

Proof
Let $\{w_1, ..., w_k\}$ be a basis of $W$. Let $x \in W \cap W^\perp$. Then $\langle x, x \rangle = 0$ so $x = 0$. Hence $W \cap W^\perp = 0$.

All we need to prove is that $\dim W + \dim W^\perp \geq \dim V$. Let $\{w_1, ..., w_k\}$ be a basis of $W$. Define $L: V \to \mathbb{C}^k$ by $L(v) = \begin{pmatrix} \langle v, w_1 \rangle \\ \langle v, w_2 \rangle \\ \vdots \\ \langle v, w_k \rangle \end{pmatrix}$.

Then $L$ is a linear map and $\ker L = W^\perp$ so $\dim W + \dim W^\perp = k + \dim W^\perp = k + \dim \ker L \geq \dim \text{im} L + \dim \ker L = \dim V$ ■

$G$-invariant Inner Products
Let $V$ be a $\mathbb{C}G$-module. An inner product $\langle , \rangle$ on $V$ is $G$-invariant if $\langle gv, gw \rangle = \langle v, w \rangle$ for all $v, w \in V$ and $g \in G$.

Proposition 87
Let $G$ be a finite group and $V$ a finite dimensional $\mathbb{C}G$-module. Then there exists a $G$-invariant inner product on $V$.

Proof
Let $\langle , \rangle_0$ be any inner product on $V$. For $v, w \in V$ define $\langle v, w \rangle = \sum_{g \in G} \langle gv, gw \rangle_0$

We claim that this is an inner product on $V$:

For any $a, b \in \mathbb{C}, u, v, w \in V$:

$\langle au + bv, w \rangle = \sum_{g \in G} \langle g(au + bv), gw \rangle_0 = \sum_{g \in G} \langle ag(u) + bg(v), gw \rangle_0$

$= \sum_{g \in G} ag(u), gw \rangle_0 + b \langle g(v), gw \rangle_0 = a \langle u, w \rangle + b \langle v, w \rangle$

For any $v, w \in V$:

$\langle v, w \rangle = \sum_{g \in G} \langle gv, gw \rangle_0 = \sum_{g \in G} \langle gw, gv \rangle_0 = \langle w, v \rangle$

For any $v \in V \setminus \{0\}$:

$\langle v, v \rangle = \sum_{g \in G} \langle gv, gv \rangle_0 \geq \langle v, v \rangle_0 > 0$

We now show that $\langle , \rangle$ is $G$-invariant. Let $h \in G, v, w \in V$. Then:

$\langle hv, hw \rangle = \sum_{g \in G} \langle g(hv), g(hw) \rangle_0 = \sum_{g \in G} \langle (gh)v, (gh)w \rangle_0 = \sum_{k \in G} \langle kv, kv \rangle_0 = \langle v, w \rangle$ ■
We are now able to prove Maschke’s Theorem:

**Theorem 81 (Maschke)**

Let $G$ be a finite group, $V$ a finite dimensional $\mathbb{C}G$-module. For every submodule $W \subset V$ there exists a submodule $X \subset V$ such that $V = W \oplus X$

**Proof**

Choose a $G$-invariant inner product $\langle , \rangle$ on $V$, which exists by Proposition 87. Put $X = W^T$. By Lemma 85 $V = W \oplus W^\perp$. It is left to prove that $W^\perp$ is a submodule.

Let $x \in W^\perp, y \in W$ and $g \in G$. Then $\langle gx, y \rangle = \langle g^{-1}gx, g^{-1}y \rangle$ because $\langle , \rangle$ is $G$-invariant. So $\langle gx, y \rangle = \langle x, g^{-1}y \rangle = 0$ because $x \in W^\perp$ and $g^{-1}y \in W$ because $W$ is a submodule. Hence $gx \in W^\perp$ so $gW \subset W$.

**Corollary 88**

Let $G$ be a finite group and $V$ a finite dimensional $\mathbb{C}G$-module. Then $V$ is a finite sum of simple submodules.

**Proof**

Let $n = \dim V$. We proceed by induction on $n$.

For $n = 0$, we are done. Let $n > 0$; if $V$ is simple we are done so suppose not. Then there are non-zero submodules $W, X \subset V$ by Maschke’s Theorem so that $V = W \oplus X$. Then in particular $\dim W < n$ and $\dim X < n$ so by induction hypothesis they are direct sums of simple submodules: $W = W_1 \oplus W_2 \oplus \ldots \oplus W_k$ and $X = X_1 \oplus \ldots \oplus X_l$ then $V = W_1 \oplus W_2 \oplus \ldots \oplus W_k \oplus X_1 \oplus \ldots \oplus X_l$ as required.
Chapter 5: Characters

For a matrix $A \in M_n(\mathbb{C})$ with $A = (a_{ij})_{ij}$ then the trace is $\text{tr}(A) = \sum_{i=1}^{n} a_{ii}$

Claim

Let $A, B, C \in M_n(\mathbb{C})$. Then:

1. $\text{tr}(AB) = \text{tr}(BA)$
2. If $A$ is invertible then $\text{tr}(ACA^{-1}) = \text{tr}(C)$

Proof

1. Write $A = (a_{ij})_{ij}$ and $B = (b_{ij})_{ij}$, then the $(i, i)$th entry of $AB$ is $\sum_{j=1}^{n} a_{ij}b_{ji}$ so
   $\text{tr}(AB) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij}b_{ji}$ which is symmetric in $A, B$ so $\text{tr}(AB) = \text{tr}(BA)$
2. Put $B = CA^{-1}$ in part 1. 

If $A$ is a basis of a finite dimensional vector space $V$ and $f : V \to V$ a linear map, we define $\text{tr}(f) = \text{tr}(A, f, A)$ [Note that this does not depend on the choice of basis because $(B, f, B) = (B, \text{id}, A)(A, f, A)(A, \text{id}, B)$ and then use part 2 of the previous claim to see $\text{tr}(A, f, A) = \text{tr}(B, f, B)$].

Character

Let $G$ be a group.

1. The character of a representation $\rho$ of $G$ is $\chi_{\rho} : G \to \mathbb{C}$ which maps $\chi_{\rho}(x) = \text{tr}(\rho(x))$
2. The character of $G$ is the character of some representation of $G$
3. The character of a finite-dimensional $\mathbb{C}G$-module $V$ is $\chi_{\rho} : G \to \mathbb{C}$ mapping $x \to \text{tr}(t_{x}^{y})$

Note that if $(V, A)$ affords $\rho$ then $\chi_{\rho} = \chi_{\rho}$.

Proposition 93

Let $\rho, \sigma$ be representations of $G$. If $\rho \sim \sigma$ then $\chi_{\rho} = \chi_{\sigma}$

Proof

Let $T \in GL(n, \mathbb{C})$ such that $\sigma(x) = T\rho(x)T^{-1}$ for all $x \in G$. Then $\chi_{\sigma}(x) = \text{tr}(\sigma(x)) = \text{tr}(T\rho(x)T^{-1}) = \text{tr}(T\rho(x)) = \chi_{\rho}(x)$. 

Remark

This is why characters are so useful; they are independent of equivalence class of representations. Later we’ll prove the converse: $\chi_{\rho} = \chi_{\sigma} \Rightarrow \rho \sim \sigma$

In particular, note that $\chi_{\rho \circ \sigma} = \chi_{\rho} + \chi_{\sigma}$

Proposition 95

Let $\chi$ be a character of a group $G$. Then $\chi(gxg^{-1}) = \chi(x)$ for all $g, x \in G$.

Proof

Say $\chi = \chi_{\rho}$. Then $\chi(gxg^{-1}) = \chi_{\rho}(gxg^{-1}) = \text{tr}(\rho(gxg^{-1})) = \text{tr}(\rho(g)\rho(x)\rho(g^{-1})) = \text{tr}(\rho(x)) = \chi_{\rho}(x) = \chi(x)$. 

5.1 Reminder on Conjugacy Classes

Two elements \(x, y\) in a group \(G\) are conjugate if there exists \(g \in G\) with \(gxg^{-1} = y\). The relation \(x \sim y\) if \(x\) and \(y\) are conjugate is an equivalence relation with the equivalence classes are called conjugacy classes.

Put \(x^g = g^{-1}xg\) then \(x^G = \{x^g : g \in G\}\) so \(x^G\) is the conjugacy class of \(x\) in \(G\).

Conjugacy Classes

Define \(K(G) := \{\)conjugacy classes in \(G\}\) and \(k(G) := |K(G)|\).

Easy Exercises:

Let \(g, h, x, y \in G\) then it is clear that:

1. \((xy)^g = x^gy^g\); that is there exists an automorphism \(G \rightarrow G\) mapping \(x \rightarrow x^g\)
2. \((x^g)^h = x^{gh}\); that is conjugation defines an action of \(G\) on itself.
3. Let \(G\) be a group and \(m \in \mathbb{Z}\) then \((x^g)^m = (x^m)^g\)
4. Let \(C \in K(G)\). Define \(C^m := \{x^m : x \in C\}\). Then \(C^m \in K(G)\)

Centre of a Group

The centre of a group \(G\) is the set \(Z(G) := \{a \in G : ag = ga \ \forall g \in G\}\) so \(a^G = \{a\} \Leftrightarrow a \in Z(G)\)

If \(a \in Z(G)\) then \(a\) is called central.

Lemma 95.1

Let \(A\) be a generating set of a group \(G\) and \(C \subseteq G\). For \(g \in G\), define \(C^g := \{x^g : x \in C, g \in G\}\).

The following are equivalent:

1. \(C^g = C\) for all \(g \in G\)
2. \(C^a = C\) for all \(a \in A\)
3. For every \(D \in K(G)\), either \(D \subseteq C\) or \(D \cap C = \emptyset\)

Example 96

Recall that \(D_{2n} = \langle r, s | r^n, s^2, (rs)^2 \rangle\). Prove that if \(n\) is odd then the conjugacy classes of \(D_{2n}\) are \(\{1\}, \{r^m, r^{-m}\}\) where \(1 \leq m \leq (n-1)/2\) and \(\{sr^k : k \in \mathbb{Z}\} = :E\)

Solution

\(\{1\}\) is always in \(K(G)\). Now \(r^s = s^{-1}rs = srs = r^{-1}\) so \(C := \{r, r^{-1}\}\) is contained in a conjugacy class by Lemma 95.1. Then \(C \in K(D_{2n})\) as soon as \(x^r, x^s \in C\) for all \(x \in C\). Well \(r^r = r\) and \((r^{-1})^r = r^{-1}\) and \(r^s = r^{-1}\) and \((r^{-1})^x = r\) so \(C\) is a conjugacy class. By the Easy exercise 4 above, \(C^m\) is also a conjugacy class; they are all distinct if \(1 \leq m \leq (n-1)/2\).

