REPRESENTATION THEORY

SIMON WADSLEY

Lecture 1

1. Introduction

Representation Theory is the study of how symmetries occur in nature; that is the study of how groups act by linear transformations on vector spaces.

Recall that an action of a group G on a set X is a map $\cdot\colon G\times X \to X; (g,x)\mapsto g\cdot x$ such that

(i) $e\cdot x = x$ for all $x\in X$;
(ii) $(gh)\cdot x = g\cdot(h\cdot x)$ for all $g,h\in G$ and $x\in X$.

Recall also that to define such an action is equivalent to defining a group homomorphism $\rho\colon G\to S(X)$ where $S(X)$ denotes the symmetric group on the set X.

A *representation* ρ of a group G on a vector space V is a group homomorphism $\rho\colon G\to GL(V)$, the group of invertible linear transformations of V.

We want to understand all representations of G on finite dimensional vector spaces. Of course, vector spaces do not come equipped with a notion of distance. If we want to study distance preserving transformations of a (f.d.) real/complex inner product space we should instead consider homomorphisms $G\to O(V)$, the group of orthogonal transformations of V or $G\to U(V)$, the group of unitary transformations of V. We'll see later that this restriction doesn't make any difference to the theory in a way we will make precise.

Recall that if G acts on a set X then X may be written as a disjoint union of orbits $X=\bigcup X_i$ with G acting transitively on each X_i.

Question. What is the equivalent notion for representations?

We'll see that disjoint union of sets should correspond to direct sum of vector spaces and that there is a good equivalent notion when G is finite and k has characteristic zero. However, it is less rigid because there are many ways to decompose an n-dimensional vector spaces as a direct sum of 1-dimensional subspaces.

To understand all actions of G on sets X by using the decomposition into orbits it is enough to consider transitive actions.

The Orbit-Stabiliser theorem says that if G acts on X and $x\in X$ then there is a bijection

$$\pi\colon G/\operatorname{Stab}_G(x)\xrightarrow{\sim}\operatorname{Orb}_G(x)$$

given by

$$g\operatorname{Stab}_G(x)\mapsto g\cdot x.$$

In fact this bijection is G-equivariant: if we given $G/\operatorname{Stab}_G(x)$ the left regular action $g\cdot(h\operatorname{Stab}_G(x)) = gh\operatorname{Stab}_G(x)$ then $g\pi(y)=\pi(gy)$ for all $y\in G/\operatorname{Stab}_G(x)$. Thus as a set with G-action $\operatorname{Orb}_G(x)$ is determined by $\operatorname{Stab}_G(x)$.

Recall also that $\mathrm{Stab}_G(g\cdot x) = g\,\mathrm{Stab}_G(x)g^{-1}$ (IA Groups Ex Sheet 3). Thus $\mathrm{Orb}_G(x)$ is determined by the conjugacy class of $\mathrm{Stab}_G(x)$; that is there is a $1-1$ correspondance

$$\{\text{sets with a transitive } G\text{-action}\}/\sim \longleftrightarrow \{\text{conj. classes of subgroups of } G\}$$

given by $X \mapsto \{Stab_G(x) \mid x \in X\}$ and $\{gHg^{-1} \mid g \in G\} \mapsto G/H$.

Question. What is the equivalent notion for representations?

Suppose that X, Y are two sets with G-action. We say that $f\colon X \to Y$ is G-equivariant if $g \cdot f(x) = f(g\cdot x)$ for all $g \in G$ and $x \in X$. Note that if f is G-equivariant and $x \in X$ then $f(\mathrm{Orb}_G(x)) = \mathrm{Orb}_G(f(x))$ (exercise). Notice also that $f|_{\mathrm{Orb}_G(x)}$ is determined by $f(x)$ and $\mathrm{Stab}_G(x) \leqslant \mathrm{Stab}_G(f(x))$. In fact this condition is also sufficient so

$$|\{G-\text{equivariant functions } \mathrm{Orb}_G(x) \to Y\}| = |\{y \in Y \mid \mathrm{Stab}_G(x) \leqslant \mathrm{Stab}_G(y)\}.$$

Question. What is the equivalent notion for representations

Our main goal is to classify all representations of a (finite) group G and understand maps between them. A secondary goal is to use this theory to better understand groups (eg Burnside's p^aq^b theorem that says there are no finite simple groups whose order has precisely two distinct prime factors).

1.1. **Linear algebra revision.** By *vector space* we will always mean a finite dimensional vector space over a field k. For this course k will usually be algebraically closed and of characteristic zero, for example $\mathbb{C}$. However there are rich theories for more general fields.

Given a vector space V, we define

$$GL(V) = \mathrm{Aut}(V) = \{f\colon V \to V \mid f \text{ linear and invertible}\}$$

the *general linear group* of V; $GL(V)$ is a group under composition of linear maps.

Because all our vector spaces are finite dimensional, $V \cong k^d$ for some $d \geqslant 0$. Such an isomorphism determines a basis $e_1, \ldots, e_d$ for V. Then

$$GL(V) \cong \{A \in \mathrm{Mat}_d(k) \mid \det(A) \neq 0\}.$$

This isomorphism is given by the map that sends the linear map f to the matrix A such that $f(e_i) = A_{ji}e_j$.

Exercise. Check that this does indeed define an isomorphism of groups. ie check that f is an isomorphism if and only if $\det A \neq 0$; and that the given map is a bijective group homomorphism.

If $k = \mathbb{R}^d$ and $\langle -,-\rangle$ is an inner product on V then

$$O(V) := \{f \in GL(V) \mid \langle f(v), f(w)\rangle = \langle v, w\rangle\ \forall v, w \in V\}$$

Choosing an orthonormal basis defines an isomorphism

$$O(V) \cong \{A \in \mathrm{Mat}_d(\mathbb{R}) \mid AA^T = I\} =: O(d).$$

If $k = \mathbb{C}$ and $\langle -,-\rangle$ is a (Hermitian) inner product on V,

$$U(V) := \{f \in GL(V) \mid \langle f(v), f(w)\rangle = \langle v, w\rangle\ \forall v, w \in V\}$$

This time choosing an o.n. basis defines an isomorphism

$$U(V) \cong \{A \in \mathrm{Mat}_d(\mathbb{C}) \mid A\bar{A}^T = I\} =: U(d).$$

Lecture 2

1.2. Group representations.

Definition. A *representation* ρ of a group G on a vector space V is a group homomorphism $\rho\colon G \to GL(V)$.

By abuse of notation we will sometimes refer to the representation by ρ, sometimes by the pair (ρ, V) and sometimes just by V with the ρ implied. This can sometimes be confusing but we have to live with it.

Thus defining a representation of G on V corresponds to assigning a linear map $\rho(g)\colon V \to V$ to each $g \in G$ such that

(i) $\rho(e) = \mathrm{id}_V$;
(ii) $\rho(gh) = \rho(g)\rho(h)$ for all $g, h \in G$;
(iii) $\rho(g^{-1}) = \rho(g)^{-1}$ for all $g \in G$.

Exercise. Show that (iii) is redundant in the above.

Given a basis for V a representation ρ is an assignment of a matrix $\rho(g)$ to each $g \in G$ such that (i),(ii) and (iii) hold.

Definition. The *degree* of ρ or *dimension* of ρ is $\dim V$.

Definition. We say a representation ρ is *faithful* if $\ker \rho = \{e\}$.

Examples.

(1) Let G be any group and $V = k$. Then $\rho\colon G \to \mathrm{Aut}(V); g \mapsto \mathrm{id}$ is called the *trivial representation.*
(2) Let $G = C_2 = \{\pm 1\}$, $V = \mathbb{R}^2$, then
$$\rho(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \rho(-1) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$
is a group rep of G on V.
(3) Let $G = (\mathbb{Z}, +)$, V a vector space, and ρ a representation of G on V. Then necessarily $\rho(0) = \mathrm{id}_V$, and $\rho(1)$ is some invertible linear map f on V. Now $\rho(2) = \rho(1+1) = \rho(1)^2 = f^2$. Inductively we see $\rho(n) = f^n$ for all $n > 0$. Finally $\rho(-n) = (f^n)^{-1} = (f^{-1})^n$. So $\rho(n) = f^n$ for all $n \in \mathbb{Z}$.
Notice that conversely given any invertible linear map $f\colon V \to V$ we may define a representation of G on V by $\rho(n) = f^n$.
Thus we see that there is a 1-1 correspondence between representations of $\mathbb{Z}$ and invertible linear transformations given by $\rho \mapsto \rho(1)$.
(4) Let $G = (\mathbb{Z}/N, +)$, and $\rho\colon G \to GL(V)$ a rep. As before we see $\rho(n) = \rho(1)^n$ for all $n \in \mathbb{Z}$ but now we have the additional constraint that $\rho(N) = \rho(0) = \mathrm{id}_V$.
Thus representations of $\mathbb{Z}/N$ correspond to invertible linear maps f such that $f^N = \mathrm{id}_V$. Of course any linear map such that $f^N = \mathrm{id}_V$ is invertible so we may drop the word invertible from this correspondence.

Exercise. Check the details

(5) If G is a group generated by $x_1, \ldots, x_n$ and with relations (words in x_i, x_i^{-1} equal to the identity in G) $r_1(x_1, \ldots, x_n), \ldots, r_m(x_1, \ldots, x_n)$, then there is a 1-1 correspondence between representations of G on V and n-tuples of invertible linear maps $(A_1, \ldots, A_n)$ on V such that $r_i(A_1, \ldots, A_n) = \mathrm{id}_V$.

(6) Let $G = S_3$, the symmetric group of $\{1,2,3\}$, and $V = \mathbb{R}^2$. Take an equilateral triangle in V centred on 0; then G acts on the triangle by permuting the vertices. Each such symmetry induces a linear transformation of V. For example $g = (12)$ induces the reflection through the vertex three and the midpoint of the opposite side, and $g = (123)$ corresponds to a rotation by $2\pi/3$.

Exercise. Choose a basis for $\mathbb{R}^2$. Write the coordinates of the vertices of the triangle in this basis. For each $g \in S_3$ write down the matrix of the corresponding linear map. Check that this does define a representation of S_3 on V. Would the calculations be easier in a different basis?

(7) Given a finite set X we may form the vector space kX of functions X to k with basis $\langle \delta_x \mid x \in X\rangle$ where $\delta_x(y) = \delta_{xy}$.

Then an action of G on X induces a representation $\rho\colon G \to \mathrm{Aut}(kX)$ by $(\rho(g)f)(x) = f(g^{-1}\cdot x)$ called the *permutation representation* of G on X.

To check this is a representation we must check that each $\rho(g)$ is linear, that $\rho(e) = \mathrm{id}$ and $\rho(gh) = \rho(g)\rho(h)$ for each $g, h \in G$.

For the last observe that for each $x \in X$,

$$\rho(g)(\rho(h)f)(x) = (\rho(h)f)(g^{-1}x) = f(h^{-1}g^{-1}x) = \rho(gh)f(x).$$

Notice that $\rho(g)\delta_x(y) = \delta_{x,g^{-1}\cdot y} = \delta_{g\cdot x,y}$ so $\rho(g)\delta_x = \delta_{g\cdot x}$. So by linearity $\rho(g)(\sum_{x\in X}\lambda_x\delta_x) = \sum \lambda_x \delta_{g\cdot x}$.

(8) In particular if G is finite then the action of G on itself induces the *regular representation* kG of G. The regular representation is always faithful because $g\delta_e = \delta_e$ implies that $ge = e$ and so $g = e$.

(9) If $\rho\colon G \to GL(V)$ is a representation of G then we can use ρ to define a representation of G on V^*

$$\rho^*(g)(f)(v) = f(\rho(g^{-1})v); \quad \forall f \in V^*, v \in V.$$

Exercise. Prove that ρ^* is a representation of V. Moreover, show that if $e_1, \ldots, e_n$ is a basis for V and $\epsilon_1, \ldots, \epsilon_n$ is its dual basis then the matrices representing $\rho(g)$ and $\rho^*(g)$ are related by $\rho(g)^* = (\rho(g)^{-1})^t$.

(10) More generally, if $(\rho, V), (\rho', W)$ are representations of G then $(\alpha, \mathrm{Hom}_k(V,W))$ defined by

$$\alpha(g)(f)(v) = \rho'(g)f(\rho(g)^{-1}v); \quad \forall g \in G, f \in \mathrm{Hom}_k(V,W), v \in V$$

is a rep of G.

Note that if $W = k$ is the trivial rep. this reduces to example 9. If instead $V = k$ then $\mathrm{Hom}_k(k,W) \cong W; f \mapsto f(1)$ is an isomorphism of representations in a sense to be defined next lecture.

Lecture 3

1.3. **The category of representations.** We want to classify all representations of a group G but first we need a good notion of when two representations are the same.

Notice that if $\rho\colon G \to GL(V)$ is a representation and $\varphi\colon V \to V'$ is a vector space isomorphism then we may define $\rho'\colon G \to GL(V')$ by $\rho'(g) = \varphi \circ \rho(g) \circ \varphi^{-1}$. Then ρ' is also a representation.

Definition. We say that $\rho\colon G \to GL(V)$ and $\rho'\colon G \to GL(V')$ are *isomorphic* representations if there is a linear isomorphism $\varphi\colon V \to V'$ such that

$$\rho'(g) = \varphi \circ \rho(g) \circ \varphi^{-1} \text{ for all } g \in G$$

i.e. if $\rho'(g) \circ \varphi = \varphi \circ \rho(g)$. We say that φ *intertwines* ρ and ρ'.

Notice that if φ intertwines ρ and ρ' and φ' intertwines ρ' and ρ'' then $\varphi'\varphi$ intertwines ρ and ρ'' and φ^{-1} intertwines ρ' and ρ. Thus isomorphism is an equivalence relation.

If $\rho\colon G \to GL_d(k)$ is a matrix representation then an intertwining map $k^d \to k^d$ is an invertible matrix P and the matrices of the reps it intertwines are related by $\rho'(g) = P\rho(g)P^{-1}$. Thus matrix representations are equivalent precisely if they correspond to the same representation with respect to different bases.

Examples.

(1) If $G = \{e\}$ then a representation of G is just a vector space and two vector spaces are isomorphic as representations if and only if they have the same dimension.

(2) If $G = \mathbb{Z}$ then $\rho\colon G \to GL(V)$ and $\rho'\colon G \to GL(V')$ are isomorphic reps if and only if there are bases of V and V' such that $\rho(1)$ and $\rho'(1)$ are the same matrix. In other words isomorphism classes of representations of $\mathbb{Z}$ correspond to conjugacy classes of invertible matrices. Over $\mathbb{C}$ the latter is classified by Jordan Normal Form (more generally by rational canonical form).

(3) If $G = C_2 = \{\pm 1\}$ then isomorphism classes of representations of G correspond to conjugacy classes of matrices that square to the identity. Since the minimal polynomial of such a matrix divides $X^2 - 1 = (X-1)(X+1)$ provided the field does not have characteristic 2 every such matrix is conjugate to a diagonal matrix with diagonal entries all ± 1.

    Exercise. Show that there are precisely $n + 1$ isomorphism classes of representations of C_2 of dimension n.

(4) If X, Y are finite sets with a G-action and $f\colon X \to Y$ is a G-equivariant bijection then $\varphi\colon kX \to kY$ defined by $\varphi(\theta)(y) = \theta(f^{-1}y)$ intertwines kX and kY. (Note that $\varphi(\delta_x) = \delta_{f(x)}$)

Note that two isomorphic representations must have the same dimension but that the converse is not true.

Definition. Suppose that $\rho\colon G \to GL(V)$ is a rep. We say that a k-linear subspace W of V is *G-invariant* if $\rho(g)(W) \subset W$ for all $g \in G$ (ie $\rho(g)(w) \in W$ for all $g \in G$ and $w \in W$).

In that case we call W a *subrepresentation* of V; we may define a representation $\rho_W\colon G \to GL(W)$ by $\rho_W(g)(w) = \rho(g)(w)$ for $w \in W$.

We call a subrepresentation W of V *proper* if $W \neq V$ and $W \neq 0$. We say that $V \neq 0$ is *irreducible* or *simple* if it has no proper subreps.

Examples.

(1) Any one-dimensional representation of a group is irreducible.

(2) Suppose that $\rho\colon \mathbb{Z}/2 \to GL(k^2)$ is given by $-1 \mapsto \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ (char $k \neq 2$). Then there are precisely two proper subreps spanned by $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ respectively.

Proof. It is easy to see that these two subspaces are G-invariant. Any proper subrep must be one dimensional and so by spanned by an eigenvector of $\rho(-1)$. But the eigenspaces of $\rho(-1)$ are precisely those already described. □

(3) If G is C_2 then the only irreducible representations are one-dimensional.

Proof. Suppose $\rho\colon G \to GL(V)$ is an irreducible rep. The minimal polynomial of $\rho(-1)$ divides $X^2-1=(X-1)(X+1)$. Thus $\rho(-1)$ has an eigenvector v. Now $0 \neq \langle v \rangle$ is a subrep. of V. Thus $V = \langle v \rangle$. □

Notice we've shown along the way that there are precisely two simple reps of G if k doesn't have characteristic 2 and only one if it does.

(4) If $G = D_6$ then every irreducible complex representation has dimension at most 2.

Proof. Suppose $\rho\colon G \to GL(V)$ is an irred. G-rep. Let r be a non-trivial rotation and s a reflection in G. Then $\rho(r)$ has a eigenvector v, say. So $\rho(r)v = \lambda v$ for some $\lambda \neq 0$. Consider $W := \langle v, \rho(s)v \rangle \subset V$. Since $\rho(s)\rho(s)v = v$ and $\rho(r)\rho(s)v = \rho(s)\rho(r)^{-1}v = \lambda^{-1}\rho(s)v$, W is G-invariant. Since V is irred, $W = V$. □

Exercise. Classify all irred reps of D_6 up to iso (Hint: $\lambda^3 = 1$ above). Note in particular that D_6 has an irred. rep. of degree 2.

Lemma. *Suppose $\rho\colon G \to GL(V)$ is a rep. and $W \subset V$. Then the following are equivalent:*

(i) W is a subrep;
(ii) there is a basis $v_1, \ldots, v_d$ of V such that $v_1, \ldots, v_r$ is a basis of W and the matrices $\rho(g)$ are all block upper triangular;
(iii) for every basis $v_1, \ldots, v_d$ of V such that $v_1, \ldots, v_r$ is a basis of W the matrices $\rho(g)$ are all block upper triangular.

Proof. Think about it! □

Definition. If W is a subrep of a rep (ρ, V) of G then we may define a *quotient representation* by $\rho_{V/W}\colon G \to GL(V/W)$ by $\rho(g)(v+W) = \rho(g)(v) + W$. Since $\rho(g)W \subset W$ for all $g \in G$ this is well-defined.

Next time, we want to formulate a 'first isomorphism theorem for representations'.

Lecture 4

We'll start dropping ρ now and write g for $\rho(g)$ where it won't cause confusion.

Definition. If (ρ, V) and (ρ', W) are reps of G we say a linear map $\varphi\colon V \to W$ is a *G-linear* map if $\varphi g = g\varphi$ (ie $\varphi \circ \rho(g) = \rho'(g) \circ \varphi$) for all $g \in G$. We write

$$\mathrm{Hom}_G(V,W) = \{\varphi \in \mathrm{Hom}_k(V,W) \mid \varphi \text{ is } G \text{ linear}\},$$

a k-vector space.

Remarks.

(1) If $W \leqslant V$ is a subrep then the natural inclusion map $\iota\colon W \to V$ is in $\mathrm{Hom}_G(W,V)$ and the natural projection map $\pi\colon V \to V/W$ is in $\mathrm{Hom}_G(V, V/W)$.

(2) $\varphi \in \mathrm{Hom}_k(V, W)$ is an intertwining map precisely if ϕ is a bijection and ϕ is in $\mathrm{Hom}_G(V, W)$.
(3) Recall that $\mathrm{Hom}_k(V, W)$ is a G-rep via $(g\varphi)(v) = g(\varphi(g^{-1}v))$ for $\varphi \in \mathrm{Hom}_k(V, W)$, $g \in G$ and $v \in V$. Then $\varphi \in \mathrm{Hom}_G(V, W)$ precisely if $g\varphi = \varphi$ for all $g \in G$.

Note if $\varphi \in \mathrm{Hom}_G(V, W)$ is a vector space isomorphism then φ intertwines the isomorphic reps V and W.

Lemma. *Suppose (ρ, V) and (ρ', W) are representations of G and $\varphi \in \mathrm{Hom}_G(V, W)$ then*

(i) $\ker\varphi$ *is a subrep of* V*.*
(ii) $\mathrm{Im}\varphi$ *is a subrep of* W*.*
(iii) $V/\ker\varphi$ *is isomorphic to* $\mathrm{Im}\varphi$ *as reps of* G*.*

Proof.
(i) if $v \in \ker\varphi$ and $g \in G$ then $\varphi(gv) = g\varphi(v) = 0$
(ii) if $w = \varphi(v) \in \mathrm{Im}\varphi$ and $g \in G$ then $gw = \varphi(gv) \in \mathrm{Im}\varphi$.
(iii) We know that the linear map φ induces a linear isomorphism

$$\overline{\varphi}\colon V/\ker\varphi \to \mathrm{Im}\varphi; v + \ker\varphi \mapsto \varphi(v)$$

then $g\overline{\varphi}(v + \ker\varphi) = g(\varphi(v)) = \varphi(gv) = \overline{\varphi}(gv + \ker\varphi)$ □

2. Complete reducibility and Maschke's Theorem

Question. Given a representation V and a subrepresentation W when can we find a vector space complement of W that is also a subrepresentation?

Example. Suppose $G = C_2$, $V = \mathbb{R}^2$ and $\rho(-1) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, $W = \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle$ has many vector space complements but only one of them, $\left\langle \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\rangle$, is a subrep.

Definition. We say a representation V is a *direct sum* of U and W if U and W are subreps of V such that $V = U \oplus W$ as vector spaces (ie $V = U + W$ and $U \cap W = 0$).

Given two representations (ρ_1, U) and (ρ_2, W) we may define a representation of G on $U \oplus W$ by $\rho(g)(u, w) = (\rho_1(g)u, \rho_2(g)w)$.

Examples.

(1) If G acts on a finite set X so that X may be written as the disjoint union of two G-invariant subsets X_1 and X_2. Then $kX \cong kX_1 \oplus kX_2$ under $f \mapsto (f|_{X_1}, f|_{X_2})$.
   That is $kX = \{f \mid f(x) = 0\ \forall x \in X_2\} \oplus \{f \mid f(x) = 0\ \forall x \in X_1\}$.
   More generally if the G-action on X decomposes into orbits as a disjoint union $X = \bigcup \mathcal{O}_i$ then $kX \cong \bigoplus k\mathcal{O}_i$.
(2) If G acts transitively on a finite set X then $U := \{f \in kX \mid \sum_{x\in X} f(x) = 0\}$ and $W := \{f \in kX \mid f \text{ is constant}\}$ are subreps of kX. If k is charactersitic 0 then $kX = U \oplus W$. What happens if k has characteristic $p > 0$?
(3) (Exercise) Show that the $\mathbb{C}$-rep of $\mathbb{Z}$ on $\langle e_1, \dots, e_n\rangle$ given by $\rho(1)(e_1) = e_1$ and $\rho(1)(e_i) = e_i + e_{i-1}$ for $i > 1$ has precisely $n - 1$ proper subreps $\langle e_1, \dots, e_k\rangle$ for $1 \leqslant k < n$. Deduce that no proper subrep has a G-invariant complement.

