

Groups and Representation Theory

1.

1. Revision and basics.

Definition: The pair (G, \circ) is a group (or G is a group wrt \circ) if G is a set, and

- is a map: $G \times G \rightarrow G$ with (i) $a \circ (b \circ c) = (a \circ b) \circ c \quad \forall a, b, c \in G$.

(ii) \exists identity $e \in G$ such that $e \circ g = g \circ e = g \quad \forall g \in G$,

(iii) for each $g \in G$, $\exists g^{-1}$ such that $g \circ g^{-1} = e = g^{-1} \circ g$.

A group may (or may not) be commutative (abelian), i.e. $a \circ b = b \circ a \quad \forall a, b \in G$.

A subgroup H of G is a subset of G which is a group wrt \circ restricted to $H \times H$. Write $H \leq G$.

Remark: A non-empty subset H of G is a subgroup if $a, b \in H \Rightarrow a^{-1} b \in H$.

Examples: $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$

Exercise: All subgroups of $(\mathbb{Z}, +)$ are $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$, ($n \in \mathbb{Z}_+$)

Example: $X = \{1, \dots, n\}$. $\text{Sym } X = S_n =$ group of all permutations on X , under composition.

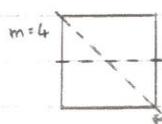
$\text{Alt } X (= A_n) =$ the alternating group of all even permutations on X .

- a subgroup of S_n of index 2.

Example: F a field; $GL_n(F) =$ all $n \times n$ matrices over F with non-zero determinant under.
"General Linear Group."

Example: Dihedral groups (order $2m$). $D_{2m} = D_{2m} (= D_m !)$

- the group of symmetries of a regular n -gon



'a', rotation through $\frac{2\pi}{m}$

'b', a reflection.

Elements are: a^i ($i \leq m$), m rotations

$a^i b$ ($i \leq m$), m reflections.

Another set of generators: a, b , where a is a reflection through the axis at angle $\frac{\pi}{m}$ with axis of b . - a reflection group on \mathbb{R}^2 .

Exercise: Any subgroup of D_{2m} is either cyclic of order dividing m , or dihedral of order dividing $2m$.

Recall: Lagrange: $H \leq G$, G finite $\Rightarrow |H| \mid |G|$.

Partial converse: $|G| = p^am$ ($p \nmid m$) $\Rightarrow \exists H \leq G$, $|H| = p^a$. "Sylow subgroups".

Definition: G, H groups. $\theta: G \rightarrow H$ is a homomorphism if $\theta(g_1 \circ g_2) = \theta(g_1) \circ \theta(g_2) \quad \forall g_1, g_2 \in G$.
(it is an isomorphism if it is bijective).

The kernel of a (general) homomorphism θ , $\ker \theta = \{g \in G \mid \theta_g = e_H\}$.

(θ is injective iff $\ker \theta = \{e_G\}$).

A subgroup H of G is normal in G if $gHg^{-1} = H$ for all $g \in G$, where $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$. Write $H \trianglelefteq G$. (So kernels are normal).

If $K \trianglelefteq G$, then form a quotient group G/K with elements all the left cosets of K in G . (Left coset: $gK = \{gk \mid k \in K\}$). Multiplication: $g_1 K \cdot g_2 K = g_1 g_2 K$. This is well-defined, and we get a group. ($x_i \in g_i K, i=1,2, \Rightarrow x_i = g_i k_i, \text{ some } k_i \in K \Rightarrow x_1 x_2 = g_1 k_1 g_2 k_2 = g_1 g_2 k_1 k_2 \in g_1 g_2 K$)
(use normality)

Theorem 1 (First Isomorphism Theorem): Let $\theta: G \rightarrow H$ be a homomorphism with $K = \ker \theta$. Then

- (a) $K \trianglelefteq G$, and $G/K \cong \theta G$, the image of G under θ ,
- (b) there is a natural 1-1 correspondence between the set X of all subgroups of G containing K and the set Y of all subgroups of θG . Moreover, this preserves normality.

Corollary 2: The homomorphic images of G are, up to isomorphism, exactly G/K for various $K \trianglelefteq G$.

Proof: If $H = \theta G$ then $H \cong G/\ker \theta$ (by Theorem 1). Conversely, if $K \trianglelefteq G$ then G/K is a homomorphism image of G under the natural homomorphism $g \mapsto gK$.

Proof of Theorem 1: (a) $K \leq G$ (check). $K \trianglelefteq G: k \in K, g \in G \Rightarrow \theta(gkg^{-1}) = \theta(g)\theta(k)\theta(g)^{-1} = e$, so $gkg^{-1} \in K$.

The mapping $\bar{\theta}: G/K \rightarrow \theta G; gK \mapsto \theta g$ is an isomorphism. It is well-defined and 1-1:

$g_1 K = g_2 K$ iff $g_2^{-1}g_1 K = K$ iff $g_2^{-1}g_1 \in K$ iff $\theta(g_2^{-1}g_1) = e$ iff $\theta(g_1) = \theta(g_2)$.

Onto is clear, as is $\bar{\theta}$ being a homomorphism.

(b) If $K \leq X \leq G$ then $\theta X \leq \theta G$, so θ induces a map $\tilde{\theta}: X \rightarrow Y$. If $Y \leq \theta G$, write $\tilde{\theta}^{-1}Y$ for the subgroup $\{g \in G \mid \theta g \in Y\}$ (usual notation for this: $\theta^{-1}Y$ - pre-image of Y), then $\tilde{\theta}$ and $\tilde{\theta}^{-1}$ are inverse to each other, and so are bijections.

Finally, normality preserved for $\tilde{\theta}, \tilde{\theta}^{-1}$: eg, if $Y \trianglelefteq \theta G$ then $\tilde{\theta}^{-1}Y \trianglelefteq G$. See: let $x \in \tilde{\theta}^{-1}Y$, so $\theta x \in Y$. For $g \in G$, $\theta(gxg^{-1}) = \theta g \theta x (\theta g)^{-1} \in Y$, since $Y \trianglelefteq \theta G$, so $gxg^{-1} \in \theta^{-1}Y$. \square

$\theta: G \rightarrow H$ is a permutation representation of G if $H = \text{Sym } X$ for some X .

$\theta: G \rightarrow H$ is a linear representation of G if $H = GL_n(F)$ for some n , some F .

A group is simple if it has no non-trivial normal subgroups.

If G is a finite group then G has a composition series: $1 = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_k = G$, with each quotient G_i/G_{i-1} being simple. For, take G_{k-1} to be a maximal normal subgroup of G , so G/G_{k-1} is simple by Theorem 1. Continue in G_{k-1} .

Warning: eg. C_6, S_3 have the same composition series.

2. Permutation Representations; Sylow Theorems

Definition: G a group, X a set. G acts on X if there is a mapping $*: G \times X \rightarrow X$ such that $(g_1, x) \mapsto g_1 * x$ (or $g(x)$, gx) satisfying:

$$(\text{A1}) \quad g_1 * (g_2 * x) = (g_1 g_2) * x, \quad (\text{A2}) \quad e * x = x \quad \forall x \in X, g_i \in G.$$

Lemma 1: If G acts on X , then (i) for each $g \in G$, the function $\varphi_g: X \rightarrow X; x \mapsto g \cdot x$ is a permutation on X .

(ii) the map $\varphi: G \rightarrow \text{Sym } X; g \mapsto \varphi_g$ is a homomorphism - a permutation representation of G .

Proof: (i) $\varphi_{g^{-1}}$ is the inverse of φ_g : $\varphi_g(\varphi_{g^{-1}}(x)) = g \cdot (g^{-1} \cdot x) \stackrel{(A1)}{=} (gg^{-1}) \cdot x \stackrel{(A2)}{=} x$ for each $x \in X$,
so $\varphi_g \varphi_{g^{-1}} = i = \varphi_{g^{-1}} \varphi_g$, similarly.

(ii) From (i) and (A1).

The kernel of the action is $K = \{g \in G \mid g \cdot x = x \ \forall x \in X\}$. Then $K \trianglelefteq G$, and $G/K \leq \text{Sym } X$ (Theorem)

The set X splits into orbits under G : x_1, x_2 are in the same orbit if $\exists g \in G$ such that $g \cdot x_1 = x_2$.
The action is transitive if X is an orbit.

The stabiliser G_x of the point x is $G_x = \{g \in G \mid x = g \cdot x\}$, and it is a subgroup of G .

Note: $G_{g \cdot x} = g G_x g^{-1}$.

Example 2: (i) $H \triangleleft G$, $X = (G:H)$, the set of left cosets of H in G , $g \cdot xH = gxH$. Axioms are fine.

"The left coset action". It is transitive, $G_H = H$, $G_{xH} = xHx^{-1}$. The kernel of this action is the largest normal subgroup of G which is contained in H .

If $H = \{e\}$ - left regular action of G . $X = G$, $g \cdot x = gx$. $G_x = \{e\}$, $G \leq \text{Sym } G$.

(ii) Conjugation action:

(a) $X = G$, $g \cdot x = gxg^{-1}$. Kernel = $Z(G)$, the centre of G .

$G_x = \{g \in G \mid gx = xg\} = C_G(x)$, the centraliser of x in G .

Orbit of x is $cl_G(x) = \{gxg^{-1} \mid g \in G\}$ - conjugacy class of x in G .

(b) $X = \text{set of all subgroups of } G$, $g \cdot H = ghg^{-1}$.

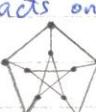
The stabiliser of H is $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ ($H \trianglelefteq N_G(H)$). - the normaliser.
Orbit of H is $cl_G(H)$.

(iii) $G = S_n$ - natural action on $[1, n] = \{1, \dots, n\}$

Induced actions: $X_k = \binom{[n]}{k}$, the set of all k -subsets of $[1, n]$. Action is pointwise;
the stabiliser of an element $\{1, \dots, k\}$ in X_k is $S_k \times S_{n-k}$.

(iv*) Groups on combinatorial or algebraic objects.

G a graph; $\text{Aut } G$ acts on vertices, preserving adjacency.

E.g. Peterson graph:  $\text{Aut Pet} = S_5$, (vertices out of $\binom{5}{2}$, joined if disjoint).

Definition: The actions of G on X and on Y are G -isomorphic if $\exists \psi: X \rightarrow Y$, bijective, such that $\psi(g \cdot x) = g \cdot \psi(x) \ \forall g \in G, x \in X$.

Theorem 3: If G is transitive on X , and $x \in X$, then the actions of G on X and on $(G:G_x)$ are G -isomorphic.

Proof: The map $\psi: X \rightarrow (G:G_x); h \cdot x \mapsto hG_x$ is a G -isomorphism. It is well-defined and 1-1:
 $h_1 \cdot x = h_2 \cdot x$ iff $h_2^{-1}h_1 \in G_x$ iff $h_2G_x = h_1G_x$. Onto is clear.

It is a G -homomorphism: $\psi(g \cdot h \cdot x) \stackrel{(A1)}{=} \psi((gh)x) = ghG_x = g \cdot hG_x = g \cdot \psi(h \cdot x)$
Left coset action.

Corollary 4 (Lagrange): G finite, acting on X . Let $x \in X$. Then $|G:G_x| = |\text{G-orbit on } x|$.

In particular, if G is transitive on X , then $|G:G_x| = |X|$.

Example 5*: $H, K \leq G$. $(G:H), (G:K)$ are G -isomorphic iff H, K are G -conjugate.

Theorem 6 (Sylow Theorems): Let G be a finite group of order $p^a m$ (p prime, $p \nmid m$). Then,

- (i) \exists a Sylow p -subgroup of order p^a ,
- (ii) any two such are conjugate in G ,
- (iii) the number n_p of Sylow p -subgroups is $1 \pmod{p}$ (and divides m)

Note: A p -group is a group of order p^r , some r .

Proof: (i) Let X be the set of all p^a -subsets of G . Then, $|X| = \binom{p^a m}{p^a} = \frac{p^a m}{p^a} \cdot \frac{p^a m - 1}{p^a - 1} \cdots \frac{p^a m - p^a + 1}{1}$.

Note that $|X|$ is prime to p : for any $k < p^a$, the numbers $p^a m - k$ and $p^a - k$ are divisible by the same power of p .

G acts on X by left multiplication, i.e. if $M \in X$, put $g \times M = \{gm \mid m \in M\} \in X$.

Let X_i be a G -orbit ($i \in X$) of size prime to p , and let $M \in X_i$.

Then, $G_M \leq G$ and $p^a \mid |G_M|$ since $|G_M| = |G|/|X_i|$. And, $|G_M| \leq |M| = p^a$, since $M = G_M \times M = \{gm \mid g \in G_M, m \in M\}$, so M is the union of right G_M -cosets.

So $|G_M| = p^a$ and G_M is a Sylow p -subgroup.

(ii) Prove a bit more:

Lemma 7: P a Sylow p -subgroup of G , Q any p -subgroup $\Rightarrow Q \leq xPx^{-1}$, for some $x \in G$.

Proof: Q acts on the set $\{G:P\}$ by left multiplication. Now, $|G:P|$ is prime to p , and $|Q|$ is a power of p , so there is a Q -orbit of size 1, say $\{xP\}$. Then, for all $q \in Q$, $qxP = xP$, so $x^{-1}qx \in P$, so $Q \leq xPx^{-1}$.

(iii) Let P be a Sylow p -subgroup of G . It acts on the set of all Sylow p -subgroups by conjugation. The orbits have various powers of p . If $\{Q\}$ is an orbit of size 1, then $P \leq N_G(Q)$. Then P, Q are Sylow in $N_G(Q)$, so are conjugate in $N_G(Q)$. So $P = Q$ since $Q \trianglelefteq N_G(Q)$. So there is unique P -orbit of size 1, namely $\{P\}$, so $n_p \equiv 1 \pmod{p}$.

(And $n_p \mid |G|$, since G is transitive on the set of Sylow subgroups)

Note: $n_p = |G:N_G(P)|$ for $P \in \text{Syl}_p(G)$

Applications of Sylow's Theorems

Lemma 8: If $|G| = p \cdot q$ with $p > q$ primes, then G has a normal Sylow p -subgroup.

Moreover, if $p \nmid q$, then G is cyclic.

Proof: $n_p = 1 \Rightarrow$ the Sylow p -subgroup is normal in G . If $n_q > 1$ then $n_q = p$, so $p \equiv 1 \pmod{q}$.

If $n_q = 1$ then G is cyclic: $P \in \text{Syl}_p(G)$, $Q \in \text{Syl}_q(G)$. $Q \trianglelefteq G$. P acts on the elements of Q by conjugation, so all orbits size 1, so $P \leq C(Q) = \bigcap_{x \in Q} C(x)$. Let $P = \langle x \rangle$, $Q = \langle y \rangle$, then $xy = yx$, so xy is order pq .

Lemma 9: $|G| = p^2 q$ (p, q primes) $\Rightarrow G$ has a normal Sylow subgroup.

Proof: If $n_p > 1$ then $n_p = q \equiv 1 \pmod{p}$. If now $n_q > 1$ then $n_q = p^2$. So we have $p^2(q-1)$ elements of order q . So only have space for p^2 elements of order not q , so $n_p = 1$ after all.

Remark: Burnside p^aq^b theorem shows that $|G| = p^aq^b \Rightarrow G$ not simple.

Lemma 10: If P is a finite p -group then $Z(P) \neq \{e\}$.

Proof: Act by P on $X = P$ by conjugation. The orbits have sizes various powers of p , and $\{e\}$ is an orbit of size 1. So at least p elements of P are in orbits of size 1 - these lie in $Z(P)$.

Lemma 11: If $|P| = p^a$ then P has subgroups of order p^b for all $b \leq a$.

Proof: Induction on a . Let $x \in Z(P)$, of order p . Now $\langle x \rangle \triangleleft P$, so $\bar{P} = P/\langle x \rangle$ is a p -group of order p^{a-1} . By induction, there is a subgroup \bar{Q} of \bar{P} of order p^{b-1} . By the isomorphism theorem (III(a)), there is a subgroup Q of P with $x \in Q$ such that $\bar{Q} = Q/\langle x \rangle$. Then $|Q| = p^b$.

Remark: Similar proof shows that a composition series of a finite p -group has all quotients cyclic order p .

Corollary 12: If $|G| = p^a m$ then G contains subgroups of order p^b for any $b \leq a$ (but they are no longer all conjugate, etc.)

Proposition 13: If G is a non-abelian simple group with a subgroup of index $n > 1$, then $G \leq A_n$.

Moreover, $n \geq 5$ with equality iff $G \cong A_5$

Proof: Take $H \triangleleft G$ of index n . Let G act on the set of left cosets of H in G by left multiplication. We get a permutation representation (non-trivial), $\varphi: G \rightarrow S_n$.