We have left to prove: Any two elements of \(E\) are conjugate.

\((sr^k)^r = r^{-1}sr^{k+1} = sr^{k+2}\)

So \(sr^k \sim sr^{k+2} \sim sr^{k+4} \sim \ldots\) but \(r^n = 1\) and \(n\) odd so all elements of \(E\) are conjugate.

Example

By the Universal Property, it is easy to show that there exists a unique representation \(\rho : D_6 \rightarrow GL(2, \mathbb{C})\) mapping \(\rho(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\) and \(\rho(r) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}\). We want to compute \(\chi_\rho\). By
Proposition 95, it is sufficient to compute $\chi_\rho(x)$ for only one $x$ from each conjugacy class. For example, $K(D_6) = \{[1], \{r, r^{-1}\}, \{s, sr, sr^{-2}\}\}$ hence we construct the table:

<table>
<thead>
<tr>
<th>$x$</th>
<th>1</th>
<th>$r$</th>
<th>$s$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\chi_\rho(x)$</td>
<td>2</td>
<td>$-1$</td>
<td>0</td>
</tr>
</tbody>
</table>

$\mathbb{C}(G)$
For a group $G$ denote the set of functions $G \to \mathbb{C}$. We make it into a vector space by pointwise operations:

$$(ap + bq)(x) = ap(x) + bq(x), \quad \forall a, b \in \mathbb{C}, p, q \in \mathbb{C}(G), x \in G$$

For $p, q \in \mathbb{C}(G)$, define $(p, q)_\mathbb{C} := \frac{1}{|G|} \sum_{x \in G} p(x)\overline{q(x)}$

Lemma 99

$(\cdot, \cdot)_\mathbb{C} : \mathbb{C}(G) \times \mathbb{C}(G) \to \mathbb{C}$ is an inner product.

Proof

It is a simple matter of checking the conditions in the definition. ■

Class Function

A class function on a group $G$ is a function $f : G \to \mathbb{C}$ such that $f(gxg^{-1}) = f(x)$ for all $g, x \in G$; that is $f$ is constant on the conjugacy classes. Let $CF(G) := \{\text{class functions on } G\} \subset \mathbb{C}(G)$ so $\chi_\rho \in CF(G)$ by Proposition 95.

Remark

$CF(G)$ is a subspace of $\mathbb{C}(G)$ of dimension $k(G)$.

Lemma 101

Let $\rho$ be a representation of a finite group $G$ and $g \in G$.

1. $\chi_\rho(1) = \deg \rho$
2. $\chi_\rho(g)$ is a sum of roots of unity.
3. $\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$

Proof

1. $\chi_\rho(1) = \text{tr}(\rho(1)) = \text{tr}(I_{\deg \rho}) = \deg \rho$
2. Let $\omega_1, ..., \omega_n$ be the eigenvalues of $\rho(g)$. Now $|G| < \infty$ so $|g| < \infty$ say $g^r = 1$ for $r > 0$. Then $\omega_i^r = 1$ for all $i$; that is $\omega_i$ is a root of unity for all $i$. Therefore $\chi_\rho(g) = \omega_1 + \cdots + \omega_n$ is a sum of roots of unity.
3. The eigenvalues of $\rho(g^{-1})$ are $\omega_1^{-1}, ..., \omega_n^{-1}$ which are $\overline{\omega_1}, ..., \overline{\omega_n}$ because $\omega_i^r = 1$ for all $i$. So $\chi_\rho(g^{-1}) = \text{tr}(\rho(g^{-1})) = \overline{\omega_1} + \cdots + \overline{\omega_n} = \overline{\omega_1 + \cdots + \omega_n} = \text{tr}(\rho(g)) = \overline{\chi_\rho(g)}$ ■

Degree of a Character

The degree of a character $\chi$ is $\chi(1)$. So $\deg \chi_\rho = \deg \rho$ by part 1 of Lemma 101.
Irreducible Character
An irreducible character is the character of some irreducible representation. Let \( I(G) := \{\text{irreducible characters of } G\} \).

5.2 Schur’s Lemma and Orthogonality

Claim
Let \( L: V \to W \) be a \( \mathbb{C}G \)-homomorphism. Then \( \ker L \subset V \) and \( \text{im } L \subset W \) are submodules.

Proof
Let \( v_1, v_2 \in \ker L \). Then for \( a, b \in \mathbb{C} \) we have \( L(v_1) = 0 = L(v_2) \). Then \( L(av_1 + bv_2) = aL(v_1) + bL(v_2) = 0 \) so \( av_1 + bv_2 \in \ker L \).

Let \( w_1, w_2 \in \text{im } L \). Then \( w_1 = L(v_1) \) and \( w_2 = L(v_2) \) for some \( v_1, v_2 \in V \). Then \( aw_1 + bw_2 = aL(v_1) + bL(v_2) = L(av_1 + bv_2) \) so \( aw_1 + bw_2 \in \text{im } L \).

Let \( g \in G \). Then \( L(gv_1) \) is in \( \text{im } L \) so \( L(gv_1) = gL(v_1) \) so \( g \) is in \( \text{im } L \). Take \( v \in \ker L \). Then \( L(gv) = gL(v) = g(0) = 0 \) so \( g \) is in \( \ker L \).

Hence \( \ker L \) and \( \text{im } L \) are submodules.

Theorem 102 (Schur’s Lemma)
Let \( V, W \) be simple \( \mathbb{C}G \)-modules. Then:

1. Every \( \mathbb{C}G \)-homomorphism \( L: V \to W \) is either 0 or a \( \mathbb{C}G \)-isomorphism.
2. Every \( \mathbb{C}G \)-homomorphism \( L: V \to V \) is scalar multiplication by some complex number.

Proof
1. Suppose \( L \neq 0 \). Then \( \ker L \subset V \) is a submodule of \( V \) but not \( V \) so \( \ker L = 0 \) hence \( L \) is injective. Similarly, \( \text{im } L \subset W \) is a submodule of \( W \) but not 0 so \( \text{im } L = W \) hence \( L \) is surjective.

2. Note \( V \neq 0 \) because \( V \) is simple. Let \( v \in V \) be an eigenvector with eigenvalue \( \lambda \in \mathbb{C} \). Put \( M: V \to V \) by \( M(x) = Lx - \lambda x \). It is clear that \( M \) is a \( \mathbb{C}G \)-homomorphism since it is a linear combination of \( \mathbb{C}G \)-homomorphisms. But \( M(v) = Lv - \lambda v = 0 \) so \( M \) is not injective. Hence by part 1, \( M \) is constantly 0 so \( Lx = \lambda x \) for all \( x \in V \) hence \( L \) is scalar multiplication by scalar \( \lambda \).

Lemma 103
Let \( \rho, \sigma \) be representations of a finite group \( G \) of degrees \( n, m \) respectively. Take \( A \subset M_{m \times n}(\mathbb{C}) \) and \( T = \sum_{h \in G} \sigma(h^{-1})A\rho(h) \). Then \( T \) is an intertwiner.

Proof
We must prove that \( \sigma(x)T = T\rho(x) \) for all \( x \in G \). Well
\[
\sigma(x)T = \sigma(x) \sum_{h \in G} \sigma(h^{-1})A\rho(h) = \sum_{h \in G} \sigma(xh^{-1})A\rho(h) = \sum_{k \in G} \sigma(k^{-1})A\rho(kx) = \sum_{k \in G} \sigma(k^{-1})A\rho(k) \rho(x) = T\rho(x).
\]
Retranslating this Lemma in terms of \( \mathbb{C}G \)-modules, it says “for a linear map \( L:V \to W \) define another linear map \( L':V \to W \) by \( L'(x) = \sum_{g \in G} (t_g^{W} \circ L \circ t_g^{-1}) (x) \). Then \( L' \) is a \( \mathbb{C}G \)-homomorphism.”

If \( A \) is a matrix let \( A_{ij} \) denote its entry in position \((i, j)\). Let \( n \) be the number of rows of \( A \) which equals the number of rows of \( B \). Then

\[
(AB)_{ij} = \sum_{k=1}^{n} A_{ik}B_{kj} \quad \text{likewise} \quad (ABC)_{ij} = \sum_{s,t} A_{is}B_{st}C_{tj}
\]

Theorem 105 (Orthogonality for Characters)

Let \( \rho, \sigma \) be irreducible representations of a finite group \( G \) with \( \langle p, q \rangle_G = \frac{1}{|G|} \sum_{g \in G} \rho(g)q(g) \).

Then:

1. \( \rho \circ \sigma \Rightarrow (\chi_\rho, \chi_\sigma)_G = 0 \)
2. \( (\chi_\rho, \chi_\rho)_G = 1 \)

Proof

Let \( E(i,j) \) be the \((\deg \sigma) \times (\deg \rho)\) matrix with a 1 in position \((i, j)\) and zeroes elsewhere. Then \( (AE(i,j)B)_{ij} = \sum_{s,t} A_{is}E(i,j)_{st}B_{tj} = A_{ii}B_{jj} \).

Put \( T(i,j) = \sum_{g \in G} \sigma(g^{-1})E(i,j)\rho(g) \) which is an intertwiner from \( \rho \) to \( \sigma \) by Lemma 103.

Moreover, \( \sum_{ij} T(i,j)_{ij} = \sum_{ij} \sum_{g \in G} (\sigma(g^{-1})E(i,j)\rho(g))_{ij} = \sum_{g \in G} \sum_{ij} (\sigma(g^{-1})E(i,j)\rho(g))_{ij} = \sum_{g \in G} \sum_{ij} (\sigma(g^{-1})\rho(g))_{ij} = \sum_{g \in G} \sum_{ij} (\sigma(g^{-1})\rho(g))_{ij} = \sum_{g \in G} \sum_{ij} (\sigma(g^{-1})\rho(g))_{ij} = |G|(\chi_\rho, \chi_\sigma)_G \)

1. \( T(i,j) : \rho \to \sigma \) is an intertwiner between non-equivalent irreducible modules then by Schur’s Lemma \( T(i,j) = 0 \) so the above shows that \( |G|(\chi_\rho, \chi_\sigma)_G = 0 \Rightarrow (\chi_\rho, \chi_\sigma)_G = 0 \)
2. \( T(i,j) : \rho \to \rho \) is an intertwiner so by Schur’s Lemma \( T(i,j) \) is a scalar matrix \( T(i,j) = \lambda_{ij}I_n \) for \( \lambda_{ij} \in \mathbb{C} \) and \( n = \deg \rho \). Then

\[
n|G|(\chi_\rho, \chi_\rho)_G = n \sum_{ij} (T(i,j)_{ij}) = n \sum_{ij} (\lambda_{ij}I_n)_{ij} = n \sum_{i} (\lambda_{ii}I_n)_{ii} = n \sum_{i} \lambda_{ii}
\]

\[
= tr \sum_{i} T(i,i) = tr \sum_{i} \sum_{g \in G} \rho(g^{-1})E(i,i)\rho(g)
\]

\[
= tr \sum_{i} \sum_{g \in G} \rho(g^{-1})E(i,i)\rho(g) = tr \sum_{g \in G} \rho(g^{-1}) \sum_{i} E(i,i)\rho(g)
\]

\[
= tr \sum_{g \in G} \rho(g^{-1})\rho(g) = n|G|
\]

Hence \( (\chi_\rho, \chi_\rho)_G = 1 \)

Corollary 108

Let \( G \) be a finite group. Then \( G \) has at most \( k(G) \) non-equivalent irreducible representations.
Proof
Suppose not. Take $\rho_1, ... , \rho_s$ to be non-equivalent irreducible representations with $s > k(G)$. But $k(G) = \dim CF(G)$ and $\chi_i := \chi_{\rho_i} \in CF(G)$ for all $i$, so the $\chi_i$ are linearly dependent, say $\sum_i a_i \chi_i = 0$ and not all $a_i = 0$ (say $a_k \neq 0$). Then

$$0 = (0, \chi_k) = \left( \sum_i a_i \chi_i, \chi_k \right) = \sum_i a_i \chi_i, \chi_k = a_k$$

Contradiction. ■

Later we will prove the converse: $k(G) =$ the number of non-equivalent irreducible representations.