Proposition. *Suppose $\rho\colon G \to GL(V)$ is a rep. and $V = U \oplus W$ as vector spaces. Then the following are equivalent:*

(i) $V = U \oplus W$ *as reps;*
(ii) *there is a basis* $v_1, \dots, v_d$ *of* V *such that* $v_1, \dots, v_r$ *is a basis of* U *and* $v_{r+1}, \dots v_d$ *is a basis for* W *and the matrices* $\rho(g)$ *are all block diagonal;*
(iii) *for every basis* $v_1, \dots, v_d$ *of* V *such that* $v_1, \dots, v_r$ *is a basis of* U *and* $v_{r+1}, \dots, v_d$ *is a basis for* W *and the matrices* $\rho(g)$ *are all block diagonal.*

Proof. Think about it! □

But warning:

Example. $\rho\colon \mathbb{Z}/2 \to GL_2(\mathbb{R})$; $1 \mapsto \begin{pmatrix} -1 & -2 \\ 0 & 1 \end{pmatrix}$ defines a representation (check). The representation $\mathbb{R}^2$ breaks up as $\langle e_1 \rangle \oplus \langle e_1 - e_2 \rangle$ as subreps even though the matrix is upper triangular but not diagonal.

We've seen by considering $G = \mathbb{Z}$ that it is not true that for every reperesentation of a group G, every subrepresentation has a G-invariant complement. However, we can prove the following remarkable theorem.

Theorem (Maschke's Theorem)**.** *Let G be a finite group and (ρ, V) a representation of G over a field k of characteristic zero. Suppose $W \subset V$ is an invariant subspace. Then there is a G-invariant complement to W ie a G-invariant subspace U of V such that $V = U \oplus W$.*

Corollary (Complete reducibility)**.** *If G is a finite group, (ρ, V) a representation over a field of characteristic zero. Then $V \cong W_1 \oplus \cdots W_r$ is a direct sum of representations with each W_i irreducible.*

Proof. By induction on $\dim V$. If $\dim V = 0$ or V is irreducible then the result is clear. Otherwise V has a non-trivial G-invariant subspace W.

By the theorem there is a G-invariant complement U and $V \cong U \oplus W$ as G-reps. But $\dim U, \dim W < \dim V$, so by induction they each break up as a direct sum of irreducibles subreps. Thus V does also. □

Example. We saw before that every representation of $\mathbb{Z}/2$ over $\mathbb{C}$ is a direct sum of 1-dimensional subreps as we may diagonalise $\rho(-1)$. Let's think about how this might generalise:

Suppose that G is a finite abelian group, and (ρ, V) is a complex representation of G. Each element $g \in G$ has finite order so has a minimal polynomial dividing $X^n - 1$ for $n = o(g)$. In particular it has distinct roots. Thus there is a basis for V such that $\rho(g)$ is diagonal. But because G is abelian $\rho(g)$ and $\rho(h)$ commute for each pair $g, h \in G$ and so the $\rho(g)$ may be simultaneously diagonalised (Sketch proof: if each $\rho(g)$ is a scalar matrix the result is clear. Otherwise pick $g \in G$ such that $\rho(g)$ is not a scalar matrix. Each eigenspace $E(\lambda)$ of $\rho(g)$ will be G-invariant since G is abelian. By induction on $\dim V$ we may solve the problem for each subrep $E(\lambda)$ and then put these subreps back together). Thus V decomposes as a direct sum of one-dimensional reps. Of course, this technique can't work in general because (a) $\rho(g)$ and $\rho(h)$ won't commute in general; (b) not every irreducible rep is one-dimensional in general. Thus we'll need a new idea.

Example. Let G act on a finite set X, and consider the real permutation representation $\mathbb{R}X = \{f \colon X \to \mathbb{R}\}$ with $(\rho(g)f)(x) = f(g^{-1}x)$.

Idea: with respect to the given basis δ_x all the matrices $\rho(g)$ are orthogonal; that is they preserve distance. This is because the standard inner product with respect to the basis is $\langle f_1, f_2\rangle = \sum_{x\in X} f_1(x)f_2(x)$ and so for each $g \in G$

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

since g permutes the elements of X.

In particular if W is a subrep of $\mathbb{R}X$ and $W^\perp := \{v \in \mathbb{R}X \mid \langle v, W\rangle = 0\}$ then if $g \in G$ and $v \in W^\perp$ and $w \in W$ we have (suppressing the ρ) $\langle w, gv\rangle = \langle g^{-1}w, v\rangle = 0$ since $g^{-1}w \in W$. Thus G preserves $W^\perp$ which is thus a G-invariant complement to W.

Lecture 5

Recall the statement of Maschke's theorem.

Theorem (Maschke's Theorem)**.** *Let G be a finite group and (ρ, V) a representation of G over a field k of characteristic zero. Suppose $W \subset V$ is an invariant subspace. Then there is a G-invariant complement to W ie a G-invariant subspace U of V such that $V = U \oplus W$.*

We're going to prove this first for $k = \mathbb{C}$ using inner products and the idea from the example at the end of the last lecture and then adapt the proof to general characteristic zero fields.

Recall, if V is a complex vector space then a Hermitian inner product is a positive definite Hermitian sesquilinear map $(-,-)\colon V \times V \to \mathbb{C}$ that is a map satisfying

(i) $(ax + by, z) = \overline{a}(x, z) + \overline{b}(y, z)$ and $(x, ay + bz) = a(x, y) + b(x, z)$ for $a, b \in \mathbb{C}$, $x, y, z \in V$ (sesquilinear);
(ii) $(x, y) = \overline{(y, x)}$ (Hermitian);
(iii) $(x, x) > 0$ for all $x \in V\backslash\{0\}$ (positive definite).

If $W \subset V$ is a linear subspace of a complex vector space with a Hermitian inner product and $W^\perp = \{v \in V \mid (v, w) = 0\ \forall w \in W\}$ then $W^\perp$ is a vector space complement to W in V.

Definition. A Hermitian inner product on a G-rep V is G-invariant if $(gx, gy) = (x, y)$ for all $g \in G$ and $x, y \in V$; equivalently if $(gx, gx) = (x, x)$ for all $g \in G$ and $x \in V$.

Lemma. *If $(-,-)$ is a G-invariant Hermitian inner product on a G-rep V and $W \subset V$ is a subrep then $W^\perp$ is a G-invariant complement to W.*

Proof. It suffices to prove that $W^\perp$ is G-invariant since $W^\perp$ is a complement to W.

Suppose $g \in G$, $x \in W^\perp$ and $w \in W$. Then $(gx, w) = (x, g^{-1}w) = 0$ since $g^{-1}w \in W$. Thus $gx \in W^\perp$ as required. □

Proposition (Weyl's unitary trick)**.** *If V is a complex representation of a finite group G, then there is a G-invariant Hermitian inner product on V.*

Proof. Pick any Hermitian inner product $\langle -,-\rangle$ on V (e.g. choose a basis $e_1,\dots,e_n$ and take the standard inner product $\langle \sum \lambda_i e_i, \sum \mu_i e_i\rangle = \sum \overline{\lambda_i}\mu_i$). Then define a new inner product $(-,-)$ on V by averaging:

$$(x,y) := \frac{1}{|G|}\sum_{g\in G}\langle gx, gy\rangle.$$

It is easy to see that $(-,-)$ is a Hermitian innder product because $\langle -,-\rangle$ is so. For example if $a,b\in\mathbb{C}$ and $x,y,z\in V$, then

$$\begin{aligned}(x, ay+bz) &= \frac{1}{|G|}\sum_{g\in G}\langle gx, g(ay+bz)\rangle \\ &= \frac{1}{|G|}\sum_{g\in G}\langle gx, ag(y)+bg(z)\rangle \\ &= \frac{1}{|G|}\sum_{g\in G}(a\langle gx,gy\rangle + b\langle gx,gz\rangle) \\ &= a(x,y)+b(z,y)\end{aligned}$$

as required.

But now if $h\in G$ and $x,y\in V$ then

$$(hx,hy) = \frac{1}{|G|}\sum_{g\in G}\langle ghx, ghy\rangle = \frac{1}{|G|}\sum_{g'\in G}\langle g'x, g'y\rangle$$

and so $(-,-)$ is G-invariant. □

Corollary. *For every complex representation V of a finite group G, every subrepresentation has a G-invariant complement and so V splits as a direct sum of irreducible subreps.*

Proof. Apply the Proposition and then the Lemma. □

Corollary (of Weyl's unitary trick)**.** *Every finite subgroup G of $GL_n(\mathbb{C})$ is conjugate to a subgroup of $U(n)$.*

Proof. First notice that $G \leqslant U(n)$ if and only if $(gx,gy)=(x,y)$ for all $x,y\in\mathbb{C}^n$ and $g\in G$ — here $(-,-)$ denotes the standard inner product with respect to the standard basis of $\mathbb{C}^n$.

By the unitary trick we can find a G-invariant Hermitian inner product $\langle -,-\rangle$ and choose an orthonormal basis for $\mathbb{C}^n$ with respect to $\langle -,-\rangle$ using Gram-Schmidt, say.

Let P be the change of basis matrix from the standard basis to the newly constructed basis. Then $\langle Pa,Pb\rangle = (a,b)$ for $a,b\in V$. So for each $g\in G$

$$(P^{-1}gPa, P^{-1}gPb) = \langle gPa, gPb\rangle = \langle Pa,Pb\rangle = (a,b).$$

Thus $P^{-1}gP\in U(n)$ for each $g\in G$ as required. □

Thus studying all complex representations of a finite group G is equivalent to studying unitary (ie distance preserving) ones.

We now adapt our proof of complete reducibility to handle any field of characteristic k, even if there is no notion of inner product.

Theorem (Maschke's Theorem)**.** *Let G be a finite group and V a representation of G over a field k of characteristic zero. Then every subrep W of V has a G-invariant complement.*

Proof. Choose some projection $\pi\colon V \to W$; ie a k-linear map $\pi\colon V \to W$ such that $\pi(w) = w$ for all $w \in W$.

Now $\ker \pi$ is a vector space complement to W since (1) if $v \in \ker \pi \cap W$ then $v = 0$ and (2) $\pi(v - \pi(v)) = 0$ for all $v \in V$ so $V = W + \ker \pi$. Moreover $\ker \pi$ is G-invariant if $\pi \in \mathrm{Hom}_G(V, W)$. So we try to build a G-linear projection $V \to W$ by averaging π.

Recall that $\mathrm{Hom}_k(V, W)$ is a rep of G via $(g\varphi)(v) = g(\varphi(g^{-1}v))$. Let $\pi'\colon V \to W$ be defined by

$$\pi' := \frac{1}{|G|} \sum_{g \in G} (g\pi)$$

Then $\pi'(w) = \frac{1}{|G|} \sum_{g\in G} g(\pi(g^{-1}w)) = w$ since $g(\pi(g^{-1}w)) = w$ for all $g \in G$ and $w \in W$. Moreover for $h \in G$, $(h\pi') = \frac{1}{|G|} \sum_{g \in G} (hg)\pi = \pi'$.

Thus $\pi' \in \mathrm{Hom}_G(V, W)$ and π' is a G-invariant projection $V \to W$. So $\ker \pi'$ is the required G-invariant complement to W. □

Remarks.

(1) We can explicitly compute π' and $\ker \pi'$ given (ρ, V) and W.

(2) Notice that we only use $\mathrm{char}\, k = 0$ when we invert $|G|$. So in fact we only need that the characteristic of k does not divide $|G|$.

(3) For any G-reps V, W, the map

$$\mathrm{Hom}(V, W) \to \mathrm{Hom}_G(V, W)$$

given by $\varphi \mapsto \frac{1}{|G|} \sum_{g\in G} g\varphi$ when the characteristic of k does not divide $|G|$ is a k-linear projection.

(4) In fact every irreducible representation of G is a submodule of the regular representation kG (see Ex Sheet 1 Q10 or the section on characters for a proof in characteristic zero).

An observation that we should have made earlier: if $\theta\colon H \to G$ is a group homomorphism then every representation $\rho\colon G \to GL(V)$ of G induces a representation $\rho\theta\colon H \to GL(V)$ of H.

If H is a subgroup of G and θ is inclusion we call this *restriction to H*.

3. Schur's Lemma

We've proven in characteristic zero that every representation V of a finite group G decomposed $V = \bigoplus V_i$ with V_i irreducible. We might ask how unique this is. Three possible hopes:

(1) (uniqueness of decomposition) For each V there is only one way to decompose $V = \bigoplus V_i$ with V_i irreducible (cf orbit decomposition for group actions on sets).

(2) (uniqueness of isotypical decomposition) For each V there exist unique subreps $W_1, \ldots, W_k$ st $V = \bigoplus W_i$ and if $V_i \leqslant W_i$ and $V_j' \leqslant W_j$ are irred. subreps then $V_i \cong V_j'$ if and only if $i = j$ (cf eigenspaces of a diagonalisable linear map).

(3) (uniqueness of factors) If $\bigoplus_{i=1}^k V_i \cong \bigoplus_{i=1}^{k'} V_i'$ with V_i, V_i' irreducible then $k = k'$ and there is $\sigma \in S_k$ such that $V'_{\sigma(i)} \cong V_i$ (cf dimensions of eigenspaces of a diagonalisable linear map).

Lecture 6

We ended last time asking whether the following might be true for a representation V of a finite group G over k of characteristic zero:

(1) (uniqueness of decomposition) For each V there is only one way to decompose $V = \bigoplus V_i$ with V_i irreducible (cf orbit decomposition for group actions on sets).
(2) (uniqueness of isotypical decomposition) For each V there exist unique subreps $W_1, \ldots, W_k$ st $V = \bigoplus W_i$ and if $V_i \leqslant W_i$ and $V_j' \leqslant W_j$ are irred. subreps then $V_i \cong V_j'$ if and only if $i = j$ (cf eigenspaces of a diagonalisable linear map).
(3) (uniqueness of factors) If $\bigoplus_{i=1}^k V_i \cong \bigoplus_{i=1}^{k'} V_i'$ with V_i, V_i' irreducible then $k = k'$ and there is $\sigma \in S_k$ such that $V'_{\sigma(i)} \cong V_i$ (cf dimensions of eigenspaces of a diagonalisable linear map).

Notice that (1) is clearly too strong. For example if G is the trivial group and $\dim V > 1$ then every line in V gives an irreducible subrep. This non-uniqueness is roughly measured in this case by $GL(V)$.

Notice also that (2) (and so (3)) is true for $\mathbb{Z}/2\mathbb{Z}$ — the W_i are the eigenspaces of $\rho(1)$.

Theorem (Schur's Lemma)**.** *Suppose that V and W are irreducible reps of G over k. Then*

(i) every element of $\mathrm{Hom}_G(V, W)$ is either 0 or an isomorphism,
(ii) if k is algebraically closed then $\dim_k \mathrm{Hom}_G(V, W)$ is either 0 or 1 .

In other words irreducible representations are rigid.

Proof. (i) Let φ be a non-zero G-linear map from V to W. Then $\ker\varphi$ is a G-invariant subspace of V. Thus $\ker\varphi = 0$, since it cannot be the whole of V. Similarly $\mathrm{im}\varphi$ is a subrep of W so $\mathrm{im}\varphi = W$ since it cannot be 0. Thus φ is both injective and surjective, so an isomorphism.

(ii) Suppose $\varphi_1, \varphi_2 \in \mathrm{Hom}_G(V, W)$ are non-zero. Then by (i) they are both isomorphisms. Consider $\varphi = \varphi_1^{-1}\varphi_2 \in \mathrm{Hom}_G(V, V)$. Since k is algebraically closed we may find λ an eigenvalue of φ then $\varphi - \lambda\,\mathrm{id}_V$ has non-trivial kernel and so is zero. Thus $\varphi_1^{-1}\varphi_2 = \lambda\,\mathrm{id}_V$ and $\varphi_2 = \lambda\varphi_1$ as required. □

Proposition. *If V, V_1 and V_2 are k-representations of G then*

$$\mathrm{Hom}_G(V, V_1 \oplus V_2) \cong \mathrm{Hom}_G(V, V_1) \oplus \mathrm{Hom}_G(V, V_2)$$

and

$$\mathrm{Hom}_G(V_1, \oplus V_2, V) \cong \mathrm{Hom}_G(V_1, V) \oplus \mathrm{Hom}_G(V_2, V).$$

Proof. Let $\pi_i \colon V_1 \oplus V_2 \to V_i$ be the G-linear projection onto V_i with kernel V_{3-i}. Then the map $\mathrm{Hom}_G(V, V_1 \oplus V_2) \to \mathrm{Hom}_G(V, V_1) \oplus \mathrm{Hom}_G(V, V_2)$ given by $\varphi \mapsto (\pi_1\varphi, \pi_2\varphi)$ has inverse $(\psi_1, \psi_2) \mapsto \psi_1 + \psi_2$.

Similarly the map $\mathrm{Hom}_G(V_1, \oplus V_2, V) \cong \mathrm{Hom}_G(V_1, V) \oplus \mathrm{Hom}_G(V_2, V)$ given by $\varphi \mapsto (\varphi|_{V_1}, \varphi|_{V_2})$ has inverse $(\psi_1, \psi_2) \mapsto \psi_1\pi_1 + \psi_2\pi_2$. □

Corollary. *Suppose k is algebraically closed and*

$$V \cong \bigoplus_{i=1}^{r} V_i$$

is a decomposition of a k-rep. of G into irreducible components.

Then for each irreducible representation W of G,

$$|\{i \mid V_i \cong W\}| = \dim \operatorname{Hom}_G(W, V).$$

Proof. By induction on r. If $r = 0, 1$ we're done.

If $r > 1$ consider V as $\left(\bigoplus_{i=1}^{r-1} V_i\right) \oplus V_r$. By the Proposition

$$\dim \operatorname{Hom}_G(W, \left(\bigoplus_{i=1}^{r-1} V_i\right) \oplus V_r) = \dim \operatorname{Hom}_G(W, \bigoplus_{i=1}^{r-1} V_i) + \dim \operatorname{Hom}_G(W, V_r).$$

Now the result follows by the induction hypothesis. □

Important question: How do we actually compute these numbers $\dim \operatorname{Hom}_G(V, W)$.

Corollary. *(of Schur's Lemma) If a finite group G has a faithful complex irreducible representation then the centre of G, $Z(G)$ is cyclic.*

Proof. Let V be a faithful complex irreducible rep of G, and let $z \in Z(G)$. Then let $\varphi_z : V \to V$ be defined by $\varphi_z(v) = zv$. Since $gz = zg$ for all $g \in G$, $\varphi_z \in \operatorname{Hom}_G(V, V) = \mathbb{C}\,\mathrm{id}_V$ by Schur, $\varphi_z = \lambda_z \,\mathrm{id}_V$, say.

Now $Z(G) \to \mathbb{C}; z \mapsto \lambda_z$ is a representation of $Z(G)$ that must be faithful since V is faithful. In particular $Z(G)$ is isomorphic to a finite subgroup of $\mathbb{C}^\times$. But every such subgroup is cyclic. □

Corollary. *(of Schur's Lemma) Every irreducible complex representation of a finite abelian group G is one-dimensional.*

Proof. Let (ρ, V) be a complex irred. rep of G. For each $g \in G$, $\rho(g) \in \operatorname{Hom}_G(V, V)$. So by Schur, $\rho(g) = \lambda_g \,\mathrm{id}_V$ for some $\lambda_g \in \mathbb{C}$. Thus for $v \in V$ non-zero, $\langle v \rangle$ is a subrep of V. □

Corollary. *Every finite abelian group G has precisely $|G|$ complex irreducible representations.*

Proof. Let ρ be an irred. complex rep of G. By the last corollary, $\dim \rho = 1$. So $\rho : G \to \mathbb{C}^\times$ is a group homomorphism.

Since G is a finite abelian group $G \cong C_{n_1} \times \cdots \times C_{n_k}$ some $n_1, \ldots, n_k$. Now if $G = G_1 \times G_2$ is the direct product of two groups then there is a 1-1 correspondance between the set of group homomorphisms $G \to \mathbb{C}^\times$ and the of pairs $(G_1 \to \mathbb{C}^\times, G_2 \to \mathbb{C}^\times)$ given by restriction $\varphi \mapsto (\varphi|_{G_1}, \varphi|_{G_2})$. Thus we may reduce to the case $G = C_n = \langle x \rangle$ is cyclic.

Now ρ is determined by $\rho(x)$ and $\rho(x)^n = 1$ so $\rho(x)$ must be an nth root of unity. Moreover we may choose $\rho(x)$ however we like amongst the nth roots of 1. □

Examples.

$G = C_4 = \langle x \rangle$.

	1	x	x^2	x^3
ρ_1	1	1	1	1
ρ_2	1	i	-1	$-i$
ρ_3	1	-1	1	1
ρ_4	1	$-i$	-1	i

$G = C_2 \times C_2 = \langle x, y \rangle$.

	1	x	y	xy
ρ_1	1	1	1	1
ρ_2	1	-1	1	-1
ρ_3	1	1	-1	-1
ρ_4	1	-1	-1	1

Note there is no natural correspondence between elements of G and representations ρ.

Note too that the rows of these matrices are orthogonal with respect to the standard Hermitian inner product: $\langle v, w \rangle = \sum \overline{v_i} w_i$.

Lemma. *If (ρ_1, V_1) and (ρ_2, V_2) are non-isomorphic one-dimensional representations of a finite group G then $\sum_{g \in G} \overline{\rho_1(g)} \rho_2(g) = 0$*

Proof. We've seen that $\mathrm{Hom}_k(V_1, V_2)$ is a G-rep under $g\varphi(v) = \rho_2(g)\varphi\rho_1(g^{-1})$ and $\sum_{g \in G} g\varphi \in \mathrm{Hom}_G(V_1, V_2) = 0$ by Schur. Since $\rho_1(g)$ is always a root of unity, $\rho_1(g^{-1}) = \overline{\rho_1(g)}$. Pick an isomorphism $\varphi \in \mathrm{Hom}_k(V_1, V_2)$. Then $0 = \sum_{g \in G} \rho_2(g)\varphi\rho_1(g^{-1}) = \sum_{g \in G} \overline{\rho_1(g)}\rho_2(g)\varphi$ as required. □

Lecture 7

Last time we finished by proving the following:

Lemma. *If (ρ_1, V_1) and (ρ_2, V_2) are non-isomorphic one-dimensional representations of a finite group G then $\sum_{g \in G} \overline{\rho_1(g)} \rho_2(g) = 0$*

Corollary. *Suppose G is a finite abelian group then every complex representation V of G has a unique isotypical decomposition.*

Proof. For each homomorphism $\theta_i \colon G \to \mathbb{C}^\times$ $(i = 1, \ldots, |G|)$ we can define W_i to be the subspace of V defined by

$$W_i = \{v \in V \mid \rho(g)v = \theta_i(g)v \text{ for all } g \in G\}.$$

Since V is completely reducible and every irreducible rep of G is one dimensional $V = \sum W_i$. We need to show that for each i $W_i \cap \sum_{j \neq i} W_j = 0$. It is equivalent to show that $\sum w_i = 0$ with $w_i \in W_i$ implies $w_i = 0$ for all i.

But $\sum w_i = 0$ with w_i in W_i certainly implies $0 = \rho(g) \sum w_i = \sum \theta_i(g) w_i$. By choosing an ordering $g_1, \ldots, g_{|G|}$ of G we see that the $|G| \times |G|$ matrix $\theta_i(g_j)$ is invertible by the lemma. Thus $w_i = 0$ for all i as required. □

Summary so far. We want to classify all representations of groups G. We've seen that if G is finite and k has characteristic zero then every representation V decomposes as $V \cong \bigoplus n_i V_i$ with V_i irreducible and $n_i \geqslant 0$. Moreover if k is also algebraically closed, we've seen that $n_i = \dim \mathrm{Hom}_G(V_i, V)$.

Our next goals arre to classify all irreducible representations of a finite group and understand how to compute the n_i given V. We're going to do this using character theory.

4. Characters

4.1. **Definitions.** We'll now always assume $k = \mathbb{C}$ although almost always a field of characteristic zero containing all nth roots of unity would suffice. We'll also assume that G is finite.

Definition. Given a representation $\rho\colon G \to GL(V)$, the *character* of ρ is the function $\chi = \chi_\rho = \chi_V : G \to k$ given by $g \mapsto \operatorname{tr}\rho(g)$.