Then, $\ker \varphi \triangleleft G$, so $\ker \varphi = \{e\}$ as G simple. So $G \leq \operatorname{PSL}(2, q)$. Now, $\varphi(G)$ is simple and $\varphi(G) \cap A_n \triangleleft \varphi(G)$ (as $A_n \triangleleft S_n$). So $\varphi(G) \leq A_n$.

Moreover, $n \geq 5$ since A_4 contains no non-abelian simple groups. And, if $n=5$, $G \cong A_5$ since no proper subgroups of A_5 are non-abelian and simple.

Remark: Galois - no non-abelian simple groups of order < 60 .

Example: G simple of order 60 $\Rightarrow G \cong A_5$.

Proof: $n_5 = 6$ ($\neq 1$, as G simple), 24 elements of order 5. $n_3 = 10$ (not 4), 20 elements of order 3. $n_2 = 5$ or 15. $n_2 = 5 \Rightarrow G \cong A_5$ by proposition 13. And $n_2 \neq 15$: here there are Sylow 2-subgroups $P \neq Q$ with $1 \neq t \in P \cap Q$. Then $P, Q \leq C(t)$ as P, Q abelian, so $C(t)$ has order divisible by 4 and greater than 4, so is 12 \Rightarrow index 5, so $G \cong A_5$ - Contradiction.

Remark*: $n_5(G) = 6 \Rightarrow \exists \varphi: G \rightarrow A_5$, homomorphism, injective. So we may assume $G \triangleleft A_6$. G is transitive in the natural action. Since G has index 6 in A_6 , we have a homomorphism $\tau: A_6 \rightarrow A_6$, injective (assuming A_6 simple). Hence τ is an automorphism of A_6 , taking G to the stabiliser of a point in the right-hand A_6 . So $\tau(G) = A_5$. Moreover, note that 3 does not divide the order of the stabiliser in G in the original action, so all elements of order 3 in G have two cycles size 3. But, in $\tau(G)$, we have 3-cycles. So τ sends the conjugacy classes of elements of type 3^2 in A_6 to conjugacy classes of elements of type $3 \cdot 1^3$ - so τ is an "outer" automorphism of A_6 . *

Linear Groups

For a field, $n \in \mathbb{N}$. The general linear group, $GL_n(F)$, is the group of all $n \times n$ matrices over F of $\det \neq 0$. [= $GL(V)$, the group of all non-singular transformations on V]. The special linear group, $SL_n(F)$, is the group of all $n \times n$ matrices over F with $\det = 1$.

$SL_n(F) \triangleleft GL_n(F)$: $SL_n(F)$ is the kernel of $\det: GL_n(F) \rightarrow F^*$ ($= F \setminus \{0\}$)

The centre Z of $GL_n(F)$ consists of all scalar matrices.

If $F = \mathbb{F}_q$, the field of $q = p^a$ elements, write $GL_n(q)$, etc, for the above.

$$|GL_n(q)| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1}) = q^{\frac{1}{2}n(n-1)} \prod_{i=1}^n (q^i - 1). \quad |SL_n(q)| = |GL_n(q)| / q - 1.$$

$$\begin{aligned} \text{Projective Linear groups: } PGL_n(F) &= GL_n(F)/Z. \quad |PGL_n(F)| = |SL_n(q)| \\ PSL_n(F) &= SL_n(F)/Z \cap SL_n(F). \quad |PSL_n(F)| = |SL_n(q)| / (n, q - 1) \end{aligned}$$

A Sylow p -subgroup of $GL_n(p^a)$: $U = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\}$ - upper unitriangular matrices, order $p^{\frac{1}{2}n(n-1)}$.
Normaliser: $B = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$.

Some actions: $GL_n(F)$ acts naturally on the set of vectors (non-zero) in $V = V_n(F)$. Instead, sometimes one considers the action on the set of all 1-dimensional subspaces of V , $PGL_{n-1}(F)$. This latter is not faithful - the kernel is $Z = \{ \text{scalar matrices} \}$.

Example: $n=2$. $F = \mathbb{C}$. $|GL_2(\mathbb{C})| = 2 \mapsto \frac{az+b}{cz+d}$

Example*: $GL_3(2)$ - order 168.



7 points, 7 lines. [Points 1-d subspaces, Lines 2-d subspaces].

$PGL_2(2)$.

3. Reflection Groups

V , Euclidean space dimension n over \mathbb{R} with inner product (\cdot, \cdot) .

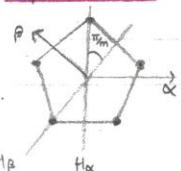
$$O(V) = \{ g \in GL(V) \mid (gv, gw) = (v, w) \forall v, w \in V \}.$$

$0 \neq \alpha \in V$; hyperplane H_α in V : $H_\alpha = \alpha^\perp = \{ v \in V \mid (\alpha, v) = 0 \}$ - codimension 1.

Reflection s_α in H_α - $s_\alpha: v \mapsto v - \frac{2(v, \alpha)}{(\alpha, \alpha)} \alpha$. Note that s_α fixes H_α pointwise, and sends α to $-\alpha$, so it has matrix $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ with respect to some basis.

Here, interested in finite reflection groups; that is, finite subgroups of $O(V)$, generated by reflections. Such a group is essential if no non-zero vector is fixed by the whole group.

(i) Type $F_2(m)$ - these dihedral groups, Dih_{2m} , order $2m$. Here, $n=2$ - rank 2.



H_α, H_β at angle $\frac{\pi}{m}$.

$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -\cos 2\theta & \sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{pmatrix}$ are matrices of s_α, s_β wrt a standard basis.

$I_2(m) = \langle s_\alpha, s_\beta \rangle$. [Note that $s_\alpha s_\beta$ is a rotation of order m].

(iii) Type An - these isomorphic to S_{n+1} . Consider U , dimension $n+1$, with an orthonormal basis $B = \{\epsilon_1, \dots, \epsilon_{n+1}\}$. Now, Sym_{n+1} acts naturally on B , so that $g: \Sigma c_i \epsilon_i \mapsto \Sigma c_i \epsilon_{g(i)}$. All $g \in \text{Sym}_{n+1}$ fix the vector $v = \epsilon_1 + \dots + \epsilon_{n+1}$. Put $V = v^\perp = \{\sum c_i \epsilon_i \mid \sum c_i = 0\}$ - so $\text{Sym}_{n+1} < O(V)$. Now $g = (jk)$ is a reflection on V ; on U it takes $\epsilon_j - \epsilon_k \mapsto -(\epsilon_j - \epsilon_k)$, $\epsilon_j + \epsilon_k \mapsto \epsilon_j + \epsilon_k$, $\epsilon_l \mapsto \epsilon_l$ ($l \neq j, k$). So, a reflection on U , hence also on V . (fixes $(\epsilon_j - \epsilon_k)^\perp$ pointwise).

(iv) Type Bn. This is $S_2 \wr S_n$. $\dim V = n$. Now S_n acts naturally by permuting a fixed orthonormal basis: each permutation can be thought of as a permutation matrix, a matrix with all entries 0 or 1, with precisely one non-zero entry in each row and each column.

The group B_n consists of $n \times n$ matrices with all entries 0, +1, -1, with precisely one non-zero entry in each row and each column. (Check this is a group).

We have a homomorphism $\delta: B_n \rightarrow \text{Sym}_n$, $a \mapsto |a|$ (i.e. replace each -1 by +1), with Kernel consisting of diagonal matrices with entries ± 1 along the diagonal. So the Kernel is elementary abelian of order 2^n . Also, δ is onto. We get: $|B_n| = 2^n \cdot n!$.

It is a reflection group: generator reflections are, for example, transpositions in Sym_n , plus, for each i , $v_{ij}: \epsilon_i \mapsto -\epsilon_i$, $\epsilon_j \mapsto +\epsilon_j$ ($i \neq j$).

(v) Type Dn - subgroups index 2 in B_n , taking matrices in B_n with an even number of -1's, generated by reflections, e.g. all transpositions, plus, for $1 \leq i \leq j \leq n$, $v_{ij}: \epsilon_i \mapsto -\epsilon_j$, $\epsilon_j \mapsto -\epsilon_i$ ($i \neq j$).

(vi) Some sporadic examples: $H_3, H_4, F_4, E_6, E_7, E_8$.

Root Systems.

Lemma 1: Let s_α be a reflection in $O(V)$, let $t \in O(V)$. Then $ts_\alpha t^{-1} = s_{t(\alpha)}$.

Proof: $ts_\alpha t^{-1}$ is a reflection; $t(\alpha)$ is negated by $ts_\alpha t^{-1}$; $t(t(\alpha))$ is fixed pointwise by $ts_\alpha t^{-1}$, since $t(t(\alpha)) \perp t(\alpha)$, since $t \in O(V)$.

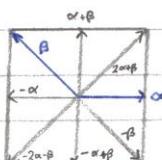
Definition: The finite non-empty subset Φ of V is a root system if:

(i) for $\alpha \in \Phi$, $c \in \mathbb{R}$, $c\alpha \in \Phi$ iff $c = \pm 1$ (R1)

(ii) for any $\alpha \in \Phi$, $s_\alpha(\Phi) = \Phi$ (so $s_\alpha(\beta) \in \Phi$ for $\alpha, \beta \in \Phi$) (R2)

By lemma 1, if we take W any finite reflection group, take all unit vectors perpendicular to reflecting hyperplanes for all the reflections in W , we get a root system. Sometimes it is useful to vary the length. Conversely, starting from a root system, we obtain the reflection group $W = \{s_\alpha \mid \alpha \in \Phi\}$.

Example: $B_2 = I_2(4)$:



Definition: Given a root system Φ , a fundamental subsystem Δ is a basis for $\langle \Phi \rangle$, (F1), such that each element in Φ , when written as a linear combination of Δ , has all coefficients non-negative or non-positive. (F2)

Example: α, β in above example are fundamental.

Definition: The transitive relation $<$ on V is an order on V:

$$(01) v \neq w \Rightarrow v < w \text{ or } w < v.$$

$$(02) v, w, x \in V, v < w \Rightarrow v + x < w + x.$$

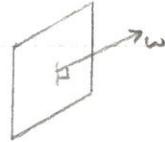
$$(03) v, w \in V, c \in \mathbb{R}, v < w \Rightarrow cv < cw \text{ (if } c > 0\text{)} \text{ or } cw < cv \text{ (if } c < 0\text{)}$$

Example: Lexicographic order wrt a fixed basis v_1, \dots, v_n .

Example: H_w , basis v_1, \dots, v_n . Lexicographic order wrt w, v_1, \dots, v_n .

Positive vectors in $V \setminus H_w$ are those with $(v, w) > 0$.

Given Φ , choose w so that $(\alpha, w) \neq 0$ for $\alpha \in \Phi$.



Given Φ , given order on V , define $\Phi^+ = \{\alpha \in \Phi \mid \alpha > 0\}$ - positive roots.

$\Phi^- = \{\alpha \in \Phi \mid \alpha < 0\}$ - negative roots.

Theorem 2: Let Φ be a root system in V ; let Φ^+ be a positive subsystem. There is a unique fundamental subsystem contained in Φ^+ .

Conversely, given a fundamental subsystem, there is a unique positive subsystem containing it.

Proof: Existence of Δ in Φ^+ . Take Δ to be the smallest subset of Φ^+ such that each element of Φ^+ is a non-negative linear combination of elements in Δ .

Claim: $\alpha, \beta \in \Delta \Rightarrow (\alpha, \beta) \leq 0$.

Proof: Assume not, so $(\alpha, \beta) > 0$. Consider $s_\alpha(\beta) = \beta - c\alpha$, where $c = \frac{2(\alpha, \beta)}{(\alpha, \alpha)} > 0$.

$s_\alpha(\beta) \in \Phi$. If $s_\alpha(\beta) \in \Phi^+$, then β is redundant in Δ : $s_\alpha \beta = \sum_{\gamma \in \Delta} c_\gamma \gamma = c_\beta \beta + \sum_{\gamma \neq \beta} c_\gamma \gamma$. ($c_\gamma \geq 0$).

So, $\beta = c\alpha + (c_\beta - 1)\beta + \sum_{\gamma \neq \beta} c_\gamma \gamma$ ($c > 0, c_\beta \geq 0, \text{ so } c_\beta - 1 \leq 0$). So, $\beta = \frac{c}{1-c_\beta} \alpha + \sum_{\gamma \neq \beta} \frac{c_\gamma}{1-c_\beta} \gamma$.

This is contrary to the minimality of Δ .

If $s_\alpha(\beta) \in \Phi^-$, then α is redundant in Δ . [Exercise, as above. See in $\mathbb{R}^2 = \langle \alpha, \beta \rangle$ that $s_\alpha \beta \in \Phi^-, (\alpha, \beta) > 0 \Rightarrow s_\beta \alpha \in \Phi^+$].

Claim: Δ is linearly independent.

Proof: Assume not, so $\sum_{i \in \Delta} c_i \alpha_i = 0$, with not all $c_i = 0$. Rearrange to get $\sum a_i \alpha_i = \sum b_i \alpha_i =: v$, with the a_i being the positive c_i , and b_i being $-1 \times$ the negative terms c_i .

Then, $0 \leq (v, v) = (\sum a_i \alpha_i, \sum b_i \alpha_i) = \sum_{i,j} a_i b_j (\alpha_i, \alpha_j) \leq 0$. So $v = 0 \nabla$.

Uniqueness of Δ in Φ^+ : It equals the set $\{\alpha \in \Phi^+ \mid \text{if } \alpha = \sum_{\beta \in \Phi^+} c_\beta \beta \text{ with all } c_\beta \geq 0 \text{ then all but one } c_\beta = 0\}$.
[Use linear dependence of Δ].

Conversely: must have $\Phi^+ = \{\sum_{i \in \Delta} c_i \alpha_i \text{ in } \Phi \mid \text{all } c_i \geq 0\}$

[this is Φ^+ in the lexicographic order arising from (ordered) Δ].

Corollary 3: Δ , fundamental subsystem of Φ . If $\alpha \neq \beta \in \Delta$, then $(\alpha, \beta) \leq 0$.

Remark: If a root system, Δ fundamental subsystem corresponding to a positive subsystem Φ^+ , $w \in W = \langle s_\alpha | \alpha \in \Phi \rangle \Rightarrow w(\Delta) = \{w(\alpha) | \alpha \in \Delta\}$ is a fundamental subsystem of the positive subsystem $w(\Phi^+)$.

Towards the converse:

Lemma 4: $\alpha \in \Delta \subset \Phi^+ \subset \Phi$, then α is the only positive root which becomes negative on applying s_α . I.e., $s_\alpha(\Phi^+ \setminus \{\alpha\}) = \Phi^+ \setminus \{\alpha\}$.

Proof: Let $\beta \in \Phi^+ \setminus \{\alpha\}$, so $\beta = \sum_{\delta \in \Delta} c_\delta \delta$, all $c_\delta > 0$ and $c_{\delta_0} > 0$, some $\delta_0 \in \Delta$, $\delta_0 \neq \alpha$.

Now, $s_\alpha \beta = \beta - \frac{2(\alpha, \beta)}{(\alpha, \alpha)} \alpha$; in terms of Δ , the coefficient of δ_0 is unchanged, so all coefficients > 0 (by F2). So $s_\alpha \beta \in \Phi^+$.

Theorem 5: Any two positive (respectively fundamental) subsystems of the root system Φ are W -conjugate - i.e, given Π, Π' positive, $\exists w \in W = \langle s_\alpha | \alpha \in \Phi \rangle$ with $w(\Pi) = \Pi'$.

Proof: Induction on $|\Pi \cap (-\Pi')| := m$. $m=0$, $\Pi = \Pi'$. So let $m > 0$, and assume that it holds for $m-1$. Let Δ be the fundamental subsystem of Π ; then $\Delta \nsubseteq \Pi'$. (Theorem 2 converse) Let $\alpha \in \Delta \cap (-\Pi')$. Then $s_\alpha(\Pi) \cap (\Pi') = (\Pi \cap (-\Pi')) \setminus \{\alpha\}$ by Lemma 4. So, $|\{s_\alpha \gamma | \gamma \in \Pi \cap (-\Pi')\}| = m-1$. By induction, applied to the positive systems $s_\alpha \Pi$ and Π' , there exists a $w \in W$ with $w(s_\alpha \Pi) = \Pi'$. Now, $w s_\alpha \in W$, and sends Π to Π' .

Example: Type A_n . (Sym_{n+1} , dimension n). $V = V_n(\mathbb{R})$. ϵ_i orthonormal basis of a space U , of dimension $n+1$, such that $V = (\epsilon_1 + \dots + \epsilon_{n+1})^\perp$. All reflections come from transpositions. For the transposition $(i j)$ can take root $\epsilon_i - \epsilon_j$; $i \neq j$, so $\Phi = \{\epsilon_i - \epsilon_j | i \neq j\}$. Can take $\Delta = \{\epsilon_i - \epsilon_{i+1} | i \leq n\}$, corresponding to $\Phi^+ = \{\epsilon_i - \epsilon_j | i < j\}$. [Note: $\epsilon_i - \epsilon_j = (\epsilon_i - \epsilon_{i+1}) + (\epsilon_{i+1} - \epsilon_{i+2}) + \dots + (\epsilon_{j-1} - \epsilon_j)$, $i < j$]. Other fundamental sets are $w\Delta$, for various $w \in Sym_{n+1}$.