Theorem 109
Let $\rho_1, ... , \rho_s$ be a maximal set of non-equivalent irreducible representations of a finite group $G$. Then for each $i$ there exists a unique $n_i \geq 0$ such that $\rho = n_1 \rho_1 \oplus ... \oplus n_s \rho_s$ where $n_i \rho_i$ is the diagonal sum of $n_i$ copies of $\rho_i$.

Moreover, $n_i = \left( \chi_\rho, \chi_{\rho_i} \right)_G$ and is called the multiplicity of $\rho_i$ in $\rho$.

Proof
Existence:
This follows immediately from Corollary 88.

Uniqueness:
Assume $\rho \sim n_1 \rho_1 \oplus ... \oplus n_s \rho_s$ and write $\chi_i = \chi_{\rho_i}$. Then

$$\left( \chi_\rho, \chi_{\rho_i} \right)_G = \left( \sum_i n_i \chi_{\rho_j}, \chi_{\rho_i} \right)_G = \sum_i n_i \chi_{\rho_j}, \chi_{\rho_i} = n_i$$

Corollary 110
Let $\rho$ be a representation of a finite group $G$. Then $\rho$ is irreducible if and only if $\left( \chi_\rho, \chi_\rho \right)_G = 1$

Proof
[⇒] This was proved in Theorem 105 (Orthogonality of Characters).

[⇐] Write $\rho \sim n_1 \rho_1 \oplus ... \oplus n_s \rho_s$ with all $\rho_i$ non-equivalent. Then $1 = \left( \chi_\rho, \chi_\rho \right)_G = \left( \sum_i n_i \chi_{\rho_i}, \sum_i n_i \chi_{\rho_i} \right)_G = \sum_i n_i \chi_{\rho_i}, \chi_{\rho_i} = \sum_i n_i^2$ and $n_i \in \mathbb{N} \cup \{0\}$. So $n_i = 0$ for all $i$ except one of them, say $n_k = 1$. Then $\rho \sim \rho_k$ and hence $\rho$ is irreducible. ■
Chapter 6: Regular Representations

Let $G$ be a group. Let $V^{reg} = V^{reg}(G)$ be a vector space with basis $\{e_x : x \in G\}$ (a copy of $G$). So every element of $V^{reg}(G)$ can be written uniquely as a linear combination $\sum_{x \in G} a_x e_x$ for $a_x \in \mathbb{C}$, with only finitely many $a_x \neq 0$.

Define $G \times V^{reg} \to V^{reg}$ mapping $(g, \sum_x a_x e_x) \mapsto g(\sum_x a_x e_x) := \sum_x a_x e_{gx}$. In particular $g(e_x) = e_{gx}$. This is clearly an action: $1(\sum_x a_x e_x) = \sum_x a_x e_{g x}$ and $g(h(\sum_x a_x e_x)) = g(\sum_x a_x e_{hx}) = \sum_x a_x e_{ghx} = (gh)(\sum_x a_x e_x)$.

So $V^{reg}$ is a $\mathbb{C}G$-module called the regular module. From now on, assume $G$ is finite.

Choosing a total ordering on $A = \{e_x : x \in G\}$, the representation afforded by $(V^{reg}, A)$ is called the regular representation $\rho^{reg}$. Its character $\chi^{reg}$ is called the regular character.

Example 112

Take $G = C_2 \times C_2 = \{1, x, y, xy\}$ let $A = (e_1, e_2, e_y, e_{xy})$ then $\rho^{reg}(x) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ and $\rho^{reg}(y) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ similarly, $\rho^{reg}(xy) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$

Lemma 114

Let $G$ be a finite group. Then $\chi^{reg}(1) = |G|$ and $\chi^{reg}(g) = 0$ for all $g \in G \setminus \{1\}$.

Proof

Firstly, $\chi^{reg}(1) = \dim V^{reg} = |G|$.

Let $g \in G \setminus \{1\}$. Then any nonzero entry of $\rho^{reg}(g)$ is in position $(gx, x)$. But this is not on the diagonal as $g \neq 1$ so the diagonal consists of zeroes; hence $\chi^{reg}(g) = \text{tr} \rho^{reg}(g) = 0$. □

Lemma 115

Let $\chi_1, \ldots, \chi_s$ be the irreducible characters of a finite group $G$. Put $d_i = \chi_i(1)$. Then $\chi^{reg} = \bigoplus_{i=1}^s d_i \chi_i$.

Proof

Let $n_i = (\chi^{reg}, \chi_i)_G$. By Theorem 109, we have $\chi^{reg} = \bigoplus_{i=1}^s n_i \chi_i$.

Again using Lemma 114 above, $\chi^{reg}(g) = 0$ unless $g = 1$, so:

$$n_i = (\chi^{reg}, \chi_i)_G = \frac{1}{|G|} \sum_{g \in G} \chi^{reg}(g) \chi_i(g^{-1}) = \frac{1}{|G|} \chi^{reg}(1) \chi_i(1) = \chi_i(1) = d_i \quad \Box$$

Corollary 117

Let $\chi_1, \ldots, \chi_s$ be the irreducible characters of a finite group $G$, and $d_i = \chi_i(1)$. Then $|G| = d_1^2 + \cdots + d_s^2$.

Proof

By Lemmas 114 and 115, we have $|G| = \chi^{reg}(1) = \sum_{i=1}^s d_i \chi_i(1) = \sum_{i=1}^s d_i^2$. □
Theorem 118
Let \( I(G) = \{ \text{irreducible character of } G \} \). Then \( |I(G)| = k(G) \)

Proof
Let \( s = |I(G)| \) and \( k = k(G) \). We know that \( s \leq k \) by Theorem 108. We need to prove that \( s \geq k \).

Recall \( I(G) \subseteq CF(G) \) and \( \dim CF(G) = k \) and \( CF(G) \) has an inner product (the one restricted from \( \mathbb{C}G \)). It is sufficient to prove: for any \( f \in CF(G) \) and \( f \perp I(F) \) (that is \( (f, \rho)_G = 0 \) \( \forall \rho \in I(G) \)) implies \( f = 0 \).

Let \( \rho \) be a representation of \( G \) and define \( \rho^f = \sum_{g \in G} f(g)\rho(g^{-1}) \).

Claim
\( \rho^f \) is an intertwiner; that is \( \rho^f \rho(x) = \rho(x)\rho^f \) for all \( x \in G \).

Proof
We use the fact that \( g \to xgx^{-1} \) is a bijection from \( G \to G \) and \( f \in CF(G) \):

\[
\rho(x)^f \rho(x)^{-1} = \rho(x) \left( \sum_{g \in G} f(g)\rho(g^{-1}) \right) \rho(x^{-1}) = \sum_{g \in G} f(g)\rho(xgx^{-1}x^{-1}) \\
= \sum_{g \in G} f(x^{-1}hx)\rho(h^{-1}) = \sum_{g \in G} f(h)\rho(h^{-1}) = \rho^f \]

Let \( \rho \) be an irreducible representation, so \( \rho^f \) is an intertwiner between irreducible \( \rho \) and itself. By Schur’s Lemma, \( \rho^f \) is a scalar multiple \( \rho^f = \alpha I_n \) for some \( \alpha \in \mathbb{C} \) and \( n = \deg \rho \). To find \( \alpha \):

\[
n \alpha = tr(\alpha I_n) = tr(\rho^f) = tr \left( \sum_{g \in G} f(g)\rho(g^{-1}) \right) = \sum_{g \in G} f(g)tr(\rho(g^{-1})) = \sum_{g \in G} f(g)\chi_{\rho}(g) \\
= |G|(f, \chi_{\rho})_G
\]

Now, \( f \perp \chi_{\rho} \) by assumption, because \( \chi_{\rho} \in I(G) \). Hence \( n \alpha = |G|(f, \chi_{\rho})_G = 0 \) and so \( \alpha = 0 \).

Observe that if \( \rho \) is not irreducible, we can write \( \rho \sim n_1 \rho_1 \oplus \ldots \oplus n_s \rho_s \) for some irreducible \( \rho_i \) and \( \rho \to \rho^f \) is a linear map so by the above argument;

\[
\rho^f = n_1 \rho_1^f \oplus \ldots \oplus n_s \rho_s^f = 0 + \cdots + 0
\]

Hence \( \rho^f = 0 \) for all representations \( \rho \). In particular it is true for the case \( \rho = \rho^{reg} \). Then

\[
0 = (\rho^{reg})^f = \sum_{g \in G} f(g)\rho^{reg}(g^{-1})
\]

Now, the matrices \( \rho^{reg}(g) \) for \( g \in G \) are linearly independent (look at the first row). Hence \( f = 0 \).
**Linear Character:**
A Character $G$ is linear if it has degree 1.

**Theorem 119**
A finite group $G$ is abelian if and only if all its irreducible characters are linear.

**Proof**
Let $k = k(G) = |I(G)|$. Let $\chi_1, \ldots, \chi_k$ be the irreducible characters of $G$ and $d_i = \chi_i(1)$. By Corollary 117 we have $|G| = d_1^2 + \cdots + d_k^2$ and $d_i \in \mathbb{N}$. Therefore:

$$G \text{ is abelian } \iff |G| = k = \text{ number of conjugacy classes } \iff d_i = 1 \text{ for all } i$$
Chapter 7: Character Tables

7.1 Definition and first Examples
Let $G$ be a finite group. If $C \in K(G)$ and $g \in C$, for $f \in CF(G)$, we often write $f(C) := f(g)$. Let $C_1, \ldots, C_k$ be the conjugacy classes of $G$, and suppose $C_1 = \{1\}$. Let $\chi_1, \ldots, \chi_k$ be the irreducible characters and $\chi_1 = 1_G$ the trivial character; $\chi_1(x) = 1$ for all $x$.