Since for matrices $\operatorname{tr}(AB) = \operatorname{tr}(BA)$, the character does not depend on the choice of basis for V $[\operatorname{tr}(X^{-1}AX) = \operatorname{tr}(AXX^{-1}) = \operatorname{tr}(A)]$. By the same argument we also see that equivalent reps have the same character.

Example. Let $G = D_6 = \langle s, t \mid s^2 = 1, t^3 = 1, sts^{-1} = t^{-1}\rangle$, the dihedral group of order 6. This acts on $\mathbb{R}^2$ by symmetries of the triangle; with t acting by rotation by $2\pi/3$ and s acting by a reflection. To compute the character of this rep we just need to know the eigenvalues of the action of each element. Each reflection (element of the form st^i) will act by a matrix with eigenvalues ± 1. Thus $\chi(st^i) = 0$ for all i. The rotations t^r act by matrices $\begin{pmatrix} \cos 2\pi r/3 & -\sin 2\pi r/3 \\ \sin 2\pi r/3 & \cos 2\pi r/3 \end{pmatrix}$ thus $\chi(t^r) = 2\cos 2\pi r/3 = -1$ for $r = 1, 2$.

Proposition. *Let (ρ, V) be a complex rep of G with character χ*

(i) $\chi(e) = \dim V$;
(ii) $\chi(g) = \chi(hgh^{-1})$ *for all* $g, h \in G$;
(iii) $\chi(g^{-1}) = \overline{\chi(g)}$;
(iv) *If χ' is the character of (ρ', V') then $\chi + \chi'$ is the character of $V \oplus V'$.*

Proof.
(i) $\chi(e) = \operatorname{tr}\operatorname{id}_V = \dim V$.
(ii) $\rho(hgh^{-1}) = \rho(h)\rho(g)\rho(h)^{-1}$. Thus $\rho(hgh^{-1})$ and $\rho(g)$ are conjugate and so have the same trace.
(iii) if $\rho(g)$ has eigenvalues $\lambda_1, \ldots, \lambda_n$ (with multiplicity) then $\chi(g) = \sum \lambda_i$. But as $o(g)$ is finite each λ_i must be a root of unity. Thus $\overline{\chi(g)} = \sum \overline{\lambda_i} = \sum \lambda_i^{-1}$ but of course the λ_i^{-1} are the eigenvalues of g^{-1}.
(iv) is clear. □

The proposition tells us that the character of ρ contains very little data; just a complex number for each conjugacy class in G. The extraordinary thing that we will see is that it contains all we need to know to reconstruct ρ up to isomorphism.

Definition. We say a function $f\colon G \to \mathbb{C}$ is a *class function* if $f(hgh^{-1}) = f(g)$ for all $g, h \in G$. We'll write $\mathcal{C}_G$ for the complex vector space of class functions on G.

Notice that if $\mathcal{O}_1, \ldots, \mathcal{O}_r$ is a list of the conjugacy classes of G then the 'delta functions' $\delta_{\mathcal{O}_i}\colon G \to \mathbb{C}$ given by $y \mapsto 1$ if $y \in \mathcal{O}_i$ and $y \mapsto 0$ otherwise form a basis for $\mathcal{C}_G$. In particular $\dim \mathcal{C}_G$ is the number of conjugacy classes in G.

Example. $G = D_6 = \langle s, t \mid s^2 = t^3 = e, sts = t^{-1}\rangle$ has conjugacy classes $\{e\}, \{t, t^{-1}\}, \{s, st, st^2\}$.

We make $\mathcal{C}_G$ into a Hermitian inner product space by defining

$$\langle f, f'\rangle = \frac{1}{|G|}\sum \overline{f(g)} f'(g).$$

It is easy to check that this does define an Hermitian inner product and that the functions $\delta_{\mathcal{O}_i}$ are pairwise orthogonal. Notice that $\langle \delta_{\mathcal{O}_i}, \delta_{\mathcal{O}_i}\rangle = \frac{|\mathcal{O}_i|}{|G|} = \frac{1}{|\mathcal{C}_G(x_i)|}$ for any $x_i \in \mathcal{O}_i$.

Thus if $x_1, \ldots, x_r$ are conjugacy class representatives, then we can write

$$\langle f, f'\rangle = \sum_{i=1}^{r} \frac{1}{|C_G(x_i)|}\overline{f(x_i)}f'(x_i).$$

Example. $G = D_6$ as above, then $\langle f, f'\rangle = \frac{1}{6}\overline{f(e)}f'(e) + \frac{1}{2}\overline{f(s)}f'(s) + \frac{1}{3}\overline{f(t)}f'(t)$.

4.2. **Orthogonality of characters.**

Theorem (Orthogonality of characters)**.** *If V and V' are complex irreducible representations of a finite group G then $\langle \chi_V, \chi_{V'}\rangle$ is 1 if $V \cong V'$ and 0 otherwise.*

Notice that this theorem tells us that the characters of irreducible reps form part of an orthonormal basis for $\mathcal{C}_G$. In particular the number of irreducible representations is bounded above by the number of conjugacy classes of G. In fact we'll see that the characters span the space of class functions and so that the number of irreps is precisely the number of conjugacy classes in G. We saw this when G is abelian last time.

Lemma. *If V and W are reps of a finite group G then*

$$\chi_{\mathrm{Hom}_k(V,W)}(g) = \overline{\chi_V(g)}\chi_W(g)$$

for each $g \in G$.

Proof. Given $g \in G$ we may choose bases $v_1, \ldots, v_n$ for V and $w_1, \ldots, w_m$ for W such that $gv_i = \lambda_i v_i$ and $gw_j = \mu_j w_j$. Then the functions $f_{ij}(v_k) = \partial_{ik} w_j$ extend to linear maps that form a basis for $\mathrm{Hom}(V, W)$ and $(g.f_{ij})(v_i) = \lambda_i^{-1}\mu_j w_j$ thus $gf_{ij} = \lambda_i^{-1}\mu_j f_{ij}$ and $\chi_{\mathrm{Hom}(V,W)}(g) = \sum_{i,j} \lambda_i^{-1}\mu_j = \chi_V(g^{-1})\chi_W(g) = \overline{\chi_V(g)}\chi_W(g)$. □

Lemma. *If U is a rep of G then*

$$\dim\{u \in U \mid gu = u\ \forall g \in G\} = \langle 1, \chi_U\rangle = \frac{1}{|G|}\sum_{g\in G}\chi_U(g).$$

Proof. Define $\pi\colon U \to U$ by $\pi(u) = \frac{1}{|G|}\sum_{g\in G} gu$, and $U^G := \{u \in U \mid gu = u\}$. Then $h\pi(u) = \pi(u)$ for all $u \in U$ so $\pi(u) \in U^G$ for all $u \in U$. Moreover $\pi_{U^G} = \mathrm{id}_{U^G}$ by direct calculation. Thus

$$\dim U^G = \operatorname{tr}\mathrm{id}_{U^G} = \operatorname{tr}\pi = \frac{1}{|G|}\sum_{g\in G}\chi_U(g)$$

as required. □

Lecture 8

Recall,

Lemma. *If V, W are reps of a finite group G then $\chi_{\mathrm{Hom}_k(V,W)} = \overline{\chi_V}\chi_W$.*

Lemma. *If U is a rep of a finite group G then*

$$\dim\{u \in U \mid gu = g\ \forall g \in G\} = \langle \mathbf{1}, \chi_U\rangle.$$

We can use these two lemmas to prove

Proposition. *If V and W are representations of G then*

$$\dim \operatorname{Hom}_G(V,W) = \langle \chi_V, \chi_W \rangle.$$

Proof. By the lemmas $\dim \operatorname{Hom}_G(V,W) = \langle \mathbf{1}, \overline{\chi_V}\chi_W \rangle$. But it is easy to see that $\langle \mathbf{1}, \overline{\chi_V}\chi_W \rangle = \langle \chi_V, \chi_W \rangle$ as required. □

Corollary (Orthogonality of characters)**.** *If χ, χ' are characters of irreducible reps then $\langle \chi, \chi' \rangle = \delta_{\chi,\chi'}$.*

Proof. Apply the Proposition and Schur's Lemma □

Suppose now that $V_1, \ldots, V_k$ is the list of all irreducible complex reps of G up to isomorphism and the corresponding characters are $\chi_1, \ldots, \chi_k$. Then Maschke's Theorem tells us that any representation V may be written as a direct sum of copies of the V_i, $V \cong \bigoplus n_i V_i$. Thus $\chi = \sum n_i \chi_i$.

As the χ_i are orthonormal we may compute $\langle \chi, \chi_i \rangle = n_i$. This is another proof that the decomposition factors of V are determined by their composition factors. However we get more: the composition factors of V can be computed purely from its character; that is if we have a record of each of the irreducible characters, then we now have a practical way of calculating how a given representation breaks up as a direct sum of its irreducible components. Our main goal now is to investigate how we might produce such a record of the irreducible characters.

Corollary. *If ρ and ρ' are reps of G then they are isomorphic if and only if they have the same character.*

Proof. We have already seen that isomorphic reps have the same character. Suppose that ρ and ρ' have the same character χ. Then they are each isomorphic to $\langle \chi_1, \chi \rangle \rho_1 \oplus \cdots \oplus \langle \chi_k, \chi \rangle \rho_k$ and thus to each other. □

Notice that complete irreducibility was a key part of the proof of this corollary, as well as orthogonality of characters. For example the two reps of $\mathbb{Z}$ given by $1 \mapsto id_{\mathbb{C}^2}$ and $1 \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ are not isomorphic but have the same trace. Complete irreducibility tells us we don't need to worry about gluing.

Corollary. *If ρ is a complex representation of G with character χ then ρ is irreducible if and only if $\langle \chi, \chi \rangle = 1$.*

Proof. One direction follows immediately from the theorem on orthogonality of characters. For the other direction, assume that $\langle \chi, \chi \rangle = 1$. Then we may write $\chi = \sum n_i \chi_i$ for some non-negative integers n_i. By orthogonality of characters $1 = \langle \chi, \chi \rangle = \sum n_i^2$. Thus $\chi = \chi_j$ for some j, and χ is irreducible. □

This is a good way of calcuating whether a representation is irreducible.

Examples.

(1) Consider the action of S_3 on $\mathbb{C}^2$ by extending the symmetries of a triangle. $\chi(1) = 2$, $\chi(12) = \chi(23) = \chi(13) = 0$, and $\chi(123) = \chi(132) = -1$. Now

$$\langle \chi, \chi \rangle = \frac{1}{6}(2^2 + 3 \cdot 0^2 + 2 \cdot (-1)^2) = 1$$

so this rep is irreducible.

(2) Consider the action of S_4 on $\mathbb{C}X$ for $X = \{1, 2, 3, 4\}$ induced from the natural action of S_4 on X. The conjugacy classes in S_4 are 1 of size 1, (ab) of size $\binom{4}{2} = 6$, (abc) of size $4.2 = 8$, $(ab)(cd)$ of size 3 and $(abcd)$ of size 6.

We can compute that the character of this rep is given by

$$\chi(g) = \#\{\text{fixed points of } g\}.$$

So $\chi(1) = 1$, $\chi((ab)) = 2$, $\chi((abc)) = 1$ and $\chi((ab)(cd) = \chi(abcd) = 0$. Thus $\langle\chi, \chi\rangle = 1/24(4^2+6\cdot2^2+8\cdot1^2+3\cdot0^2) = 2$. Thus if we decompose $\chi = \sum n_i\chi_i$ into irreducibles we know $\sum n_i^2 = 2$ then we must have $\chi = \chi' + \chi''$ with χ' and χ'' non-isomorphic irreps.

Notice that $\langle\mathbf{1}, \chi\rangle = 1/24(4+6\cdot2+8\cdot1+0) = 1$ so one of the irreducible constituents is the trivial rep. The other has character $\chi - \mathbf{1}$.

In fact we have seen these subreps explicitly in this case. The constant functions gives a trivial subrep and the orthogonal complement with respect to the standard inner product (that is the set of functions that sum to zero) gives the other.

Theorem (The character table is square)**.** *The irreducible characters of a finite group G form a basis for the space of class functions $\mathcal{C}_G$ on G.*

Proof. We already know that the irreducible characters are linearly independent (and orthonormal) we need to show that they span $\mathcal{C}_G$. Let $I = \langle\chi_1, \dots, \chi_r\rangle$ be the span of the irred. characters. We need to show that $I^\perp = 0$.

Suppose $f \in \mathcal{C}_G$. For each representation (ρ, V) of G we may define $\varphi \in \operatorname{Hom}(V, V)$ by $\varphi = \frac{1}{|G|}\sum_{g\in G}\overline{f(g)}\rho(g)$.

Now,

$$\rho(h)^{-1}\varphi\rho(h) = \frac{1}{|G|}\sum_{g\in G}\overline{f(g)}\rho(h^{-1}gh) = \frac{1}{|G|}\sum_{g'\in G}\overline{f(g')}\rho(g')$$

since f is a class function, and we see that in fact $\varphi \in \operatorname{Hom}_G(V, V)$. Moreover, if $f \in I^\perp$, then

$$\operatorname{tr}\varphi = \langle f, \operatorname{tr}\rho\rangle = 0.$$

Now if V is an irreducible representation then Schur's Lemma tells us that $\varphi = \lambda\operatorname{id}_V$ for some $\lambda \in \mathbb{C}$. Since $\operatorname{tr}\varphi = 0$ it follows that $\lambda = 0$ and so $\varphi = 0$.

But every representation breaks up as a direct sum of irreducible representations $V = \bigoplus V_i$ and φ breaks up as $\bigoplus\varphi_i$. So $\varphi = 0$ always.

But if we take V to be the regular representation $\mathbb{C}G$ then $\varphi\partial_e = |G|^{-1}\sum_{g\in G}\overline{f(g)}\partial_g = \overline{f}$. Thus $f = 0$. □

Corollary. *The number of irreducible representations is the number of conjugacy classes in the group.*

Corollary. *For each $g \in G$, $\chi(g)$ is real for every character χ if and only if g is conjugate to g^{-1}.*

Proof. Since $\chi(g^{-1}) = \overline{\chi(g)}$, $\chi(g)$ is real for every character χ if and only if $\chi(g) = \chi(g^{-1})$ for every character χ. Since the irreducible characters span the space of class functions this is equivalent to g and g^{-1} living in the same conjugacy class. □

4.3. **Character tables.** We now want to classify all the irreducible representations of a given finite group and we know that it suffices to write down the characters of each one.

The character table of a group is defined as follows: we list the conjugacy classes of G, $\mathcal{O}_1, \ldots, \mathcal{O}_k$ (by convention always $\mathcal{O}_1 = \{e\}$) and choose $g_i \in \mathcal{O}_i$ we then list the irreducible characters $\chi_1, \ldots, \chi_k$ (by convention $\chi_1 = \chi_{\mathbb{C}}$ the character of the trivial rep. Then we write the matrix

$$\begin{array}{c|cccccc} & e & g_2 & \cdots & g_i & \cdots & g_k \\ \hline \chi_1 & 1 & 1 & \cdots & 1 & \cdots & 1 \\ \vdots & & & & \vdots & & \\ \chi_j & \cdots & \cdots & \cdots & \chi_j(g_i) & \cdots & \cdots \\ \vdots & & & & \vdots & & \\ \chi_k & & & & \vdots & & \end{array}$$

Examples.

(1) $C_3 = \langle x \rangle$

$$\begin{array}{c|ccc} & e & x & x^2 \\ \hline \chi_1 & 1 & 1 & 1 \\ \chi_2 & 1 & \omega & \omega^2 \\ \chi_3 & 1 & \omega^2 & \omega \end{array}$$

Notice that the rows are indeed orthogonal. The columns are too in this case.

(2) S_3

There are three conjugacy classes: the identity is in a class on its own $\mathcal{O}_1$; the three transpositions live in a another class $\mathcal{O}_2$; and the two 3-cycles live in the third class $\mathcal{O}_3$.

There are three irreducible representations all together. We know that the trivial representation $\mathbf{1}$ has character $\mathbf{1}(g) = 1$ for all $g \in G$. We also know another 1-dimensional representation $\epsilon \colon S_3 \to \{\pm 1\}$ given by $g \mapsto 1$ if g is even and $g \mapsto -1$ if g is odd.

To compute the character χ of the last representation we may use orthogonality of characters. Let $\chi(e) = a$, $\chi((12)) = b$ and $\chi((123)) = c$ (a, b and c are each real since each g is conjugate to its inverse). We know that $0 = \langle \mathbf{1}, \chi \rangle = \frac{1}{6}(a + 3b + 2c)$, $0 = \langle \epsilon, \chi \rangle = \frac{1}{6}(a - 3b + 2c)$, and $1 = \langle \chi, \chi \rangle = \frac{1}{6}(a^2 + 3b^2 + 2c^2)$. Thus we see quickly that $b = 0$, $a + 2c = 0$ and $a^2 + 2c^2 = 0$. We also know that a is a positive integer. Thus $a = 2$ and $c = -1$.

$$\begin{array}{c|ccc} & 1 & 3 & 2 \\ & e & (12) & (123) \\ \hline \mathbf{1} & 1 & 1 & 1 \\ \epsilon & 1 & -1 & 1 \\ \chi & 2 & 0 & -1 \end{array}$$

In fact we already knew about this 2-dimensional representation; it is the one coming from the symmetries of a triangle inside $\mathbb{R}^2$.

Lecture 9

Recall the character table of S_3.

Example. S_3

	1	3	2
	e	(12)	(123)
1	1	1	1
ϵ	1	-1	1
χ	2	0	-1

The rows are orthogonal under $\langle f, f' \rangle = \sum_1^3 \frac{1}{|C_G(g_i)|}\overline{f(g_i)}f'(g_i)$.

But the columns are also orthogonal with respect to the standard inner product. If we compute their length we get:

$$1^2 + 1^2 + 2^2 = 6 = |S_3|$$
$$1^2 + (-1)^2 + 0^2 = 2 = |C_{S_3}((12))|$$
$$1^2 + 1^2 + (-1)^2 = 3 = |C_{S_3}((123))|.$$

Proposition (Column Orthogonality)**.** *If G is a finite group and $\chi_1, \ldots, \chi_r$ is a complete list of the irreducible characters of G then for each $g, h \in G$,*

$$\sum_{i=1}^r \overline{\chi_i(g)}\chi_i(h) = \begin{cases} 0 & \text{if } g \text{ and } h \text{ are not conjugate in } G \\ |C_G(g)| & \text{if } g \text{ and } h \text{ are conjugate in } G. \end{cases}$$

In particular $\sum_{i=1}^r \dim V_i^2 = |G|$.

Proof of Proposition. Let X be character table thought of as a matrix; $X_{ij} = \chi_i(g_j)$ and let D be the diagonal matrix whose diagonal entries are $|C_G(g_i)|$

Orthogonality of characters tell us that

$$\sum_k |C_G(g_k)|^{-1}\overline{X_{ik}}X_{jk} = \partial_{ij}$$

ie $\overline{X}D^{-1}X^t = I$.

Since X is square we may write this as $D^{-1}\overline{X}^t = X^{-1}$. Thus $\overline{X}^t X = D$. That is $\sum_k \overline{\chi_k(g_i)}\chi_k(g_j) = \partial_{ij}|C_G(g_i)|$ as required. □

Examples.
$G = S_4$

$\lvert C_G(x_i)\rvert$	24	8	3	4	4
$\lvert[x_i]\rvert$	1	3	8	6	6
	e	$(12)(34)$	(123)	(12)	(1234)
1	1	1	1	1	1
ϵ	1	1	1	-1	-1
χ_3	3	-1	0	1	-1
$\epsilon\chi_3$	3	-1	0	-1	1
χ_5	2	2	-1	0	0

The trivial **1** and sign ϵ characters may be constructed in the same way as for S_3. We calculated last time that the natural permuation character breaks up as the sum of a trivial character and a character whose values $\chi_3(g)$ are the number of fixed points of g minus 1.

We saw on Example Sheet 1 (Q2) that given a 1-dimensional represntation θ and an irreducible representation ρ we may form another irreducible representation $\theta \otimes \rho$ by $\theta \otimes \rho(g) = \theta(g)\rho(g)$. It is not hard to see that $\chi_{\theta\otimes\rho}(g) = \theta(g)\chi_\rho(g)$. Thus we get another irreducible character $\epsilon\chi_3$.

We can then complete the character table using column orthogonality: We note that $24 = 1^2 + 1^2 + 3^2 + 3^2 + \chi_5(e)^2$ thus $\chi_5(e) = 2$. Then using $\sum_1^5 \chi_i(1)\chi_i(g) = 0$ we can construct the remaining values in the table.

Notice that the two dimensional representation corresponding to χ_5 may be obtained by composing the surjective group homomorphism $S_4 \to S_3$ (with kernel the Klein-4-group) with the irreducible two dimension rep of S_3.
$G = A_4$. Each irreducible representation of S_4 may be restricted to A_4 and its character values on elements of A_4 will be unchanged. In this way we get three characters of A_4, $\mathbf{1}$, $\psi_2 = \chi_3|_{A_4}$ and $\psi_3 = \chi_5|_{A_4}$. If we compute $\langle \mathbf{1}, \mathbf{1}\rangle$ we of course get 1. If we compute $\langle \psi_2, \psi_2\rangle$ we get $\frac{1}{12}(3^2 + 3(-1)^2 + 8(0^2)) = 1$ so ψ_2 remains irreducible. However $\langle \psi_3, \psi_3\rangle = \frac{1}{12}(2^2 + 3(2^2) + 8(-1)^2) = 2$ so ψ_3 breaks up into two non-isomorphic irreducible reps of A_4.

Exercise. Use this infomation to construct the whole character table of A_4.

4.4. **Permuation representations.** Suppose that X is a finite set with a G-action. Recall that $\mathbb{C}X = \{f\colon X \to \mathbb{C}\}$ is a representation of G via $gf(x) = f(g^{-1}x)$.

Lemma. *If χ is the character of $\mathbb{C}X$ then $\chi(g) = |\{x \in X \mid gx = x\}|$.*

Proof. If $X = \{x_1, \ldots, x_d\}$ and $gx_i = x_j$ then $g\partial_{x_i} = \partial_{x_j}$ so the ith column of g has a 1 in the jth entry and zeros elsewhere. So it contributes 1 to the trace precisely if $x_i = x_j$. □

Corollary. *If $V_1, \ldots, V_k$ is a complete list of irreducible reps of a finite group G then the regular representation decomposes as $\mathbb{C}G \cong n_1V_1 \oplus \cdots \oplus n_kV_k$ with $n_i = \dim V_i = \chi_i(e)$. In particular $|G| = \sum(\dim V_i)^2$.*

Proof. $\chi_{\mathbb{C}G}(e) = |G|$ and $\chi_{kG}(g) = 0$ for $g \neq e$. Thus if we decompose kG we obtain
$$n_i = \langle \chi_{\mathbb{C}G}, \chi_i\rangle = \frac{1}{|G|}|G|\chi_i(e) = \chi_i(e)$$
as required. □

Proposition (Burnside's Lemma)**.** *Let G be a finite group and X a finite set with a G-action and χ the character of $\mathbb{C}X$. Then $\langle \mathbf{1}, \chi\rangle$ is the number of orbits of G on X.*

Proof. If we decompose X into a disjoint of orbits $X_1 \cup \cdots \cup X_k$ then we've seen that $\mathbb{C}X = \bigoplus_{i=1}^k \mathbb{C}X_i$. So $\chi_X = \sum_{i=1}^k \chi_{X_i}$ and we may reduce to the case that G-acts transitively on X.

Now
$$\begin{aligned} |G|\langle \chi_X, 1\rangle &= \sum_{g\in G} \chi_X(g) = \sum_{g\in G} |\{x \in X \mid gx = x\} \\ &= |\{(g,x) \in G \times X \mid gx = x\}| = \sum_{x\in X} |\{g \in G \mid gx = x\} \\ &= \sum_{x\in X} |\operatorname{Stab}_G(x)| = |X||\operatorname{Stab}_G(X)| = |G| \end{aligned}$$

as required. □

If X is a set with a G-action we may view $X \times X$ as a set with a G-action via $(g,(x,y)) \mapsto (gx,gy)$.