Note: $Sym_{n+1} = \langle s_\alpha | \alpha \in \Delta \rangle$

Theorem 6: Given a root system Φ , with Δ a fundamental subset. If $W = \langle s_\alpha | \alpha \in \Phi \rangle$, then $W = \langle s_\alpha | \alpha \in \Delta \rangle$.

Proof: Write $W_i = \langle s_\alpha | \alpha \in \Delta \rangle$. Have $W_i \leq W$.

Claim: $\beta \in \Phi^+ \Rightarrow W_i \beta \cap \Delta \neq \emptyset$.

Proof: Write $ht \sum_{\alpha \in \Delta} c_i \alpha := \sum c_i$. Take $\gamma \in W_i(\beta) \cap \Phi^+$ of minimal height.

$(\gamma = \sum_{\alpha \in \Delta} c_i \alpha, c_i \geq 0)$. Now, $0 < (\gamma, \gamma) = \sum c_i (\gamma, \alpha_i) \Rightarrow (\gamma, \alpha_i) > 0$ for some $\alpha_i \in \Delta$ with $c_i > 0$. Then, $\gamma = \alpha_i$. For if not, $s_{\alpha_i} \gamma \in \Phi^+$ by Lemma 4, and $s_{\alpha_i} \gamma = \gamma - \frac{2(\alpha_i, \gamma)}{(\alpha_i, \alpha_i)} \alpha_i$, so $ht s_{\alpha_i} \gamma < ht \gamma$ - contrary to minimality.

Claim: $W_i \Delta = \Phi$. ($W_i \Delta = \{w(\alpha) | w \in W_i, \alpha \in \Delta\}$).

Proof: Let $\beta \in \Phi$. If $\beta \in \Phi^+$, then $w\beta \in \Delta$ for some $w \in W_i$, so $\beta \in w^{-1}\Delta$.

If $\beta \in \Phi^-$, then $w(-\beta) = \alpha \in \Delta$, for some $w \in W_i$, $\alpha \in \Delta$, so $\beta = w^{-1}s_\alpha \alpha$.

Finally, $W_i = W$: Let $\beta \in \Phi$. Then $\beta = w(\alpha)$ for some $w \in W_i$, $\alpha \in \Delta$, so $s_\beta = s_{w(\alpha)} = ws_\alpha w^{-1} \in W_i$.

Corollary 7: Any root lies in some fundamental set.

Corollary 8: Any reflection group of rank 2 is dihedral. For it is generated by two reflections, so dihedral by exercise sheet 2, question 1.

Generators and Relations.

$\Delta \subset \Phi^+$, fixed. $W = \langle s_\alpha | \alpha \in \Phi \rangle = \langle s_\alpha | \alpha \in \Delta \rangle$.

Write $s_i := s_{\alpha_i}$ for $\alpha_i \in \Delta$ - fundamental reflections.

Now, $s_i s_j \in \Delta$, order m_{ij} , so have $(s_i s_j)^{m_{ij}} = 1$ - Fundamental relations. (Note: $m_{ii} = 1$)
We are going to prove that all relations can be deduced from the fundamental relations.

Definition: $w \in W$. Write $l(w)$ for the minimal length of an expression for w in terms of the fundamental reflections. And, $n(w) = |w \Phi^+ \cap \Phi^-| =$ number of positive roots made negative by w .

Note: $n(1) = 0 = l(1)$, and $l(w) = 1 \Rightarrow n(w) = 1$. In fact, about to show $n(w) = l(w) \quad \forall w \in W$.

Lemma 9: If $\alpha \in \Delta$, $w \in W$, then $n(ws_\alpha) = \begin{cases} n(w) + 1 & \text{if } w(\alpha) \in \Phi^+ \\ n(w) - 1 & \text{if } w(\alpha) \in \Phi^- \end{cases}$. $[n(s_\alpha w) = \begin{cases} n(w) + 1 & \text{if } w^{-1}\alpha \in \Phi^+ \\ n(w) - 1 & \text{if } w^{-1}\alpha \in \Phi^- \end{cases}]$.

Proof: Φ^+ : $\alpha \longleftarrow$

\downarrow $\alpha \longleftarrow \Phi^+ \setminus \{\alpha\}$. s_α permutes $\Phi^+ \setminus \{\alpha\}$.

Now apply w : $n(ws_\alpha) = n(w) \pm 1$, with + precisely when $w \in \Phi^+$. (Then $ws_\alpha \in \Phi^-$).

Theorem 10 (Deletion Theorem): Let $w = s_{i_1} \dots s_{i_r}$, with s_{i_j} fundamental, and suppose $n(w) < r$. Then there exists j, k (with $1 \leq j < k \leq r$) such that $w = s_{i_1} \dots \hat{s}_{i_j} \dots \hat{s}_{i_k} \dots s_{i_r}$.
I.e. can delete s_{i_j} and s_{i_k} from the expression.

Corollary 11: $n(w) = l(w)$

Proof: $n \leq l$: $w = s_{i_1} \dots s_{i_r}$ reduced (so $l = l(w)$), then $w = \hat{s}_{i_1} \dots \hat{s}_{i_r}$. Now, $n(1) = 0$, and each s_{i_j} "increases" n by ± 1 (lemma 9), so l such changes. So $n(w) \leq l = l(w)$.
 $n \geq l$: by Theorem 10: If $n(w) < l$, can shorten.

Proof of Theorem 10: By lemma 9, for some $k \leq r$, $s_{i_1} \dots s_{i_{k-1}} \alpha_{i_k} \in \Phi^-$ (otherwise $n(w) = r$).

For some $j < k$, $s_{i_j} s_{i_{j+1}} \dots s_{i_{k-1}} \alpha_{i_k} \in \Phi^-$, but $s_{i_{j+1}} \dots s_{i_{k-1}} \alpha_{i_k} \in \Phi^+$. It follows that $\alpha_{i_j} = s_{i_{j+1}} \dots s_{i_{k-1}} \alpha_{i_k}$ (since α_{i_j} is unique root in Φ^+ sent to Φ^- by s_{i_j}).

Thus, $s_{\alpha_{i_j}} = s_{i_j} = s_{s_{i_{j+1}} \dots s_{i_{k-1}} \alpha_{i_k}} = (s_{i_{j+1}} \dots s_{i_{k-1}}) s_{i_k} (s_{i_{j+1}} \dots s_{i_{k-1}})^{-1}$. So, $s_{i_j} s_{i_{k-1}} s_{i_k} = s_{i_{j+1}} \dots s_{i_{k-1}}$.

Corollary 12: For $w \in W$, equivalent are: $w=1$, $l(w)=0$, $n(w)=0$, $w\Phi^+ = \Phi^-$.

Corollary 13: There is a unique element $w_0 \in W$ with $w_0(\Phi^+) = \Phi^-$; we have $l(w_0) = |\Phi^+| = \frac{1}{2}|\Phi|$.

Proof: Φ^- is positive in some order, so $\exists w_0$. Unique by lemma 2.

Theorem 14: Δ fundamental set in the root system \mathbb{P} . $\langle s_i \mid \alpha_i \in \Delta \rangle = \langle s_i \mid s_i^2 = 1 \rangle$. Then any relation $s_{i_1} \dots s_{i_r} = 1$ in $\langle s_i \mid s_i^2 = 1 \rangle$ is a consequence of the relations $(s_i s_j)^{m_{ij}} = 1$. [fundamental or Coxeter relations]

* Proof: Induction on r . Note that r is even, say $r = 2q$ (since $\det s_i = -1$).

Case $r=2$: $s_{i_1} s_{i_2} = 1$, so $s_{i_2} = s_{i_1}^{-1} = s_{i_1}$, so we have $s_{i_1}^2 = 1$ - a Coxeter relation.

Now, $r > 2$. Assume okay for shorter relations. [To simplify notation, delete the i].

$s_{i_1} \dots s_{q+1} = s_{i_1} \dots s_{q+2}$ (1). As $q+1 > q-1$, $\exists i < j \leq q+1$ such that $s_{i_1} \dots s_j = s_{i_1} \dots s_{j-1} \dots$

So $s_{i_1} \dots s_j s_{j-1} \dots s_{q+1} = 1$ (2).

If this is shorter than r letters, can deduce this from the fundamental relations, so from (1) and the fundamental relations, have $s_{i_1} \dots \hat{s}_i \dots \hat{s}_j \dots s_{q+1} = s_{i_1} \dots s_{q+2}$ - i.e. a shorter relation, which we can deduce from the fundamental relations.

So, only problem is if (2) has r letters, so $i=1, j=q+1$, so $s_{i_1} \dots s_{q+1} = s_{i_1} \dots s_q$ (3).

Try instead: $s_{i_1} \dots s_r s_{i_1} = 1$. Then the above will work, unless $s_3 \dots s_{q+2} = s_2 \dots s_{q+1}$ (4), so

$s_3 s_2 s_3 \dots s_{q+1} s_{q+2} s_{q+1} \dots s_4 = 1$. Try again - will work unless $s_3 s_2 \dots s_{q+1} = s_3 s_2 s_3 \dots s_q$ (5)

Compare (3) and (5) - have $s_1 = s_3$. Now try $s_3 \dots s_r s_{i_1} = 1$ - will work unless $s_2 = s_4$.

By induction, will succeed unless $s_1 = s_3 = \dots = s_{q-1}$ and $s_2 = s_4 = \dots = s_r$.

So the only remaining case is $s_1 s_2 \dots s_r s_{i_1} = (s_1 s_2)^q = 1$. Since m_{12} is the order of $s_1 s_2$, we have $m_{12} | q$, and the relation follows from the relation $(s_1 s_2)^{m_{12}} = 1$.

Remark: A more geometric proof is in Grove & Benson, pp 88-92. *

Coxeter Graphs

$\Delta \subset \mathbb{P}^+ \subset \mathbb{P}$, $\langle s_\alpha \mid \alpha \in \Delta \rangle = \langle s_i \mid \alpha_i \in \Delta \rangle$, $m_{ij} = o(s_i s_j)$. The corresponding Coxeter graph: vertices $1, \dots, n$. Join i, j by an edge if $m_{ij} \geq 3$, label the edge by m_{ij} if $m_{ij} > 3$.

Example: $I_2(m) = \text{Dih}_{2m}$



$\begin{matrix} m \\ 1 & 2 \end{matrix}$

Example: A_n ($= \text{Sym}_{n+1}$). Fundamental reflections can be taken to be: $(12), (23), \dots, (n \ n+1)$



Generalised Coxeter graph: any such labelled graph.

Corresponding Coxeter matrix: $n \times n$, $a_{ij} = -\cos \frac{\pi}{m_{ij}}$

Examples: • $I_2(m)$ has matrix $\begin{pmatrix} 1 & -\cos \frac{\pi}{m} \\ -\cos \frac{\pi}{m} & 1 \end{pmatrix}$

• A_n has matrix $\begin{pmatrix} \frac{1}{2} & 0 & & \\ 0 & \ddots & & \\ & & \ddots & 0 \\ & & 0 & \frac{1}{2} \end{pmatrix} \quad \left[-\frac{1}{2} = -\cos \frac{\pi}{3} \right]$

Lemma 15: If W_1, W_2 are essential reflection groups on V with the same Coxeter graph then they are conjugate in $O(V)$.

Proof: Take the roots to be unit vectors. Let Δ_1, Δ_2 be fundamental sets for the root systems Ξ_1, Ξ_2 , defining W_1, W_2 respectively. Let $\varPhi: \Delta_1 \rightarrow \Delta_2$, extend linearly. Then \varPhi preserves angles and lengths (on Δ_1 , hence on $\langle \Delta_1 \rangle$). So $\varPhi \in O(V)$. And, \varPhi conjugates the generators of W_1 to the generators of W_2 , so takes W_1 to W_2 .

Lemma 16: Δ fundamental set in Ξ , consisting of unit vectors. Then the Coxeter matrix is positive definite.

Proof: The Coxeter matrix is the matrix of the inner product of $\langle \Xi \rangle$ with respect to the basis Δ .

Lemma 17: If the Coxeter graph on Δ is not connected, say splits ~~into~~ vertices into A, Δ_2 , then $W = W_1 \times W_2$, W_i a reflection group on $V_i = \langle \Delta_i \rangle$, $w_i = \langle s_j | x_j \in \Delta_i \rangle$.

Proof: No edges from Δ_1 to Δ_2 , so $\langle \Delta \rangle = \langle \Delta_1 \rangle \perp \langle \Delta_2 \rangle$. If $\alpha \in \Delta_1$, then s_α is trivial on V_2 and $s_\alpha(V_1) \subset V_1$. If $w \in W$, write it as the product of fundamental reflections; since $s_\alpha s_\beta = s_\beta s_\alpha$ for $\alpha \in \Delta_1, \beta \in \Delta_2$, so we can rearrange to get $w = w_1 w_2$ with $w_i \in W_i$. Hence $W_1 \triangleleft W$, $W_1 \cap W_2 = 1$, so $W = W_1 \times W_2$.

Theorem 18 (Classification of irreducible root systems): The positive definite connected (generalised) Coxeter graphs are precisely $A_n, B_n (n \geq 2), D_n (n \geq 4), I_2(m), F_4, E_6, E_7, E_8, H_3, H_4$. (See example sheet 2)

Lemma 19: Let Γ' be a (generalised) Coxeter graph obtained from the (generalised) Coxeter graph Γ by deleting vertices (and adjacent edges) and/or by decreasing some labels (including removing some edges). If the Coxeter matrix $A(\Gamma)$ of Γ is positive definite, then so is $A(\Gamma')$, the Coxeter matrix of Γ' .

Proof: Number the vertices of Γ so that precisely $1, \dots, k$ are in Γ' . Writing $C = A(\Gamma)$, $D = A(\Gamma')$, we have $c_{ij} \leq d_{ij} \quad \forall i, j \leq k$. If D is not positive definite, then $\exists \mathbf{x} \in \mathbb{R}^k, \mathbf{x} \neq 0$ with $\sum_{i,j \leq k} d_{ij} x_i x_j \leq 0$. Let $\mathbf{v} = (|x_1|, \dots, |x_k|, 0, \dots, 0) \in \mathbb{R}^k$. Then $\mathbf{v} \neq 0$, so $\sum c_{ij} |x_i| |x_j| > 0$. But, $0 \geq \sum d_{ij} x_i x_j \geq \sum d_{ij} |x_i| |x_j| \geq \sum c_{ij} |x_i| |x_j| > 0$ - Contradiction.

Lemma 20: If the vertex n in Γ is joined to a unique vertex, say $n-1$, and if $m_{n,n-1}$ is 3 or 4, then $\det 2A = 2\det 2B - (m_{n,n-1} - 2)\det 2C$, where $A = A(\Gamma)$, $B = A(\Gamma \setminus \{n\})$, $C = A(\Gamma \setminus \{n, n-1\})$.

Proof: $2A = \begin{pmatrix} 2 & & 0 \\ & \ddots & \\ 0 & & x^2 \end{pmatrix}$, $\det 2A = 2\det 2B - x^2 \det 2C$, and $x^2 = m-2$ if $m=3$ or 4.

Remark: If A is the Coxeter matrix of one of the root systems A_n, \dots, H_4 , then $\det 2A$ is given on exercise sheet 2, question 9.

In particular, A is positive definite. (Look at principal minors)

Lemma 21: The Coxeter matrices of the "extended" Coxeter diagrams (in table on page 3 of example sheet 3) have $\det 0$.

Proof: e.g. \tilde{A}_n : Have $2\tilde{A}_n = \begin{pmatrix} 2 & -1 & & \\ -1 & 2 & \dots & \\ & \ddots & \ddots & -1 \\ & & -1 & 2 \end{pmatrix}$. Adding all rows gives a zero row. Etc.

Example: $\det 2\tilde{B}_2 = 2\det 2B_2 - 2\det 2A_1 = 0$.

Proof of Theorem 18: Use lemmas 19 and 21 - exercise.

Example: must have a labelled tree (using lemmas 19 and 21 for \tilde{A}_n)
No proper subgraph of $I_2(m)$ with $m \geq 5$.

Crystallographic Root Systems.

In applications (e.g. in Lie Theory) often have a further condition on root systems.

Definition: The finite set Φ of vectors in V is a crystallographic root system if:

(R1): $\alpha \in \Phi \Rightarrow c\alpha \in \Phi$ iff $c = \pm 1$,

(R2): $\alpha, \beta \in \Phi \Rightarrow s_\beta \alpha \in \Phi$,

(R3) $\alpha, \beta \in \Phi \Rightarrow \frac{2(\alpha, \beta)}{(\alpha, \alpha)} \in \mathbb{Z}$ - Cartan integers.