The matrix \( \left( \chi_i(C_j) \right)_{ij} \) is the character table of $G$.

There are non-isomorphic groups with the same character table; $D_8$ and $Q_8$ are such examples.

Example 122
Let $G = \langle c | c^4 \rangle$. By Theorem 119, $G$ has four irreducible linear characters $\chi_1, \ldots, \chi_4$. Then putting $c = \sqrt{-1}$ we have:

<table>
<thead>
<tr>
<th></th>
<th>$C_2$</th>
<th>$C_3$</th>
<th>$C_4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\chi_1$</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$\chi_2$</td>
<td>$c$</td>
<td>$c^2$</td>
<td>$c^3$</td>
</tr>
<tr>
<td>$\chi_3$</td>
<td>$c^2$</td>
<td>$c^4$</td>
<td>$c^6$</td>
</tr>
<tr>
<td>$\chi_4$</td>
<td>$c^3$</td>
<td>$c^6$</td>
<td>$c^9$</td>
</tr>
</tbody>
</table>

Example 123
Let $G = D_6$. We know $K(D_6) = \{1^G, r^G, s^G\}$. First we look for linear characters of $D_6$. Recall that $D_6 = \langle r, s | r^3, s^2, (rs)^2 \rangle$ a linear character is just a homomorphism from $D_6 \to \mathbb{C}^*$. By the Universal Property we are looking for $\alpha, \beta \in \mathbb{C}^*$ (the images of $r, s$) satisfying the relations in the presentation; $1 = \alpha^3 = \beta^2 = (\alpha \beta)^2$. Solving for $\alpha, \beta$ gives $\alpha = 1, \beta \in \{-1, 1\}$. We get two rows:

<table>
<thead>
<tr>
<th></th>
<th>$r$</th>
<th>$s$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\chi_1$</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$\chi_2$</td>
<td>1</td>
<td>$-1$</td>
</tr>
</tbody>
</table>

Let $\chi_3$ be the last row. We compute $\chi_3(1)$ by $6 = \sum_i \chi_i(1)^2 = 1 + 1 + \chi_3(1)^2 \Rightarrow \chi_3(1) = 2$. We find the last row by $\chi^{reg} = \sum_i \chi_i(1) \chi_i$ so

\[
2\chi_3(r) + \chi_2(r) + \chi_1(r) = 0 \Rightarrow \chi_3(r) = -1
\]

\[
2\chi_3(s) + \chi_2(s) + \chi_1(s) = 0 \Rightarrow \chi_3(s) = 0
\]
7.2 Properties of Character Tables

Proposition 124
Let $\chi, \mu$ be irreducible characters of a finite group $G$ and $\deg \mu = 1$

1. $\overline{\chi} : g \rightarrow \chi(g^{-1})$ is again an irreducible character of $G$ called the dual of $\chi$.
2. $\chi \mu : g \rightarrow \chi(g)\mu(g)$ is again an irreducible character of $G$ called a twist.

Proof
Let $\rho$ be a representation so that $\chi = \chi_\rho$.

1. Define $\sigma(g) = \rho(g)^{-T} := (\rho(g)^{-1})^T$ then $\sigma$ is a representation because $\sigma(gh) = \rho(gh)^{-T} = (\rho(h)^{-1}\rho(g)^{-1})^T = \rho(g)^{-T}\rho(h)^{-T} = \sigma(g)\sigma(h)$ and $\sigma(1) = \rho(1)^{-T} = I_n^{-T} = I_n$.
   Moreover, $\chi_\sigma(g) = tr(\sigma(g)) = tr(\rho(g)^{-T}) = tr(\rho(g^{-1})) = \chi_\rho(g^{-1}) = \chi(g^{-1}) = \overline{\chi(g)}$ so $\overline{\chi}$ is a character of $G$. To prove it is irreducible:
   $$(\overline{\chi}, \overline{\chi})_G = \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)}\overline{\chi(g)} = \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)}\chi(g) = (\chi, \chi)_G = 1$$
   Hence $\overline{\chi}$ is irreducible.
2. Define $\sigma(g) = \rho(g)\mu(g)$. Then $\sigma$ is a representation because $\sigma(gh) = \rho(gh)\mu(gh) = \rho(g)\mu(g)\rho(h)\mu(h) = \sigma(g)\sigma(h)$ because $\mu(g) \in \mathbb{C}$ (it is a linear character). Also $\sigma(1) = \rho(1)\mu(1) = \rho(1)$ so $\sigma$ is a representation of $G$.
   Therefore $\chi_\sigma(g) = tr(\sigma(g)) = tr(\rho(g)\mu(g)) = \mu(g)tr(\rho(g)) = \mu(g)\chi(g) = (\mu\chi)(g)$ so $\mu\chi$ is a character of $G$. It is irreducible because
   $$(\mu\chi, \mu\chi)_G = \frac{1}{|G|} \sum_{g \in G} \mu(g)\chi(g)\overline{\mu(g)\chi(g)} = \frac{1}{|G|} \sum_{g \in G} \mu(g)\overline{\mu(g)}\overline{\chi(g)}\overline{\chi(g)} = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\chi(g)} = (\chi, \chi)_G = 1$$
   so $\mu\chi$ is irreducible.

Remark
The product of two characters is always a character. The proof of this is out of scope.

Lemma 125:
Let $A \in M_n(\mathbb{C})$. The following are equivalent:

1. The rows of $A$ are orthonormal.
2. $AA^T = I_n$
3. $A^T A = I_n$
4. The columns of $A$ are orthonormal.

Proof
1 $\leftrightarrow$ 2 and 3 $\leftrightarrow$ 4 are clear from linear algebra.
If $AB = I_n$, then $\det A \det B = \det I_n = 1$ so there exists $A^{-1}$. Therefore
$$AA^T = I_n \Rightarrow A^T A = (A^{-1}A)A^T A = A^{-1} \left( AA^T \right) A = A^{-1} A = I_n$$
Theorem 126 (Row and Column Orthogonality)
Let $G$ be a finite group and $\chi_1, \ldots, \chi_k$ be its irreducible characters. Let $C_1, \ldots, C_k$ be its conjugacy classes and $n_j = |C_j|$. Then for $s, t \in \{1, \ldots, k\}$:

1. (Row Orthogonality):
   $$\sum_{j=1}^{k} n_j \chi_s(C_j) \overline{\chi_t(C_j)} = |G| \delta_{st}$$

2. (Column Orthogonality):
   $$\sum_{i=1}^{k} \chi_i(C_s) \overline{\chi_i(C_t)} = \frac{|G| \delta_{st}}{n_s}$$

Proof

1. By Theorem 105 (Orthogonality of characters)
   $$|G| \delta_{st} = \sum_{g \in G} f(g) \overline{f(g)}$$ where $f(g) = \chi_s(g) \overline{\chi_t(g^{-1})}$ is a class function of $g$. Taking terms from the same conjugacy class together gives the result.

2. Write $a_{uw} = \left( \frac{n_u}{|G|} \right)^{\frac{1}{2}} \chi_u(C_w)$. The rows of $A = a_{uw}$ are orthonormal by part 1. By Lemma 125, so are the columns; so we get the expression in part 2. ■

Example 127
Let $G$ be a group, $|G| = 12$ and $k(G) = 4$ such that one of its characters is

| $\chi_2$ |
|---|---|---|---|
| $C_2$ | $C_3$ | $C_4$ |
| 1 | 1 | $\omega$ | $\omega^2$ |

Where $\omega = \exp \left( \frac{2\pi i}{3} \right)$. We will find the full character table for $G$.

Solution
The trivial character is always there. $\chi_3 := \overline{\chi_2}$ is also a character, so we have

| $\chi_1$ |
|---|---|---|---|
| $C_2$ | $C_3$ | $C_4$ |
| 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | 1 | $\omega$ | $\omega^2$ |
| $\chi_3$ | 1 | 1 | $\omega$ | $\omega^2$ |

Let $\chi_4$ be the last row. We find $\chi_4(1)$ by: $12 = \sum \chi_i(1)^2 = 1 + 1 + 1 + \chi_4(1)^2$ so $\chi_4(1) = 3$. To find the remaining entries we use orthogonality of columns, getting $\chi_4(C_2) = -1$ and $\chi_4(C_3) = 0$

7.3 Characters and Normal Subgroups

Kernel of characters:
Let $\rho$ be a representation of $G$. We define $\ker \chi_\rho := \ker \rho = \{ g \in G : \rho(g) = 1 \}$ (this is well defined because a representation $\rho$ is determined by $\chi_\rho$ up to equivalence and equivalent characters have the same kernel.)

Lemma 129
Let $\chi$ be a character of $G$. Then $\ker \chi = \{ g \in G : \chi(g) = \chi(1) \}$
Proof
Let $\rho$ be a representation of $G$ so that $\chi = \chi_\rho$.

1. Take an element $g \in \ker \chi$. Then $\rho(g) = I_n$ so $\chi(g) = \text{tr}(\rho(g)) = \text{tr}(I_n)$, so $g \in \{g \in G : \chi(g) = \chi(1)\}$.

2. Let $g \in G$ so that $\chi(g) = \chi(1)$. By Lemma 101, there are roots of unity $\omega_1, \ldots, \omega_n$ where $n = \deg \rho$ such that $\chi(g) = \omega_1 + \cdots + \omega_n$ but $\chi(g) = \chi(1) = n$ so $n = \omega_1 + \cdots + \omega_n$ hence $\omega_1 = \cdots = \omega_n = 1$. Then as $\rho(g)$ is diagonalisable, $\rho(g) = I_n$. ■

**Theorem 130 (Lifting)**
Let $f : G \to H$ be a homomorphism of finite groups with kernel $N$.

1. There exists a map $p : \{\text{characters of } H\} \to \{\text{characters } \chi \text{ of } G \text{ with } N \subseteq \ker \chi\}$ defined by $p(\chi) = \chi \circ f$
2. If $f$ is surjective then $p$ is bijective.