Corollary. *If G is a finite group and X is a finite set with a G-action and χ is the character of the permutation representation $\mathbb{C}X$ then $\langle \chi, \chi \rangle$ is the number of G-orbits on $X \times X$.*

Proof. Notice that (x,y) is fixed by $g \in G$ if and only if both x and y are fixed. Thus $\chi_{X\times X}(g) = \chi_X(g)\chi_X(g)$ by the lemma.

Now $\langle \chi_X, \chi_X \rangle = \frac{1}{|G|}\sum_{g\in G} \chi_X(g)\chi_X(g) = \langle \mathbf{1}, \chi_{X\times X} \rangle$ and the result follows from Burnside's Lemma. $\square$

Remark. If X is any set with a G-action with $|X| > 1$ then $\{(x,x) | x \in X\} \subset X \times X$ is G-stable and so is the complement $\{(x,y) \in X \times X \mid x \neq y\}$.

We say that G acts 2-*transitively* on X if G has only two orbits on $X \times X$. Given a 2-transitive action of G on X we've seen that the character χ of the permutation representation satisfies $\langle \chi, \chi \rangle = 2$ and $\langle \mathbf{1}, \chi \rangle = 1$. Thus $\mathbb{C}X$ has two irreducible summands — the constant functions and the functions f such that $\sum_{x\in X} f(x) = 0$.

Exercise. If $G = GL_2(\mathbb{F}_p)$ then decompose the permutation rep of G coming from the action of G on $\mathbb{F}_p \cup \{\infty\}$ by Mobius transformations.

Lecture 10

5. The character ring

Given a finite group G, the set of class functions $\mathcal{C}_G$ comes equipped with certain algebraic structures: it is a commutative ring under pointwise addition and multiplication — ie $(f_1+f_2)(g) = f_1(g)+f_2(g)$ and $f_1 f_2(g) = f_1(g) f_2(g)$ for each $g \in G$, the additive identity is the constant function value 0 and the multiplicative identity constant value 1; there is a ring automorphism $*$ of order two given by $f^*(g) = f(g^{-1})$; and there is an inner product given by $\langle f_1, f_2 \rangle = \frac{1}{|G|}\sum_{g\in G} f_1^*(g) f_2(g)$.

We will see that all this structure is related to structure on the category of representations: we have already seen some of this. If V_1 and V_2 are representations with characters χ_1 and χ_2 then $\chi_1 + \chi_2 = \chi_{V_1 \oplus V_2}$ and $\langle \chi_1, \chi_2 \rangle = \dim \mathrm{Hom}_G(V_1, V_2)$.

Definition. The *character ring* $R(G)$ of a group G is defined by

$$R(G) := \{\chi_1 - \chi_2 \mid \chi_1, \chi_2 \text{ are characters of reps of } G\} \subset \mathcal{C}_G.$$

We'll see that the character ring inherits all the algebraic structure of $\mathcal{C}_G$ mentioned above.

5.1. Duality.

Recall,

Definition. If G is group and (ρ, V) is a representation of G then the *dual representation* (ρ^*, V^*) of G is given by $(\rho^*(g)\theta)(v) = \theta(\rho(g^{-1})v)$ for $\theta \in V^*$, $g \in G$ and $v \in V$.

Lemma. $\chi_{V^*} = \chi^*(V)$.

Proof. This is a special case of our earlier computation $\chi_{\mathrm{Hom}_k(V,W)} = \overline{\chi_V}\chi_W$ with W the trivial representation. $\square$

Definition. We say that V is *self-dual* if $V \cong V^*$ as representations of G.

Over $\mathbb{C}$, V is self-dual if and only if $\chi_V(g) \in \mathbb{R}$ for all $g \in G$.

Examples.

(1) $G = C_3 = \langle x \rangle$ and $V = \mathbb{C}$. Ifρ is given by $\rho(x) = \omega = e^{\frac{2\pi i}{3}}$ then $\rho^*(x) = \omega^2 = \overline{\omega}$ so V is not self-dual
(2) $G = S_n$: since g is always conjugate to its inverse in S_n, $\chi^* = \chi$ always and so every representation is self-dual.
(3) Permuatation representations $\mathbb{C}X$ are always self-dual.

5.2. **Tensor products.** Suppose that V and W are vector spaces over a field k, with bases $v_1, \ldots, v_m$ and $w_1, \ldots, w_n$ respectively. We may view $V \oplus W$ either as the vector space with basis $v_1, \ldots, v_m, w_1, \ldots, w_n$ (so $\dim V \oplus W = \dim V + \dim W$) or more abstractly as the vector space of pairs (v, w) with $v \in V$ and $w \in W$ and pointwise operations.

Example. If X and Y are sets then $kX \otimes kY$ has basis $\partial_x \otimes \partial_y$ for $x \in X$ and $y \in Y$. Identifying this element with the function $\partial_{x,y}$ on $X \times Y$ given by $\partial_{x,y}(x', y') = \partial_{xx'}\partial_{yy'} = \partial_x(x')\partial_y(y')$.

Definition. The *tensor product* $V \otimes W$ of V and W is the vector space with basis given by symobls $v_i \otimes w_j$ for $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant n$ and so

$$\dim V \otimes W = \dim V \cdot \dim W.$$

Notice that now $kX \otimes kY$ is isomorphic to $kX \times Y$ under $\partial_x \otimes \partial_y \mapsto \partial_{x,y}$.

If $v = \sum \lambda_i v_i \in V$ and $w = \sum \mu_j w_j \in W$, it is common to write $v \otimes w$ for the element $\sum_{i,j} (\lambda_i \mu_j) v_i \otimes w_j \in V \otimes W$. But note that usually not every element of $V \otimes W$ may be written in the form $v \otimes w$ (eg $v_1 \otimes w_1 + v_2 \otimes w_2$).

Lemma. *There is a bilinear map $V \times W \to V \otimes W$ given by $(v, w) \mapsto v \otimes w$.*

Proof. First, we should prove that if $x, x_1, x_2 \in V$ and $y, y_1, y_2 \in W$ then

$$x \otimes (y_1 + y_2) = x \otimes y_1 + x \otimes y_2$$

and

$$(x_1 + x_2) \otimes y = x_1 \otimes y + x_2 \otimes y.$$

We'll just do the first; the second is symmetric.

Write $x = \sum_i \lambda_i v_i$, $y_k = \sum_j \mu_j^k w_j$ for $k = 1, 2$. Then

$$x \otimes (y_1 + y_2) = \sum_{i,j} \lambda_i (\mu_j^1 + \mu_j^2) v_i \otimes w_j$$

and

$$x \otimes y_1 + x \otimes y_2 = \sum_{i,j} \lambda_i \mu_j^1 v_i \otimes w_j + \sum_{i,j} \lambda_i \mu_j^2 v_i \otimes w_j.$$

These are equal.

We should also prove that for $\lambda \in k$ and $v \in V$ and $w \in W$ then

$$(\lambda v) \otimes w = \lambda (v \otimes w) = v \otimes (\lambda w).$$

The proof is similar to the above. □

Exercise. Show that given vector spaces U, V and W there is a $1-1$ correspondence between

$$\{\text{linear maps } V \otimes W \to U\} \leftrightarrow \{\text{bilinear maps } V \times W \to U\}$$

given by composition with the bilinear map $(v, w) \to v \otimes w$ above.

Lemma. *If $x_1, \dots, x_m$ is any basis of V and $y_1, \dots, y_m$ is any basis of W then $x_i \otimes y_j$ for $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant n$ is a basis for $V \otimes W$. Thus the definition of $V \otimes W$ does not depend on the choice of bases.*

Proof. It suffices to prove that the set $\{x_i \otimes y_j\}$ spans $V \otimes W$ since it has size mn. But if $v_i = \sum_r A_{ri} x_r$ and $w_j = \sum_s B_{sj} y_s$ then $v_i \otimes w_j = \sum_{r,s} A_{ri} B_{sj} x_r \otimes y_s$. □

Remark. In fact we could have defined $V \otimes W$ in a basis independent way in the first place: let F be the (infinite dimensional) vector space with basis $v \otimes w$ for every $v \in V$ and $w \in W$; and R be the subspace generated by $(\lambda v) \otimes w - \lambda(v \otimes w)$, $v \otimes (\lambda w) - \lambda(v \otimes w)$ for $v \in V$, $w \in W$ and $\lambda \in k$ along with $(x_1 + x_2) \otimes y - x_1 \otimes y - x_2 \otimes y$ and $x \otimes (y_1 + y_2) - x \otimes y_1 - x \otimes y_2$ for $x, x_1, x_2 \in V$ and $y, y_1, y_2 \in W$; then $V \otimes W \cong F/R$ naturally.

Exercise. Show that for vector spaces U, V and W there is a natural (basis independent) isomorphism

$$(U \oplus V) \otimes W \to (U \otimes W) \oplus (V \otimes W).$$

Lecture 11

Definition. Suppose that V and W are vector spaces with bases $v_1, \dots, v_n$ and $w_1, \dots, w_n$ and $\varphi\colon V \to V$ and $\psi\colon W \to W$ are linear maps. We can define $\varphi \otimes \psi\colon V \otimes W \to V \otimes W$ as follows:

$$(\varphi \otimes \psi)(v_i \otimes w_j) = \varphi(v_i) \otimes \psi(w_j).$$

Example. If φ is represented by the matrix A_{ij} and ψ is represented by the matrix B_{ij} and we order the basis $v_i \otimes w_j$ lexicographically (ie $v_1 \otimes w_1, v_1 \otimes w_2, \dots, v_1 \otimes w_n, v_2 \otimes w_1, \dots, v_m \otimes w_n$) then $\varphi \otimes \psi$ is represented by the block matrix

$$\begin{pmatrix} A_{11}B & A_{12}B & \cdots \\ A_{21}B & A_{22}B & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

Lemma. *The linear map $\varphi \otimes \psi$ does not depend on the choice of bases.*

Proof. It suffices to show that for any $v \in V$ and $w \in W$,

$$(\varphi \otimes \psi)(v \otimes w) = \varphi(v) \otimes \psi(w).$$

Writing $v = \sum \lambda_i v_i$ and $w = \sum \mu_j w_j$ we see

$$(\varphi \otimes \psi)(v \otimes w) = \sum_{i,j} \lambda_i \mu_j \varphi(v_i) \otimes \psi(w_j) = \varphi(v) \otimes \psi(w)$$

as required. □

Remark. The proof really just says $V \times W \to V \otimes W$ defined by $(v, w) \mapsto \varphi(v) \otimes \psi(w)$ is bilinear and $\varphi \otimes \psi$ is its correspondent in the bijection

$$\{\text{linear maps } V \otimes W \to V \otimes W\} \to \{\text{bilinear maps } V \times W \to V \otimes W\}$$

from last time.

Lemma. *Suppose that $\varphi, \varphi_1, \varphi_2 \in \operatorname{Hom}_k(V, V)$ and $\psi, \psi_1, \psi_2 \in \operatorname{Hom}_k(W, W)$*

(i) $(\varphi_1 \varphi_2) \otimes (\psi_1 \psi_2) = (\varphi_1 \otimes \psi_1)(\varphi_2 \otimes \psi_2) \in \operatorname{Hom}_k(V \otimes W, V \otimes W)$*;*
(ii) $\mathrm{id}_V \otimes \mathrm{id}_W = \mathrm{id}_{V \otimes W}$*; and*
(iii) $\operatorname{tr}(\varphi \otimes \psi) = \operatorname{tr} \varphi \cdot \operatorname{tr} \psi$.

Proof. Given $v \in V$, $w \in W$ we can use the previous lemma to compute

$$(\varphi_1\varphi_2) \otimes (\psi_1\psi_2)(v \otimes w) = \varphi_1\varphi_2(v) \otimes \psi_1\psi_2(w) = (\varphi_1 \otimes \psi_1)(\varphi_2 \otimes \psi_2)(v \otimes w).$$

Since elements of the form $v \otimes w$ span $V \otimes W$ and all maps are linear it follows that

$$(\varphi_1\varphi_2) \otimes (\psi_1\psi_2) = (\varphi_1 \otimes \psi_1)(\varphi_2 \otimes \psi_2)$$

as required.

(ii) is clear.

For the formula relating traces it suffices to stare at the example above:

$$\operatorname{tr}\begin{pmatrix} A_{11}B & A_{12}B & \cdots \\ A_{21}B & A_{22}B & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} = \sum_{i,j} B_{ii}A_{jj} = \operatorname{tr} A \operatorname{tr} B.$$

□

Definition. Given two representation (ρ, V) and (ρ', W) of a group G we can define the representation $(\rho \otimes \rho', V \otimes W)$ by $(\rho \otimes \rho')(g) = \rho(g) \otimes \rho'(g)$.

Proposition. *If (ρ, V) and (ρ', W) are representations of G then $(\rho \otimes \rho', V \otimes W)$ is a representation of G and $\chi_{\rho\otimes\rho'} = \chi_\rho \cdot \chi_{\rho'}$.*

Proof. This is an straightforward consequence of the lemma. □

Remarks.

(1) It follows that $R(G)$ is closed under multiplication.
(2) Tensor product of representations defined here is consistent with our earlier notion when one of the representations is one-dimensional.
(3) It follows from the lemma that if (ρ, V) is a representation of G and (ρ', W) is a representation of another group H then we may make $V \otimes W$ into a rep of $G \times H$ via
$$\rho_{V\otimes W}(g, h) = \rho(g) \otimes \rho'(h).$$
In the proposition we take the case $G = H$ and then restrict this representation to the diagonal subgroup $G \cong \{(g, g)\} \subset G \times G$.
(4) If X, Y are finite sets with G-action it is easy to verify that $kX \otimes kY \cong kX \times Y$ as representations of G (or even of $G \times G$).

Now return to our assumption that $k = \mathbb{C}$.

Proposition. *Suppose G and H are finite groups.*

Let $(\rho_1, V_1), \dots, (\rho_r, V_r)$ be a complete list of the irreducible complex representations of G and $(\rho'_1, W_1), \dots, (\rho'_s, W_s)$ a complete list of the irreducible complex representations of H. For each $1 \leqslant i \leqslant r$ and $1 \leqslant j \leqslant s$, $(\rho_i \otimes \rho'_j, V_i \otimes W_j)$ is an irreducible complex representation of $G \times H$. Moreover, all the irreducible representations of $G \times H$ arise in this way.

We have seen this before when G and H are abelian since then all these representations are 1-dimensional.

Proof. Let $\chi_1, \dots, \chi_r$ be the characters of $V_1, \dots, V_r$ and $\psi_1, \dots, \psi_s$ the characters of $W_1, \dots, W_s$.

The character of $V_i \otimes W_j$ is $\chi_i \otimes \psi_j \colon (g, h) \mapsto \chi_i(g)\psi_j(h)$. Then

$$\langle \chi_i \otimes \psi_j, \chi_k \otimes \psi_l \rangle_{G\times H} = \langle \chi_i, \chi_k \rangle_G \langle \psi_j, \psi_l \rangle_H = \partial_{ik}\partial_{jl}.$$

So the $\chi_i \otimes \psi_j$ are irreducible and pairwise distinct.

Now $\sum_{i,j} \dim(V_i \otimes W_j)^2 = (\sum_i \dim V_i^2)(\sum_j \dim W_j^2) = |G||H| = |G \times H|$ so we must have them all. □

Exercise. Show both directly and using characters that if U, V, W are representations of G then $V \otimes W \cong \mathrm{Hom}_k(V^*, W)$ and $\mathrm{Hom}_k(V \otimes W, U) \cong \mathrm{Hom}_k(V, \mathrm{Hom}_k(W, U))$ as representations of G.

Question. If V and W are irreducible then must $V \otimes W$ be irreducible?

We've seen the answer is yes is one of V and W is one-dimensional but it is not usually true.

Example. $G = S_3$

	1	3	2
	e	(12)	(123)
$\mathbf{1}$	1	1	1
ϵ	1	-1	1
V	2	0	-1

Clearly, $\mathbf{1} \otimes W = W$ always. $\epsilon \otimes \epsilon = \mathbf{1}$, $\epsilon \otimes V = V$ and $V \otimes V$ has character χ^2 given by $\chi^2(1) = 4$, $\chi^2(12) = 0$ and $\chi^2(123) = 1$. Thus χ^2 decomposes as $\mathbf{1} + \epsilon + \chi$.

In fact $V \otimes V, V \otimes V \otimes V, \ldots$ are never irreducible if $\dim V > 1$.

Given a vector space V, define $\sigma = \sigma_V : V \otimes V \to V \otimes V$ by $\sigma(v \otimes w) \mapsto w \otimes v$ for all $v, w \in V$ (exercise: check this does uniquely define a linear map). Notice that $\sigma^2 = \mathrm{id}$ and so σ decomposes $V \otimes V$ into two eigenspaces:

$$S^2V := \{a \in V \otimes V \mid \sigma a = a\}$$
$$\Lambda^2 V := \{a \in V \otimes V \mid \sigma a = -a\}$$

Lemma. *Suppose $v_1, \ldots, v_m$ is a basis for V.*

(i) S^2V has a basis $v_iv_j := \frac{1}{2}(v_i \otimes v_j + v_j \otimes v_i)$ for $1 \leqslant i \leqslant j \leqslant d$.

(ii) $\Lambda^2 V$ has a basis $v_i \wedge v_j := \frac{1}{2}(v_i \otimes v_j - v_j \otimes v_i)$ for $1 \leqslant i < j \leqslant d$.

Thus $\dim S^2V = \frac{1}{2}m(m+1)$ *and* $\dim \Lambda^2 V = \frac{1}{2}m(m-1)$.

Remark. We usually write $v_i \wedge v_j := -v_j \wedge v_i$ for $j < i$ and $v_i \wedge v_i = 0$.

Proof. It is easy to check that the union of the two claimed bases form a basis for $V \otimes V$, that the v_iv_j do all live in S^2V and that the $v_i \wedge v_j$ do all live in $\Lambda^2 V$. Everything follows. □

Proposition. *Let (ρ, V) be a representation of G.*

(i) S^2V and $\Lambda^2 V$ are subreps of $V \otimes V$ and $V \otimes V = S^2V \oplus \Lambda^2 V$.

(ii) for $g \in G$,

$$\chi_{S^2V}(g) = \frac{1}{2}(\chi(g)^2 + \chi(g^2))$$
$$\chi_{\Lambda^2 V}(g) = \frac{1}{2}(\chi(g)^2 - \chi(g^2)).$$

Proof. For (i) we need to show that if $a \in V \otimes V$ and $\sigma_V(a) = \lambda a$ for $\lambda = \pm 1$ then $\sigma_V \rho(g)(a) = \lambda \rho(g)(a)$ for each $g \in G$. For this it suffices to prove that $\sigma g = g\sigma$ (ie $\sigma \in \mathrm{Hom}_G(V \otimes V, V \otimes V)$). But $\sigma \circ g(v \otimes w) = gw \otimes gv = g \circ \sigma(v \otimes w)$.

To compute (ii), let $v_1, \dots, v_m$ be a basis of eigenvectors for $\rho(g)$ with eigenvalues $\lambda_1, \dots, \lambda_m$. Then $g(v_i v_j) = (\lambda_i \lambda_j) v_i v_j$ and $g(v_i \wedge v_j) = (\lambda_i \lambda_j) v_i \wedge v_j$.

Thus $\chi_{S^2V}(g) = \sum_{i \leqslant j} \lambda_i \lambda j$, whereas

$$\chi(g)^2 + \chi(g^2) = (\sum_i \lambda_i)^2 + \sum_i \lambda_i^2 = 2 \sum_{i \leqslant j} \lambda_i \lambda j.$$

Similarly $\chi_{\Lambda^2 V}(g) = \sum_{i<j} \lambda_i \lambda_j$, and

$$\chi(g)^2 - \chi(g^2) = (\sum_i \lambda_i)^2 - \sum_i \lambda_i^2 = \sum_{i<j} \lambda_i \lambda_j.$$

□

Lecture 12

Recall that given a representation V of G we've defined subrepresentations S^2V and $\Lambda^2 V$ of $V \otimes V$ such that

$$\chi_{S^2V}(g) = \frac{1}{2}(\chi(g)^2 + \chi(g^2))$$
$$\chi_{\Lambda^2V}(g) = \frac{1}{2}(\chi(g)^2 - \chi(g^2)).$$

Example. S_4

	1	3	8	6	6
	e	$(12)(34)$	(123)	(12)	(1234)
$\mathbf{1}$	1	1	1	1	1
ϵ	1	1	1	-1	-1
χ_3	3	-1	0	1	-1
$\epsilon\chi_3$	3	-1	0	-1	1
χ_5	2	2	-1	0	0
χ_3^2	9	1	0	1	1
$\chi_3(g^2)$	3	3	0	3	-1
$S^2\chi_3$	6	2	0	2	0
$\Lambda^2\chi_3$	3	-1	0	-1	1

Thus $S^2\chi_3 = \chi_5 + \chi_3 + \mathbf{1}$ and $\Lambda^2\chi_3 = \epsilon\chi_3$. Notice that given $\mathbf{1}$ and ϵ and χ_3 we could've constructed the remaining two irreducible characters using $S^2\chi_3$ and $\Lambda^2\chi_3$.

Exercise. Show that if V is self-dual then either $\langle \mathbf{1}, \chi_{S^2V}\rangle \neq 0$ or $\langle \mathbf{1}, \chi_{\Lambda^2V}\rangle \neq 0$.

Last time we thought about S^2V and Λ^2V by considering the 'swap' action of C_2 on $V \otimes V$; $v \otimes w \mapsto w \otimes v$. More generally, for any vector space V we may consider $V^{\otimes n} = V \otimes \cdots \otimes V$. Then for any $\sigma \in S_n$ we can define a linear map $\rho(\sigma)\colon V^{\otimes n} \to V^{\otimes n}$ by

$$\rho(\sigma)\colon v_1 \otimes \cdots v_n \mapsto v_{\sigma^{-1}(1)} \otimes \cdots v_{\sigma^{-1}(n)}$$

for $v_1, \dots, v_n \in V$

Exercise. Show that this defines a representation of S_n on $V^{\otimes n}$.

If V is a representation of a group G then the action of G on $V^{\otimes n}$ via

$$v_1 \otimes \cdots \otimes v_n \mapsto gv_1 \otimes \cdots \otimes gv_n$$

commutes with the S_n-action. Thus we can decompose $V^{\otimes n}$ as a rep of S_n and each isotypical component should be a G-invariant subspace of $V^{\otimes n}$. In particular we can make the following definition.

Definition. Suppose that V is a vector space we define

(i) the n^{th} *symmetric power* of V to be
$$S^nV := \{a \in V^{\otimes n} \mid \sigma_\omega(a) = a \text{ for all } \omega \in S_n\}$$
and

(ii) the n^{th} *exterior (or alternating) power* of V to be
$$\Lambda^nV := \{a \in V^{\otimes n} \mid \sigma_\omega(a) = \epsilon(\omega)a \text{ for all } \omega \in S_n\}.$$

Note that $S^nV \oplus \Lambda^nV = \{a \in V^{\otimes n} \mid \sigma_\omega(a) = a \text{ for all } \omega \in A_n\} \subsetneq V^{\otimes n}$.

We also define the following notation for $v_1, \ldots, v_n \in V$,
$$v_1 \cdots v_n := \frac{1}{n!}\sum_{\sigma \in S_n} v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)} \in S^nV$$
and
$$v_1 \wedge \cdots \wedge v_n := \frac{1}{n!}\sum_{\sigma \in S_n} \epsilon(\sigma) v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)} \in \Lambda^nV.$$

Exercise. Show that if $v_1, \ldots, v_d$ is a basis for V then
$$\{v_{i_1} \cdots v_{i_n} \mid 1 \leqslant i_1 \leqslant \cdots \leqslant i_n \leqslant d\}$$
is a basis for S^nV and
$$\{v_{i_1} \wedge \cdots \wedge v_{i_n} \mid 1 \leqslant i_1 < \cdots < i_n \leqslant d\}$$
is a basis for Λ^nV. Hence given $g \in V$, compute the character values $\chi_{S^nV}(g)$ and χ_{Λ^nV} in terms of the eigenvalues of g on V.