Lemma 22: In a crystallographic root system, all the labels m_{ij} are in $\{2, 3, 4, 6\}$ for $i \neq j$.

Proof: $\frac{2(\alpha_i, \alpha_j)}{(\alpha_i, \alpha_i)} = 4 \cos^2 \theta_{ij}$, where θ_{ij} is the obtuse angle between α_i and α_j .

So $4 \cos^2 \theta_{ij} \in \{0, 1, 2, 3, 4\}$, so $\theta_{ij} \in \{\frac{\pi}{2}, \frac{2\pi}{3}, \frac{3\pi}{4}, \frac{5\pi}{6}\}$.

[Also getting information about the ratios $\frac{|\alpha_i|}{|\alpha_j|} = 2, 1, \sqrt{2}, \sqrt{3}$]

Remark: This shows that each root in such a system lies in a \mathbb{Z} -span of Δ .
(Exercise. Hint: induction on height α).

Cartan matrix is the integral $n \times n$ matrix $A_{ij} = \frac{2(\alpha_i, \alpha_j)}{(\alpha_i, \alpha_i)}$

Dynkin diagram - like Coxeter graph, except that edges labelled 4 are replaced by double edges, and those labelled 6 by triple edges. Eg: $I_2(4) \xrightarrow[4]{\text{---}} \bullet \bullet$.

Any $W = \langle s_\alpha \mid \alpha \in \Phi \rangle$ for Φ crystallographic is a Weyl group.

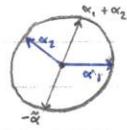
Examples 23: iii) A_n . ϵ_i , orthonormal in \mathbb{R}^{n+1} . $V = \{\sum \lambda_i \epsilon_i \mid \sum \lambda_i = 0\}$.

Roots: $\epsilon_i - \epsilon_j$, $i \neq j$ - $n(n+1)$ such.

Fundamental set: $\alpha_i = \epsilon_i - \epsilon_{i+1}$ ($1 \leq i \leq n$)

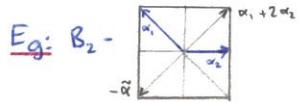
Highest root: $\tilde{\alpha} = \epsilon_1 - \epsilon_{n+1} = \alpha_1 + \dots + \alpha_n$

Eg: A_2 -



A_n : goes to "extended" \tilde{A}_n : by inclusion of $\tilde{\alpha}$.

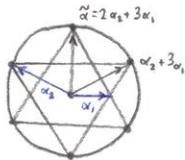
(iii) B_n . $V = \mathbb{R}^n$. \mathbb{E} , all the vectors in standard lattice of length 1 or $\sqrt{2}$.
 $2n$ short vectors, $\pm \epsilon_i$. $2n(n-1)$ long vectors, $\pm \epsilon_i \pm \epsilon_j$.
 Δ : $\alpha_i = \epsilon_i - \epsilon_{i+1}$ ($i < n$), $\alpha_n = \epsilon_n$.
 $\tilde{\alpha} = \epsilon_1 + \epsilon_2 = \alpha_1 + 2\alpha_2 + \dots + 2\alpha_n$.



Extended Coxeter graph for B_n ($n \geq 3$):

iv) C_n , "inverse" or "dual" to B_n . Replace each α by $\frac{2}{(\alpha, \alpha)}\alpha$.
 $2n$ long roots, $\pm 2\epsilon_i$. $2n(n-1)$ short roots, $\pm \epsilon_i \pm \epsilon_j$.
 Δ : $\alpha_i = \epsilon_i - \epsilon_{i+1}$, $\alpha_n = 2\epsilon_n$.
 $\tilde{\alpha} = 2\epsilon_1 = 2\alpha_1 + \dots + 2\alpha_{n-1} + \alpha_n$.

(iv) G_2 is $I_2(6)$:



Extended diagram:

$\Delta \subset \mathbb{E}$. Highest root $\tilde{\alpha}$ - existence clear. Have $(\tilde{\alpha}, \alpha_i) \geq 0 \quad \forall \alpha_i \in \Delta$ (else $s_i \tilde{\alpha}$ is higher). So $\tilde{\alpha}$ is in the fundamental domain (exercise sheet 2, question 11).

Lemma 24: The stabiliser W of $\tilde{\alpha}$ (and any v in fundamental domain) is generated by the fundamental reflections corresponding to $\alpha_i \perp \tilde{\alpha}$.

Proof: Write $W_i = \langle s_i \mid \alpha_i \in \Delta \cap \tilde{\alpha}^\perp \rangle$. $W_i \subseteq W_{\tilde{\alpha}}$ - clear.

Let $w \in W_{\tilde{\alpha}}$. Use induction on $l(w)$. If $l(w) = 0$ then $w \in W_i$, so ~~w~~ assume $l(w) > 0$, and true for shorter elements. Now, $n(w) > 0$. Let $\alpha \in \Delta$ with $w\alpha \in \mathbb{E}$.

Now, $0 \leq (\tilde{\alpha}, \alpha) = (w\tilde{\alpha}, w\alpha) \leq 0$ as ~~w~~ $\in \mathbb{E}^\perp$ and $w\tilde{\alpha} = \tilde{\alpha}$. So $\alpha \perp \tilde{\alpha}$.

And, $ws_\alpha \in W_{\tilde{\alpha}}$, $l(ws_\alpha) = n(w)-1$, so $ws_\alpha \in W_i$. So $w \in W_i$.

Note: How we use $W_{\tilde{\alpha}} = \langle s_{\alpha_i} \mid \alpha_i \in \Delta \cap \tilde{\alpha}^\perp \rangle$.

Eg: $W = A_n$: $\tilde{\alpha}$ perpendicular to $\alpha_1, \dots, \alpha_{n-1}$.



So $W_{\tilde{\alpha}} = \langle s_2, s_{n-1} \rangle = A_{n-2}$.

Lemma 25: W is transitive on the set of all long (short) roots.

Example: $|A_n| = \# \text{roots}. |A_{n-2}| = n(n+1). (n-1)! = (n+1)!$

Proof: Each root is conjugate to a fundamental root, so enough to show one W -orbit of long (short) fundamental roots, since, from classification, all long (short) fundamental roots are at the same end of the diagram, and we may assume we are ~~not~~ considering two joined fundamental roots, and this is now a question about A_2 - easy.

Important subgroups, parabolic subgroups, generated by various subsets of the fundamental set.

Example: A_n - a maximal parabolic - corresponds to $n = n_1 + n_2$. - $S_{n_1} \times S_{n_2}$.

Back to linear groups, from this point of view: $G = GL_n(F)$, $U = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\}$, $B = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$.
 $B = N(U) = UH$ (H diagonal). $N := N(H)$ - all monomial matrices.

Weyl group of GL_n : $N/H \cong \text{Sym}_n$.

4. Representation Theory

- of finite groups over $F = \mathbb{C}$. G a finite group (or, $\text{char } F \nmid |G|$).

Representations; Modules

Representation space of G over \mathbb{C} , or a $\mathbb{C}G$ -space is a finite dimensional vector space V over \mathbb{C} , with G acting on V linearly:

have $*$: $G \times V \rightarrow V$ such that for $g, h \in G$, $v, u \in V$, $\lambda \in \mathbb{C}$ have $(gh)v = g(hv)$,
 $g(u+v) = gu+gv$, $1v = v$, $g(\lambda v) = \lambda gv$.

Thus, for each $g \in G$, get a linear transformation: $\rho(g) \in GL(V)$, and the map $\rho: G \rightarrow GL(V)$; $g \mapsto \rho(g)$ is a homomorphism - a linear representation of G .

This way, V becomes a $\mathbb{C}G$ -module. Write $R = \mathbb{C}G = \left\{ \sum_{g \in G} \lambda_g g \mid \lambda_g \in \mathbb{C} \right\}$, with $\sum \lambda_g g + \sum \mu_h h = \sum (\lambda_g + \mu_h) g$, $(\sum \lambda_g g)(\sum \mu_h h) = \sum_{g,h} \lambda_g \mu_h gh$.

With these operations, $\mathbb{C}G$ is a ring (non-commutative unless G is abelian)

V is a left R -module if R is a ring. V an abelian group, with $x: R \times V \rightarrow V$ such that $r(v+w) = rv+rw$, $(r+s)v = rv+sv$, $(rs)v = r(sv)$, $1v = v$.

$\rho: G \rightarrow GL(V)$, linear representation of degree n . ($\dim V = n$), B a basis of V .

The map $g \mapsto [\rho(g)]_B$ is a homomorphism $G \rightarrow GL_n(\mathbb{C})$ - a matrix representation.

What if we take basis B' instead B ?

Definition: The matrix representations $\rho, \sigma: G \rightarrow GL_n(\mathbb{C})$ are equivalent (or similar) if $\exists T \in GL_n(\mathbb{C})$ such that $\rho(g) = T\sigma(g)T^{-1} \quad \forall g \in G$.

Definition: A linear map $T: V \rightarrow W$ between $\mathbb{C}G$ -spaces is a $\mathbb{C}G$ -homomorphism if $T(g*v) = g*(Tv)$.

$\text{Hom}_{\mathbb{C}G}(V, W)$ - linear maps $V \rightarrow W$, $\text{Hom}_{\mathbb{C}G}(V, W) \sim \mathbb{C}G$ -homomorphisms.

If $V = W$, write $\text{End}_{\mathbb{C}G}(V, V)$, $\text{End}_{\mathbb{C}G}(V, V)$ for these.

The degree of ρ is the dimension of V . The representation is faithful if $\ker \rho =$

Examples: i) $G \rightarrow \mathbb{C}^*$; $g \mapsto 1$. Degree = 1. "Trivial representation."

ii) $G = C_N = \langle x | x^N = 1 \rangle$. $\rho: G \rightarrow GL_n(\mathbb{C})$ is determined by $\rho(x)$ [as $\rho(gx) = \rho(g)\rho(x)$].

Let ω be an ordinary N th root of unity, and let $\rho: G \rightarrow \mathbb{C}^*$; $x^i \mapsto \omega^i$.

Get N such representations of degree 1.

Some "further" examples: $\rho_1: C_3 \rightarrow GL_2(\mathbb{C})$; $x^i \mapsto \begin{pmatrix} \omega^i & 0 \\ 0 & \omega^{-i} \end{pmatrix}$ or
 $\rho_2: C_3 \rightarrow GL_2(\mathbb{C})$; $x^i \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$.

Definition: The subspace W of V is a $\mathbb{C}G$ -subspace if closed under the action of G
- so $gw \in W \forall g \in G, w \in W$.

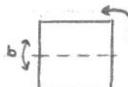
In this case, choosing B sensibly, have $[\rho(g)]_B = \begin{pmatrix} A(g) & C(g) \\ 0 & B(g) \end{pmatrix} \quad \forall g \in G$.

We say that the $\mathbb{C}G$ -space V is reducible if it has a non-trivial $\mathbb{C}G$ -subspace.

Otherwise it is irreducible.

If $V = U \oplus W$, with U, W non-trivial $\mathbb{C}G$ -subspaces, then V is decomposable. If no such exists, V is indecomposable.

Example: $G = D_8 = \langle a, b | a^4 = b^2 = 1, bab = a^{-1} \rangle$



$$\rho(a) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \rho(b) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Thinking of ρ as given wrt standard basis, have $\rho(a): \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} -y \\ x \end{pmatrix}$, $\rho(b): \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x \\ -y \end{pmatrix}$. So this representation is irreducible. $[\begin{pmatrix} x \\ y \end{pmatrix} \in W \subseteq V - \text{apply } \rho(a), \rho(b) \text{ and get } \begin{pmatrix} x \\ y \end{pmatrix} = 0]$.

Schur's Lemma

Lemma 2 (Schur's Lemma): (a) Assume V, W are irreducible $\mathbb{C}G$ -modules. Then any $\mathbb{C}G$ -homomorphism $\theta: V \rightarrow W$ is either 0 or an isomorphism.

(b) Assume V is an irreducible $\mathbb{C}G$ -module, over F algebraically closed. Then any $\mathbb{C}G$ -endomorphism on V is a scalar multiple of I .

Proof: Let $\theta: V \rightarrow W$, an $\mathbb{C}G$ -homomorphism. Note that $\ker \theta \leq V$ and $\theta V \leq W$, as submodules.

[Eg, θV is a vector subspace, and given $w \in \theta V$, $g \in G$, say $w = \theta v$, have $gw = g\theta v = \theta gv \in \theta V$.]

(a) Assume $\theta \neq 0$. Then $\ker \theta \neq V$, so $\ker \theta = 0$ (as V irreducible). So θ is injective.

And $0 \neq \theta V \leq W$, so $\theta V = W$ (as W is irreducible). So θ is surjective.

(b) Since F is algebraically closed, θ has an eigenvalue λ . Then, $\theta - \lambda I$ is a singular endomorphism on the irreducible module V , so $\theta = \lambda I$, by (a).

Corollary 3: If V, W are irreducible $\mathbb{C}G$ -modules, then $\dim_{\mathbb{C}} \text{Hom}_{\mathbb{C}G}(V, W) = \begin{cases} 1 & \text{if } V \cong W \\ 0 & \text{otherwise.} \end{cases}$

Proof: If $V \not\cong W$, then $\text{Hom}_{\mathbb{C}G}(V, W) = 0$ by lemma 2(a).

If $V \cong W$ and $\theta_1, \theta_2: V \rightarrow W$ are two non-zero $\mathbb{C}G$ -homomorphisms, then θ_2 is invertible (by lemma 2(a)), and $\theta_2^{-1}\theta_1: V \rightarrow V$ is a non-zero $\mathbb{C}G$ -endomorphism.

Corollary 4: If the finite group G has a faithful irreducible complex representation, then the centre $Z(G)$ is cyclic.

Proof: Let $\rho: G \rightarrow \text{GL}_n(\mathbb{C})$, faithful. Let $z \in Z(G)$; then $gz = zg$ for all $g \in G$. Hence the map $v \mapsto zv$ for $v \in V$ is a $\mathbb{C}G$ -endomorphism on V . Thus there exist $\lambda_z \in \mathbb{C}$ such that $zv = \lambda_z v$ for all v . Then the map $z \mapsto \lambda_z$ is a homomorphism $Z(G) \rightarrow \mathbb{C}^*$, injective (since ρ is faithful). So $Z(G)$ is isomorphic to a finite subgroup of \mathbb{C}^* and hence is cyclic.
[If $|Z(G)| = n$, the image is $\langle e^{\frac{2\pi i}{n}} \rangle$.]

Corollary 5: If G is an abelian group, then every irreducible $\mathbb{C}G$ -module has degree 1.

Proof: Consider the $\mathbb{C}G$ -module V . For $x \in G$, the map $\theta_x: v \mapsto xv$ is a $\mathbb{C}G$ -endomorphism on V (as $xg = gx \forall g \in G$). So, $\theta_x = \lambda_x i$ for some $\lambda_x \in \mathbb{C}$; that is, $xv = \lambda_x v$ for all $v \in V$. So any vector subspace of V is in fact a $\mathbb{C}G$ -subspace, and as V is irreducible, have $\dim V = 1$.

Corollary 6: Let G be a finite abelian group isomorphic to $C_{n_1} \times \dots \times C_{n_r}$, with each C_{n_i} cyclic. Then G has precisely $|G|$ irreducible representations, each of degree 1.

Remark: All finite abelian groups are like this!

Proof: $G = C_{n_1} \times \dots \times C_{n_r}$, where $C_{n_i} = \langle x_i \mid x_i^{n_i} = 1 \rangle$.

Let $\rho: G \rightarrow \text{GL}_n(\mathbb{C})$, irreducible. Then $n=1$, by corollary 5. Let $\rho: (1, \dots, 1, x_i, 1, \dots, 1) \mapsto \lambda_i (\in \mathbb{C})$, then $\lambda_i^{n_i} = 1$, so λ_i is an n_i th root of 1. Now, the values $\lambda_1, \dots, \lambda_r$ determine ρ , for: any $g \in G$ can be written as $(x_1^{i_1}, \dots, x_r^{i_r})$, $0 \leq i_j < n_j$. This is: $(x_1, \dots, 1)^{i_1} (1, x_2, \dots, 1)^{i_2} \dots (1, \dots, 1, x_r)^{i_r}$, so $\rho(g) = \lambda_1^{i_1} \dots \lambda_r^{i_r}$. Thus ρ corresponds to an r -tuple $(\lambda_1, \dots, \lambda_r)$ with $\lambda_i^{n_i} = 1$.

Conversely, any r -tuple like this yields a representation (in this way) of degree 1. Thus we get all the $|G|$ ($= n_1 n_2 \dots n_r$) inequivalent representations, and they are of degree 1.