Proof
1. Let $\chi$ be a character of $H$, say $\chi = \chi_\rho$ where $\rho$ is a representation of $H$. Then $\rho \circ f : G \to GL$ is a representation because the composition of two group homomorphisms is a homomorphism, and its character is $\chi_\rho \circ \chi_f = p(\chi)$. Also, the kernel of $\rho \circ f$ contains the kernel of $f$, so $N \subseteq \ker p(\chi)$.
2. $p$ is surjective:
   Let $\chi$ be a character of $G$ with $N \subseteq \ker \chi$, say $\chi = \chi_\sigma$. Define a representation $\rho$ by $\rho(f(x)) = \sigma(x)$ which is well defined because $f(x) = f(y) \Rightarrow \sigma(x) = \sigma(y)$ and $f$ is surjective. Then $p(\rho) = \sigma$.
   $p$ is injective:
   Let $p(\chi_1) = p(\chi_2)$. Then $\chi_1 \circ f = \chi_2 \circ f$ so $\chi_1 = \chi_2$. ■

**Theorem 131**
Let $G$ be a finite group.

1. For irreducible characters $\chi_1, \ldots, \chi_n$ of $G$, $\ker \chi_1 \cap \ldots \cap \ker \chi_n \unlhd G$
2. All normal subgroups of $G$ arise this way.

Proof
1. Clearly $\ker(\chi_i) \unlhd G$ since $\rho$ is a homomorphism. The intersection of normal subgroups is again a normal subgroup, so the result follows.
2. Let $N \unlhd G$ and $f : G \to G/N$ be the natural epimorphism. Let $\rho$ be any injective representation of $G/N$ (for example take $\rho^{reg}$). Then $\rho \circ f$ is a representation of $G$ with kernel $N$ by Theorem 130. Write $\rho \circ f = \sigma_1 \oplus \ldots \oplus \sigma_n$ with $\sigma_i$ irreducible. Put $\chi_i = \chi_{\sigma_i}$ then $N = \ker(\rho \circ f) = \ker(\sigma_1 \oplus \ldots \oplus \sigma_n) = \ker \sigma_1 \cap \ldots \cap \ker \sigma_n = \ker \chi_1 \cap \ldots \cap \ker \chi_n$. ■
7.4 Linear Characters and the Derived Subgroup

Commutator
The commutator of $x$ and $y$ in a group $G$ is $[x, y] := xyx^{-1}y^{-1}$. The derived subgroup or commutator subgroup of a group $G$ is $G' := [G, G] = \langle \{[g, h] : g, h \in G \} \rangle$. Note $[x, y] = 1 \iff xy = yx \iff x, y$ commute.

Example 133

1. $G$ is abelian if and only if $G' = 1$
2. $S'_n = A_n$ and $A'_n = A_n$ if $n \geq 4$

Proposition 134
Let $G$ be a group. Then

1. $G' \leq G$
2. Let $N \trianglelefteq G$ then $G/N$ is abelian if and only if $G' \subseteq N$

Proof

1. Let $x, y \in G$. We prove $[x, y]^g \in G'$ as follows:
   For $g \in G$, $z \to z^g$ is an automorphism of $G$ so
   
   $[x, y]^g = (xyx^{-1}y^{-1})^g = x^g y^g (x^{-1})^g (y^{-1})^g = [x^g, y^g] \in G'$

2. $G/N$ is abelian $\iff [xN, yN] = 1$ for all $x, y \in G$ $\iff (xN)(yN)(xN)^{-1}(yN)^{-1} = 1$ for all $x, y \in G$ $\iff xyx^{-1}y^{-1}N = N \forall x, y \in G$ $\iff [x, y]N = N \forall x, y \in G$ $\iff [x, y] \in N \forall x, y \in G$ $\iff G' \subseteq N$.

Proposition 135
Let $G$ be a group.

1. A linear character of $G$ is the same thing as the lift to $G$ of a linear character of $G/G'$
2. The number of linear characters of $G$ is the same as $|\hat{G}/\hat{G}'|$

Proof

1. $\left(\Rightarrow\right)$ Let $\lambda$ be a linear character of $G$. Then $\lambda$ is a homomorphism $\lambda : G \to \mathbb{C}$ and $\mathbb{C}$ is abelian so $\lambda(G)$ is abelian. By Proposition 134 part 2, $G' \subset \ker \lambda$ and so by Theorem 130 $\lambda$ is a lift (that is $\lambda = \chi \circ f$ for $\chi$ a character of $G/G'$ and $f : G \to G/G'$ the natural map). Clear that $\deg \lambda = \deg \chi$ since $f(1) = G' = 1$ so $\chi$ is linear.

2. We know that $G/G'$ is abelian so by Theorem 119, all of its irreducible characters are linear, and it has $|\hat{G}/\hat{G}'|$ conjugacy classes so $\hat{G}/\hat{G}'$ has precisely $|\hat{G}/\hat{G}'|$ linear characters. By Part 1, there is a bijection between the linear characters of $G$ and the linear characters of $G/G'$ so in particular they have the same number of linear characters.

Example
If $k(G) = 3$ then $(\chi_1(1), ..., \chi_3(1)) \neq (1, 1, 5)$. 
Suppose it does. By Proposition 135, \[ \frac{|G|}{|G'|} = 2 \] so 2 divides $|G|$. But $|G| = 1^2 + 1^2 + 5^2 = 27$ which is a contradiction. ■

7.5 More Examples

Example 136

Some generalities on $S_n$. There exists an index 2 subgroup $A_n \leq S_n$, so there exists a linear character $\chi : S_n \to \{-1, 1\} \subset \mathbb{C}^*$ called the sign character or sign representation.

Let $\rho^P$ be the permutation representation of $S_n$:

$$\rho(g)(e_i) = e_{g(i)}$$

The character of $\rho^P$ is the map $g \to |\{x \in \{1, \ldots, n\} : g(x) = x\}|$

Let $n = 4$. First we compute $K(S_4)$ and the sizes of the conjugacy classes:

<table>
<thead>
<tr>
<th>$C$</th>
<th>1</th>
<th>(12)</th>
<th>(123)</th>
<th>(1234)</th>
<th>(12)(34)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td>C</td>
<td>$</td>
<td>1</td>
<td>6</td>
<td>8</td>
</tr>
</tbody>
</table>

Let $\chi_1$ be the trivial character. Let $\chi_2$ be the sign character. Let $p$ be the permutation character. Unfortunately, $p$ is not irreducible. Consider $\chi_3 = p - \chi_1$ then

<table>
<thead>
<tr>
<th>$C$</th>
<th>1</th>
<th>(12)</th>
<th>(123)</th>
<th>(1234)</th>
<th>(12)(34)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td>C</td>
<td>$</td>
<td>1</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>$\chi_1$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$\chi_2$</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>$p$</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\chi_3$</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>-1</td>
<td>-1</td>
</tr>
</tbody>
</table>

Observe that $(\chi_3, \chi_3)_G = \frac{1}{24}(3^2 + 6 \times 1^2 + 6 \times 1^2 + 3 \times 1^2) = 1$ so $\chi_3$ is irreducible.

Define $\chi_4 = \chi_2 \chi_3$ then $\chi_4$ is an irreducible character since it is a twist. Observe $\chi_4 \notin \{\chi_1, \chi_2, \chi_3\}$ by looking at the table.

We have one more character call it $\chi_5$. We find $\chi_5(1)$ by $24 = |G| = \sum_{i=1}^{5} \chi_i(1)^2$ so $\chi_5(1) = 2$.

We find the remaining entries by Column Orthogonality:

<table>
<thead>
<tr>
<th>$C$</th>
<th>1</th>
<th>(12)</th>
<th>(123)</th>
<th>(1234)</th>
<th>(12)(34)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td>C</td>
<td>$</td>
<td>1</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>$\chi_1$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$\chi_2$</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>$\chi_3$</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>$\chi_4$</td>
<td>3</td>
<td>-1</td>
<td>0</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>$\chi_5$</td>
<td>2</td>
<td>0</td>
<td>-1</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

Example 137

Take $G = \{ g : \frac{a}{5x} \to \frac{a}{5x} : \exists a, b \in \frac{Z}{5Z}, a \neq 0 \text{ with } g(x) = ax + b \}$

Denote particular elements of $G$ by $r, s$ where $r(x) = x + 1$ and $s(x) = 2x$.

1. Claim

$G = \langle r, s \rangle$

Solution
\[ s^2(x) = 4x, s^3(x) = 8x = 3x, s^4(x) = 6x = x \] so transformations of the form \( x \to ax \) are in \( G \). Then the composition \( r^b \left( s^k(x) \right) - s^k(x) + b \) hence \( G = \langle r, s \rangle \).

2. **Claim**

\[ r^s = 1, s^4 = 1, rs^{-1} = r^2 \]

**Solution**

\[ s^4(x) = 16x = x, r^5(x) = x + 5 = x, rs^{-1}(x) = sr(3x) = s(3x + 1) = 6x + 2 = x + 2 = r^2(x) \]

3. **Claim**

Any element of \( G \) can be written uniquely as \( r^k s^l \) where \( 0 \leq k \leq 4 \) and \( 0 \leq l \leq 3 \)

**Solution**

From part 1, we actually proved that every element of \( G \) is of the form \( r^k s^l \) where \( k, l \in \mathbb{Z} \) then as \( r^k = s^4 = 1 \) we can reduced \( k, l \) into the intervals \( 0 \leq k \leq 4 \) and \( 0 \leq l \leq 3 \). Uniqueness follows from comparison with \( |G| = 20 \).

**Remark**

In fact, \( G = C_5 \rtimes C_4 \)

4. Define \( f: G \to \left( \frac{\mathbb{Z}}{5} \right)^* \) by \( f(x \to ax + b) = a \)

**Claim**

\( f \) is a homomorphism and there exists a homomorphism \( h: G \to C_4 = \langle c | c^4 \rangle \)

**Solution**

Let \( u, v \in G \) with \( u(x) = ax + b \) and \( v(x) = cx + d \). Then \( uv(x) = u(cx + d) = acx + ad + b \) so \( f(uv) = ac \) and \( f(u)f(v) = ac \)

But \( \left( \frac{\mathbb{Z}}{5} \right)^* \cong C_4 \) which defines \( h \).

5. **Claim**

The Conjugacy classes of \( G \) are \( \{1\}, \{r, r^2, r^3, r^4\}, C_1 := \{r^k s: k \in \mathbb{Z}\}, C_2 := \{r^k s^2: k \in \mathbb{Z}\}, C_3 := \{r^k s^3: k \in \mathbb{Z}\} \)

**Solution**

\( \{1\} \) is always a conjugacy class. Observe \( r^s = r^2, (r^2)^s = r^4, (r^4)^s = r^3, (r^3)^s = r \) and \( \{r, r^2, r^3, r^4\} \) is certainly invariant under conjugation of \( r \). We do not need to check anything else since \( G \) is generated by \( r, s \).

\[ \left( r^k s \right)^r = r^{-1} r^k s r = r^{-1} r^k r^2 s = r^{k+1} s \]
\[ \left( r^k s \right)^s = s^{-1} r^k s s = r^{2k} s \]

Therefore \( C_1 \) is contained in a conjugacy class. Observe \( (C_1)^2 = C_2 \) and \( (C_1)^3 = C_3 \) so as two conjugacy classes are either equal or disjoint, they partition the finite group \( G \). Hence \( C_1, C_2, C_3 \) are conjugacy classes as required.