For any vector space V, $\Lambda^{\dim V} \cong k$ and $\Lambda^nV = 0$ if $n > \dim V$.

Exercise. Show that if (ρ, V) is a representation of G then the representation of G on $\Lambda^{\dim V}V \cong k$ is given by $g \mapsto \det \rho(g)$; ie the $\dim V^{th}$ exterior power of V is isomorphic to $\det \rho$.

In characteristic zero, we may stick these vector spaces together to form algebras.

Definition. Given a vector space V we may define the *tensor algebra* of V,
$$TV := \oplus_{n \geqslant 0} V^{\otimes n}$$
(where $V^{\otimes 0} = k$). Then TV is a (non-commutative) graded ring with the product of $v_1 \otimes \cdots \otimes v_r \in V^{\otimes r}$ and $w_1 \otimes \cdots \otimes w_s \in V^{\otimes s}$ given by
$$v_1 \otimes \cdots \otimes v_r \otimes w_1 \otimes \cdots \otimes w_s \in V^{\otimes r+s}.$$
with graded quotient rings the *symmetric algebra* of V,
$$SV := TV/(x \otimes y - y \otimes x \mid x, y \in V),$$
and the *exterior algebra* of V,
$$\Lambda V := TV/(x \otimes y + y \otimes x \mid x, y \in V).$$

One can show that $SV \cong \bigoplus_{n\geqslant 0} S^n V$ under $x_1 \otimes \cdots \otimes x_n \mapsto x_1 \cdots x_n$ and $\Lambda V \cong \bigoplus_{n\geqslant 0} \Lambda^n V$ under $x_1 \otimes \cdots \otimes x_n \mapsto x_1 \wedge \cdots \wedge x_n$.

Now SV is a commutive ring and ΛV is graded-commutative; that is if $x \in \Lambda^r V$ and $y \in \Lambda^s V$ then $x \wedge y = (-1)^{rs} y \wedge x$.

We've now got a number of ways to build representations:

- permutation representations coming from group actions;
- via representations of quotient groups and groups containing our group (restriction);
- tensor products;
- symmetric and exterior powers;
- decomposition of these into irreducible components;
- character theoretically using orthogonality of characters.

We're now going to discuss one more way related to restriction.

6. Induction

Suppose that H is a subgroup of G. Restriction turns representations of G into representations of H. We would like a way of building representations of G from representations of H. There is a good way of doing so called induction although it is a little more delicate than restriction.

If G is a finite group and W is a k-vector space we may define $\mathrm{Hom}(G, W)$ to be the vector space of all functions $G \to W$ under pointwise addition and scalar multiplication. This may be made into a representation of G by defining

$$(g \cdot f)(x) := f(g^{-1}x)$$

for each $g, x \in G$. If $w_1, \ldots, w_n$ is a basis for W then $\{\partial_g w_i \mid g \in G, 1 \leqslant i \leqslant n\}$ is a basis for $\mathrm{Hom}(G, W)$. So $\dim \mathrm{Hom}(G, W) = |G| \dim W$.

Lemma. $\mathrm{Hom}(G, W) \cong (\dim W)kG$ *as representations of* G.

Proof. Given a basis $w_1, \ldots, w_n$ for W, define the linear map

$$\Theta\colon \bigoplus_{i=1}^{n} kG \to \mathrm{Hom}(G, W)$$

by

$$\Theta((f_i)_{i=1}^n)(x) = \sum_{i=1}^{n} f_i(x) w_i.$$

It is easy to see that Θ is injective because the w_i are linearly independent so by comparing dimensions we see that Θ is a vector-space isomorphism.

It remains to prove that Θ is G=linear. If $g, x \in G$ then

$$g \cdot (\Theta((f_i)_{i=1}^n))(x) = \sum_{i=1}^{n} f_i(g^{-1}x) w_i = \Theta(g \cdot (f_i)_{i=1}^n)(x)$$

as required. □

Exercise. Use the basis of $\mathrm{Hom}(G, W)$ given above to find a character-theoretic proof of the lemmma.

Now, if H is a subgroup of G and W is a representation of H then we can define

$$\mathrm{Hom}_H(G,W) := \{f \in \mathrm{Hom}(G,W) \mid f(xh) = h^{-1}f(x)\ \forall x \in G, h \in H\},$$

a k-linear subspace of $\mathrm{Hom}(G,W)$.

Example. If $W = \mathbf{1}$ is the trivial representation of H and $f \in \mathrm{Hom}(G,\mathbf{1})$, then $f \in \mathrm{Hom}_H(G,\mathbf{1})$ if and only if $f(xh) = f(x)$ for $h \in H$ and $x \in G$. That is $\mathrm{Hom}_H(G,\mathbf{1})$ consists of the functions that are constant on each left coset in G/H. Thus $\mathrm{Hom}_H(G,\mathbf{1})$ can be identified with kG/H. One can check that this identification is G-linear.

Lemma. $\mathrm{Hom}_H(G,W)$ *is a G-invariant subspace of* $\mathrm{Hom}(G,W)$.

Proof. Let $f \in \mathrm{Hom}_H(G,W)$, $g,x \in G$ and $h \in H$ we must show that

$$(g\cdot f)(xh) = h^{-1}(g\cdot f)(x).$$

But $(g\cdot f)(xh) = f(g^{-1}xh) = h^{-1}f(g^{-1}x) = h^{-1}(g\cdot f)(x)$ as required. □

Definition. Suppose that H is a subgroup of G of finite index and W is a representation of H. We define the *induced representation* to be $\mathrm{Ind}_H^G W := \mathrm{Hom}_H(G,W)$

Lecture 13

Recall from last time:

Definition. Suppose that H is a subgroup of G and W is a representation of H. We define the *induced representation* by

$$\mathrm{Ind}_H^G W := \mathrm{Hom}_H(G,W) = \{f\colon G \to W \mid f(xh) = h^{-1}f(x) \text{ for all } x \in G, h \in H\}$$

Remark. Since $\mathrm{Ind}_H^G \mathbf{1} = kG/H$, Ind_H^G does not send irreducibles to irreducibles in general.

Proposition. *Suppose W is a representation of H then*

(i) $\dim \mathrm{Ind}_H^G W = \frac{|G|}{|H|}\dim W$*;*

(ii) for $g \in G$,

$$\chi_{\mathrm{Ind}_H^G W}(g) = \frac{1}{|H|}\sum_{\substack{x\in G\\ x^{-1}gx\in H}} \chi_W(x^{-1}gx).$$

Remarks.

(1) $x^{-1}gx \in H$ if and only if $gxH = xH$ so if W is the trivial representation the rhs of formula in (ii) becomes $|\{xH \in G/H \mid gxH = xH\}|$ and we get the permutation character of kG/H as required.

(2) If we write χ_W° for the function on G such that $\chi_W^\circ(g) = \chi_W(g)$ if $x \in H$ and $\chi_W^\circ(g) = 0$ if $g \notin H$, then the formula in (ii) becomes

$$\chi_{\mathrm{Ind}_H^G W}(g) = \frac{1}{|H|}\sum_{x\in G}\chi_W^\circ(x^{-1}gx);$$

this is clearly a class function.

(3) If $[h_1],\dots,[h_m]$ is a list of the H-conjugacy classes such that $x^{-1}gx \in [h_i]$ some $x \in G$ then we can write this as

$$\chi_{\operatorname{Ind}_H^G W}(g) = \sum_{i=1}^{m} \frac{|C_G(g)|}{|C_H(h_i)|}\chi_W(h_i).$$

This is the most useful formula for computation.

Example. $G = S_3$ and $H = A_3 = \{1, (123), (132)\}$.

If W is any rep of H then

$$\begin{aligned} \chi_{\operatorname{Ind}_H^G W}(e) &= 2\chi_W(e), \\ \chi_{\operatorname{Ind}_H^G W}((12)) &= 0, \text{ and} \\ \chi_{\operatorname{Ind}_H^G W}((123)) &= \chi_W((123)) + \chi_W((132)). \end{aligned}$$

So

A_3	1	(123)	(132)
χ_1	1	1	1
χ_2	1	w	w^2
χ_3	1	w^2	w

S_3	1	(12)	(123)
$\operatorname{Ind}\chi_1$	2	0	2
$\operatorname{Ind}\chi_2$	2	0	-1
$\operatorname{Ind}\chi_3$	2	0	-1

So $\operatorname{Ind}_H^G \chi_2 = \operatorname{Ind}_H^G \chi_3$ is the 2-dimensional irreducible character of S_3 and $\operatorname{Ind}_H^G \chi_1 = \mathbf{1} + \epsilon$ as expected.

Proof of Proposition. Let $x_1,\dots,x_r$ be left coset representatives in G/H. Then $f \in \operatorname{Hom}_H(G,W)$ is determined by the values of $f(x_1),\dots,f(x_r) \in W$.

Moreover, given $w_1,\dots,w_r \in W$ we can define $f \in \operatorname{Hom}_H(G,W)$ via $f(x_ih) = h^{-1}w_i$ for $i = 1,\dots,r$ and $h \in H$. Thus

$$\Theta\colon \operatorname{Hom}_H(G,W) \to \bigoplus_{i=1}^{r} W$$

defined by $f \mapsto (f(x_i))_{i=1}^r$ is an isomorphism of vector spaces and part (i) is done.

Following this argument, we see that given $w \in W$, and $1 \leqslant i \leqslant r$, we can define $\varphi_{i,w} \in \operatorname{Hom}_H(G,W)$ by

$$\varphi_{i,w}(x_jh) = \partial_{ij}h^{-1}w$$

for each $h \in H$ and $1 \leqslant j \leqslant r$.

Now given $g \in G$, let's consider how g acts on a $\varphi_{i,w}$. For each coset representative x_i there is a unique $\sigma(i)$ and $h_i \in H$ such that $g^{-1}x_i = x_{\sigma(i)}h_i \in x_{\sigma(i)}H$, and

$$(g\cdot\varphi_{i,w})(x_j) = \varphi_{i,w}(g^{-1}x_j) = \varphi_{i,w}(x_{\sigma(j)}h_j) = \partial_{i\sigma(j)}h_j^{-1}w.$$

Thus $g\cdot\varphi_{i,w} = \varphi_{\sigma^{-1}(i),h^{-1}_{\sigma^{-1}(i)}w}$.

Thus g acts on $\bigoplus_{i=1}^r W$ via a block permutation matrix and we only get contributions to the trace from the non-zero diagonal blocks which correspond to the fixed points of σ. Moreover if $\sigma(i) = i$ then g acts on W_i via $h_i^{-1} = x_i^{-1}gx_i$

Thus

$$\operatorname{tr} g_{\operatorname{Ind}_H^G W} = \sum_i \chi_W^\circ(x_i^{-1}gx_i).$$

Since $G = \{x_ih \mid h \in H\}$ and $\chi_W^\circ(h^{-1}gh) = \chi_W^\circ(g)$ for all $g \in G$ and $h \in H$ we may rewrite this as

$$\operatorname{tr} g_{\operatorname{Ind}_H^G W} = \frac{1}{|H|}\sum_{x\in G}\chi_W^\circ(xgx^{-1})$$

as required. $\square$

If V is a representation of G, we'll write $\operatorname{Res}_H^G V$ for the representation of H obtained by restriction.

Proposition (Frobenius reciprocity)**.** *Let V be a representation of G, and W a representation of H, then*

(i) $\langle \chi_V, \operatorname{Ind}_H^G \chi_W\rangle_G = \langle \operatorname{Res}_H^G \chi_V, \chi_W\rangle_H$*;*
(ii) $\operatorname{Hom}_G(V, \operatorname{Ind}_H^G W) \cong \operatorname{Hom}_H(\operatorname{Res}_H^G V, W)$.

Proof. We've already seen that (i) implies (ii).
Now

$$\begin{aligned}
\langle \chi_V, \operatorname{Ind}_H^G \chi_W\rangle_G &= \frac{1}{|G|}\sum_{g\in G}\overline{\chi_V(g)}\chi_{\operatorname{Ind}_H^G W}(g)\\
&= \frac{1}{|G||H|}\sum_{g\in G}\sum_{x\in G}\overline{\chi_V(g)}\chi_W^\circ(x^{-1}gx)\\
&= \frac{1}{|G|}\sum_{x\in G}\sum_{g'\in G}\overline{\chi_V(xg'x^{-1})}\chi_W^\circ(g') \qquad\qquad (g' = x^{-1}gx)\\
&= \frac{1}{|H|}\sum_{g'\in H}\overline{\chi_V(g')}\chi_W(g')\\
&= \langle \operatorname{Res}_H^G \chi_V, \chi_W\rangle_H
\end{aligned}$$

as required. $\square$

Exercise. Prove (ii) directly by considering

$$\Theta\colon \operatorname{Hom}_G(V, \operatorname{Hom}_H(G, W)) \to \operatorname{Hom}_H(V, W)$$

defined by $\Theta(f)(v) = f(v)(e)$.

6.1. **Mackey Theory.** This is the study of representations like $\operatorname{Res}_K^G \operatorname{Ind}_H^G W$ for H, K subgroups of G and W a representation of H. We can (and will) use it to characterise when $\operatorname{Ind}_H^G W$ is irreducible.

Recall that if G acts transitively on a set X then for $x \in X$ there is a bijection $G/\operatorname{Stab}_G(x) \tilde{\to} X$ given by $g\operatorname{Stab}_G(x) \mapsto gx$ that commutes with the G-action (ie $g'(g\operatorname{Stab}_G(x)) = (g'g)\operatorname{Stab}_G(x) \mapsto g'gx = g'(gx)$).

If H, K are subgroups of G we can restrict the action of G on G/H to K

$$K \times G/H \to G/H; (k, gh) \mapsto kgH.$$

The the union of an orbit of this action is called a *double coset*. The union of the K-orbit of gH is written $KgH := \{kgh \mid k \in K, h \in H\}$.

Definition. $K\backslash G/H := \{KgH \mid g \in G\}$ is the set of double cosets.

The double cosets $K\backslash G/H$ partition G.

Notice that $kgH = gH$ if and only if $k \in gHg^{-1}$. Thus as a set with a K-action, $KgH \tilde{\to} K/(K \cap gHg^{-1})$.

Proposition. *If G, H, K as above then*

$$\operatorname{Res}_K^G \operatorname{Ind}_H^G \mathbf{1} \cong \bigoplus_{g\in K\backslash G/H} \operatorname{Ind}_{gHg^{-1}\cap K}^K \mathbf{1}.$$

Proof. This follows from the discussion above, together with the general facts that $\operatorname{Ind}_H^G \mathbf{1} = kG/H$ and that if $X = \bigcup X_i$ is a decomposition of X into orbits then $kX \cong \bigoplus kX_i$. □

Lecture 14

Recall from last time,

Proposition. *If G is a finite group and H,K are subgroups of G, then*

$$\operatorname{Res}_K^G \operatorname{Ind}_H^G \mathbf{1} \cong \bigoplus_{g \in K\backslash G/H} \operatorname{Ind}_{gHg^{-1}\cap K}^K \mathbf{1}.$$

Given any representation (ρ, W) of H and $g \in G$, we can define $({}^g\rho, {}^gW)$ to be the representation of ${}^gH := gHg^{-1} \leqslant G$ on the underlying vector space W given by $({}^g\rho)(ghg^{-1}) = \rho(h)$ for $h \in H$.

Theorem (Mackey's Restriction Formula)**.** *If G is a finite group with subgroups H and K, and W is a representation of H then*

$$\operatorname{Res}_K^G \operatorname{Ind}_H^G W \cong \bigoplus_{g \in K\backslash G/H} \operatorname{Ind}_{K\cap {}^gH}^K \operatorname{Res}_{{}^gH\cap K}^{{}^gH} {}^gW.$$

Proof. For each double coset KgH we can define

$$V_g = \{f \in \operatorname{Ind}_H^G W \mid f(x) = 0 \text{ for all } x \notin KgH\}.$$

Then V_g is a K-invariant subspace of $\operatorname{Ind}_H^G W$ since we always have $(kf)(x) = f(k^{-1}x)$. Thus there is a decomposition

$$\operatorname{Res}_K^G \operatorname{Ind}_H^G W \cong \bigoplus_{g \in K\backslash G/H} V_g$$

and it suffices to show that for each g,

$$V_g \cong \operatorname{Ind}_{K\cap {}^gH}^K \operatorname{Res}_{{}^gH\cap K}^{{}^gH} {}^gW$$

as representations of K.

Note $\dim V_g = \dim W|\operatorname{Orb}_K(gH)| = \dim W \frac{|K|}{|Stab_K(gH)|} = \dim W \frac{|K|}{|K\cap gHg^{-1}|}$ and this last is $\dim \operatorname{Ind}_{K\cap {}^gH}^K \operatorname{Res}_{{}^gH\cap K}^{{}^gH} {}^gW$. So it suffices to find an injective K-linear map $\Theta\colon V_g \to \operatorname{Hom}_{K\cap {}^gH}(K, {}^gW)$.

Define such a Θ by $\Theta(f)(k) = f(kg)$. If $ghg^{-1} \in K$ for some $h \in H$,

$$\begin{aligned}\Theta(f)(kghg^{-1}) &= f(kgh)\\ &= \rho(h^{-1})f(kg)\\ &= ({}^g\rho)(ghg^{-1})^{-1}\Theta(f)(k)\end{aligned}$$

Thus $\operatorname{Im}\Theta \leqslant \operatorname{Ind}_{K\cap {}^gH}^K \operatorname{Res}_{K\cap {}^gH}^{{}^gH} {}^gW$.

Also, if $k' \in K$ then

$$(k'\Theta(f))(k) = f(k'^{-1}kg) = (k'f)(kg) = \Theta(k'f)(k)$$

and so Θ is K-linear. □

Corollary (Character version of Mackey's Restriction Formula)**.** *If χ is a character of a representation of H then*
$$\operatorname{Res}^G_K \operatorname{Ind}^G_H \chi = \sum_{g\in K\backslash G/H} \operatorname{Ind}^K_{{}^gH\cap K} {}^g\chi.$$
where ${}^g\chi$ is the class function on ${}^gH\cap K$ given by ${}^g\chi(x) = \chi(g^{-1}xg)$.

Exercise. Prove this corollary directly with characters

Corollary (Mackey's irreducibility criterion)**.** *If H is a subgroup of G and W is a representation of H, then $\operatorname{Ind}^G_H W$ is irreducible if and only if*

(i) W is irreducible and

(ii) for each $g\in G\backslash H$, the two representations $\operatorname{Res}^{{}^gH}_{H\cap{}^gH} {}^gW$ and $\operatorname{Res}^H_{{}^gH\cap H} W$ of $H\cap^g H$ have no irreducible factors in common.

Proof.
$$\begin{aligned}\operatorname{Hom}_G(\operatorname{Ind}^G_H W, \operatorname{Ind}^G_H W) &\overset{\text{Frob. recip.}}{\cong} \operatorname{Hom}_H(W, \operatorname{Res}^G_H \operatorname{Ind}^G_H W)\\ &\overset{\text{Mackey}}{\cong} \bigoplus_{g\in H\backslash G/H} \operatorname{Hom}_H(W, \operatorname{Ind}^H_{H\cap{}^gH} \operatorname{Res}^{{}^gH}_{H\cap{}^gH} {}^gW)\\ &\overset{\text{Frob. recip.}}{\cong} \bigoplus_{g\in H\backslash G/H} \operatorname{Hom}_{H\cap{}^gH}(\operatorname{Res}^H_{H\cap{}^gH} W, \operatorname{Res}^{{}^gH}_{H\cap{}^gH} {}^gW)\end{aligned}$$

We know that $\operatorname{Ind}^G_H W$ is irreducible precisely if this space has dimension 1. The summand corresponding to the coset $HeH = H$ is $\operatorname{Hom}_H(W,W)$ which has dimension 1 precisely if W is irreducible and the other summands are all zero precisely if condition (ii) of the statement holds. □

Corollary. *If H is a normal subgroup of G ,and W is an irreducible rep of H then $\operatorname{Ind}^G_H W$ is irreducible if and only if ${}^g\chi_W \neq \chi_W$ for all $g\in G\backslash H$.*

Proof. Since H is normal, $gHg^{-1} = H$ for all $g\in G$. Moreover ${}^gW$ is irreducible since W is irreducible.

So by Mackey's irreducibility criterion, $\operatorname{Ind}^G_H W$ irreducible precisely if $W \not\cong {}^gW$ for all $g\in G\backslash H$. This last is equivalent to $\chi_W \neq {}^g\chi_W$ as required. □

Examples.

(1) $H = \langle r\rangle \cong C_n$, the rotations in $G = D_{2n}$. The irreducible characters χ of H are all of the form $\chi(r^j) = e^{\frac{2\pi ijk}{n}}$. We see that $\operatorname{Ind}^G_H \chi$ is irreducible if and only if $\chi(r^j)\neq\chi(r^{-j})$ for some j. This is equivalent to χ not being real valued.

(2) $G = S_n$ and $H = A_n$. If $g\in S_n$ is a cycle type that splits into two conjugacy classes in A_n and χ is an irreducible character of A_n that takes different values of the two classes then $\operatorname{Ind}^G_H \chi$ is irreducible.

(3) (Exercise) Let $G = GL_2(\mathbb{F}_p)$ be the group of invertible 2×2-matrices with coefficients in the field with p elements and let B be the subgroup of upper-triangular matrices. Show that $B\backslash G/B$ has two elements B and BsB where $s = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$.

Deduce that if χ is a character of B given by $\chi\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right) = \chi_1(a)\chi_2(b)$ with χ_1, χ_2 characters $\mathbb{F}_p^\times \to \mathbb{C}$ then $\mathrm{Ind}_B^G \chi$ is irreducible if and only if $\chi_1 \neq \chi_2$.

Lecture 15

6.2. **Frobenius groups.**

Definition. A *Frobenius group* is a finite group G that has a transitive action on a set X with $|X| > 1$ such that each $g \in G\backslash\{e\}$ fixes at most one $x \in X$ and $\mathrm{Stab}_G(x) \neq \{e\}$ for some (all) $x \in X$.

Examples.

(a) $G = D_{2n}$ with n odd acting naturally on the vertices of an n-gon.

(b) $G = \left\{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{F}_p, a \neq 0\right\}$ acting on $X = \left\{\begin{pmatrix} x \\ 1 \end{pmatrix} \mid x \in \mathbb{F}_p\right\}$ by matrix multiplication.

Lemma. *G is a Frobenius group if and only if G has a proper subgroup H such that $H \cap gHg^{-1} = \{e\}$ for all $g \in G\backslash H$.*

Proof. Suppose the action of G on X shows G to be Frobenius and pick $x \in X$.

Let $H := \mathrm{Stab}_G(x)$ for some fixed $x \in X$, a proper subgroup of G. Then $gHg^{-1} = \mathrm{Stab}_G(gx)$ for each $g \in G$. Since no element of $G\backslash\{e\}$ fixes more than one $x \in X$ it follows that $gHg^{-1} \cap H = \{e\}$ for each $g \in G\backslash H$.

Conversely, let $X = G/H$ with the left regular action. □

Theorem. *(Frobenius) Let G be a finite group acting transitively on a set X. If each $g \in G\backslash\{e\}$ fixes at most one element of X then*

$$K = \{1\} \cup \{g \in G \mid gx \neq x \text{ for all } x \in X\}$$

is a normal subgroup of G of order $|X|$.

Remarks.

(1) Any Frobenius group satisfies the conditions of the theorem. The normal subgroup K is called the Frobenius kernel and the group H is called the Frobenius complement.
(2) No proof of the theorem is known that does not use representation theory.
(3) In his thesis Thompson proved, amongst other things, that the Frobenius kernel must be a direct product of its Sylow subgroups.

Proof. For $x \in X$, let $H = \mathrm{Stab}_G(x)$.