Maschke's Theorem

If $\rho(g) = \begin{pmatrix} A(g) & C(g) \\ 0 & B(g) \end{pmatrix}$ for each $g \in G$, then we can change basis and split into (\oplus) .
So reducible \Rightarrow decomposable, over \mathbb{C} (or $\text{char } F \nmid |G|$).

Theorem 7 (Maschke's Theorem): Assume that G is a finite group, F a field of characteristic 0, ($\text{or } \text{char } F = p > 0$, $p \nmid |G|$). If U is an $\mathbb{F}G$ -subspace of the $\mathbb{F}G$ -space V , then there exists an $\mathbb{F}G$ -subspace W such that $V = U \oplus W$.

Remark: The assumptions are necessary. For example, if $G \leq \text{GL}_2(F)$ with (i) $G = \{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mid \text{ne } \mathbb{Z} \}$ if $F = \mathbb{C}$, (iii) $G = \{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mid R \in \mathbb{F}_p \}$ if $F = \mathbb{F}_p$, then G has a unique 1-dimensional $\mathbb{F}G$ -subspace.

Proof of Theorem 7: Write $V = U \oplus W_0$, where W_0 is any vector space complement. Let θ be the corresponding projection $V \rightarrow U$ given by $u + w_0 \mapsto u$. Modify θ to get an $\mathbb{F}G$ -map Φ :
 $\Phi_v := \frac{1}{|G|} \sum_{g \in G} g \theta g^{-1} v$. Then Φ is \mathbb{F} -linear, being a composition of \mathbb{F} -linear maps: g, θ, g^{-1} .
Also, if $x \in G$, $\Phi(xv) = \frac{1}{|G|} \sum_{g \in G} g \theta g^{-1} (xv) = \frac{1}{|G|} \sum_{g \in G} xgh \theta h^{-1} v = x \cdot \frac{1}{|G|} \sum_{h \in G} h \theta h^{-1} v = x \Phi(v)$, as required for Φ .

$$\text{(let } h^{-1} = g^{-1}x\text{)}$$

$$\text{linearity of } x$$

Next, $\Phi(u) = u$. And for $\Phi(u) = \frac{1}{|G|} \sum_{g \in G} g \Phi(g^{-1}u) = \frac{1}{|G|} \sum_{g \in G} gg^{-1}u = u$, since $g \in G \Rightarrow g^{-1}u \in G$
 $\Rightarrow \Phi(g^{-1}u) = g^{-1}u$.

Let $W = \ker \Phi$; this is an $\mathbb{C}G$ -subspace. Also, $U \cap W = \{0\}$ [as $\Phi|_U = \text{id}_U$], and
 $V = U \oplus W$. [as $v = \Phi(v) + (v - \Phi(v))$].

Corollary 8: If G is finite, any finite dimensional $\mathbb{C}G$ -module is the direct sum of irreducible modules.

Remark: All finitely generated $\mathbb{C}G$ -modules are completely reducible.

Warning: "Irreducible" \Rightarrow "completely reducible". Not to be confused with "absolutely reducible".

Proof of corollary 8: Induction on dimension. If V is irreducible, then nothing to prove.

If not, U is a non-trivial $\mathbb{C}G$ -subspace, then $V = U \oplus W$ for some $\mathbb{C}G$ -subspace W . By induction, $U = U_1 \oplus \dots \oplus U_k$, $W = W_1 \oplus \dots \oplus W_l$ with U_i, W_j irreducible, and hence $V = U_1 \oplus \dots \oplus U_k \oplus W_1 \oplus \dots \oplus W_l$.

There is some uniqueness:

Theorem 9: G finite, V a $\mathbb{C}G$ -module, $V = U_1 \oplus \dots \oplus U_n = W_1 \oplus \dots \oplus W_m$, with the U_i, W_j all irreducible. Let X be an irreducible $\mathbb{C}G$ -module; let U be the sum of all the U_i which are isomorphic to X , and let W be the sum of all the W_j which are isomorphic to X . Then $U = W$.

In particular, the number of the U_i isomorphic to X equals the number of the W_j isomorphic to X , and $n = m$.

Remarks: (i) This submodule U above is the homogeneous component, $V(X)$, of V corresponding to the irreducible $\mathbb{C}G$ -module X .

(ii) Cannot expect $U_i = W_j$ in general. Eg: $V = \mathbb{C}^2$, $G = \mathbb{Z}/2\mathbb{Z}$.

Proof of Theorem 9: Let $\theta_{kj}: U_k \xrightarrow{i_k} V \xrightarrow{\pi_j} W_j$ be the composition $\pi_j \circ i_k$, where i_k is the inclusion map and π_j is the projection. Then θ_{kj} is a $\mathbb{C}G$ -homomorphism, so is 0 unless $U_k \cong W_j$ (Schur). If $U_k \cong X$, it follows that $U_k \subseteq W$, since all the other projections are 0. So $U \subseteq W$, and also $W \subseteq U$, so $U = W$.
The "in particular" follows by dimensions.

Remark 10: In fact, writing $\langle X, V \rangle$ for the number of summands isomorphic to X irreducible $\mathbb{C}G$ -module X in any direct sum decomposition of the $\mathbb{C}G$ -module V into irreducibles, we have $\langle X, V \rangle = \dim_{\mathbb{C}} \text{Hom}_{\mathbb{C}G}(X, V) = \dim_{\mathbb{C}} \text{Hom}_{\mathbb{C}G}(V, X)$.

For, by Schur, we have $\dim_{\mathbb{C}} \text{Hom}_{\mathbb{C}G}(X, U_i) = \begin{cases} 1 & \text{if } X \cong U_i \\ 0 & \text{otherwise} \end{cases}$, and, by $\theta \mapsto (\pi_i \circ \theta, \pi_i \circ \theta)$, have $\text{Hom}_{\mathbb{C}G}(X, Y_1 \oplus Y_2) \cong \text{Hom}_{\mathbb{C}G}(X, Y_1) \oplus \text{Hom}_{\mathbb{C}G}(X, Y_2)$. [π_i is the projection: $Y_1 \oplus Y_2 \rightarrow Y_i$]. This has inverse $(\theta_1, \theta_2) \mapsto \theta_1 + \theta_2$.

[The other isomorphism, $\text{Hom}_{\mathbb{C}G}(X_1 \oplus X_2, Y) \cong \text{Hom}_{\mathbb{C}G}(X_1, Y) \oplus \text{Hom}_{\mathbb{C}G}(X_2, Y)$ is given by $\theta \mapsto (\theta|_{X_1}, \theta|_{X_2})$]

Corollary II: Let V be a $\mathbb{C}G$ -module. Then V is irreducible iff $\dim_{\mathbb{C}} \text{End}_{\mathbb{C}G}(V) = 1$.

Proof: (\Rightarrow) Schur.

(\Leftarrow) Maschke and Remark 10.

Remarks 12: In remark 10, we used and will use: (a) $\text{Hom}_{\mathbb{C}G}(X, Y_1 \oplus Y_2) \cong \text{Hom}_{\mathbb{C}G}(X, Y_1) \oplus \text{Hom}_{\mathbb{C}G}(X, Y_2)$
(b) $\text{Hom}_{\mathbb{C}G}(X_1 \oplus X_2, Y) \cong \text{Hom}_{\mathbb{C}G}(X_1, Y) \oplus \text{Hom}_{\mathbb{C}G}(X_2, Y)$.

Sketch proof: (a) $\theta: X \rightarrow Y_1 \oplus Y_2$ induces maps $\pi_i: \theta: X \rightarrow Y_i$. Get a map $\theta \mapsto \pi_1 \theta + \pi_2 \theta$, linear.

Inverse: given $\theta_i: X \rightarrow Y_i$, the map $\theta_1 + \theta_2: x \mapsto \theta_1 x + \theta_2 x$ is in the LHS.

(b) If $\theta: X_1 \oplus X_2 \rightarrow Y$; $x_1 + x_2 \mapsto \theta(x_1 + x_2)$. Let $\theta_i = \theta|_{X_i}$, then the map $\theta \mapsto \theta|_{X_1} + \theta|_{X_2}$.

Inverse: given $\theta_i: X_i \rightarrow Y$, define $\theta = \theta_1 x + \theta_2 x$.

Examples: (a) $G = C_n = \langle x \mid x^n = 1 \rangle$, V a $\mathbb{C}G$ -module. Then x on V can be diagonalised, so V is the direct sum of the various eigenspaces V_λ , for λ various N th roots of 1. These V_λ are the homogeneous components corresponding to the irreducible representation, $x^j \mapsto \lambda^j$.

(b) $G = D_{2n} = \langle x, y \mid x^n = y^2 = 1, yxy = x^{-1} \rangle$, V a $\mathbb{C}G$ -module. Restrict to $\langle x \rangle$, then $V|_{\langle x \rangle} = \bigoplus_{\lambda=1}^N V_\lambda$, where $V_\lambda = \{v \mid xv = \lambda v\}$. If $v \in V_\lambda$, then $yv \in V_{\lambda^{-1}}$, for $y(xy)v = (yx^{-1})v = y\lambda^{-1}v = \lambda^{-1}(yv)$.

For $\lambda \neq \lambda^{-1}$, we get a 2-dimensional $\mathbb{C}G$ -submodule $\langle v, yv \rangle$, with x acting as $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ and y acting as $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, since $y^2 = 1$. This is irreducible. Writing $W_\lambda = V_\lambda \oplus V_{\lambda^{-1}}$ as vector spaces, have W_λ the homogeneous component corresponding to this 2-dimensional irreducible representation. This construction gives $\frac{N-1}{2}$, respectively $\frac{N-2}{2}$, 2-dimensional representations of D_n for N odd, respectively N even.

For $\lambda = \lambda^{-1}$, we get $\langle v \rangle$ is an irreducible $\mathbb{C}G$ -module, with x acting as λ and y as 1 or -1, since $y^2 = 1$. We get two such irreducibles if N is odd (as $\lambda = 1$ here), and four such if N is even (as $\lambda = -1$ also possible).

Correspondingly, V_λ splits into two (possibly trivial) homogeneous components, $V_{\lambda,+}$ (with $xv = \lambda v$, $yv = v$ $\forall v$) and $V_{\lambda,-}$ (with $xv = \lambda v$, $yv = -v$ $\forall v$). Here, $\lambda = 1$, or $\lambda = -1$ and N even.

Remark: To find all these 2-dimensional irreducibles of D_{2n} , it is easier to note that the matrices $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ ($\lambda = \lambda^{-1}$) and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ generate a dihedral group of order $2k$ for some $k \mid N$, and hence a homomorphic image of D_{2n} .

The Group Algebra $\mathbb{C}G$.

$\mathbb{C}G = \left\{ \sum_{g \in G} \lambda_g g \mid \lambda_g \in \mathbb{C} \right\}$. It is a ring, and it is a vector space over \mathbb{C} , tied together.

So it is an algebra.

I.e.: $\left. \begin{array}{l} \sum \lambda_g g + \sum \mu_g g = \left(\sum (\lambda_g + \mu_g) g \right) \\ \lambda \in \mathbb{C}, \quad \lambda \sum \lambda_g g = \sum (\lambda \lambda_g) g \end{array} \right\}$ vector space over \mathbb{C} , basis G , dimension $|G|$.

$$\left(\sum \lambda_h h \right) \left(\sum \mu_g g \right) = \sum_{h,g} \lambda_h \mu_g h g = \sum_{g \in G} \left(\sum_h \lambda_h \mu_{hg} \right) g$$

Note: To have an algebra over \mathbb{C} , need an additive abelian group and multiplication by scalars to make it a vector space over \mathbb{C} , and multiplication to make it a ring with 1 (not commutative in general), so that $\lambda(rs) = (\lambda r)s = r(\lambda s)$

Hence, $\mathbb{C}G$ is also a $\mathbb{C}G$ -module, the left-regular $\mathbb{C}G$ -module, of degree $|G|$

Theorem 13: Every irreducible $\mathbb{C}G$ -module is isomorphic to a submodule of the left-regular module. The number of distinct irreducible $\mathbb{C}G$ -modules is finite.

Proof: Fix a direct sum decomposition, $\mathbb{C}G = U_1 \oplus \dots \oplus U_s$, of the regular module into irreducibles (Maschke). Let V be an irreducible $\mathbb{C}G$ -module, and let $0 \neq v \in V$. The map $\theta: \mathbb{C}G \rightarrow V$ given by $\sum \lambda_g g \mapsto \sum \lambda_g gv$ is a $\mathbb{C}G$ -homomorphism. Consider $\theta_i = \theta|_{U_i}$. These are $\mathbb{C}G$ -homomorphisms. Also, some θ_i is not 0 (since θ is not 0). But then this θ_i is an isomorphism from U_i to V , by Schur.

Proposition 14: If V is a $\mathbb{C}G$ -module, then $\text{Hom}_{\mathbb{C}G}(\mathbb{C}G, V) \cong V$ as vector spaces.

Proof: The map $\theta \mapsto \theta(1)$, from $\text{Hom}_{\mathbb{C}G}(\mathbb{C}G, V)$ to V , is a \mathbb{C} -linear isomorphism. It is clearly linear. Kernel is 0, since if $\theta(1) = 0$, then $\theta(g) = g\theta(1) = g0 = 0, \forall g$, so $\theta = 0$. It is onto: $v \in V$ is the image of $\theta: r \mapsto rv$.

Corollary 15: If V is an irreducible $\mathbb{C}G$ -module, and if $\mathbb{C}G = U_1 \oplus \dots \oplus U_s$ with the U_i irreducible, the number $\langle V, \mathbb{C}G \rangle$ of the U_i isomorphic to V equals $\dim V$.

Proof: By remark 12(b), and proposition 14.

Corollary 16: If V_1, \dots, V_k are the distinct irreducible $\mathbb{C}G$ -modules, then $|G| = \sum_{i=1}^k (\dim_{\mathbb{C}} V_i)^2$.

Proof: $\dim_{\mathbb{C}} \mathbb{C}G = |G|$, and each V_i appears $\dim V_i$ times in a direct sum decomposition of $\mathbb{C}G$ into irreducibles.

Examples: G abelian $\Rightarrow |G|$ irreducibles, all dimension 1.

$G = D_{2N}$: N even $\Rightarrow \frac{N-2}{2}$ irreducibles of degree 2, 4 of degree 1.

N odd $\Rightarrow \frac{N-1}{2}$ irreducibles of degree 2, 2 of degree 1.

Theorem 17 (Wedderburn): If G is a finite group and V_1, \dots, V_k are all the distinct irreducible $\mathbb{C}G$ -modules, then $\mathbb{C}G \cong \bigoplus_{i=1}^k \text{Hom}_{\mathbb{C}}(V_i, V_i)$, as algebras.

Proof: Define $\theta_i: \mathbb{C}G \rightarrow \text{Hom}_{\mathbb{C}}(V_i, V_i)$ by $r \mapsto (v \mapsto rv)$ and $\theta: \mathbb{C}G \rightarrow \bigoplus_{i=1}^k \text{Hom}_{\mathbb{C}}(V_i, V_i)$ by $r \mapsto (\theta_i(r), \dots, \theta_k(r))$.

Then θ is an algebra homomorphism, since each θ_i is. Further, θ is injective: $r \in \ker \theta \Rightarrow r \in \ker \theta_i, \forall i \Rightarrow r$ acts as 0 on each $V_i \Rightarrow r$ acts as 0 on $\mathbb{C}G \Rightarrow r = 0$.

Finally, θ is surjective, by dimensions.

Theorem 18: The number k of distinct irreducible $\mathbb{C}G$ -modules equals the number of conjugacy classes.

Proof: The centre of $\text{Hom}_{\mathbb{C}}(V_i, V_i)$ is $\{\lambda I \mid \lambda \in \mathbb{C}\}$. So the centre of the right hand side in Wedderburn has dimension k , the number of the V_i . The assertion of the theorem now follows from the next proposition.

Proposition 19: If G has conjugacy classes C_1, \dots, C_k , write $C_i = \sum_{g \in C_i} g$. Then $\{C_1, \dots, C_k\}$ is a basis for the centre $Z(\mathbb{C}G)$ of $\mathbb{C}G$.

Proof: If $x \in G$, then $x C_i x^{-1} = x (\sum_{g \in C_i} g) x^{-1} = \sum_{g \in C_i} xgx^{-1} = C_i$. So each $C_i \in Z(\mathbb{C}G)$.

Clearly the C_i are linearly independent (they have different support). They span $Z(\mathbb{C}G)$: $r = \sum_{g \in G} \lambda_g g \in Z(\mathbb{C}G)$. Then $xrx^{-1} = r \forall x \in G$, so the coefficients λ_g are constant on each conjugacy class of G . So each $\sum \lambda_g g$ is a combination of the C_i .

Characters.