6. We now find the character table for \( G \):

Lifting the four irreducible characters of \( C_4 \) through the homomorphism \( h \) yields 4 linear characters of \( G \). We can then find \( \chi_5 \) by \( 20 = \sum_{i=1}^{5} \chi_5(1)^2 \) and then use Column Orthogonality:
<table>
<thead>
<tr>
<th>$C$</th>
<th>1</th>
<th>$r$</th>
<th>$s$</th>
<th>$s^2$</th>
<th>$s^3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td>C</td>
<td>$</td>
<td>1</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>$\chi_1$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$\chi_2$</td>
<td>1</td>
<td>1</td>
<td>$i$</td>
<td>$-1$</td>
<td>$-i$</td>
</tr>
<tr>
<td>$\chi_3$</td>
<td>1</td>
<td>1</td>
<td>$-1$</td>
<td>1</td>
<td>$-1$</td>
</tr>
<tr>
<td>$\chi_4$</td>
<td>1</td>
<td>1</td>
<td>$-i$</td>
<td>$-1$</td>
<td>$i$</td>
</tr>
<tr>
<td>$\chi_5$</td>
<td>4</td>
<td>$-1$</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Chapter 8: Restriction and Induction

8.1 Notation and basic properties

Let \( H \leq G \) be finite groups. We define maps

\[
\begin{align*}
\text{Restriction } p \to p_H: & \quad \rho_H(x) = \rho(x) \quad \forall x \in H \\
\text{Induction } q \to q^G: & \quad q^G(x) = \frac{1}{|H|} \sum_{y \in G} q^0(yxy^{-1}) \quad \text{where } q^0(z) = \begin{cases} q(z) & \text{if } z \in H \\ 0 & \text{if } z \notin H \end{cases}
\end{align*}
\]

A more flexible notation is the following:

For an assertion \( P \), denote by \([P] = \begin{cases} 1 & \text{if } P \text{ is true} \\ 0 & \text{if } P \text{ is false} \end{cases}\). Then

\[
q^G(x) = \frac{1}{|H|} \sum_{y \in G} q(yxy^{-1})[yxy^{-1} \in H]
\]

With the convention that "undefined \( \times 0 \)" = 0

**Proposition 138**

\( p_H \) and \( q^G \) are again class functions.

**Proof**

For \( p_H \) this is trivial, since it is a projection of a class function.

For \( q^G \), take any \( x, y \in G \) then

\[
q^G(yxy^{-1}) = \frac{1}{|H|} \sum_{z \in G} q^0(zyxy^{-1}z^{-1}) = \frac{1}{|H|} \sum_{z \in G} q^0(tzt^{-1}) = q^G(x) \quad \blacksquare
\]

**Proposition 139 (Frobenius Reciprocity)**

Let \( H \leq G \), let \( p \in CF(G) \) and \( q \in CF(H) \). Then \( (p_H, q)_H = (p, q^G)_G \)

**Proof**

\[
(q^G, p)_G = \frac{1}{|G|} \sum_{x \in G} q^G(x)p(x) = \frac{1}{|G||H|} \sum_{x, y \in G} q(yxy^{-1})[yxy^{-1} \in H]p(x)
\]

\[
= \frac{1}{|G||H|} \sum_{x, y \in G} q(yxy^{-1})[yxy^{-1} \in H]p(yxy^{-1}) = \frac{1}{|G||H|} \sum_{z, y \in G} q(z)[z \in H]p(z)
\]

\[
= \frac{1}{|H|} \sum_{z \in H} q(z)p(z) = \frac{1}{|H|} \sum_{z \in H} q(z)p_H(z) = (q, p_H)_H \quad \blacksquare
\]

**Exercise**

Let \( G \) be a finite group, \( q \in CF(G) \).

Then \( q \) is a character of \( G \) if and only if for all \( p \in I(G) \), \( (p, q)_G \in \mathbb{Z}_{\geq 0} \).

**Proof**

The irreducible characters \( \chi_1, ..., \chi_k \) are an orthonormal basis of \( CF(G) \). Now \( q \) is a character if and only if \( \sum \chi_i(q, \chi_i)_G \) is a character if and only if \( (q, \chi_i)_G \in \mathbb{Z}_{\geq 0} \). \( \blacksquare \)
Corollary 140
Let $H \leq G$. Let $q$ be a character of $H$. Then $q^G$ is a character of $G$.

Proof
Let $p \in I(G)$. Then $(p, q^G)_G = (p_H, q)_H$ by Frobenius Reciprocity. Since $p_H, q$ are character of $H$, the inner product is an element of $\mathbb{Z}_{\equiv 0}$. Then by the exercise, $q^G$ is a character of $G$. ■

8.2 How to compute an induced character in practice
It is very easy to compute the induced character of the trivial conjugacy class:

Proposition 141

$$p^G(1) = [G:H]p(1)$$

Proof
We proceed by direct calculation:

$$p^G(1) = \frac{1}{|H|} \sum_{y \in G} p(y y^{-1})[y y^{-1} \in H] = \frac{1}{|H|} \sum_{1 \in H} p(1)[1 \in H] = \frac{|G|}{|H|} p(1) = [G:H]p(1)$$

Proposition 142
Let $H \leq G$ be finite groups, $p \in CF(G)$. Let $C \in K(G)$. Let $D_1, \ldots, D_k$ be the conjugacy classes in $H$ contained in $C$. Then

$$p^G(C) = \frac{[G:H]}{|C|} \sum_{i=1}^{k} |D_i| p(D_i)$$

Moreover, if $k > 1$ we say that $C$ splits.

Proof

Claim
For $g \in C$, $\frac{|\{x \in G : xgx^{-1} \in D_i\}|}{|g|} = \frac{|D_i|}{|C|}$

Proof
Define $f : G \to C$ by $x \mapsto xgx^{-1}$. Then $f^{-1}(aha^{-1}) = \{y \in G : ygy^{-1} = aha^{-1} \} = a \{z \in G : zgz^{-1} = h \} a^{-1} = af^{-1}(h) a^{-1}$. So $|f^{-1}(h)|$ is independent of conjugate elements. Therefore

$$|f^{-1}(h)| = \frac{|G|}{|C|}$$

So $|\{x \in G : xgx^{-1} \in D_i\}| = \sum_{x \in D_i} |f^{-1}(h)| = \frac{|G|}{|C|} |D_i|$ ■

We now complete the proof:

$$p^G(C) = \frac{1}{|H|} \sum_{y \in G} p(y y^{-1})[y y^{-1} \in H] = \frac{1}{|H|} \sum_{1=1}^{k} \sum_{y \in G} [y y^{-1} \in D_i] p(y y^{-1}$$

$$= \frac{1}{|H|} \sum_{1=1}^{k} |\{y \in G : ygy^{-1} \in D_i\}| p(D_i)$$

By the claim:
\[ p^G(C) = \frac{1}{|H|} \sum_{i=1}^{k} \frac{|G||D_i|}{|C|} p(D_i) = \frac{|G:H|}{|G|} \sum_{i=1}^{k} |D_i| p(D_i) \]

**Example 143**

Computing induced characters using 142 and "induction tables". Namely, we induce to \(S_3\) the irreducible characters of \(S_2\) and \(A_3\). The character tables for these groups are the following:

<table>
<thead>
<tr>
<th>(S_2)</th>
<th>1</th>
<th>(12)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\chi_1)</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>(\chi_2)</td>
<td>1</td>
<td>-1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(A_3)</th>
<th>1</th>
<th>(123)</th>
<th>(321)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\chi_1)</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>(\chi_2)</td>
<td>1</td>
<td>(\omega)</td>
<td>(\omega^2)</td>
</tr>
<tr>
<td>(\chi_3)</td>
<td>1</td>
<td>(\omega^2)</td>
<td>(\omega)</td>
</tr>
</tbody>
</table>

First, for each conjugacy class \(C\) of \(S_3\) we write \(C: k\), or rather, one element of \(C\). For each conjugacy class \(D\) of \(S_2\) we write \(D: |D|\) in the same column as the conjugacy class \(C \in K(S_3)\) such that \(D \subseteq C\).

Then \((\chi_1)^{S_3}(1) = 1 \times 1 \times \frac{6}{2} \times \frac{1}{1} = 3\), and for the other elements use \(p^G(C) = \frac{|G:H|}{|G|} \sum_{i=1}^{k} |D_i| p(D_i)\).

<table>
<thead>
<tr>
<th>(S_3)</th>
<th>1:1</th>
<th>(12):3</th>
<th>(123):2</th>
</tr>
</thead>
<tbody>
<tr>
<td>(S_2)</td>
<td>1:1</td>
<td>(12):1</td>
<td></td>
</tr>
<tr>
<td>((\chi_1)^{S_3})</td>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>((\chi_2)^{S_3})</td>
<td>3</td>
<td>-1</td>
<td>0</td>
</tr>
</tbody>
</table>

Next for \(A_3\): now there is splitting; \((123), (321)\) are conjugate in \(S_3\) but not in \(A_3\). (It’s the only splitting occurring).

<table>
<thead>
<tr>
<th>(A_3)</th>
<th>1:1</th>
<th>(123):3</th>
</tr>
</thead>
<tbody>
<tr>
<td>((\chi_3)^{S_3})</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>((\chi_4)^{S_3})</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>((\chi_5)^{S_3})</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

\((\chi_k)^{S_3}(1) = |G:H|\chi_k(1)\)

\((\chi_k)^{S_3}((12)) = 0\) (empty sum)

\((\chi_4)^{S_3}((123)) = \frac{2}{2}(\omega + \omega^2) = -1\)

**Example 145**

We will compute the full character table for \(A_5\) using induction from \(A_4\) and \(C_5\). Write \(G = A_5, H = A_4, K = \langle x \rangle, x = (12345)\).

a. Let \(C\) be a conjugacy class in \(S_n\). Prove that at most two conjugacy classes of \(A_n\) are in \(C\).

*Solution*

Let \(a, b, c \in A_n \cap C\) and assume that \(a, b\) are not conjugate in \(A_n\) and \(b, c\) are not either; \(a^x = b, b^y = c\) for \(x, y \in S_n \setminus A_n\) so \(xy \in A_n\) hence \((a^x)^y = a^{xy} = c\) so \(a, c\) are conjugate in \(A_n\).

b. For each conjugacy class in \(A_4\) or \(A_5\), find its cardinality and give one element.