We know that $\mathrm{Stab}_G(gx) = gHg^{-1}$. But by the hypothesis on the action

$$\mathrm{Stab}_G(gx) \cap \mathrm{Stab}_G(x) = \{e\}$$

whenever $gx \neq x$. Thus H has $|X|$ conjugates and G has $(|H| - 1)|X|$ elements that fix precisely one element of X.

But $|G| = |H||X|$ by the orbit-stabiliser theorem, and so

$$|K| = |H||X| - (|H| - 1)|X| = |X|$$

as required. We must show that it is a normal subgroup of G.

Our strategy will be to prove that it is the kernel of some representation of G.

Suppose $e \neq h \in H$ and that $h = gh'g^{-1}$ for some $g \in G$ and $h' \in H$ then $h \in \mathrm{Stab}_G(x) \cap \mathrm{Stab}_G(gx)$, so $gx = x$ and $g \in H$. Thus

- h and h' in H are conjugate in G if and only if they are conjugate in H.
- $|C_G(h)| = |C_H(h)|$ for $e \neq h \in H$

Now if χ is a character of H we can compute $\operatorname{Ind}_H^G \chi$:

$$\operatorname{Ind}_H^G \chi(g) = \begin{cases} |X|\chi(e) & \text{if } g = e \\ \chi(h) & \text{if } g = h \in H\backslash\{e\} \\ 0 & \text{if } g \in K\backslash\{e\} \end{cases}$$

Suppose now that $\chi_1, \ldots, \chi_r$ is a list of the irreducible characters of H and let $\theta_i = \operatorname{Ind}_H^G \chi_i + \chi_i(e)\mathbf{1}_G - \chi_i(e)\operatorname{Ind}_H^G \mathbf{1}_H \in R(G)$ for $i = 1, \ldots, r$ and so

$$\theta_i(g) = \begin{cases} \chi_i(e) & \text{if } g = e \\ \chi_i(h) & \text{if } g = h \in H \\ \chi_i(e) & \text{if } g \in K \end{cases}$$

If θ_i were a character then the corresponding representation would have kernel containing K. Since $\theta_i \in R(G)$ we can write it as a $\mathbb{Z}$-linear combination of irreducible characters $\theta_i = \sum n_i \psi_i$, say.

Now we can compute

$$\begin{aligned} \langle \theta_i, \theta_i \rangle_G &= \frac{1}{|G|} \sum_{g \in G} |\theta_i(g)|^2 \\ &= \frac{1}{|G|} \left(\sum_{h \in H\backslash\{e\}} |X||\chi_i(h)|^2 + \sum_{k \in K} \chi_i(e)^2 \right) \\ &= \frac{|X|}{|G|} \left(\sum_{h \in H} |\chi_i(h)|^2 \right) \\ &= \langle \chi_i, \chi_i \rangle_H = 1 \end{aligned}$$

But on the other hand it must be $\sum n_i^2$. Thus θ_i is $\pm\psi$ for some character ψ of G. Since $\theta_i(e) > 0$ it must actually be an irreducible character.

To finish we write $\theta = \sum \chi_i(e)\theta_i$ and so $\theta(h) = \sum \chi_i(e)\chi_i(h) = 0$ for $h \in H\backslash\{e\}$ by column orthogonality, and $\theta(k) = \sum \chi_i(e)^2 = |H|$ for $k \in K$. Thus $K = \ker\theta$ is a normal subgroup of G. □

7. Arithmetic properties of characters

In this section we'll investigate how arithmetic properties of characters produce a suprising interplay between the structure of the group and properties of the character table. The highlight of this will be the proof of Burnside's famous $p^a q^b$-theorem that says that the order of a simple group cannot have precisely two distinct prime factors.

We'll need to quote some results about arithmetic without proof; proofs should be provided in the Number Fields course (or in one case Galois Theory). We'll continue with our assumption that $k = \mathbb{C}$ and also assume that our groups are finite.

7.1. **Arithmetic results.**

Definition. $x \in \mathbb{C}$ is an *algebraic integer* if it is a root of a monic polynomial with integer coefficients.

Facts.

Fact 1 The algebraic integers form a subring of $\mathbb{C}$

Fact 2 If $x \in \mathbb{Q}$ is an algebraic integer then $x \in \mathbb{Z}$ (cf Numbers and Sets 2010 Example Sheet 3 Q12)

Fact 3 Any subring of $\mathbb{C}$ that is finitely generated as an abelian group consists of algebraic integers.

Lemma. *If χ is the character of a representation of a finite group G, then $\chi(g)$ is an algebraic integer for all $g \in G$.*

Proof. We know that $\chi(g)$ is a sum of n^{th} roots of unity for $n = |G|$. Since each n^{th} root of unity is by defintion a root of $X^n - 1$ the lemma follows from Fact 1. $\square$

7.2. **The group algebra.** Before we go further we need to explain how to make the vector space kG into a ring. There are in fact two sensible ways to do this. The first of these is by pointwise multiplication: $f_1 f_2(g) = f_1(g) f_2(g)$ for all $g \in G$ will make kG into a commutative ring. But more usefully for our immediate purposes we have the convolution product

$$f_1 f_2(g) := \sum_{x \in G} f_1(gx) f_2(x^{-1})$$

that makes kG into a (possibly) non-commutative ring. Notice in particular that with this product $\partial_{g_1}\partial_{g_2} = \partial_{g_1 g_2}$ and so we may rephrase the multiplication as

$$(\sum_{g \in G} \lambda_g \partial_g)(\sum_{h \in G} \mu_h \partial_h) = \sum_{k \in G} (\sum_{gh = k} \lambda_g \mu_h) \partial_k.$$

From now on this will be the product we have in mind when we think of kG as a ring.

We notice in passing that a kG-module is the 'same' as a representation of G: given a representation (ρ, V) of G we can make it into a kG-module via

$$fv = \sum_{g \in G} f(g) \rho(g)(v).$$

for $f \in kG$ and $v \in V$. Conversely, given a finitely generated kG-module M we can view M as a representation of G via $\rho(g)(m) = \partial_g m$.

Exercise. Suppose that kX is a permutation representation of G. Calculate the action of $f \in kG$ on kX under this correspondance.

Lecture 16

For the sake of the rest of the section, we need to understand the *centre* $Z(kG)$ of kG; that is the set of $f \in kG$ such that $fh = hf$ for all $h \in kG$.

Lemma. *Suppose that $f \in kG$. Then f is in $Z(kG)$ if and only if $f \in \mathcal{C}_G$, the set of class functions on G. In particular* $\dim_k Z(kG)$ *is the number of conjugacy classes in G.*

Proof. Suppose $f \in kG$. Notice that $fh = hf$ for all $h \in kG$ if and only if $f\partial_g = \partial_g f$ for all $g \in G$, since then

$$fh = \sum_{g \in G} fh(g)\partial_g = \sum_{g \in G} h(g)\partial_g f = hf.$$

But $\partial_g f = f\partial_g$ if and only if $\partial_g f \partial_{g^{-1}} = f$ and

$$(\partial_g f \partial_{g^{-1}})(x) = (\partial_g f)(xg) = f(g^{-1}xg).$$

So if $f \in Z(kG)$ if and only if $f \in \mathcal{C}_G$ as required. □

Remark. The multiplication on $Z(kG)$ is not the same as the multiplication on $\mathcal{C}_G$ that we have seen before even though both have the same additive groups and both are commutative rings.

Definition. Suppose $\mathcal{O}_1 = \{e\}, \ldots, \mathcal{O}_r$ are the conjugacy classes of G, define the *class sums* $C_1, \ldots, C_r$ to be the class functions on G so that

$$C_i = \begin{cases} 1 & g \in \mathcal{O}_i \\ 0 & g \notin \mathcal{O}_i. \end{cases}$$

We called these $\partial_{\mathcal{O}_i}$ before. Also we'll fix $g_i \in \mathcal{O}_i$ for simplicity.

We've seen that the class sums form a basis for $Z(kG)$.

Proposition. *There are non-negative integers a_{ijk} such that $C_iC_j = \sum_k a_{ijk}C_k$ for $i, j, k \in \{1, \ldots, r\}$.*

The a_{ijk} are called the *structure constants* for $Z(kG)$.

Proof. Since $Z(kG)$ is a ring, we can certainly write $C_iC_j = \sum a_{ijk}C_k$ for some $a_{ijk} \in k$.

However, we can explicitly compute for $g_k \in \mathcal{O}_k$,

$$(C_iC_j)(g_k) = \sum_{x \in G} C_i(g_kx)C_j(x^{-1}) = |\{(x, y) \in \mathcal{O}_i \times \mathcal{O}_j \mid xy = g_k\}|,$$

a non-negative integer. □

Suppose now that (ρ, V) is an irreducible representation of G. Then if $z \in Z(kG)$ we see that $z\colon V \to V$ given by $zv = \sum_{g \in G} z(g)\rho(g)v \in \mathrm{Hom}_G(V, V)$.

By Schur's Lemma it follows that z acts by a scalar $\lambda_z \in k$ on V. In this way we get an algebra homomorphism $w_\rho\colon Z(kG) \to k; z \mapsto \lambda_z$.

Taking traces we see that

$$\dim V \cdot \lambda_z = \sum_{g \in G} z(g)\chi_V(g).$$

So

$$w_\rho(C_i) = \frac{\chi(g_i)}{\chi(e)}|\mathcal{O}_i| \text{ for } g_i \in \mathcal{O}_i.$$

We now see that w_ρ only depends on χ_ρ (and so on the isomorphism class of ρ) and we write $w_\chi = w_\rho$.

Lemma. *The values $w_\chi(C_i)$ are algebraic integers.*

Note this isn't *a priori* obvious since $\frac{1}{\chi(e)}$ will not be an algebraic integer for $\chi(e) \neq 1$.

Proof. Since w_χ is an algebra homomorphism $Z(kG) \to k$,

$$w_\chi(C_i)w_\chi(C_j) = \sum_k a_{ijk} w_\chi(C_k).$$

So the subring of $\mathbb{C}$ generated by $w_\chi(C_i)$ for $i = 1, \dots, r$ is a finitely generated abelian group. The result follows from Fact 3 above. $\square$

Exercise. Show that

$$a_{ijk} = \frac{|G|}{|C_G(g_i)||C_G(g_j)|} \sum_\chi \frac{\chi(g_i)\chi(g_j)\chi(g_k^{-1})}{\chi(1)}.$$

(Hint: use column orthogonality, the last lemma and its proof.)

7.3. **Degrees of irreducibles.**

Theorem. *If V is an irreducible representation of a group G then* $\dim V$ *divides* $|G|$.

Proof. Let χ be the character of V. We'll show that $\frac{|G|}{\chi(e)}$ is an algebraic integer and so (since it is rational) an actual integer by Fact 2 above.

$$\begin{aligned}\frac{|G|}{\chi(e)} &= \frac{1}{\chi(e)} \sum_{g \in G} \chi(g)\chi(g^{-1}) \\ &= \sum_{i=1}^r \frac{1}{\chi(e)} |\mathcal{O}_i| \chi(g_i)\chi(g_i^{-1}) \\ &= \sum_{i=1}^r w_\chi(C_i)\chi(g_i^{-1})\end{aligned}$$

But the set of algebraic integers form a ring (by Fact 1 above) and each $w_\chi(C_i)$ and $\chi(g_i^{-1})$ is an algebraic integer so $\frac{|G|}{\chi(e)}$ is an algebraic integer as required. $\square$

Examples.

(1) If G is a p-group and χ is an irreducible character then $\chi(e)$ is always a power of p. In particular if $|G| = p^2$ then, since $\sum_\chi \chi(e)^2 = p^2$, every irreducible rep is 1-dimensional and so G is abelian.

(2) If $G = A_n$ or S_n and $p > n$ is a prime, then p cannot divide the dimension of an irreducible rep.

In fact a stronger result is true:

Theorem (Burnside (1904)). *If (ρ, V) is an irreducible representation then* $\dim V$ *divides* $|G/Z(G)|$.

You should compare this with $|\mathcal{O}_i| = |G|/|C_G(g_i)|$ divides $|G/Z(G)|$.

Proof. If $z \in Z = Z(G)$ then by Schur's Lemma z acts on V by $\lambda_z I$ for some $\lambda_z \in k$.

For each $m \geqslant 2$, consisder the irreducible representation of G^m given by

$$\rho^{\otimes m} \colon G^m \to GL(V^{\otimes m}).$$

If $z = (z_1, \ldots, z_m) \in Z^m$ then z acts on $V^{\otimes m}$ via $\prod_{i=1}^m \lambda_{z_i} I$. Thus if $\prod_1^m z_i = 1$ then $z \in \ker \rho^{\otimes m}$.

Let $Z' = \{(z_1, \ldots, z_m \in Z^m \mid \prod_{i=1}^m z_i = 1\}$ so $|Z'| = |Z|^{m-1}$. We may view $\rho^{\otimes m}$ as a degree $(\dim V)^m$ irreducible representation of G^m/Z'.

Since $|G^m/Z'| = |G|^m/|Z|^{m-1}$ we can use the previous theorem to deduce that $(\dim V)^m$ divides $|G|^m/|Z|^{m-1}$.

By choosing m very large and considering prime factors we can deduce the result: if p^r divides $\dim V$ then p^{rm} divides $|G/Z|^m|Z|$ for all m and so p^r divides $|G/Z|$. □

Proposition. *If G is a simple group then G has no irreducible representations of degree 2.*

Proof. If G is cyclic then G has no irreducible representations of degree bigger than 1, so we may assume G is non-abelian.

If $|G|$ is odd then we may apply the theorem above.

If $|G|$ is even then G has an element x of order 2. By example sheet 2 Q2, for every irreducible χ, $\chi(x) \equiv \chi(e) \mod 4$. So if $\chi(e) = 2$ then $\chi(x) = \pm 2$, and $\rho(x) = \pm I$. Thus $\rho(x) \in Z(\rho(G))$, a contradiction since G is non-abelian simple. □

Lecture 17

7.4. Burnside's $p^a q^b$ Theorem.

Theorem (Burnside (1904))**.** *Let p, q be primes and G a group of order $p^a q^b$ with a, b non-negative integers such that $a + b \geqslant 2$, then G is not simple.*

Remarks.

(1) It follows that every group of order $p^a q^b$ is soluble. That is, there is a chain of subgroups $G = G_0 \geqslant G_1 \geqslant \cdots \geqslant G_r = \{e\}$ with G_{i+1} normal in G_i and G_i/G_{i+1} abelian for all i.
(2) Note that $|A_5| = 2^2 \cdot 3 \cdot 5$ so the order of a simple group can have precisely 3 prime factors.
(3) If $b = 0$ then we've seen this before; $Z(G)$ has an element of order p which generates a proper normal subgroup.
(4) The first purely group theoretic proof of the $p^a q^b$-theorem appeared in 1972.
(5) In 1963 Feit and Thompson published a 255 page paper proving that every group of odd order in soluble.

The key step in the proof of the $p^a q^b$-theorem is the following:

Proposition. *If G is a non-cyclic finite group with a conjugacy class $\mathcal{O}_i \neq \{e\}$ such that $|\mathcal{O}_i|$ has prime power order then $|G|$ is not simple.*

Granting the Proposition we can prove the theorem as follows: if $a, b > 0$, then let Q be a Sylow-q-subgroup of G. Since $Z(Q) \neq 1$ we can find $e \neq g \in Z(Q)$. Then q^b divides $|C_G(g)|$, so the conjugacy class containing g has order p^r for some $0 \leqslant r \leqslant a$. The theorem now follows immediately from the Proposition.

To prove the Proposition we need some Lemmas

Lemma. *Suppose $0 \neq \alpha = \frac{1}{m} \sum_{i=1}^m \lambda_i$ with all λ_i n^{th} roots of 1 is an algebraic integer. Then $|\alpha| = 1$.*

Sketch proof (non-examinable). By assumption $\alpha \in \mathbb{Q}(\epsilon)$ where $\epsilon = e^{2\pi i/n}$.

Let $\mathcal{G} = \mathrm{Gal}(\mathbb{Q}(\epsilon)/\mathbb{Q})$. It is known that $\{\beta \in \mathbb{Q}(\epsilon) \mid \sigma(\beta) = \beta \text{ for all } \sigma \in \mathcal{G}\} = \mathbb{Q}$.

Consider $N(\alpha) := \prod_{\sigma\in\mathcal{G}} \sigma(\alpha)$. Since $N(\alpha)$ is fixed by every element of $\mathcal{G}$, $N(\alpha) \in \mathbb{Q}$. Moreover $N(\alpha)$ is an algebraic integer since Galois conjugates of algebraic integers are algebraic integers — they satisfy the same integer polynomials. Thus $N(\alpha) \in \mathbb{Z}$.

But for each $\sigma \in \mathcal{G}$, $|\sigma(\alpha)| = |\frac{1}{m}\sum \sigma(\lambda_i)| \leqslant 1$. Thus $N(\alpha) = \pm 1$, and $|\alpha| = 1$ as required. □

Lemma. *Suppose χ is an irreducible character of G, and $\mathcal{O}$ is a conjugacy class in G such that $\chi(e)$ and $|\mathcal{O}|$ are coprime. For $g \in \mathcal{O}$, $|\chi(g)| = \chi(e)$ or 0.*

Proof. By Bezout, we can find $x, y \in \mathbb{Z}$ such that $a\chi(e) + b|\mathcal{O}| = 1$. Define

$$\alpha := \frac{\chi(g)}{\chi(e)} = a\chi(g) + b\frac{\chi(g)}{\chi(e)}|\mathcal{O}|$$

Then α satisfies the conditions of the previous lemma (or is zero) and so this lemma follows. □

Proof of Proposition. Suppose for contradication that G is simple and has an element $g \in G\backslash\{e\}$ that lives in a conjugacy class $\mathcal{O}$ of order p^r.

If χ is a non-trivial irreducible character of G then $|\chi(g)| < \chi(1)$ since otherwise $\rho(g)$ is a scalar matrix and so lies in $Z(\rho(G)) \cong Z(G)$.

Thus by the last lemma, for every non-trivial irreducible character, either p divides $\chi(e)$ or $|\chi(g)| = 0$. By column orthogonality,

$$0 = \sum_{\chi} \chi(e)\chi(g).$$

Thus $\frac{-1}{p} = \sum_{\chi\neq\mathbf{1}} \frac{\chi(e)}{p}\chi(g)$ is an algebraic integer in $\mathbb{Q}$. Thus $\frac{1}{p}$ in $\mathbb{Z}$ the desired contradiction. □

8. Topological groups

Consider $S^1 = U_1(\mathbb{C}) = \{g \in \mathbb{C}^\times \mid |g| = 1\} \cong \mathbb{R}/\mathbb{Z}$.

By considering $\mathbb{R}$ as a $\mathbb{Q}$-vector space we see that as a group

$$S^1 \cong \mathbb{Q}/\mathbb{Z} \oplus \bigoplus_{x\in X} \mathbb{Q}$$

for an an uncountable set X.

Thus we see that as an abstract group S^1 has uncountably many irreducible representations: for each $\lambda \in \mathbb{R}$ we can define a one-dimensional representation by

$$\rho_\lambda(e^{2\pi i\mu}) = \begin{cases} 1 & \mu \notin \mathbb{Q}\lambda \\ e^{2\pi i\mu} & \mu \in \mathbb{Q}\lambda \end{cases}$$

Then $\rho_\lambda = \rho_{\lambda'}$ if and only if $\mathbb{Q}\lambda = \mathbb{Q}\lambda'$. In this way we get uncountably many irreducible representations of S^1 (we haven't listed them all). We don't really have any control over the situation.

However, S^1 is not just a group; it comes with a topology as a subset of $\mathbb{C}$. Moreover S^1 acts naturally on complex vector spaces in a continuous way.

Definition. A *topological group* G is a group G which is also a topological space such that the multiplication map $G \times G \to G; (g, h) \mapsto gh$ and the inverse map $G \to G; g \mapsto g^{-1}$ are continuous maps.

Examples.

(1) $GL_n(\mathbb{C})$ with topology from $\mathbb{C}^{n^2}$.
(2) G finite — with the discrete topology.
(3) $O(n) = \{A \in GL_n(\mathbb{R}) \mid A^T A = I\}$; $SO(n) = \{A \in O(n) \mid \det A = 1\}$.
(4) $U(n) = \{A \in GL_n(\mathbb{C}) \mid \overline{A^T A} = I\}$; $SU(n) = \{A \in U(n) \mid \det A = 1\}$.
(5) *G profinite such as $\mathbb{Z}_p$, the completion of $\mathbb{Z}$ with respect to the p-adic metric.

Definition. A *representation* of a topological group G on a vector space V is a continuous group homomorphism $G \to GL(V)$.

Remarks.

(1) If X is a topological space then $\alpha\colon X \to GL_n(\mathbb{C})$ is continuous if and only if the maps $x \mapsto \alpha_{ij}(x) = \alpha(x)_{ij}$ are continuous for all i, j.
(2) If G is a finite group with the discrete topology. Then continous function $G \to X$ just means function $G \to X$.

Theorem. *Every one dimensional (cts) representation of S^1 is of the form $z \mapsto z^n$ for some $n \in \mathbb{Z}$.*

It is easy to see that the given maps are representations, we must show that they are the only ones.

Lecture 18

Lemma. *If $\psi\colon (\mathbb{R}, +) \to (\mathbb{R}, +)$ is a continous group homomorphism then there is some $\lambda \in \mathbb{R}$ such that $\psi(x) = \lambda x$ for all $x \in \mathbb{R}$.*

Proof. Let $\lambda = \psi(1)$. Since ψ is a group homomorphism, $\psi(n) = \lambda n$ for all $n \in \mathbb{Z}$. Then m$\psi(n/m) = \psi(n) = \lambda n$ and so $\psi(n/m) = \lambda n/m$. That is $\psi(x) = \lambda x$ for all $x \in \mathbb{Q}$. But $\mathbb{Q}$ is dense in $\mathbb{R}$ and ψ is continuous so $\psi(x) = \lambda x$ for all $x \in \mathbb{R}$. $\square$

Lemma. *If $\psi\colon (\mathbb{R}, +) \to S^1$ is a continuous group homomorphism then $\psi(x) = e^{2\pi i \lambda x}$ for some $\lambda \in \mathbb{R}$.*

Proof. Claim: if $\psi\colon \mathbb{R} \to S^1$ is any continuous function with $\psi(0) = 1$ then there is a unique continuous function $\alpha\colon \mathbb{R} \to \mathbb{R}$ such that $\alpha(0) = 0$ and $\psi(x) = e^{2\pi i \alpha(x)}$. (Sketch proof of claim: locally $\alpha(x) = \frac{1}{2\pi i} \log \psi(x)$ we can choose the branches of log to make the pieces glue together continuously).

Now given the claim, if ψ is a group homomorphism and α is the map defined by the claim we can define a continuous function $\mathbb{R}^2 \to \mathbb{R}$ by

$$\Delta(a, b) := \alpha(a + b) - \alpha(a) - \alpha(b).$$

Since $e^{2\pi i \Delta(a,b)} = \psi(a + b)\psi(a)^{-1}\psi(b)^{-1} = 1$, Δ only takes values in $\mathbb{Z}$. Thus Δ is constant. Since $\Delta(a, 0) = 0$ for all a we see that $\Delta \equiv 0$ and so α is a group homomorphism. By the previous lemma we see $\alpha(x) = \lambda x$ for some $\lambda \in \mathbb{R}$ and so $\psi(x) = e^{2\pi i \lambda x}$ as required. $\square$

Theorem. *Every one dimensional (cts) representation of S^1 is of the form $z \mapsto z^n$ for some $n \in \mathbb{Z}$.*

Proof. Let $\rho\colon S^1 \to GL_1(\mathbb{C})$ be a continuous representation. Since S^1 is compact, $\rho(S^1)$ has closed and bounded image. Since $\rho(z^n) = \rho(z)^n$ for $n \in \mathbb{Z}$, it follows that $\rho(S^1) \subset S^1$.