Recall: $A \in M_n(\mathbb{C})$. $\text{tr } A = \sum a_{ii}$ - the trace of A . $\text{tr}(PAP^{-1}) = \text{tr } A$.

So, for $\theta: V \rightarrow V$, the trace of θ is well-defined by: $\text{tr } \theta = \text{tr}[\theta]_B$ for some (any) basis B of V .

Definition: If $\rho: G \rightarrow GL(V)$, the character X_V (afforded by ρ) is $X_V(g) = \text{tr } \rho(g)$, for $g \in G$.
So $X_V: G \rightarrow \mathbb{C}$.

The character X_V is irreducible (respectively reducible) if ρ affording it is.

The character is faithful if ρ is. The principal character is the character of the trivial representation, so $X_V(g) = 1 \quad \forall g \in G$. The character X_V is linear if $\dim V = 1$.

Lemma 20: Isomorphic $\mathbb{C}G$ -modules have the same character.

Proof: If $P_w(g) = \theta P_v(g) \theta^{-1}$ for some $\theta \in \text{Hom}_G(V, W)$ invertible, then $X_V(g) = X_W(g) \quad \forall g \in G$, since conjugate matrices have the same trace.

Remark: Converse proved later.

Proposition 21: Let X_V be the character afforded by the representation $\rho: G \rightarrow GL(V)$ of G .

(a) X_V is a class function on G : $X_V(xgx^{-1}) = X_V(g) \quad \forall x \in G, g \in G$.

(b) $X_{V_1 \oplus V_2}(g) = X_{V_1}(g) + X_{V_2}(g) \quad \forall g \in G$.

(c) $X_V(1) = \dim_{\mathbb{C}} V$.

(d) if $g \in G$ has order m , then $X_V(g)$ is a sum of m th roots of 1.

(e) $X(g^{-1}) = \overline{X(g)} \quad \forall g \in G$.

(f) if g, g^{-1} conjugate in $G \Rightarrow X_V(g)$ real.

Proof: (a) Conjugate matrices have the same trace.

(b) $P_{V_1 \oplus V_2}(g) = \begin{pmatrix} P_{V_1}(g) & 0 \\ 0 & P_{V_2}(g) \end{pmatrix}$, so $\text{tr}_{V_1 \oplus V_2} = \text{tr}_{V_1} + \text{tr}_{V_2}$.

(c) $X_V(1) = \text{tr } I_n = n$, where $n = \dim V$.

(d) $g^m = 1 \Rightarrow \rho(g)$ satisfies $X^m - 1 \Rightarrow$ can be diagonalised: $\rho(g) = \begin{pmatrix} w_1 & & \\ & \ddots & \\ & & w_m \end{pmatrix}$, (wrt suitable basis) and $w_i^m = 1$.

(e) $\rho(g)^{-1} = \begin{pmatrix} \bar{w}_1 & & \\ & \ddots & \\ & & \bar{w}_m \end{pmatrix}$.

(f) from (e) and (a).

Corollary 22: If $g \in G$ of order 2, then $X(g) \in \mathbb{Z}$ and $X(g) \equiv X(1) \pmod{2}$.

Proof: Can diagonalise g into $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} I_r & 0 \\ 0 & -I_s \end{pmatrix}$; then $X(g) = s-r \in \mathbb{Z}$, and $X(1) = s+r$, so $X(g) \equiv X(1) \pmod{2}$.

Proposition 23: Let ρ be a representation of G over \mathbb{C} , affording χ .

(a) $|X(g)| \leq X(1)$, with equality iff $\rho(g) = wI$, for some $w \in \mathbb{C}$.

(b) $X(g) = X(1)$ iff $g \in \ker \rho$.

Proof: (a) $\rho(g) = \begin{pmatrix} w_1 & 0 \\ 0 & w_n \end{pmatrix}$, so $|X(g)| = |w_1 + \dots + w_n| \leq |w_1| + \dots + |w_n| = n = X(1)$, with equality iff all the w_i are equal to each other.

(b) Follows from (a). $\rho(g) = wI \Rightarrow X(g) = nw = X(1) \Rightarrow w = 1$.

Proposition 24: If χ is a character of G over \mathbb{C} , then

(a) $\bar{\chi}$ is also a character (where $\bar{\chi}(g) = \overline{\chi(g)}$).

(b) if ε is a linear character of G over \mathbb{C} then $\varepsilon\chi$ is also a character.

In each case, the new character is irreducible if χ is.

Sketch Proof: If $\rho: G \rightarrow \text{GL}_n(\mathbb{C})$ affords χ , then $\bar{\rho}: g \mapsto \overline{\rho(g)}$ is a representation affording $\bar{\chi}$, and $\varepsilon\rho: g \mapsto \varepsilon(g)\rho(g)$ is a representation affording $\varepsilon\chi$. Check the rest.

Remark: In fact, $\bar{\chi}$ is the character of ρ_{V^*} : given $\theta \in V^*$, so $\theta: V \rightarrow \mathbb{C}$, linear, define $(gh)\theta = \theta(g^{-1}h)$. [need $(gh)\theta = g(h\theta)$: $(gh)\theta v = \theta(g^{-1}h^{-1}v) = (h\theta)g^{-1}v = g(h\theta)v$].

Now going to prove that characters characterise representations.

Lemma 25: If U is a $\mathbb{C}G$ -module, let $U^G = \{u \in U \mid gu = u \ \forall g \in G\}$.

Then $\dim_{\mathbb{C}} U^G = \frac{1}{|G|} \sum_{g \in G} X_U(g)$.

Proof: The mapping $\pi: u \mapsto \frac{1}{|G|} \sum_{g \in G} \rho_u(g)u$ is a projection from U onto U^G . [$\pi: U \rightarrow U^G$ and $\pi|_{U^G} = \text{id}_{U^G}$]. Hence, $\dim U^G = \text{tr } \pi = \text{tr } \frac{1}{|G|} \sum_{g \in G} \rho_u(g) = \frac{1}{|G|} \sum_{g \in G} X_U(g)$.
[Represent π wrt a basis containing a basis for U^G : $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$].

Lemma 26: Let V, W be $\mathbb{C}G$ -modules, with characters X_V, X_W respectively. Then,

$$\dim_{\mathbb{C}} \text{Hom}_{\mathbb{C}G}(V, W) = \frac{1}{|G|} \sum_{g \in G} X_V(g^{-1}) X_W(g) := \langle X_V, X_W \rangle.$$

Proof: If $U = \text{Hom}_{\mathbb{C}}(V, W)$, then U is a $\mathbb{C}G$ -module with respect to the G -action $g: \theta \mapsto g_w \circ \theta \circ g_v^{-1}$. Then $U^G = \text{Hom}_{\mathbb{C}G}(V, W)$, so $\dim \text{Hom}_{\mathbb{C}G}(V, W) = \frac{1}{|G|} \sum_{g \in G} X_U(g)$, by lemma 25. Finally, $X_U(g) = X_V(g^{-1}) X_W(g)$, so the assertion follows.

To prove this last, fix $g \in G$. Choose v_1, \dots, v_n a basis for V such that $g_j v_i = \lambda_{ij} v_i$, and w_1, \dots, w_m a basis for W such that $g_j w_i = \mu_{ij} w_i$. Let δ_{ij} be the usual basis for U : $\delta_{ij} = \sum_k \lambda_{ik} \mu_{kj}$. Then, $g_j \circ \delta_{ij} \circ g_j^{-1} = \lambda_{ij}^{-1} \mu_{ij} \delta_{ij}$ (since true on the v_k), so $X_U(g) = \sum_{i,j} \lambda_{ij}^{-1} \mu_{ij} = (\sum_i \lambda_{ii}^{-1})(\sum_j \mu_{jj}) = X_V(g^{-1}) X_W(g)$.

Remark: What is behind this last bit: $\text{Hom}_{\mathbb{C}}(V, W) \cong V^* \otimes W$, so

$$X_{\text{Hom}_{\mathbb{C}}(V, W)}(g) = X_{V^* \otimes W}(g) = X_{V^*}(g) X_W(g) = X_V(g^{-1}) X_W(g)$$

Theorem 27: A finitely generated $\mathbb{C}G$ -module of the finite group G is determined by its character.

Proof: Let V be a $\mathbb{C}G$ -module. By Maschke, V is a direct sum of irreducible modules. By Schur, the irreducible module U appears with multiplicity $\dim_{\mathbb{C}} \text{Hom}_{\mathbb{C}G}(U, V)$ as a summand. By the above, this dimension is $\langle \chi_U, \chi_V \rangle$, so is determined by the characters χ_U, χ_V .

Inner Products.

The set of complex-valued functions on G forms a vector space:

$$(\theta_1 + \theta_2)(g) = \theta_1(g) + \theta_2(g); \quad (\lambda \theta)(g) = \lambda(\theta(g)).$$

The set of class functions (those constant on each conjugacy class of G) forms a subspace.

Definition 28: Define a hermitian inner product: $\langle \theta_1, \theta_2 \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\theta_1(g)} \theta_2(g)$.

Result 29: If θ_1, θ_2 are characters, then $\langle \theta_1, \theta_2 \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\theta_1(g^{-1})} \theta_2(g) = \frac{1}{|G|} \sum_{g \in G} \overline{\theta_1(g)} \theta_2(g^{-1}) = \langle \theta_2, \theta_1 \rangle$, and so is real.

Result 30: For class functions in general, $\langle \theta_1, \theta_2 \rangle = \frac{1}{|G|} \sum_{i=1}^k |\mathcal{C}_i| \overline{\theta_1(g_i)} \theta_2(g_i)$, where $\mathcal{C}_1, \dots, \mathcal{C}_k$ are conjugacy classes of G , and the g_i are chosen representatives. So, $\langle \theta_1, \theta_2 \rangle = \sum_{i=1}^k \frac{1}{|\mathcal{C}_i|} \overline{\theta_1(g_i)} \theta_2(g_i)$

Theorem 31 (First Orthogonality Relation): The irreducible characters form an orthonormal basis for the space of class functions.

Proof: Orthonormal - Schur and Lemma 26. Basis - have the right number.

Corollary 32: $W = a_1 V_1 \oplus \dots \oplus a_k V_k$ with V_i the irreducibles of G and $a_i V_i = \underbrace{V_i \oplus \dots \oplus V_i}_{a_i}$, then $a_i = \langle X_{V_i}, X_W \rangle$.

Proposition 33: $g, h \in G$ are conjugate iff $X(g) = X(h)$ for all X irreducible characters.

Proof: (\Rightarrow) Any character is a class function.

(\Leftarrow) if $X(g) = X(h)$ for all X irreducible, then $\theta(g) = \theta(h)$ for all class functions θ . In particular, if $\theta(x) = \begin{cases} 1 & \text{if } x \in \text{ccl}(g) \\ 0 & \text{otherwise} \end{cases}$, then $\theta(g) = 1 \Rightarrow \theta(h) = 1 \Rightarrow h \in \text{ccl}(g)$.

Corollary 34: g, g^{-1} are conjugate in G iff $X(g) \in \mathbb{R}$ for all irreducible characters X .

Proof: By proposition 33 and lemma 21(f).

Character tables; Orthogonality relations.

G a finite group, $F = \mathbb{C}$, $\chi_1 (= 1_G), \dots, \chi_R$ the irreducible characters of G , $\mathcal{C}_1 (= \{1\}), \dots, \mathcal{C}_k$ the conjugacy classes of elements of G , with $g_i \in \mathcal{C}_i$.

Definition: The character table of G is the $k \times k$ matrix with (i,j) -entry $\chi_i(g_j)$.

Example: $G = C_2 \times C_2 = \langle x \rangle \times \langle y \rangle$. Table:
$$\begin{array}{ccccc} & 1 & x & y & xy \\ \text{g}_i & \begin{array}{ccccc} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{array} \end{array}$$
 (using proposition 6)

Example: G non-abelian of order 8.

$Z(G)$ has order 2, so $Z(G) = \{1, z\}$. $G/Z(G) \cong C_2 \times C_2$. Conjugacy classes: $1, z, g_3, g_4, g_5$. $C(g_3) = \langle g_3, z \rangle$, order 4, so $|C_G(g_3)| = 2$.

Character degrees: $1, 1, 1, 1, 2$ (by corollary 16 and theorem 18)

Table: $|C_G(g_i)| \quad 8 \quad 8 \quad 4 \quad 4 \quad 4$

g_i	1	z	g_3	g_4	g_5
1	1	1	1	1	1
z	1	1	-1	1	-1
g_3	1	1	1	-1	-1
g_4	1	1	-1	-1	1
g_5	2	-2	0	0	0

Schur $\Rightarrow z \mapsto$ scalar matrix,

so $\pm I$, but must be $-$,

by proposition 33

$G \rightarrow G/\langle z \rangle$, $g \mapsto g\langle z \rangle \xrightarrow{\bar{\rho}_i} \mathbb{C}$,
where $\bar{\rho}_i$ are the four linear representations of $C_2 \times C_2$ - get four characters of G

$$\text{Theorem 31} \Rightarrow \frac{1}{8} (1 \cdot 2^2 + 1 \cdot (-2)^2 + 2 \cdot 1^2 + 2 \cdot 1^2 + 2 \cdot 1^2) = 1.$$

Theorem 35 (Orthogonality Relations): (i) row orthogonality: $\sum_{i=1}^k \frac{1}{|C_G(g_i)|} \overline{\chi_r(g_i)} \chi_s(g_i) = S_{rs}$.
(ii) column orthogonality: $\sum_{i=1}^k \overline{\chi_r(g_i)} \chi_r(g_i) = S_{rr} |C_G(g_i)|$.

Proof: (i) This is Theorem 31 - the characters are orthonormal.

(ii) Let A be the $k \times k$ matrix, $a_{ij} = \frac{1}{|C_G(g_i)|^{1/2}} \chi_i(g_j)$. Then $\bar{A}A^t = I$, by (i).

Hence, $A^t \bar{A} = I$, so $\bar{A}^t A = I$ - this is (ii).

Example: $G = S_4$

$|C_G(g_i)| \quad 24 \quad 3 \quad 8 \quad 4 \quad 4$

g_i	1	(123)	$(12)(34)$	(12)	(1234)
1	1	1	1	1	1
sgn	1	1	1	-1	-1
p_3	0	-1	1	1	-1
$p_3 \times \text{sgn}$	0	-1	-1	1	1
2	-1	2	0	0	0

From orthogonality relations.

$\rho_3: X = \pi - 1$, where $\pi(g)$ = number of fixed points of g .

Irreducible by orthogonality. (See later).

Example: $G = S_3$

	1	(123)	(12)
1	1	1	1
2	1	-1	0
2	-1	0	0

cf: table for S_4 - row 1,2,5, columns 1,2,4.

Remark: $V_4 \triangleleft S_4$, $S_4/V_4 \cong S_3$, hence this similarity above.

Normal Subgroups

Lemma 36: Let $N \trianglelefteq G$, $\tilde{\rho} : G/N \rightarrow GL(V)$, an (irreducible) representation of G/N .

Then $\rho : G \rightarrow GL(V)$; $g \mapsto \tilde{\rho}(gN)$ is an (irreducible) representation of G .

The corresponding characters satisfy $\chi(g) = \tilde{\chi}(gN)$. We say $\tilde{\chi}$ lifts to χ .

Proposition 37: If $N \trianglelefteq G$, the lift $\tilde{\chi} \rightarrow \chi$ above is a bijection from the set of all irreducibles of G/N to the set of those irreducible characters of G with N in their kernel.

Proof: If χ lifts from $\tilde{\chi}$ then for $x \in N$, $\chi(x) = \tilde{\chi}(xN) = \tilde{\chi}(N) = \tilde{\chi}(1)$, so $x \in \ker \chi$, by proposition 23, so $N \leq \ker \chi$.

Bijection: injection is clear: χ given from $\tilde{\chi}$.

surjection: χ afforded by $\rho : G \rightarrow GL(V)$, with $N \leq \ker \rho$, then $\tilde{\rho} : G/N \rightarrow GL(V)$; $gN \mapsto \rho(g)$ is a well-defined representation of G/N [$g_1N = g_2N \Rightarrow g_1^{-1}g_2 \in N \leq \ker \rho \Rightarrow \rho(g_1) = \rho(g_2)$], affording $\tilde{\chi}$, lifting to χ .

Finally, $\tilde{\chi}$ irreducible iff χ irreducible: Take $U \subset V$. $\rho(g)U \subset U \forall g \in G$ iff $\tilde{\rho}(gN)U \subset U \forall gN \in G/N$.

Proposition 38: (a) G is not simple iff $\chi(g) = \chi(1)$ for some χ irreducible character of G other than I_G , and some $g \in G$. (So, visible from character table).

(b) Any normal subgroup is the intersection of kernels of some irreducible representations.

Remark*: Hence we can see from the character table whether G is solvable (\exists chain $1 = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_s = G$, with $G_i \trianglelefteq G$ and G_i/G_{i-1} a p-group) nilpotent (all Sylow subgroups are normal).