*Solution*
Similarly, for $A_5$,

$$
\begin{array}{c|cccc}
A_5 & 1 & (123) & (12)(34) & (12345) & (12354) \\
1 & 1 & 4 & 4 & 3 & 1
\end{array}
$$

Need to prove $x = (12345) \sim_{A_5} (12354) = y$. Suppose they are; then there exists $z \in A_5$ with $yz = zx$. By replacing $z$ with $zx^k$ for $x \in \mathbb{Z}$ we may suppose $z(1) = 1$. Then $z = (45) \notin A_5$.

c. Let $\lambda$ be the following linear character of $H = A_4$. Compute $(1_H)^G$ and $\lambda^G$.

$$
\begin{array}{c|cccc}
1 & (123) & (321) & (12) & (34) \\
\lambda & 1 & \omega & \omega^2 & 1
\end{array}
$$

d. Prove $\chi_1 := (1_H)^G - 1_G$ is a character for $A_5$.

e. Prove that $\chi_4$ and $\chi_5$ are irreducible.

f. Find $(12345)^G \cap K$ and $(12354)^G \cap K$.

g. Let $\epsilon = \exp \left(\frac{2\pi i}{5}\right)$. Let $\mu$ be the linear character of $K$ such that $\mu(x) = \epsilon$.

h. Prove that $\chi_3 := \mu^G - \chi_5 - \chi_4$ is an irreducible character.

i. Finish the character table.

**Solution**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$1_H^G$</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\lambda^G$</td>
<td>5</td>
<td>$-1$</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

We need to prove that $((1_H)^G, 1_G)_G \geq 1$:

$60((1_H)^G, 1_G)_G = (5 \times 1 + 2 \times 20 + 1 \times 15) = 60$ so $((1_H)^G, 1_G)_G = 1$

$60(\chi_5, \chi_5)_G = 5^2 \times 1 + (-1)^2 \times 20 + 1^2 \times 15 = 60$ so $(\chi_5, \chi_5)_G = 1$ so $\chi_5$ is irreducible.

$$
\begin{array}{c|cc}
A_5 & 1:1 & (12)(34): 15 \\
\chi_4 & 4 & 1 \\
\chi_5 & 0 & -1 \\
\chi_6 & -1 & -1 \\
\end{array}
$$

Since $60(\chi_4, \chi_4)_G = 4^2 \times 1 + 1^2 \times 20 + (-1)^2 \times (12 + 12) = 60$ so $(\chi_4, \chi_4)_G = 1$ and so $\chi_4$ is irreducible.

**Claim**

We claim that $x^G \cap K = \{x, x^4\}$ and $(12354) \cap K = \{x^2, x^3\}$

**Proof**


So $x^4$ is conjugate to $x$ in $G$. So $x^2$ is conjugate to $(x^4)^2 = x^8 = x^3$. It remains to prove that $x^2 \not\in (12354)_G \cap K$. Since $x^2 = (13524)$,

$(235)(12354)(532) = (24135) = x^2$ so $x^2 \in (12354)^G \cap K$.

$\square$
To prove that $\chi_3 := \mu^2 - \chi_5 - \chi_4$ is an irreducible character, we need to prove $(\mu^2, \chi_5)_G \geq 1$, $(\mu^2, \chi_4)_G \geq 1$, $(\chi_3, \chi_5)_G = 1$. This is straightforward and I do not include it here.

Define $\chi_1 := 1_G$. Let $\alpha$ be an automorphism of $G = A_5$ mapping $\alpha(x) = (45)x(45)$. Define $\chi_2 := \chi_3 \circ \alpha$. It is clear that $\chi_2$ is irreducible because $\chi_3$ is. Then

Therefore the full character table is as follows:

Now we can find all normal subgroups of $A_5$. Observe that $(1, 1)$ and $(H, 1)$. Since every normal subgroup of $A_5$ is a of the form $\cap_{x \in A \subseteq I(A_5)} \ker \chi$ (for some subset $A \subseteq I(A_5)$, we see that the only normal subgroups of $A_5$ are $\{1, A_5\}$. That is, $A_5$ is simple.

8.3 Induction and Restriction for modules

**Definition 146**

Let $H \leq G$ be finite groups, $W$ a $CH$-module. We define $W^G$ to be a $CG$-module with character $(\chi_W)^G$. This is well defined (up to isomorphism) because:

1. $(\chi_H)^G$ is a character of $G$.
2. A $CG$-module is determined by its character.

**Definition 147**

Let $G$ be a finite group, $V$ a $CG$-module. An imprimitivity condition or ID is a sequence $(W_1, ..., W_k)$ of non-zero subspaces (not submodules) such that:

1. $V = W_1 \oplus \cdots \oplus W_k$
2. Invariance: $\forall g \in G, \exists j$ such that $gW_i = W_j$
3. Transitivity: $\forall i, j \exists g \in G$ such that $gW_i = W_j$

It is a proper ID if $k > 1$. $V$ is called primitive if it has no proper ID.

We are interested in $H := Stab_G(W_1) = \{g \in G : gW_1 = W_1\}$. Note that $Stab_G(W_i)$ is conjugate to $H$ by transitivity.
Proposition 148
Let $V$ be a $\mathbb{C}G$-module with character $q$ and with $\text{ID } V = W_1 \oplus \ldots \oplus W_k$. Put $H = \text{Stab}_G(W_1)$. Then $q = (\chi_{W_i})^G$, $\chi_{W_i}$ is a character of $H$.

Proof
Write $\chi_{W_i} = p$. Let $T$ be a left-transversal for $H$ in $G$; that is $T \subset G$ and $G = \bigcup_{t \in T} tH$. Put $W = W_1$. Then as $t$ runs through $T$, $tW$ runs through the $W_i$, so:

$$V = \bigoplus_{t \in T} tW$$

Let $(w_1, \ldots, w_n)$ be a basis for $W$. Then $\{tw_i; t \in T, 1 \leq i \leq k\}$ is a basis for $V$. We calculate $q(g)$ (for $g \in G$) using this basis.

The contribution to $q(g)$ of $tw_i$ is $0$ unless $gtw = tw$; that is $t^{-1}gt \in H$.

From now on, assume $h = t^{-1}gt \in H$ and $t \in T$ fixed. Write $hw_i = \sum_j a_{ij} w_j$ for all $i$. Then $p(t^{-1}gt) = \sum_i a_{ii}$

Now $g(tw_i) = thw_i = \sum_j a_{ij} tw_j$ so the contribution to $q(g)$ of $tw_i$ is $a_{ii}$. So the contribution of $\{tw_i; 1 \leq i \leq n\}$ is $\sum_i a_{ii} = p(t^{-1}gt)$. So

$$q(g) = \sum_{t \in T} p^0(t^{-1}gt)$$

$$= \frac{1}{|H|} \sum_{h \in H} \sum_{t \in T} p^0(t^{-1}gt) \overset{p \in CF(H)}{=} \frac{1}{|H|} \sum_{h \in H} \sum_{t \in T} p^0(h^{-1}t^{-1}gth) \overset{T \text{ is a left transversal}}{=} \frac{1}{|H|} \sum_{h \in G} p^0(h^{-1}gh)$$

$$= p^G(g) \blacksquare$$

Proposition 148.1 (Not in notes)
Let $H \leq G$, $W$ a $\mathbb{C}H$-module. Then

$$W^G \equiv \{ u: G \to W : \forall x \in H, y \in G, u(xy) = xu(y) \} \quad (*)$$

On which $G$ acts by $(gu)(x) = u(xg)$ for all $g \in G, u \in W^G, x \in G$.

Proof
Non-examinable. See 8.13 for the details. \blacksquare

$(*)$ is meaningful for $|G| = \infty$ and $\dim W = \infty$ and $\mathbb{C}$ replaced by any commutative ring, and called the induced module.
Chapter 9: Algebraic Integers and Burnside’s Theorem

Easy Exercises:

1. Every abelian finite simple group is of prime order $p$ and thus cyclic.
2. Let $G$ be a finite simple group of order $p^a$ for $p$ prime. Then $a = 1$ and $G \cong C_p$.

The smallest non-abelian finite simple group is $A_5$ and $|A_5| = 60$

Theorem (Burnside)
There is no finite simple group of order $p^aq^b$ where $p, q$ are distinct primes.
(The proof will use characters, although they are not mentioned in the proof.)

9.1 Algebraic Integers

Lemma 150

a. A polynomial $f = \sum_{i=1}^{n} a_ix^i$ is said to be monic (of degree $n$) if $a_n = 1$.

b. A complex number $\alpha$ is called an algebraic number if there exists $f \in \mathbb{Q}[x] \setminus \{0\}$ such that $f(\alpha) = 0$. The set of algebraic numbers is denoted $\overline{\mathbb{Q}}$.

c. A complex number $\alpha$ is called an algebraic integer (AI) if there exists a monic polynomial $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$. The set of algebraic integers is denoted $\mathbb{I}$.

d. Let $\alpha \in \overline{\mathbb{Q}}$ then there exists a unique $f \in \mathbb{Q}[x]$, monic of least degree so that $f(\alpha) = 0$. It is called the minimum polynomial (MP) of $\alpha$.

e. Two algebraic numbers are said to be conjugate over $\mathbb{Q}$ if they have the same minimum polynomials.

Proof
We only need to prove $d$, but this follows by applying the Well-Ordering Principle to the degrees of the set $\{f \in \mathbb{Q}[x]: f(\alpha) = 0, \text{ } f \text{ } \text{monic}\}$. Note that this set is non-empty because $\alpha$ is an algebraic number, and we can multiply through by a constant to make $f$ monic without changing the degree.

Example
$\sqrt{2}, -\sqrt{2}$ have the same minimum polynomial $x^2 - 2$ so they are conjugate.

Example
Let $T \in M(n, \mathbb{Z})$ then every complex eigenvalue $\alpha$ of $T$ is in $\mathbb{I}$ because it is the root of $\det(xI_n - T)$.

Theorem 152

a. $\overline{\mathbb{Q}}$ is a subfield of $\mathbb{C}$

b. $\mathbb{I}$ is a subring of $\mathbb{C}$

c. $\mathbb{I} \cap \mathbb{Q} = \mathbb{Z}$

d. Let $\alpha \in \overline{\mathbb{Q}}$ and $f \in \mathbb{Q}[x]$ be such that $f(\alpha) = 0$. Then the minimum polynomial of $\alpha$ divides $f$ in $\mathbb{Q}[x]$.

e. The MP of an $\alpha \in \mathbb{I}$ is in $\mathbb{Z}[x]$
f. Let \( \alpha, \beta \in \overline{Q} \). Then every conjugate to \( \alpha + \beta \) is of the form \( \alpha' + \beta' \) where \( \alpha, \alpha' \) are conjugate and \( \beta, \beta' \) are conjugate.