Now let $\psi\colon \mathbb{R} \to S^1$ be defined by $\psi(x) = \rho(e^{2\pi i x})$, a continuous homomorphism. By the most recent Lemma, $\rho(e^{2\pi i x}) = \psi(x) = e^{2\pi i \lambda x}$ for some $\lambda \in \mathbb{R}$.

Since also $\rho(e^{2\pi i}) = 1$ we see $\lambda \in \mathbb{Z}$. $\square$

Our most powerful idea for studying representations of finite groups has been averaging over the group; that is the operation $\frac{1}{|G|}\sum_{g\in G}$. When considering more general topological groups we should replace $\sum$ by $\int$.

Definition. Let G be a topological group. Let $C(G) = \{f\colon G \to \mathbb{C} \mid f \text{ is continuous}\}$. Then a linear map $\int_G\colon C(G) \to \mathbb{C}$ (write $\int_G f = \int_G f(g)\,\mathrm{d}g$) is called a *Haar measure* if

(i) $\int_G 1 = 1$ (so $\int_G$ is normalised so total volume is 1);
(ii) $\int_G f(xg)\,\mathrm{d}g = \int_G f(g)\,\mathrm{d}g = \int_G f(gx)\,\mathrm{d}g$ for all $x \in G$ (so $\int_G$ is translation invariant).

Examples.
(1) If G finite, then $\int_G f = \frac{1}{|G|}\sum_{g\in G} f(g)$.
(2) If $G = S^1$, $\int_G f = \frac{1}{2\pi}\int_0^{2\pi} f(e^{i\theta})\,\mathrm{d}\theta$.

Theorem. *If G is a compact Hausdorff group, then there is a unique Haar measure on G.*

Proof. Omitted $\square$

All the examples of topological groups from last time are compact Hausdorff except $GL(\mathbb{C}^n)$ which is not compact. We've seen a Haar measure on S^1 and will compute one on $SU(2)$ later. We'll follow standard practice and write 'compact group' instead of 'compact Hausdorff group'.

Corollary (Weyl's Unitary Trick)**.** *If G is a compact group then every representation (ρ, V) has a G-invariant invariant Hermitian inner product.*

Proof. Same as for finite groups: let $(-,-)$ be any inner product on V, then

$$\langle v, w\rangle = \int_G (\rho(g)v, \rho(g)w)\,\mathrm{d}g$$

is the required G-invariant inner product. $\square$

Thus every representation of a compact group is equivalent to a unitary representation.

Corollary (Maschke's Theorem)**.** *If G is a compact group then every representation of G is completely reducible.*

Proof. Same as for finite groups: Given a rep (ρ, V) choose a G-invariant inner product. If W is a subrep of V then $W^\perp$ is a G-invariant complement. $\square$

We can use the Haar measure to put an inner product on the space $\mathcal{C}_G$ of (continuous) class functions:

$$\langle f, f'\rangle := \int_G \overline{f(g)} f'(g)\,\mathrm{d}g.$$

If $\rho\colon G \to GL(V)$ is a representation then $\chi_\rho := \operatorname{tr}\rho$ is a continuous class function since each $\rho(g)_{ii}$ is continuous.

Corollary (Orthogonality of Characters)**.** *If G is a compact group and V and W are irreducible reps of G then*

$$\langle \chi_V, \chi_W \rangle = \begin{cases} 1 & \text{if } V \cong W \\ 0 & \text{if } \chi_V \neq \chi_W. \end{cases}$$

Proof. Same as for finite groups:

$$\begin{aligned} \langle \chi_V, \chi_W \rangle &= \int_G \overline{\chi_V(g)}\chi_W(g)\,\mathrm{d}g \\ &= \dim \operatorname{Hom}_G(\mathbf{1}, \operatorname{Hom}(V, W)) \\ &= \dim \operatorname{Hom}_G(V, W). \end{aligned}$$

Then apply Schur's Lemma.

Note along the way we require that $\chi_V(g^{-1}) = \overline{\chi_V(g)}$ which follows from the fact that we may assume that $\rho_V(G) \subset U(V)$ and so the eigenvalues of $\rho_V(g)$ are contained in S^1 for all $g \in G$.

We also need to define a projection maps $\pi\colon U \to U^G$ for $U = \operatorname{Hom}_k(V, W)$. For this we choose a basis $u_1, \ldots, u_n$ of U and define π to be the linear map represented by the matrix $\pi_{ij} = \int_G \rho(g)_{ij}\,\mathrm{d}g$. □

It is also possible to make sense of 'the characters are a basis for the space of class functions' but this requires a little knowledge of Hilbert space.

Example. $G = S^1$.

We've already seen that the one-dimensional reps of S^1 are all of the form $z \mapsto z^n$ for $n \in \mathbb{Z}$. Since S^1 is abelian we can use our usual argument to see that these are all irreducible reps — given any rep ρ we can find a simultaneous eigenvector for each $\rho(g)$. Thus the 'character table' of S^1 has rows χ_n indexed by $\mathbb{Z}$ with $\chi_n(e^{i\theta}) = e^{in\theta}$.

Now if V is any rep of S^1 then by Machke's Theorem V breaks up as a direct sum of one dimensional subreps and so its character χ_V is of the form

$$\chi_V(z) = \sum_{n \in \mathbb{Z}} a_n z^n$$

with a_n non-negative integers and only finitely many non-zero. As usual a_n is the number of copies of $\rho_n\colon z \mapsto z^n$ in the decomposition of V. Thus we can compute

$$a_n = \langle \chi_n, \chi_V \rangle = \frac{1}{2\pi}\int_0^{2\pi} \chi_V(e^{i\theta})e^{-in\theta}\,\mathrm{d}\theta.$$

Thus

$$\chi_V(e^{i\theta}) = \sum_{n \in \mathbb{Z}} \left(\frac{1}{2\pi}\int_0^{2\pi} \chi_V(e^{i\theta'})e^{-in\theta'}\,\mathrm{d}\theta' \right) e^{in\theta}.$$

So Fourier decomposition gives the decomposition of χ_V into irreducible characters and the Fourier mode is the multiplicity of an irreducible character.

Remark. In fact by the theory of Fourier series any continuous function on S^1 can be uniformly approximated by a finite $\mathbb{C}$-linear combination of the χ_n.

Moreover the χ_n form a complete orthonormal set in the Hilbert space of square-integrable complex-valued functions on S^1. That is every function f on S^1 such that $\int_0^{2\pi}|f(e^{i\theta})|^2\,\mathrm{d}\theta$ exists has a unique series expansion

$$f(e^{i\theta}) = \sum_{n\in\mathbb{Z}}\left(\frac{1}{2\pi}\int_0^{2\pi} f(e^{i\theta'})e^{-in\theta'}\,\mathrm{d}\theta'\right)e^{in\theta}$$

converging in the norm $||f|| = \frac{1}{2\pi}\int_0^{2\pi}|f(e^{i\theta})|^2\,\mathrm{d}\theta$.

Lecture 19

8.1. **Conjugacy classes of $SU(2)$.**

Recall that $SU(2) = \{A \in GL_2(\mathbb{C}) \mid \overline{A^T}A = I, \det A = 1\}$.

If $A = \begin{pmatrix} a & b \\ c & d\end{pmatrix} \in SU(2)$ then since $\det A = 1$, $A^{-1} = \begin{pmatrix} d & -b \\ -c & a\end{pmatrix}$.

Thus $d = \overline{a}$ and $c = -\overline{b}$. Moreover $a\overline{a} + b\overline{b} = 1$. In this way we see that

$$SU(2) = \left\{\begin{pmatrix} a & b \\ -\overline{b} & \overline{a}\end{pmatrix} \mid a, b \in \mathbb{C} \text{ and } |a|^2 + |b|^2 = 1\right\}$$

which may be viewed topologically as $S^3 \subset \mathbb{C}^2 \cong \mathbb{R}^4$.

More precisely if

$$\mathbb{H} := \mathbb{R}\cdot SU(2) = \left\{\begin{pmatrix} z & w \\ -\overline{w} & \overline{z}\end{pmatrix} \mid w, z \in \mathbb{C}\right\} \subset M_2(\mathbb{C}).$$

Then $||A||^2 = \det A$ defines a norm on $\mathbb{H} \cong \mathbb{R}^4$ and $SU(2)$ is the unit sphere in $\mathbb{H}$. If $A \in SU(2)$ and $X \in \mathbb{H}$ then $||AX|| = ||X||$ since $||A|| = 1$. So, after normalisation, usual integration of functions on S^3 defines a Haar measure on $SU(2)$.

Definition. Let $T = \left\{\begin{pmatrix} a & 0 \\ 0 & a^{-1}\end{pmatrix} \mid a \in \mathbb{C}, |a| = 1\right\} \cong S^1$, a *maximal torus* in $SU(2)$.

Also define $s = \begin{pmatrix} 0 & 1 \\ -1 & 0\end{pmatrix} \in SU(2)$

Lemma.
(i) if $t \in T$ then $sts^{-1} = t^{-1}$;
(ii) $s^2 = -I \in Z(SU(2))$
(iii) $N_{SU(2)}(T) = T \cup sT = \left\{\begin{pmatrix} a & 0 \\ 0 & a^{-1}\end{pmatrix}, \begin{pmatrix} 0 & a \\ -a^{-1} & 0\end{pmatrix} \mid a \in \mathbb{C}, |a| = 1\right\}$

Proof. All three parts follow from direct computation (exercise). □

Proposition.
(i) Every conjugacy class $\mathcal{O}$ in SU_2 contains an element of T.
(ii) More precisely. if $\mathcal{O}$ is a conjugacy class then $\mathcal{O} \cap T = \{t, t^{-1}\}$ for some $t \in T$ — $t = t^{-1}$ if and only if $t = \pm I$ when $\mathcal{O} = \{t\}$.
(iii) There is a bijection

$$\{\textit{conjugacy classes in } SU(2)\} \to [-1, 1]$$

given by $A \mapsto \frac{1}{2}\operatorname{tr} A$.

Proof. (i) For every unitary matrix A there is an orthonormal basis of eigenvectors of A; that is there is a unitary matrix P such that PAP^{-1} is diagonal. We want to arrange that $\det P = 1$. But we can replace P by $Q = \sqrt{\det P}P$. Thus every conjugacy class $\mathcal{O}$ in $SU(2)$ contains a diagonal matrix t. Since additionally $t \in SU(2)$, $t \in T$.

(ii) If $\pm I \in \mathcal{O}$ the result is clear.

Suppose $t \in \mathcal{O} \cap T$ for some $t \neq \pm I$. Then

$$\mathcal{O} = \{gtg^{-1} \mid g \in SU(2)\}.$$

We've seen before that $sts^{-1} = t^{-1}$ so $\mathcal{O} \cap T \supset \{t, t^{-1}\}$.

Conversely, if $t' \in \mathcal{O} \cap T$ then t' and t must have the same eigenvalues since they are conjugate. This suffices to see that $t' \in \{t^{\pm 1}\}$.

(iii) To see the given function is injective, suppose that $\frac{1}{2}\operatorname{tr} A = \frac{1}{2}\operatorname{tr} B$. Then since $\det A = \det B = 1$, A and B must have the same eigenvalues. By part (i) they are both diagonalisable and by the proof of part (ii) this suffices to see that they are conjugate.

To see that it is surjective notice that $\frac{1}{2}\operatorname{tr}\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta}\end{pmatrix} = \cos\theta$. Since $\cos\colon \mathbb{R} \to \mathbb{R}$ has image $[-1,1]$ the given function is surjective. $\square$

Let's write $\mathcal{O}_x = \{A \in SU(2) \mid \frac{1}{2}\operatorname{tr} A = x\}$ for $x \in [-1,1]$. We've proven that the $\mathcal{O}_x$ are the conjugacy classes in $SU(2)$. Clearly $\mathcal{O}_1 = \{I\}$ and $\mathcal{O}_{-1} = \{-I\}$.

Proposition. *If $-1 < x < 1$ then $\mathcal{O}_x$ is homeomorphic to S^2.*

Proof. First we observe that $\mathcal{O}_x \cong SU(2)/T$ for each $-1 < x < 1$. To see this it suffices to show that $T = C_{SU_2}\left(\begin{pmatrix}\lambda & 0 \\ 0 & \lambda^{-1}\end{pmatrix}\right)$ for $\lambda \neq \lambda^{-1}$. But

$$\begin{pmatrix} a & b \\ c & d\end{pmatrix}\begin{pmatrix}\lambda & 0 \\ 0 & \lambda^{-1}\end{pmatrix} = \begin{pmatrix}\lambda a & \lambda b \\ \lambda^{-1}c & \lambda^{-1}d\end{pmatrix}$$

and

$$\begin{pmatrix}\lambda & 0 \\ 0 & \lambda^{-1}\end{pmatrix}\begin{pmatrix} a & b \\ c & d\end{pmatrix} = \begin{pmatrix}\lambda a & \lambda^{-1}b \\ \lambda c & \lambda^{-1}d\end{pmatrix}.$$

For these to be equal for $\lambda \neq \lambda^{-1}$ we require $b = c = 0$.

Next we recall that $SU(2)$ acts on $S^2 \cong \mathbb{C} \cup \{\infty\}$ by Mobius transformations:

$$\begin{pmatrix} a & b \\ c & d\end{pmatrix} \cdot z = \frac{az+b}{cz+d}.$$

This action is transitive since for each $z \in \mathbb{C}$ there are $a, b \in \mathbb{C}$ such that $|a|^2 + |b|^2 = 1$ and $a/b = z$ (exercise). Then $\begin{pmatrix} a & -\overline{b} \\ b & \overline{a}\end{pmatrix} \cdot \infty = a/b$.

But $\operatorname{Stab}_{SU(2)}(\infty) = T$ so $SU(2)/T \cong S^2$. $\square$

8.2. **Representations of $SU(2)$.**

Now we understand the conjugacy classes of $SU(2)$, we'll try to work out its representation theory.

Let V_n be the complex vectorspace of homogeneous polynomials in two variables x, y. So $\dim V_n = n+1$. Then $GL(\mathbb{C}^2)$ acts on V_n via

$$\rho_n \colon GL(\mathbb{C}^2) \to GL(V_n)$$

given by

$$\rho_n\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) f(x,y) = f(ax+cy, bx+dy).$$

Examples.
$V_0 = \mathbb{C}$ has the trivial action.
$V_1 = \mathbb{C}^2$ is the standard representation of $GL(\mathbb{C}^2)$ on $\mathbb{C}^2$ with basis x, y.
$V_2 = \mathbb{C}^3$ has basis x^2, xy, y^2 then

$$\rho_2\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \begin{pmatrix} a^2 & ab & b^2 \\ 2ac & ad+bc & 2bd \\ c^2 & cd & d^2 \end{pmatrix}$$

Since $SU(2)$ is a subgroup of $GL_2(\mathbb{C})$ we can view V_n as a representation of $SU(2)$ by restriction. In fact as we'll see, the V_n are all irreducible reps of $SU(2)$ and every irreducible rep of $SU(2)$ is isomorphic to one of these.

Lemma. *A (continuous) class function $f\colon SU(2) \to \mathbb{C}$ is determined by its restriction to T and $f|_T$ is even ie* $f\left(\begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix}\right) = f\left(\begin{pmatrix} z^{-1} & 0 \\ 0 & z \end{pmatrix}\right)$.

Proof. We've seen that each conjugacy class in $SU(2)$ meets T and so a class fucntion is determined by its restriction to T. Then evenness follows from the additional fact that $T \cap \mathcal{O} = \{t^{\pm 1}\}$ for some $t \in T$. □

Thus we can view the character of a representation ρ of $SU(2)$ as an even function $\chi_\rho\colon S^1 \to \mathbb{C}$.

Lemma. *If χ is a character of a representation of $SU(2)$ then $\chi|_T$ is a Laurent polynomial ie a finite $\mathbb{N}$ linear combination of functions*

$$\begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix} \mapsto z^n \text{ for } n \in \mathbb{Z}.$$

Proof. If V is a representation of $SU(2)$ then $\operatorname{Res}_T^{SU(2)} V$ is a representation of T and $\chi_{\operatorname{Res}_T V}$ is the restriction of χ_V to T. But we've proven already that every representation of T has character of the given form. □

Lecture 20

Write

$$\mathbb{N}[z, z^{-1}] := \left\{ \sum_{n \in \mathbb{Z}} a_n z^n \mid a_n \in \mathbb{N} \text{ and only finitely many } a_n \neq 0 \right\}$$

and

$$\mathbb{N}[z, z^{-1}]^{ev} = \{ f \in \mathbb{N}[z, z^{-1}] \mid f(z) = f(z^{-1}) \}.$$

We showed last time that for every continuous representation V of $SU(2)$, the character $\chi_V \in \mathbb{N}[z, z^{-1}]^{ev}$ after identifying it with its restriction to T.

The next thing to do is compute the character χ_n of (ρ_n, V_n), the representation consisting of degree n homogeneous polynomials in x and y.

$$\rho_n\left(\begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix}\right)(x^i y^j) = (zx)^i (z^{-1}y)^j = z^{i-j} x^i y^j.$$

So x^iy^j is an eigenvector for each $t \in T$ and T acts on V_n via

$$\rho_n\left(\begin{pmatrix} z & 0 \\ 0 & z^{-1}\end{pmatrix}\right) = \begin{pmatrix} z^n & & & & & \\ & z^{n-2} & & & & \\ & & z^{n-4} & & & \\ & & & \ddots & & \\ & & & & z^{2-n} & \\ & & & & & z^{-n}\end{pmatrix}.$$

Thus

$$\chi_n\left(\begin{pmatrix} z & 0 \\ 0 & z^{-1}\end{pmatrix}\right) = z^n + z^{n-2} + \cdots + z^{2-n} + z^{-n} = \frac{z^{n+1} - z^{-(n+1)}}{z - z^{-1}} \in \mathbb{N}[z, z^{-1}]^{ev}.$$

Theorem. *V_n is irreducible as a reperesentation of $SU(2)$.*

Proof. Let $0 \neq W \leqslant V_n$ be a $SU(2)$-invariant subspace. We want to show that $W = V_n$.

Let $0 \neq w = \sum \lambda_i(x^{n-i}y^i) \in W$. We claim that $x^{n-i}y^i \in W$ whenever $\lambda_i \neq 0$.

We prove the claim by induction on $k = |\{i \mid \lambda_i \neq 0\}|$.

If $k = 1$ then w is a non-zero scalar multiple of $x^{n-i}y^i$ and we're done.

If $k > 1$ choose i such that $\lambda_i \neq 0$ and $z \in S^1$ such that $\{z^n, z^{n-2}, \ldots, z^{2-n}, z^n\}$ are distict complex numbers. Then

$$\rho_n\left(\begin{pmatrix} z & 0 \\ 0 & z^{-1}\end{pmatrix}\right) w - z^{n-2i}w = \sum \lambda_j(z^{n-2j} - z^{n-2i})(x^{n-j}y^j) \in W$$

since W is $SU(2)$-invariant. Now $\lambda_j(z^{n-2j} - z^{n-2i}) \neq 0$ precisely if $\lambda_j \neq 0$ and $j \neq i$. Thus by the induction hypothesis $x^jy^{n-j} \in W$ for all $j \neq i$ with $\lambda_j \neq 0$. It follows that also $x^iy^{n-i} = \frac{1}{\lambda_i}(w - \sum_{j\neq i} \lambda_j x^jy^{n-j}) \in W$ as required.

Now we know that $x^iy^{n-i} \in W$ for some i. Since

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1\end{pmatrix} x^iy^{n-i} = \frac{1}{\sqrt{2}}((x-y)^i(x+y)^{n-i}) \in W$$

we can use the claim to deduce that $x^n \in W$. Repeating the same calculation for $i = n$, we see that $(x+y)^n \in W$ and so, by the claim again, $x^iy^{n-i} \in W$ for all i.

Thus $W = V_n$. $\square$

Alternative proof:

We can identify $\mathcal{O}_{\cos\theta} = \{A \in SU(2) \mid \frac{1}{2}\operatorname{tr} A = \cos\theta\}$ with the two-sphere $\{(\mathrm{Im}(a))^2 + |b|^2 = \sin^2\theta\}$ of radius $|\sin\theta|$. Thus if f is a class-function on $SU(2)$, since f is constant on each $\mathcal{O}_{\cos\theta}$,

$$\int_{SU(2)} f(g)\,\mathrm{d}g = \frac{1}{2\pi^2}\int_0^{2\pi}\frac{1}{2}f\left(\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta}\end{pmatrix}\right)4\pi\sin^2\theta\,\mathrm{d}\theta = \frac{1}{\pi}\int_0^{2\pi} f(e^{i\theta})\sin^2\theta\,\mathrm{d}\theta.$$

Note this is normalised correctly, since $\frac{1}{\pi}\int_0^{2\pi}\sin^2\theta\,\mathrm{d}\theta = 1$. So it suffices to prove that $\frac{1}{\pi}\int_0^{2\pi}|\chi_{V_n}(e^{i\theta})|^2\sin^2\theta\,\mathrm{d}\theta = 1$ for $z = e^{i\theta}$. (exercise: verify this).

Theorem. *Every irreducible representation of $SU(2)$ is isomorphic to V_n for some $n \geqslant 0$.*

Proof. Let V be an irreducible representation of $SU(2)$ so $\chi_V \in \mathbb{N}[z, z^{-1}]^{ev}$. Now $\chi_0 = 1, \chi_1 = z + z^{-1}, \chi_2 = z^2 + 1 + z^{-2}, \ldots$ form a basis of $\mathbb{Q}[z, z^{-1}]^{ev}$ as (non-f.d.) $\mathbb{Q}$-vector spaces. Thus $\chi_V = \sum a_i\chi_i$ for some $a_i \in \mathbb{Q}$, only finitely many non-zero.

Clearing denominators and moving negative terms to the left-hand-side, we get a formula

$$m\chi_V + \sum_{i\in I} m_i\chi_i = \sum_{j\in J} m_j\chi_j$$

for some disjoint finite subsets $I, J \subset \mathbb{N}$ and $m, m_i \in \mathbb{N}$. By orthogonality of characters and complete reducibility we obtain

$$mV \oplus \bigoplus_{i\in I} m_iV_i \cong \bigoplus_{j\in J} m_jV_j$$

since V is irreducible, $V \cong V_j$ some $j \in J$. □

8.3. **Tensor products of representations of $SU(2)$.** We've seen that if V, W are representations of $SU(2)$ such that $\mathrm{Res}_T^{SU(2)} V \cong \mathrm{Res}_T^{SU(2)} W$ then $V \cong W$. We want to understand $\otimes$ for representations of $SU(2)$.

Proposition. *If $G \cong SU(2)$ or S^1 and V, W are representations of G then*

$$\chi_{V\otimes W} = \chi_V \cdot \chi_W.$$

Proof. By the discussion above we only need to consider $G \cong S^1$.