Proof: (a) (\Leftarrow) $\chi(g) = \chi(1)$, $g \neq 1 \Rightarrow g \in \ker \chi \trianglelefteq G$ (using proposition 23).

(\Rightarrow) $1 \neq N \trianglelefteq G$, $\tilde{\chi}$ irreducible non-principal character of G/N , then lift it to χ , an irreducible character of G . Then $g \in N \Rightarrow g \in \ker \chi$.

(b) $N \trianglelefteq G$. Let $\tilde{\chi}_1, \dots, \tilde{\chi}_s$ be the distinct irreducibles of G/N . Lift these to χ_1, \dots, χ_s , irreducibles of G . Then, $N = \bigcap \ker \chi_i$.

\Leftarrow : clear from proposition 37.

\Rightarrow : if $g \in G \setminus N$, then $gN \neq N$, so for some $i \leq s$, have $\tilde{\chi}_i(gN) \neq \tilde{\chi}_i(N)$, so $\star \chi_i(g) \neq \chi_i(1)$, so g is not in $\ker \chi_i$ for that i .

Definition: The derived subgroup, G' , of G is $G' = \langle aba^{-1}b^{-1} \mid a, b \in G \rangle$

Note: $G' \trianglelefteq G$, since $G' \leq G$, and $xaba^{-1}b^{-1}x^{-1} = (xax^{-1})(xbx^{-1})(xa^{-1}x^{-1})(xb^{-1}x^{-1})$

Lemma 39: Let $N \trianglelefteq G$. Then G/N abelian iff $G' \leq N$. So G' is the unique smallest normal subgroup of G with abelian quotient.

Proof: G/N abelian iff $aNbN a^{-1}Nb^{-1}N = N \forall a, b \in G$ iff $aba^{-1}b^{-1}N = N \forall a, b \in G$ iff $aba^{-1}b^{-1} \in N \forall a, b \in G$ iff $G' \leq N$.

Example: $G = D_8 = \langle a, b \mid a^4 = b^2 = 1, bab = a^{-1} \rangle$.

$\langle a^2 \rangle \trianglelefteq G$, $G/\langle a^2 \rangle$ of order 4 and so abelian, but G is not abelian, so $G' = \langle a^2 \rangle$.

Lemma 40: The number of distinct characters of degree 1 equals the index $|G : G'|$.

Proof: G/G' abelian, so have $|G : G'|$ linear characters of G ; these are all the characters of G with G' in their kernel (by proposition 38). If X is a linear character of G , then $G/\ker X \leq \mathbb{C}^\times$ by the isomorphism theorem, so $G/\ker X$ abelian, so $G' \leq \ker X$.

Permutation Characters.

G acting on a set $X = \{1, \dots, n\}$. Let V be a vector space with a basis $B = \{v_1, \dots, v_n\}$. Have $g: v_i \mapsto v_{g(i)}$, and extend. Then V is a $\mathbb{C}G$ -module - the permutation module corresponding to the action of G on X .

Lemma 41: The permutation character of G on X (ie, the character of this $\mathbb{C}G$ -module) is $\pi(g) = |\text{Fix}_X(g)| = \{x \in X \mid g \cdot x = x\}$.

Proof: Clear; contributions to $\text{tr}(g)$ precisely from those fixed by g .

Lemma 42: If π is the permutation character of G on X , then $\langle \pi, 1 \rangle = \#\text{orbits of } G \text{ on } X$.

In particular, if G transitive, then $\pi|_{G_\alpha}$ is a character with no principal constituent.

Proof: Let X split into G -orbits as $X = X_1 \cup \dots \cup X_l$.

$$\langle \pi, 1 \rangle = \frac{1}{|G|} \sum_{g \in G} \pi(g) = \frac{1}{|G|} \# \{ (g, x) \in G \times X \mid g \cdot x = x \} = \frac{1}{|G|} \sum_{\alpha \in X} |G_\alpha| = \sum_{i=1}^l \sum_{\alpha \in X_i} \frac{|G_\alpha|}{|G|} = \sum_{i=1}^l 1 = l.$$

Lemma 43: If G acts on X, Y with permutation characters π, τ , then $\langle \pi, \tau \rangle = \#\text{orb}(G, X \times Y)$.

Proof: The permutation character of G on $X \times Y$ is $\pi\tau$, where $\pi\tau(g) = \pi(g)\tau(g)$, so $\#\text{orb}(G, X \times Y) = \langle \pi\tau, 1 \rangle = \langle \pi, \tau \rangle$, as τ real.

Corollary 44: $\langle \pi, \pi \rangle = \#\text{orb}(G, X \times X)$. If G is transitive on X , this equals $\#\text{orb}(G_\alpha, X)$ for any $\alpha \in X$, the permutation rank of G on X .

Corollary 45: If G is 2-transitive on X then $\pi|_{G_\alpha}$ is an irreducible character.

Recall: G is 2-transitive on X if, for $x_1 \neq x_2, y_1 \neq y_2 \in X, \exists g \in G$ with $g \cdot x_i = y_i$.

Example: $G = A_5$, the alternating group of degree 5, has: $|G_a(g_i)|$

	60	4	3	5	5
cols:	1	(12)(34)	(123)	$(12345)^{\pm}$	$(12345)^{\pm 2}$
	1	1	1	1	1
$\pi _{G_\alpha}$:	3	-1	0	$\begin{bmatrix} \alpha & \\ & \beta \end{bmatrix}$	$\begin{bmatrix} & \beta \\ \alpha & \end{bmatrix}$
	3	-1	0	$\begin{bmatrix} & \beta \\ \alpha & \end{bmatrix}$	$\begin{bmatrix} & \alpha \\ \beta & \end{bmatrix}$
	4	0	1	-1	-1
	5	1	-1	0	0

$\alpha = \frac{1+i\sqrt{5}}{2}, \beta = \frac{1-i\sqrt{5}}{2}$ - from column orthogonality.

For $\pi|_{G_\alpha}$: 5 1 2 0 0

Fifth row - Consider $\pi|_G$ on Sylow 5-subgroups. This has: 6 2 0 1 1. Take $\pi|_G - 1$.

Consider $\pi|_{G_\alpha} = \pi|_{\{1\}}$ acting on Petersen Graph:  This has: 10 2 1 0 0. Take $\pi|_{\{1\}} - \pi|_G$.

$\langle \pi_{\{5\}}, \pi_5 \rangle = \# \text{ orbits of } A_5 \text{ on } \binom{5}{2} \times 5 = 2$. So $\pi_5 \in \pi_{\{5\}}$ (see Sheet 4 Question 4).

$\langle \pi_{\{2\}}, \pi_{\{2\}} \rangle = \# \text{ orbits of } A_5 \text{ on } \binom{5}{2} \times \binom{5}{2} = 3$.

Rows 2, 3: Obtain the 3's from $1^2 + x_1^2 + y_1^2 + 4^2 + 5^2 = 60$.

Obtain the -1's from $1 + 3x_2 + 3y_2 + 5 = 0$ and $2 + x_2^2 + y_2^2 = 4$.

Write $\boxed{\quad}$ as $\begin{matrix} \alpha \\ \beta \end{matrix}$. From columns 1, 4, have $1 + 3\alpha + 3\beta - 4 = 0 \Rightarrow \alpha + \beta = 1$.

From columns 4, 4, have $1 + \alpha^2 + \beta^2 + 1 = 5$.

From rows 1, 2, have $\alpha + \gamma = 1$, so $\beta = \gamma$. $S = \alpha$, similarly.

So we have $\alpha + \beta = 1$, $\alpha^2 + \beta^2 = 3$, so α, β roots of $x^2 - x - 1 = 0$, so $\alpha, \beta = \frac{1 \pm \sqrt{5}}{2}$.

Remark: For α, β : Need a 3×3 matrix, diagonal, conjugate to its inverse, of order 5.
Only choices are $\begin{pmatrix} 1 & w & w^{-1} \\ w & w^{-1} & 1 \\ w^{-1} & 1 & w \end{pmatrix}$ with $w = e^{2\pi i/5}$

Tensor Products.

Given characters X, Y of G , can construct a representation affording X^Y as its character, where $X^Y(g) = X(g)Y(g)$.

V, W vector spaces over \mathbb{C} , bases v_1, \dots, v_n and w_1, \dots, w_m respectively. Form a vector space $V \otimes W$ with basis $v_i \otimes w_j$ ($1 \leq i \leq n, 1 \leq j \leq m$). Vectors are $\sum \lambda_{ij} v_i \otimes w_j$. Obvious addition and multiplication by scalars so do get a vector space.

Define $v \otimes w = (\sum \lambda_i v_i) \otimes (\sum \mu_j w_j) = \sum_{i,j} \lambda_i \mu_j v_i \otimes w_j \in V \otimes W$.

Lemma 4.6: \otimes is bilinear: (i) $v \otimes \lambda w = \lambda(v \otimes w) = (\lambda v) \otimes w$.

$$\text{(ii)} (x_1 + x_2) \otimes w = x_1 \otimes w + x_2 \otimes w.$$

$$\text{(iii)} v \otimes (y_1 + y_2) = v \otimes y_1 + v \otimes y_2.$$

Note: If x_1, \dots, x_n and y_1, \dots, y_m are bases for V and W respectively, then $\{x_i \otimes y_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$ is a basis for $V \otimes W$. For, if $v_i = \sum \lambda_{ik} x_k, w_j = \sum \mu_{jl} y_l$, then $v_i \otimes w_j = \sum_{k,l} \lambda_{ik} \mu_{jl} x_k y_l$, so claim follows.

Proposition 4.7: If V, W are $\mathbb{C}G$ -modules then so is $V \otimes W$, under $\rho_{V \otimes W}(g) = \sum \lambda_i \mu_j (v_i \otimes w_j) \mapsto \sum \lambda_i \mu_j g(v_i) \otimes g(w_j)$.

Moreover, the character of $\rho_{V \otimes W}$ is $\chi_{V \otimes W}(g) = \chi_V(g)\chi_W(g)$.

Proof: $\mathbb{C}G$ -action is clear.

Character: fix g ; choose bases for V, W consisting of eigen vectors for g , so we have v_1, \dots, v_n and w_1, \dots, w_m such that $g v_i = \lambda_i v_i, g w_j = \mu_j w_j$. Then $g(v_i \otimes w_j) = \lambda_i \mu_j v_i \otimes w_j$, so $\chi_{V \otimes W}(g) = \sum_{i,j} \lambda_i \mu_j = (\sum_i \lambda_i)(\sum_j \mu_j) = \chi_V(g)\chi_W(g)$.

Remark: R a commutative ring, and M, N R -modules. Then $M \otimes N$ can be defined as the

R -module T with a linear map $t: M \times N \rightarrow T$ such that any bilinear map $f: M \times N \rightarrow V$ (any R -module V) can be factored through: $M \times N \xrightarrow{t} T \xrightarrow{f'} V$, so $\exists f': T \rightarrow V$, linear, such that $f = f' \circ t$.

It can be shown that such exists and is unique up to isomorphism.

Example: $V^* \otimes W \cong \text{Hom}_\mathbb{C}(V, W)$, $\delta \otimes w \mapsto (v \mapsto \delta(v)w)$

Powers of Characters.

$X^n(g) := (X(g))^n$. This is a character for X a character and $n \in \mathbb{N}$. - by induction.

Exercise (Sheet 4, Question 12*): If X is a faithful character of G taking s distinct values, then any irreducible character of G appears as a constituent in one of X^0, X^1, \dots, X^{s-1} .

Example: X the regular character, then $X(g) = \begin{cases} 0 & \text{if } g \neq 1 \\ |G| & \text{if } g = 1 \end{cases}$.

(Think of it as the permutation character of G in the regular action on G).

So any irreducible of G appears in the regular character.

Take $n=2$, $W=V$. We have $\tau: V \otimes V \rightarrow V \otimes V$, $v_i \otimes v_j \mapsto v_j \otimes v_i$ and extend; linear map of order 2.

Define: $S^2 V = \langle v_i \otimes v_j + v_j \otimes v_i \mid i \leq j \rangle$, $\Lambda^2 V = \langle v_i \otimes v_j - v_j \otimes v_i \mid i < j \rangle$ - eigenspaces of τ .

Note 48: We have $V \otimes V = S^2 V \oplus \Lambda^2 V$, and $S^2 V, \Lambda^2 V$ are $\mathbb{C}G$ -subspaces.

Proposition 49: Write $X_S = X_{S^2 V}$, $X_A = X_{\Lambda^2 V}$ (where X is the character on V). Then $X^2 = X_S + X_A$ and $X_S(g) = \frac{1}{2}(X^2(g) + X(g^2))$, $X_A = \frac{1}{2}(X^2(g) - X(g^2))$.

Proof: $X^2 = X_S + X_A$ by Note 48.

Fix $g \in G$, and choose the v_i to be a basis of eigenvectors of g , so $gv_i = \lambda_i v_i$.

Then $g(v_i \otimes v_j - v_j \otimes v_i) = \lambda_i \lambda_j (v_i \otimes v_j - v_j \otimes v_i)$. So $X_A(g) = \sum_{i < j} \lambda_i \lambda_j$.

Now, $X^2(g) = (\sum \lambda_i)(\sum \lambda_j) = \sum_{i,j} \lambda_i^2 + 2 \sum_{i < j} \lambda_i \lambda_j = X(g^2) + 2X_A(g)$, whence $X_A(g) = \frac{1}{2}(X^2(g) - X(g^2))$ and so $X_S(g) = X^2(g) - X_A(g) = \frac{1}{2}(X^2(g) + X(g^2))$.

Example: $G = S_5$ has 7 conjugacy classes.

c_i	1	15	20	24	10	30	20
$c(g_i)$	120	8	6	5	12	4	6
g_i	1	2^2	3	5	2	4	$3 \cdot 2$
	1	1	1	1	1	0	1
	1	1	*	1	-1	-1	-1
$X := \#_{\text{irr}}$	4	0	1	-1	2	0	-1
$X \times \text{sgn}$	4	0	1	-1	-2	0	1
$X_S - X - 1$	5	1	-1	0	1	-1	1
$p_5 \times \text{sgn}$	5	1	-1	0	-1	1	-1
X_A	6	-2	0	1	0	0	0
$X^2(g)$	16	0	1	1	4	0	1
$X(g^2)$	4	4	1	-1	4	0	1
X_S	10	2	1	0	4	0	1

$$\begin{cases} 0 & \text{if } X \text{ not a real character} \\ 1 & \text{if } \frac{1}{2}g \text{ in } X_S \\ -1 & \text{if } \frac{1}{2}g \text{ in } X_A \end{cases}$$

Proposition 50 (Frobenius-Schur Indicator): If X is an irreducible character of G , write $i(X) = \begin{cases} 0 & \text{if } X \text{ not a real character} \\ 1 & \text{if } \frac{1}{2}g \text{ in } X_S \\ -1 & \text{if } \frac{1}{2}g \text{ in } X_A \end{cases}$. Then $i(X) = \frac{1}{|G|} \sum_{g \in G} X(g^2)$. Moreover, $\sum_{x \in G} i(X)(x) = \#\{g \in G \mid g^2 = x\}$ for any $x \in G$.

Proof: $\langle X^2, 1_G \rangle = \langle X, \bar{X} \rangle = \begin{cases} 0 & \text{if } X \text{ not real} \\ 1 & \text{if } X \text{ real} \end{cases}$. For X real, have 1_G in $X^2 = X_S + X_A$ with multiplicity 1, so 1_G appears in precisely one of X_S, X_A with multiplicity 1. Hence, $i(X) = \langle X_S - X_A, 1_G \rangle = \frac{1}{|G|} \sum_{g \in G} X(g^2)$,

by Proposition 49. Moreover: Write $\theta(x) = \#\{g \in G \mid g^2 = x\}$. Then θ is a class function.

For X irreducible, $\langle \theta, X \rangle = \frac{1}{|G|} \sum_{x \in G} \theta(x) X(x) = \frac{1}{|G|} \sum_{g \in G} \sum_{g^2=x} X(g^2) = \frac{1}{|G|} \sum_{g \in G} X(g^2) = i(X)$, and so $\theta = \sum_{X \text{ irreducible}} i(X) X$ (as the X_i form an orthonormal basis of the space of class functions).

Remark (50 continued): X irreducible, afforded by G on V . Then, χ_G in $\chi_S \Leftrightarrow \text{Hom}_{\mathbb{C}G}(S^2V, \mathbb{C}) \cong \mathbb{C}$
 $\Leftrightarrow \exists$ a unique (up to scalar) G -invariant bilinear symmetric form. This can be used to show that χ_G is in χ_S iff X afforded by a real representation, ie, $p: G \rightarrow \text{GL}(W)$, with W a real space. (See Sheet 4, Question 11*, and James & Liebeck P. 266).