**Proof**

The proof of all these statements belongs to a course in Algebraic Number Theory or Galois Theory. ■

**Example**

Observe that the converse of \( f \) is false; take \( \alpha = \alpha' = \sqrt{2} \) and \( \beta' = -\sqrt{2} \). Then \( \alpha, \alpha' \) are conjugate and \( \beta, \beta' \) are conjugate. But \( \alpha + \beta = 2\sqrt{2} \) and \( \alpha' + \beta' = 0 \) which do not have the same minimum polynomial.

**Examples**

1. Let \( \omega \) be any complex root of 1, say \( \omega^n = 1 \). Then \( \omega \in \mathbb{I} \) because \( f(\omega) = 0 \) where \( f = x^n - 1 \).
2. Let \( \epsilon \) be conjugate to \( \omega \). Then \( \epsilon \) is also a root of 1. Let \( g \) be the MP of \( \omega \) (hence also of \( \epsilon \)) then \( g/f \in \mathbb{Q}[x] \) so \( f(\epsilon) = 0 \) because \( g(\epsilon) = 0 \).
3. Conversely, two roots of 1, say \( \alpha \) and \( \beta \) are conjugate \( \Leftrightarrow \langle \alpha \rangle = \langle \beta \rangle \); that is they generate the same multiplicative group. We won’t need to prove this.

**9.2 Burnside’s Theorem**

**Lemma 154**

Let \( \chi \) be a character of a finite group \( G \) and \( g \in G \). Then

1. \( \chi(g) \in \mathbb{I} \)
2. If \( \chi \) is irreducible then \( \frac{\chi(g)}{\chi(1)} |g^G| \in \mathbb{I} \)

**Proof**

a. We know that there are roots of unity \( \omega_1, ..., \omega_n \) such that \( \chi(g) = \sum_{\omega_i} \omega_i \). The result follows because \( \omega_i \in \mathbb{I} \) and \( \mathbb{I} \) is a ring.

b. Write \( \chi = \chi_{\rho} \) and \( n = \deg \rho \). For any representation \( \sigma \) put \( T(\sigma) = \sum_{h \in g^G} \sigma(h) \) and \( T = (\rho) \). Then \( T: \rho \to \rho \) is an intertwiner because for all \( x \in G \),

\[
\rho(x)^{-1} T \rho(x) = \rho(x)^{-1} \left( \sum_{h \in g^G} \rho(h) \right) \rho(x) = \sum_{h \in g^G} \rho(x^{-1}hx) = \sum_{h \in g^G} \rho(h) = T
\]

Since \( \chi \) is irreducible, it follows that \( \rho \) is irreducible and so by Schur’s Lemma \( T \) is a scalar matrix; that is \( T = \alpha I_n \). Also \( na = \text{tr} T = \text{tr} \sum_{h \in g^G} \rho(h) = \sum_{h \in g^G} \text{tr} (\rho(h)) = |g^G| \text{tr} (\rho(g)) = |g^G| \chi(g) \). Therefore

\[
\alpha = \frac{\chi(g)}{\chi(1)} |g^G|
\]

We are left to prove \( \alpha \in \mathbb{I} \). By Lemma 115 \( \rho^{reg} \sim \rho \oplus \sigma \) for some representation \( \sigma \). So every eigenvalue of \( T(\rho) \) is also an eigenvalue of \( T(\rho^{reg}) \). But \( T(\rho^{reg}) \in M(m, \mathbb{Z}) \) where \( m = |G| \). So every eigenvalue of \( T(\rho^{reg}) \) is in \( \mathbb{I} \), hence so is \( \alpha \). ■
Theorem 15
Let $\chi$ be an irreducible character of a finite group $G$. Then $\chi(1)|\left|G\right|$.

Proof
Let $C_1, \ldots, C_k$ be the conjugacy classes of $G$. By row orthogonality, $\sum_{j=1}^{k} |C_j| \overline{\chi(C_j)} \chi(C_j) = |G|$. Divide by $\chi(1)$; by 154

$$\sum_{j=1}^{k} \frac{|C_j|}{\chi(1)} \frac{\chi(C_j)}{\chi(C_j)} = \frac{|G|}{\chi(1)}$$

Therefore the LHS $\in \mathbb{I}$ because $\mathbb{I}$ is a ring therefore $\frac{|G|}{\chi(1)} \in \mathbb{I}$.

Clearly, $\frac{|G|}{\chi(1)} \in \mathbb{Q}$ so $\frac{|G|}{\chi(1)} \in \mathbb{I} \cap \mathbb{Q} = \mathbb{Z}$ so $\chi(1)|\left|G\right|$.

Proposition 156
Let $\rho$ be an irreducible representation of $G$, $g \in G$. If $\gcd(n, |g^G|) = 1$ then $\chi_{\rho}(g) = 0$ or $\rho(g)$ is a scalar matrix where $n = \deg \rho$.

Proof
Write $\lambda = \frac{1}{n} \chi_{\rho}(g)$. Choose $a, b \in \mathbb{Z}$ such that $an + b|g^G| = 1$. Multiply both sides by $\lambda$, then by Lemma 154

$$\frac{a}{\chi(1)} \chi_{\rho}(g) + \frac{b}{\chi(1)} |g^G| = \lambda \Rightarrow \lambda \in \mathbb{I}$$

Let $\omega_1, \ldots, \omega_n$ be the eigenvalues of $\rho(g)$. Then $\lambda = \frac{1}{n}(\omega_1 + \cdots + \omega_n)$ also $\omega_i$ are roots of 1 so $|\omega_i| = 1$ hence $0 \leq |\lambda| \leq 1$. We now consider the three cases:

Case 1
$|\lambda| = 0 \Rightarrow \lambda = 0$ so $\lambda = \frac{1}{n} \chi_{\rho}(g) = 0$ and so $\chi_{\rho}(g) = 0$.

Case 2
$|\lambda| = 1 \Rightarrow \omega_1 = \omega_2 = \cdots = \omega_n$. As $\rho(g)$ is diagonalizable hence $\rho(g)$ is a scalar matrix.

Case 3
In this case $0 < |\lambda| < 1$. We will deduce a contradiction, so this case never occurs.

Let $f$ be the MP for $\lambda$. Then $f = \prod_{i=1}^{k}(x - \lambda_i)$ and say $\lambda_1 = \lambda$ and $f \in \mathbb{Z}[x]$ because $\lambda \in \mathbb{I}$.

Therefore $\lambda_1 \times \cdots \times \lambda_k = (-1)^k f(0) \in \mathbb{Z}$.

Let $1 \leq i \leq k$ then $\lambda_i$ is conjugate to $\lambda$. By 152 part f, $\lambda_i$ is of the form $\lambda_i = \frac{1}{n}(\epsilon_1 + \cdots + \epsilon_n)$ where $\epsilon_i$ is some conjugate to $\omega_i$. But $\omega_i$ is a root of 1 and every conjugate of a root of 1 is itself a root of 1, so $\epsilon_i$ is a root of 1 and hence $|\epsilon_i| = 1$. As before $0 < |\lambda_i| \leq 1$ because $\lambda_i$ has MP $f$ so $\lambda_i \neq 0$.

Multiplying over all $i$ and using that $|\lambda_1| < 1$ we have $0 < |\lambda_1 \times \cdots \lambda_k| < 1$ which is a contradiction because $\lambda_1 \times \cdots \times \lambda_k \in \mathbb{Z}$.
Proposition 157
Let $p$ be a prime number and $r \in \mathbb{Z}_{\geq 0}$. Then there is no non-abelian finite simple group of order $p^r$.

Proof
Let $G$ be a non-abelian finite simple group and $g \in G$ an element with $|g^G| = p^r$. Note $g \neq 1$. Let $\chi_1, \ldots, \chi_k$ be irreducible character of $G$ with $\chi_1$ trivial. Write $\chi_i = \chi_{\rho_i}$ for all $i$. Now $G$ is simple so $\ker \rho_i \not\leq G \Rightarrow \ker \rho_i = 1$ or $G$. If $i \neq 1$ then $\rho_i$ is not trivial so $\ker \rho_i = 1$.

Claim
$\rho_i(g)$ is not a scalar matrix unless $i = 1$.

Proof
If it were then $\text{im}(\rho_i) = \rho_i(G)$ has a non-trivial central element $\rho_i(g)$. (Note $\rho_i(g) \neq 1$ because $g \neq 1$ and $\ker \rho_i = 1$). As $\ker \rho_i = 1$ we have $G \cong \rho_i(G)$.
Therefore $1 \neq Z(\rho_i(G)) \leq \rho_i(G)$. As $G$ is simple, $\rho_i(G)$ is simple hence $Z(\rho_i(G)) = \rho_i(G)$ so $\rho_i(G)$ is abelian hence $G$ is abelian. Contradiction.

By 156 if $i \neq 1$ and $p \nmid \deg \rho_i$ then $\chi_i(g) = 0$. By orthogonality of columns,

$$0 = \sum_{i=1}^{k} \chi_i(g)\overline{\chi_i(1)} = \sum_{i=1}^{k} \chi_i(g) \deg \rho_i = 1 + \sum_{i=2}^{k} \chi_i(g) \deg \rho_i = 1 + \sum_{p \mid \deg \rho_i} \chi_i(g) \deg \rho_i$$

Therefore $\sum_{i=2}^{k} \chi_i(g) \deg \rho_i = -\frac{1}{p}$ Hence as $\mathbb{I}$ is a ring, $-\frac{1}{p} \in \mathbb{I}$. Clearly, $-\frac{1}{p} \in \mathbb{Q}$ so $-\frac{1}{p} \in \mathbb{Z}$.

Contradiction.

Theorem 158 (Burnside’s $p^n q^b$ Theorem)
Let $p, q$ be distinct prime numbers and $a, b \in \mathbb{Z}_{\geq 0}$. Then there is no non-abelian finite simple group of order $p^aq^b$.

Proof
Let $G$ be such a group. Then $Z(G) \not\leq G$. $G$ is simple, so $Z(G) \in \{\{1\}, G\}$. $G$ is non-abelian, so $Z(G) = 1$. So there is just one conjugacy class of size 1, namely $\{1\}$. Let $C_1, \ldots, C_k$ be the conjugacy classes of $g$ and $C_1 = \{1\}$. As $|C_i||G|$ by 157, $pq|C_i$ if $i \neq 1$. Therefore $pq|\sum_{i \neq 1}|C_i|$.
After interchanging $p$ and $q$ if necessary, we may assume $p|\sum_{i \neq 1}|C_i|$. Therefore $p|\left(|G| - \sum_{i \neq 1}|C_i|\right) = 1$ which is a contradiction because $p$ prime