If V and W have eigenbases $e_1, \ldots, e_n$ and $f_1, \ldots, f_m$ such that $ze_i = z^{n_i}e_i$ and $zf_j = z^{m_j}f_j$ then $z(e_i \otimes f_j) = z^{n_i+m_j}(e_i \otimes f_j)$. So

$$\chi_{V\otimes W}(z) = \sum_{i,j} z^{n_i+m_j} = \left(\sum_i z^{n_i}\right)\left(\sum_j z^{m_j}\right) = \chi_V(z)\chi_W(z)$$

as required. □

Let's compute some examples for $SU(2)$:

$$\chi_{V_1\otimes V_1}(z) = (z + z^{-1})^2 = z^2 + 1 + z^{-2} + 1 = \chi_{V_2} + \chi_{V_0}$$

and

$$\chi_{V_2\otimes V_1}(z) = (z^2 + 1 + z^{-2})(z + z^{-1}) = z^3 + 2z + 2z^{-1} + z^{-3} = \chi_{V_3} + \chi_{V_1}.$$

Proposition (Clebsch–Gordan rule)**.** *For $n, m \in \mathbb{N}$,*

$$V_n \otimes V_m \cong V_{n+m} \oplus V_{n+m-2} \oplus \cdots \oplus V_{|n-m|+2} \oplus V_{|n-m|}.$$

Proof. Without loss of generality, $n \geqslant m$. Then

$$\begin{aligned}
(\chi_n \cdot \chi_m)(z) &= \frac{z^{n+1} - z^{-n-1}}{z - z^{-1}} \cdot (z^m + z^{m-2} + \cdots + z^{-m}) \\
&= \sum_{j=0}^{m} \frac{z^{n+m+1-2j} - z^{-(n+m+1-2j)}}{z - z^{-1}} \\
&= \sum_{j=0}^{m} \chi_{n+m-2j}(z)
\end{aligned}$$

□

8.4. **Representations of $SO(3)$.**

Proposition. *There is an isomorphism of topological groups $SU(2)/\{\pm I\} \cong SO(3)$.*

Corollary. *Every irreducible representation of $SO(3)$ is of the form V_{2n} for some $n \geqslant 0$.*

Proof. It follows from the Proposition that irreducible representations of $SO(3)$ correspond to irreducible representations of $SU(2)$ such that $-I$ acts trivially. But we saw before that $-I$ acts on V_n as -1 when n is odd and as 1 when n is even. $\square$

LECTURE 21

Let's prove the proposition from the end of last time:

Proposition. *There is an isomorphism of topological groups $SU(2)/\{\pm I\} \cong SO(3)$.*

Proof. Consider $\mathbb{H}^\circ = \{A \in \mathbb{H} \mid \operatorname{tr} A = 0\} = \mathbb{R}\langle \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \rangle$ equipped with the norm $||A||^2 = \det A$.

$SU(2)$ acts by isometries on $\mathbb{H}^\circ$ via $(X, A) \mapsto XAX^{-1}$ giving a group homomorphism

$$\phi\colon SU(2) \to O(3)$$

with kernel $Z(SU(2)) = \{\pm I\}$. Since $SU(2)$ is compact and $O(3)$ is Hausdorff the continuous group isomorphism $\bar{\phi}\colon SU(2)/\{\pm I\} \to \mathrm{Im}\phi$ is a homeomorphism so it suffices to prove that $\mathrm{Im}\phi = SO(3)$. Since $SU(2)$ is connected, $\mathrm{Im}\phi \subset SO(3)$.

Now

$$\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} \begin{pmatrix} ai & b \\ -\bar{b} & -ai \end{pmatrix} \begin{pmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix} = \begin{pmatrix} ai & e^{2i\theta}b \\ -e^{-i\theta}\bar{b} & -ai \end{pmatrix}$$

so $\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}$ acts on $\mathbb{R}\langle \mathbf{i}, \mathbf{j}, \mathbf{k} \rangle$ by rotation in the $\mathbf{jk}$-plane through an angle 2θ.

Exercise. Show that $\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$ acts by rotation through 2θ in the $\mathbf{ik}$-plane, and $\begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix}$ acts by rotation through 2θ in the $\mathbf{ij}$-plane. Deduce that $\mathrm{Im}\theta = SO(3)$.

$\square$

9. CHARACTER TABLE OF $GL_2(\mathbb{F}_q)$ AND RELATED GROUPS

9.1. $\mathbb{F}_q$**.** Let $p > 2$ be a prime, $q = p^a$ a power of p for some $a > 0$, and $\mathbb{F}_q$ be the field with q elements. We know that $\mathbb{F}_q^\times \cong C_{q-1}$.

Notice that $\mathbb{F}_q^\times \to \mathbb{F}_q^\times; x \mapsto x^2$ is a group homomorphism with kernel ± 1. Thus half the elements of $\mathbb{F}_q^\times$ are squares and half are not. Let $\epsilon \in \mathbb{F}_q^\times$ be a fixed non-square and let $\mathbb{F}_{q^2} := \{a + b\sqrt{\epsilon} \mid a, b \in \mathbb{F}_p\}$, the field with q elements under the obvious operations.

Every element of $\mathbb{F}_q$ has a square root in $\mathbb{F}_{q^2}$ since if λ is non-square then $\lambda/\epsilon = \mu^2$ is a square, and $(\sqrt{\epsilon}\mu)^2 = \lambda$. It follows by completing the square that every quadratic polynomial in $\mathbb{F}_q$ factorizes in $\mathbb{F}_{q^2}$.

Notice that $(a + b\sqrt{\epsilon})^q = a^q + b^q \epsilon^{\frac{q-1}{2}} \sqrt{\epsilon} = (a - b\sqrt{\epsilon})$. Thus the roots of an irreducible quadratic over $\mathbb{F}_q$ are of the form λ, λ^q.

9.2. $GL_2(\mathbb{F}_q)$. We want to compute the character table of the group

$$G := GL_2(\mathbb{F}_q) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{F}_q \text{ and } ad - bc \neq 0 \right\}.$$

The order of G is the number of bases for $\mathbb{F}_q^2$ over $\mathbb{F}_q$. This is $(q^2-1)(q^2-q)$.

First, we compute the conjugacy classes in G. We know from linear algebra that 2×2-matrices are determined by their minimal polynomials up to conjugation. By Cayley–Hamilton each element A of $GL_2(\mathbb{F}_q)$ has minimal polynomial $m_A(X)$ of degree at most 2 and $m_A(0) \neq 0$.

There are four cases.

Case 1: $m_A = X - \lambda$ for some $\lambda \in {\mathbb{F}_q}^\times$. Then $A = \lambda I$. So $C_G(A) = G$, and A lives in a conjugacy class of size 1. There are $q-1$ such classes.

Case 2: $m_A = (X-\lambda)^2$ for some $\lambda \in {\mathbb{F}_q}^\times$ so A is conjugate to $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$. Now

$$C_G\left(\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}\right) = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a,b \in \mathbb{F}_q, a \neq 0 \right\}$$

so $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ is in a conjugacy class of order $\frac{q(q-1)(q^2-1)}{(q-1)q} = q^2-1$. There are $q-1$ such classes.

Case 3: A has minimal polynomial $(X-\lambda)(X-\mu)$ for some distinct $\lambda, \mu \in {\mathbb{F}_q}^\times$. Then A is conjugate to $\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ and to $\begin{pmatrix} \mu & 0 \\ 0 & \lambda \end{pmatrix}$. Moreover

$$C_G\left(\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}\right) = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a,d \in \mathbb{F}_q^\times \right\} =: T.$$

So $\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ is in a conjugacy class of order $\frac{q(q-1)(q^2-1)}{(q-1)^2} = q(q+1)$. There are $\binom{q-1}{2}$ such classes.

Case 4: A has minimal polynomial $(X-\alpha)(X-\alpha^q)$, $\alpha = \lambda + \mu\sqrt{\epsilon}$, $\lambda, \mu \in \mathbb{F}_q$, $\mu \neq 0$. Then A is conjugate to $\begin{pmatrix} \lambda & \epsilon\mu \\ \mu & \lambda \end{pmatrix}$ and $\begin{pmatrix} \lambda & -\epsilon\mu \\ -\mu & \lambda \end{pmatrix}$. Now

$$C_G\left(\begin{pmatrix} \lambda & \epsilon\mu \\ \mu & \lambda \end{pmatrix}\right) = \left\{ \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix} \mid a^2 - \epsilon b^2 \neq 0 \right\} =: K.$$

If $a^2 = \epsilon b^2$ then ϵ is a square or $a = b = 0$. So $|K| = q^2 - 1$ and $\begin{pmatrix} \lambda & \epsilon\mu \\ \mu & \lambda \end{pmatrix}$ lives in a conjugacy class of size $\frac{q(q-1)(q^2-1)}{q^2-1} = q(q-1)$. There are $q(q-1)/2$ such classes. In summary

Representative	C_G	No of elts	No of such classes
$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$	G	1	$q-1$
$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$	$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$	q^2-1	$q-1$
$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$	T	$q(q+1)$	$\binom{q-1}{2}$
$\begin{pmatrix} \lambda & \epsilon\mu \\ \mu & \lambda \end{pmatrix}$	K	$q(q-1)$	$\binom{q}{2}$

The groups T and K are both *maximal tori*. That is they are maximal subgroups of G subject to the fact that they are conjugate to a subgroup of the group of diagonal matrices over some field extension. T is called *split* and K is called *non-split*.

Some other important subgroups of G are Z which is the subgroup of scalar matrices (the centre). $N := \left\{\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix} \mid b\in\mathbb{F}_q\right\}$ a Sylow p-subgroup of G and $B := \left\{\begin{pmatrix}a & b\\ 0 & d\end{pmatrix} \mid b\in\mathbb{F}_q, a,d\in{\mathbb{F}_q}^\times\right\}$ a *Borel subgroup* of G. Then N is normal in B and $B/N\cong {\mathbb{F}_q}^\times\times{\mathbb{F}_q}^\times\cong C_{q-1}\times C_{q-1}$.

G acts transitively on $\mathbb{F}_q\cup\{\infty\}$ via Mobius transformations

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}(z) = \frac{az+b}{cz+d} \text{ for } z\in\mathbb{F}_q$$

and

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}(\infty) = a/c$$

so $B = \mathrm{Stab}_G(\infty)$. Thus $|G| = |B|(q+1)$.

Writing $s = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ we see that

$$\begin{pmatrix}a & b\\ 0 & d\end{pmatrix} s \begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix} = \begin{pmatrix}b & a+b\beta\\ d & \beta d\end{pmatrix}$$

and these elements are all distinct. Hence BsN contains $q|B|$ elements so must be $G\backslash B$. Thus $BsN = BsB$ and $B\backslash G/B$ has two double cosets B and BsB (this is called Bruhat decomposition).

Lecture 22

Recall our notation from last time. $G = GL_2(\mathbb{F}_q) \geqslant B = \left\{\begin{pmatrix}a & b\\ 0 & d\end{pmatrix}\right\}$ has normal subgroup $N = \left\{\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}\right\}$.

Then $Z = Z(G) = \left\{\begin{pmatrix}a & 0\\ 0 & a\end{pmatrix}\right\}$, $T = \left\{\begin{pmatrix}a & 0\\ 0 & d\end{pmatrix}\right\}$, $K = \left\{\begin{pmatrix}x & \epsilon y\\ y & x\end{pmatrix}\right\}$ for some fixed non-square ϵ in $\mathbb{F}_q$.

Finally $s = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ and $G = B\cup BsB$.

By Mackey's irreduciblity criterion it follows that if W is an irreducible representation of B, then $\mathrm{Ind}_B^G W$ is an irreducible representation of G precisely if $\mathrm{Res}^B_{B\cap {}^sB} W$ and $\mathrm{Res}^{{}^sB}_{B\cap {}^sB}\, {}^sW$ have no irreducible factors in common. Since s swaps $0,\infty\in\mathbb{F}_q\cup\{\infty\}$,

$${}^sB = \mathrm{Stab}_G(0) = \left\{\begin{pmatrix}a & 0\\ c & d\end{pmatrix} \mid a,d\in{\mathbb{F}_q}^\times, c\in\mathbb{F}_q\right\}$$

and $B\cap {}^sB = T$.

The conjugacy classes in $GL_2(\mathbb{F}_q)$ are

Representative	C_G	No of elts	No of such classes
$\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix}$	G	1	$q-1$
$\begin{pmatrix}\lambda & 1\\ 0 & \lambda\end{pmatrix}$	ZN	q^2-1	$q-1$
$\begin{pmatrix}\lambda & 0\\ 0 & \mu\end{pmatrix}$	T	$q(q+1)$	$\binom{q-1}{2}$
$\begin{pmatrix}\lambda & \epsilon\mu\\ \mu & \lambda\end{pmatrix}$	K	$q(q-1)$	$\binom{q}{2}$

Let's warm ourselves up by computing the character table of B.

If $x, y \in B$ are conjugate in G then because $G = B \cup BsB$ either x is conjugate to y in B or x is conjugate to sys^{-1} (or both). So classes in G split into at most two pieces when restricted to B.

The conjugacy classes in B are

Representative	C_B	No of elts	No of such classes
$\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix}$	B	1	$q-1$
$\begin{pmatrix}\lambda & 1\\ 0 & \lambda\end{pmatrix}$	ZN	$q-1$	$q-1$
$\begin{pmatrix}\lambda & 0\\ 0 & \mu\end{pmatrix}$	T	q	$(q-1)(q-2)$

Now $B/N \cong T \cong {\mathbb{F}_q}^\times \times {\mathbb{F}_q}^\times$. So if $\Theta_q := \{\text{characters of } \mathbb{F}_q^\times \text{ of degree } 1\}$, then Θ_q is a cyclic group of order $q-1$ under pointwise operations. Moreover, for each pair $\theta, \phi \in \Theta_q$, we have a 1-dimensional representation of B given by

$$\chi_{\theta,\phi}\left(\begin{pmatrix}a & b\\ 0 & d\end{pmatrix}\right) = \theta(a)\phi(d)$$

giving $(q-1)^2$ linear reps.

Fix γ a non-trivial 1-dimensional representation of $(\mathbb{F}_q, +)$. Then for each $\theta \in \Theta_q$ we can define a 1-dimensional representation of ZN by

$$\rho_\theta\left(\begin{pmatrix}a & b\\ 0 & a\end{pmatrix}\right) = \theta(a)\gamma(b).$$

Defining μ_θ to be the character of $\operatorname{Ind}_{ZN}^B \rho_\theta$ we see that

$$\begin{aligned}
\mu_\theta\left(\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix}\right) &= (q-1)\theta(\lambda),\\
\mu_\theta\left(\begin{pmatrix}\lambda & 1\\ 0 & \lambda\end{pmatrix}\right) &= \sum_{b\in{\mathbb{F}_q}^\times} \theta(\lambda)\gamma(b)\\
&= \theta(\lambda)(q\langle \mathbf{1}, \gamma\rangle_{\mathbb{F}_q} - 1)\\
&= -\theta(\lambda)\\
\mu_\theta\left(\begin{pmatrix}\lambda & 0\\ 0 & \mu\end{pmatrix}\right) &= 0
\end{aligned}$$

So $\langle \mu_\theta, \mu_\theta \rangle = \frac{1}{q(q-1)^2}\left((q-1)(q-1)^2 + (q-1)(q-1)1\right) = 1$ and the character table of B is

	$\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix}$	$\begin{pmatrix}\lambda & 1\\ 0 & \lambda\end{pmatrix}$	$\begin{pmatrix}\lambda & 0\\ 0 & \mu\end{pmatrix}$
$\chi_{\theta,\phi}$	$\theta(\lambda)\phi(\lambda)$	$\theta(\lambda)\phi(\lambda)$	$\theta(\lambda)\phi(\mu)$
μ_θ	$(q-1)\theta(\lambda)$	$-\theta(\lambda)$	0

Let's start computing some representations of G.

As $\det\colon G \to \mathbb{F}_q^\times$ is a surjective group homomorphism, for each $i = 0, \ldots, q-2$, $\chi_i := \theta_i \circ \det$ is a 1-dimensional representation of G.

Let's start by inducing $\chi_{\theta,\phi}$ from B to G. Notice that

$$^s\chi_{\theta,\phi}\left(\begin{pmatrix}\lambda & 0\\ c & d\end{pmatrix}\right) = \chi_{\theta,\phi}\left(\begin{pmatrix}d & 0\\ c & a\end{pmatrix}\right) = \theta(d)\phi(a)$$

and so $\operatorname{Res}^{^sB}_T {}^s\chi_{\theta,\phi} = \operatorname{Res}^B_T \chi_{\theta,\phi}$ if and only if $\theta = \phi$. So $W_{\theta,\phi} := \operatorname{Ind}^G_B \chi_{\theta,\phi}$ is irreducible precisely if $\theta \neq \phi$.

Now

$$\begin{aligned}
\chi_{W_{\theta,\phi}}\left(\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix}\right) &= (q+1)\theta(\lambda)\phi(\lambda),\\
\chi_{W_{\theta,\phi}}\left(\begin{pmatrix}\lambda & 1\\ 0 & \lambda\end{pmatrix}\right) &= \theta(\lambda)\phi(\lambda),\\
\chi_{W_{\theta,\phi}}\left(\begin{pmatrix}\lambda & 0\\ 0 & \mu\end{pmatrix}\right) &= \theta(\lambda)\phi(\mu) + \phi(\lambda)\theta(\mu) \text{ and}\\
\chi_{W_{\theta,\phi}}\left(\begin{pmatrix}\lambda & \epsilon\mu\\ \mu & \lambda\end{pmatrix}\right) &= 0.
\end{aligned}$$

Notice that $W_{\theta,\phi} \cong W_{\phi,\theta}$ so we get $\binom{q-1}{2}$ irreducible representations in this way. They are known as *principal series representations*.

We consider also $W_{\mathbf{1},\mathbf{1}} \cong \operatorname{Ind}^G_B \mathbf{1} = \mathbb{C}(\mathbb{F}_q \cup \{\infty\})$. Since G acts 2-transitively on $\mathbb{F}_q \cup \infty$, $W_{\mathbf{1},\mathbf{1}}$ decomposes as $\mathbf{1} \oplus V_{\mathbf{1}}$, with $V_{\mathbf{1}}$ irreducible of degree q. This representation is known as the *Steinberg representation.*

By tensoring $W_{\mathbf{1},\mathbf{1}}$ by χ_θ we also obtain $W_{\theta,\theta} \cong \chi_\theta \oplus V_\theta$ with V_θ irreducible of degree q.

So far we have

	$\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix}$	$\begin{pmatrix}\lambda & 1\\ 0 & \lambda\end{pmatrix}$	$\begin{pmatrix}\lambda & 0\\ 0 & \mu\end{pmatrix}$	$\begin{pmatrix}\lambda & \epsilon\mu\\ \mu & \lambda\end{pmatrix}$	# of reps
χ_θ	$\theta(\lambda)^2$	$\theta(\lambda)^2$	$\theta(\lambda)\theta(\mu)$	$\theta(\lambda^2 - \epsilon\mu^2)$	$q-1$
V_θ	$q\theta(\lambda)^2$	0	$\theta(\lambda)\theta(\mu)$	$-\theta(\lambda^2 - \epsilon\mu^2)$	$q-1$
$W_{\theta,\phi}$	$(q+1)\theta(\lambda)\phi(\lambda)$	$\theta(\lambda)\phi(\lambda)$	$\theta(\lambda)\phi(\mu) + \phi(\lambda)\theta(\mu)$	0	$\frac{(q-1)(q-2)}{2}$

Lecture 23

The next natural thing to do is compute $\operatorname{Ind}_B^G \mu_i$. It has character given by

$$\begin{aligned}
\operatorname{Ind}_B^G \mu_i \left(\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}\right) =& (q+1)(q-1)\theta_i(\lambda), \\
\operatorname{Ind}_B^G \mu_i \left(\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}\right) =& -\theta_i(\lambda), \\
\operatorname{Ind}_B^G \mu_i \left(\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}\right) =& 0 \text{ and} \\
\operatorname{Ind}_B^G \mu_i \left(\begin{pmatrix} \lambda & \epsilon\mu \\ \mu & \lambda \end{pmatrix}\right) =& 0.
\end{aligned}$$

Thus

$$\begin{aligned}
\langle \operatorname{Ind}_B^G \mu_i, \operatorname{Ind}_B^G \mu_i \rangle =& \frac{1}{|G|}\left((q+1)^2(q-1)^2(q-1) + (q-1)(q^2-1)\right) \\
& \frac{1}{q}\left(q^2-1)+1\right) = q
\end{aligned}$$

so $\operatorname{Ind}_B^G \mu_i$ has many irreducible factors.

Our next strategy is to induce characters from K. We write $\alpha = \lambda + \mu\sqrt{\epsilon}$ for the matrix $\begin{pmatrix} \lambda & \epsilon\mu \\ \mu & \lambda \end{pmatrix}$. Notice that $Z \leqslant K$ with $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} = \lambda$ in our new notation.

Suppose that $\varphi\colon K \to \mathbb{C}^\times$ is a 1-dimensional character of K. Then $\Phi := \operatorname{Ind}_K^G \varphi$ has character given by $\Phi(\lambda) = q(q-1)\varphi(\lambda)$, $\Phi(\alpha) = \varphi(\alpha) + \varphi(\alpha^q)$ for $\alpha \in \mathbb{F}_{q^2}^\times$ and $\Phi = 0$ away from these conjugacy classes.

Let's compute

$$\langle \Phi, \Phi \rangle = \frac{1}{|G|}\left((q-1)q^2(q-1)^2 + \frac{q(q-1)}{2}\sum_{\nu \in K\setminus Z} |\varphi(\nu) + \varphi(\nu^q)|^2\right)$$

But

$$\begin{aligned}
\sum |\varphi(\nu) + \varphi(\nu^q)|^2 &= \sum_{\nu \in K\setminus Z} (\varphi(\nu) + \varphi(\nu^q)\left(\varphi(\nu^{-1}) + \varphi(\nu^{-q})\right) \\
&= \sum_{\nu \in K\setminus Z} \left(2 + \varphi(\nu^{q-1}) + \varphi(\nu^{1-q})\right) \\
&= 2(q^2-q) + 2\sum_{\nu \in K} \varphi^{q-1}(\nu) - 2\sum_{\lambda \in Z} \varphi(\lambda^{q-1})
\end{aligned}$$

But if $\varphi^{q-1} \neq \mathbf{1}$ then the middle term in the last sum is 0 since $\langle \varphi^{q-1}, \mathbf{1} \rangle = 0$. Since $\lambda^{q-1} = 1$ for $\lambda \in \mathbb{F}_q$ the third term is also easy to compute. Putting this together we get $\langle \Phi, \Phi \rangle = q - 1$ when $\varphi^{q-1} \neq \mathbf{1}$.

We similarly compute

$$\begin{aligned}\langle \operatorname{Ind}_B^G \mu_\theta, \Phi\rangle &= \frac{1}{|G|}\sum_{\lambda\in Z}(q^2-1)\overline{\theta(\lambda)}q(q-1)\varphi(\lambda)\\ &= (q-1)\langle \theta, \operatorname{Res}_Z^K \varphi\rangle_Z\end{aligned}$$

Thus $\operatorname{Ind}_B^G \mu_\theta$ and Φ have many factors in common when $\phi|_Z = \theta$.

Now, for each φ such that $\varphi^{q-1} \neq \mathbf{1}$ (there are q^2-q such choices) let $\theta := \operatorname{Res}_Z^K \varphi$ then our calculations tell us that if $\beta_\varphi = \operatorname{Ind}_B^G \mu_\theta - \Phi \in R(G)$ then

$$\langle \beta_\varphi, \beta_\varphi\rangle = q - 2(q-1) + (q-1) = 1.$$

Since also $\beta_\varphi(1) = q-1 > 0$ it follows that β_φ is an irreducible character. Since $\beta_\varphi = \beta_{\varphi^q}$ (and $\varphi^{q^2} = \varphi$) we get $\binom{q}{2}$ characters in this way and the character table of $GL_2(\mathbb{F}_q)$ is complete.

# classes	$q-1$	$q-1$	$\binom{q-1}{2}$	$\binom{q}{2}$	
rep	$\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix}$	$\begin{pmatrix}\lambda & 1\\ 0 & \lambda\end{pmatrix}$	$\begin{pmatrix}\lambda & 0\\ 0 & \mu\end{pmatrix}$	α, α^q	# of reps
χ_θ	$\theta(\lambda)^2$	$\theta(\lambda)^2$	$\theta(\lambda)\theta(\mu)$	$\theta(\alpha^{q+1})$	$q-1$
V_θ	$q\theta(\lambda)^2$	0	$\theta(\lambda)\theta(\mu)$	$-\theta(\alpha^{q+1})$	$q-1$
$W_{\theta,\phi}$	$(q+1)\theta(\lambda)\phi(\lambda)$	$\theta(\lambda)\phi(\lambda)$	$\theta(\lambda)\phi(\mu)+\theta(\lambda)\phi(\mu)$	0	$\binom{q-1}{2}$
β_φ	$(q-1)\varphi(\lambda)$	$-\varphi(\lambda)$	0	$-(\varphi+\varphi^q)(\alpha)$	$\binom{q}{2}$