Direct Products

Theorem 51: If G and H are finite groups with χ_1, \dots, χ_k the irreducibles of G , and ψ_1, \dots, ψ_l the irreducibles of H , then $\{\chi_i \psi_j \mid 1 \leq i \leq k, 1 \leq j \leq l\}$ are all the distinct irreducibles of $G \times H$, where $\chi_i \psi_j(gh) = \chi_i(g) \psi_j(h)$.

Proof: If V is a $\mathbb{C}G$ -module and W a $\mathbb{C}H$ -module, then $V \otimes W$ is a $\mathbb{C}(G \times H)$ -module under the action $(g, h): v_i \otimes w_j \mapsto gv_i \otimes hw_j$, (Where the v_i, w_j form bases for V, W respectively), and extend. This is a linear $G \times H$ action, with character $\chi_{V \otimes W} = \chi_V \chi_W$. We'll show these $\chi_i \psi_j$ are distinct irreducibles: $\langle \chi_i \psi_j, \chi_r \psi_s \rangle_{G \times H} = \frac{1}{|G \times H|} \sum_{(g, h)} \chi_i(g) \psi_j(h) \chi_r(g) \psi_s(h) = \left(\frac{1}{|G|} \sum_{g \in G} \chi_i(g) \chi_r(g) \right) \left(\frac{1}{|H|} \sum_{h \in H} \psi_j(h) \psi_s(h) \right) = \langle \chi_i, \chi_r \rangle_G \cdot \langle \psi_j, \psi_s \rangle_H = \delta_{i,r} \delta_{j,s}$. These are all of the irreducibles: $\sum_i \chi_i \psi_j (1)^2 = \left(\sum_i \chi_i (1)^2 \right) \left(\sum_j \psi_j (1)^2 \right) = |G| \cdot |H| = |G \times H|$.

Restriction and Induction

Throughout this section, H is a subgroup of G .

Restriction: Let $p: G \rightarrow \text{GL}(V)$ be a representation, affording the character χ . Then V is also a $\mathbb{C}H$ -module, with representation $p_H: H \rightarrow \text{GL}(V)$, the restriction of p . It affords the character χ_H (or χ_H), the restriction of χ to H .

Lemma 52: X an irreducible of G , and $\chi_H = \sum c_i \psi_i$ with ψ_i irreducible characters of H ($c_i \in \mathbb{N}_0$). Then $\sum c_i^2 \leq |G:H|$ with equality iff $\chi(g) = 0 \quad \forall g \in G \setminus H$.

Proof: $\sum c_i^2 = \langle \chi_H, \chi_H \rangle_H = \frac{1}{|H|} \sum_{h \in H} |\chi(h)|^2$. But $\langle \chi, \chi \rangle_G = \frac{1}{|G|} \sum_{g \in G} |\chi(g)|^2 = \frac{1}{|G|} \sum_{h \in H} |\chi(h)|^2 + \frac{1}{|G|} \sum_{g \in G \setminus H} |\chi(g)|^2 = k$, with $k \geq 0$. So, $\sum c_i^2 \leq |G:H|$, with equality iff $k=0$, ie iff $\chi(g) = 0 \quad \forall g \in G \setminus H$.

Example: $|S_5 : A_5| = 2$. Any irreducible of S_5 either remains irreducible in A_5 , or splits into two irreducibles (cf sheet 4, question 8). $S_5: \begin{matrix} 1 & 1 & 4 & 4 & 5 & 5 & 6 \\ \checkmark & \checkmark & \checkmark & \checkmark & \checkmark & \checkmark & \end{matrix} \quad ? \quad \begin{matrix} 1 & 4 & 5 & 3 & 3 \end{matrix}$ (zero on odd permutations)
 $A_5: \quad \begin{matrix} 1 & 4 & 5 & 3 & 3 \end{matrix}$ degrees of irreducibles.

Can get the character table of A_5 from that of S_5 , except for the values of the two irreducibles of degree 3.

Induction: Starting from a character ψ of H , get a character ψ^{G^H} (or ψ^G) of G . Write $\mathcal{C}(X, \mathbb{C})$ for the vector space of complex class functions - it is a space, with hermitian inner product. Above, we defined the linear map $\downarrow_H: \mathcal{C}(G, \mathbb{C}) \rightarrow \mathcal{C}(H, \mathbb{C})$. This has a unique adjoint $\uparrow^H: \mathcal{C}(H, \mathbb{C}) \rightarrow \mathcal{C}(G, \mathbb{C})$, a linear map satisfying $\langle \chi \downarrow_H, \psi \rangle_H = \langle \chi, \psi^{G^H} \rangle_G$.

Theorem 53 (Frobenius Reciprocity Theorem): $H \leq G$, χ a character of G , ψ a character of H . Then,

- (i) $\chi|_H$ is a character of H ,
- (ii) ψ^G is a character of G ,
- (iii) $\langle \chi|_H, \psi \rangle_H = \langle \chi, \psi^G \rangle_G$.

Proof: Characters of G (respectively H) are precisely the class functions of G (respectively H), which are linear combinations of irreducible characters of G (respectively H) with all coefficients in \mathbb{N} . Hence (i) is clear. (ii) follows from our definition, and (iii) is our definition.

Theorem 54: $H \leq G$, $\psi \in C(H, \mathbb{C})$. Then $\psi^G(g) = \frac{1}{|H|} \sum_{x \in G} \psi^0(x^{-1}gx)$, where $\psi^0(y) = \begin{cases} \psi(y) & \text{if } y \in H \\ 0 & \text{otherwise.} \end{cases}$

Proof: For any ψ , write ψ' for the RHS. We are comparing linear maps: $C(H, \mathbb{C}) \rightarrow C(G, \mathbb{C})$; $\psi \mapsto \psi^G$ and $\psi \mapsto \psi'$, so enough to check they are equal on a basis for $C(H, \mathbb{C})$, e.g., on characteristic functions of H -conjugacy classes: let $\chi_D(h) = \begin{cases} 1 & \text{if } h \in D \\ 0 & \text{otherwise,} \end{cases}$ where D is an H -conjugacy class.

Consider the G -conjugacy class \mathcal{C} . Write $\delta = \begin{cases} 1 & \text{if } D \subseteq \mathcal{C} \\ 0 & \text{otherwise.} \end{cases}$ Also, write $X_{\mathcal{C}}$ for the characteristic function of \mathcal{C} . Now, $\langle \chi_D, \psi^G \rangle = \langle \chi_D, \chi_{\mathcal{C}}|_H \rangle = \frac{1}{|H|} \cdot \delta \cdot |D|$. And, $\langle (\chi_D)', \chi_{\mathcal{C}} \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_D'(g) X_{\mathcal{C}}(g) = \frac{1}{|G|} \cdot \frac{1}{|H|} \sum_{g \in G} \chi_D^0(x^{-1}gx) X_{\mathcal{C}}(g) = \frac{1}{|G|} \cdot \frac{1}{|H|} \sum_{\substack{g \in G, \\ x \in G \text{ with } x^{-1}gx \in D}} \chi_D(x^{-1}gx) X_{\mathcal{C}}(g) = \frac{1}{|G|} \cdot \frac{1}{|H|} \cdot |S| \cdot |\mathcal{C}| \cdot |\{g \in G \mid x^{-1}gx \in D\}| = \frac{1}{|H|} \cdot |D|$.

So the inner products with each $X_{\mathcal{C}}$ equal, and as $\{X_{\mathcal{C}} \mid \mathcal{C} \text{ a } G\text{-conjugacy class}\}$ is a basis, $\chi_D \psi^G = \chi_D'$.

Corollary 55: If $T = \{t_1, \dots, t_n\}$ is a transversal for H in G - i.e. $|G:H|=n$ and $t_i H, \dots, t_n H$ are all the cosets, then $\psi^G(g) = \sum_{i=1}^n \psi^0(t_i^{-1}gt_i)$.

Proof: For any $h \in H$, $\psi^0((t_i h)^{-1} g (t_i h)) = \psi^0(h^{-1} t_i^{-1} g t_i h) = \psi^0(t_i^{-1} g t_i)$.

So, in the expression in Theorem 54, sum over the respective cosets $t_i H$.

Example: $G = D_{2N} = \langle a, b \mid a^N = b^2 = babab^{-1} = 1 \rangle$, $H = \langle a \rangle$, $T = \{1, b\}$. $\psi: a^k \mapsto w^k$, with $w^N = 1$.

Then, $\psi^G(a^k) = \psi^0(a^k) + \psi^0(a^{-k}) = w^k + w^{-k}$, $\psi^G(b) = \psi^0(b) + \psi^0(b) = 0$.

This way, we get an irreducible for each $w = (e^{2\pi i})^j$, $j \leq \frac{N-1}{2}$.

$$\langle \psi^G, \psi^G \rangle = \frac{1}{2N} \sum_{k=1}^N (w^k + w^{-k})(w^k + w^{-k}) = \frac{1}{2N} (N+N) = 1, \text{ by orthogonality in } H, \text{ and this is } 1.$$

Lemma 56: $H \leq G$. Then $1_H \psi^G$ is the permutation character of G on the set $(G:H)$ of all left cosets of H in G .

Proof: Let $T = \{t_1, \dots, t_n\}$ be a transversal for H in G . $(1_H \psi^G)(g) = \sum_{t_i \in T} 1_H^0(t_i^{-1} g t_i)$ $= \#\{t_i \in T \mid t_i^{-1} g t_i \in H\} = \#\{t_i \in T \mid g t_i \in t_i H\} = |\{t_i \in T \mid g t_i \in H\}|$.

Lemma 57: $H \leq G$, ψ class function of H . Let $x \in G$ and assume that $H \cap \text{cl}_G(x) = \bigcup_{i \in S} \text{cl}_H(x_i)$.

Then, $\psi^G(x) = 1_{C_G(x)} \cdot \sum_{i \in S} \frac{1}{|C_H(x_i)|} \cdot \psi(x_i)$. In particular, if $x \in H$ and $\text{cl}_G(x)$ remains just one H -conjugacy class, then $\psi^G(x) = \frac{1}{|C_H(x)|} \psi(x)$.

Proof: Write $\zeta_{x,x}$ for the characteristic function of the x -conjugacy class of x .

So, $\zeta_{x,x}(g) = \begin{cases} 1 & \text{if } g \in \text{cl}_G(x) \\ 0 & \text{otherwise.} \end{cases}$ Then, for any class function χ of G ,

$$\langle \zeta_{x,x}, \chi \rangle = \frac{1}{|G|} \sum_{g \in G} \zeta_{x,x}(g) \chi(g) = \frac{1}{|G|} \sum_{g \in \text{cl}_G(x)} \chi(g) = \frac{1}{|C_H(x)|} \chi(x).$$

$$\text{Thus, } \frac{1}{|C_H(x)|} \psi^G(x) = \langle \zeta_{x,x}, \psi^G \rangle = \langle \zeta_{x,x}|_H, \psi \rangle_H = \langle \sum_{i \in S} \zeta_{H,x_i}, \psi \rangle_H = \sum_{i \in S} \frac{1}{|C_H(x_i)|} \psi(x_i) \quad (\text{by Frobenius reciprocity theorem})$$

Example: $H = D_{10} \triangleleft A_5 = G$. $D_{10}:$

10	5	5	2
1	$(12345)^{\pm}$	$(12345)^{\pm 2}$	$(125)(34)$
1	1	1	1
1	1	1	-1
2	$w+w^{-1}$	w^2+w^{-2}	0
2	w^2+w^{-2}	$w+w^{-1}$	0

$A_5:$

60	5	5	4	3
1	$(12345)^{\pm}$	$(12345)^{\pm 2}$	$(125)(34)$	(123)
1	1	1	1	1
4	-1	-1	0	$-(\pi_5 - 1)$
$[1, 1^G : 6]$	+	+	2	0]
$1, 1^G - 1_G : 5$	0	0	1	-1 - irreducible.
$[2, 1^G : 12]$	$w+w^{-1}$	w^2+w^{-2}	0	0] - contains χ_2, χ_3 .
$12 - 4 - 5_1 : 3$	$1+w+w^{-1}$	$1+w^2+w^{-2}$	-1	0

Similarly, $2, 1^G = 4 + 5 + 3_2$.

Alternative approach: V an FH -module. $V^H = FG \otimes_{FH} V$.

Take t_1, \dots, t_n , a transversal for the set of left cosets of H in G , and v_1, \dots, v_m , a basis for V . Take the space V^H , generated by the basis $t_i v_j$.

Define, for $g \in G$, $g t_i v_j := \sum_{k=1}^m g t_k v_j$ if $i \exists$ unique k with $t_k^{-1} g t_i \in H$ (so $g t_i \in t_k H$).

Then, $g t_i v_j := t_k^{-1} (t_k^{-1} g t_i) v_j$. $[V^H = V \oplus t_1 V \oplus \dots \oplus t_n V]$.

This is a G -action: $g, (g_1 t_i v_j) = g_1 (t_k (t_k^{-1} g_1 t_i) v_j)$ as \exists unique k such that $t_k^{-1} g_1 t_i \in H$.
 $= t_k (t_k^{-1} g_1 t_k) (t_k^{-1} g_1 t_i) v_j$ as \exists unique k such that $t_k^{-1} g_1 t_k \in H$.
 $= t_k (t_k^{-1} (g_1 g_2) t_k) v_j = (g_1 g_2) t_k v_j$.

This has the right character: $g: t_i v_j \mapsto t_k (t_k^{-1} g t_i) v_j$, so contribution to trace iff $k=i$, i.e., iff $t_k^{-1} g t_i \in H$, then this contributes $\chi^0(t_k^{-1} g t_i)$.

Frobenius reciprocity: exercise on example sheet 4.

Additional notes: handouts.

Proposition: If g is a p -element in G and χ a character of G with $\chi(g) \in \mathbb{Z}$, then $\chi(g) \equiv \chi(1)$ mod p .

Proof: Let $\zeta = e^{\frac{2\pi i}{p}} \in \mathbb{C}$, and consider the ring $\mathbb{Z}[\zeta]$. Take p to be a maximal ideal of $\mathbb{Z}[\zeta]$ containing the ideal $p\mathbb{Z}[\zeta]$. It is easy to see that $p \cap \mathbb{Z} = p\mathbb{Z}$, so the assertion follows from the next result, slightly more general.

Lemma: Let $a, b \in G$, with $ab = ba$, b a p -element, and a of order prime to p . Then $\chi(ab) \equiv \chi(a)$ mod p .

Proof: Restrict to $H = \langle ab \rangle$. It is enough to prove this for every irreducible ψ of H .

So, ψ is degree 1 and $\psi(ab) = \psi(a)\psi(b)$. But, $\psi(b) \equiv 1$ mod p , since $\psi(b) = w$ with $w^{p^l} = 1$ for some $l \in \mathbb{N}$, so $0 = w^{p^l} - 1 \equiv (w-1)^{p^l} \pmod{p}$, whence $w \equiv 1 \pmod{p}$ as p is prime (being maximal).

Theorem: If χ is a complex irreducible character of G then $\chi(1) \mid |G|$.

Proof: Let V be a $\mathbb{C}G$ -module affording χ . If C is a conjugacy class, write $C = \sum_{g \in C} g$. Now, $Cv = \lambda v \quad \forall v \in V$, where $\lambda = \frac{|G|}{|C_G(g)|} \cdot \frac{\chi(g)}{\chi(1)}$: since $C \in \mathcal{Z}(\mathbb{C}G)$, by Schur there is a scalar $\lambda \in \mathbb{C}$ with $Cv = \lambda v \quad \forall v \in V$, and $\sum_{x \in G} \chi(x) = \lambda |G|$, so $\sum_{x \in C} \chi(x) = \lambda \chi(1)$, so $\lambda = \frac{|G| \cdot \chi(g)}{\chi(1)} = \frac{|G|}{|C_G(g)|} \cdot \frac{\chi(g)}{\chi(1)}$.

Next, λ is an algebraic integer: if x_1, \dots, x_n are the elements of G , then $Cx_i = \sum a_{ij} x_j$ with $a_{ij} \in \mathbb{Z}$, and $Cv = \lambda v$, so λ is an eigenvalue of the matrix (a_{ij}) with integer entries.

Finally, let C_1, \dots, C_k be the conjugacy classes of G ; let $g_i \in C_i$.

Then, $\frac{|G|}{\chi(1)} = \sum \frac{|G|}{|C_G(g_i)|} \cdot \frac{\chi(g_i)}{\chi(1)}$, by orthogonality, and the right hand side is an algebraic integer by the above (and note (ii) below).

Thus $\frac{|G|}{\chi(1)}$ is an algebraic integer which is also clearly a rational number, and so must be a rational integer.

Note: we have used: (i) the set A of algebraic integers is a ring,
(ii) $A \cap \mathbb{Q} = \mathbb{Z}$.

Next: The Burnside p^aq^b theorem...