PMATH 745: REPRESENTATION THEORY OF FINITE GROUPS

HEESUNG YANG

1. September 8: Review and quick definitions

In this section we review classical linear algebra and introduce the notion of representation.
N.B. Unless otherwise specified, all the vector spaces will be over $\mathbb{C}$.

Definition 1. Let V be a $\mathbb{C}$-vector space.

(i) A *linear operator* φ on V is a linear map $\varphi : V \to V$.
(ii) We define $\mathrm{GL}(V)$ to be the set of invertible linear operators on V.
(iii) We define $\mathrm{GL}_n(\mathbb{C})$ be the set of invertible $n \times n$ matrices over $\mathbb{C}$.

Proposition 2. *Let V be a $\mathbb{C}$-vector space.*

(i) If $\dim_{\mathbb{C}} V = n$, then $V \cong \mathbb{C}^n$.
(ii) If $\mathscr{B} = \{b_1, b_2, \dots, b_n\}$ is a basis for V and $v \in V$, then there exist a unique $(z_1, \dots, z_n) \in \mathbb{C}^n$ so that $v = z_1 b_1 + z_2 b_2 + \cdots + z_n b_n$.
(iii) If $f_{\mathscr{B}} : V \to \mathbb{C}^n$ is defined by $f_{\mathscr{B}}(v) = [v]_{\mathscr{B}} = (z_1, z_2, \dots, z_n)$, then $f_{\mathscr{B}}$ is a vector space isomorphism, and every isomorphism $V \cong \mathbb{C}^n$ is of this form.

Suppose that $h : V \cong W$ is an isomorphism (as vector spaces). Then h "lifts" in a natural way to an isomorphism $h^* : \mathrm{GL}(V) \to \mathrm{GL}(W)$. Note that, if $f \in \mathrm{GL}(V)$ and $g \in \mathrm{GL}(W)$ and $h^*(f) = g$, then the diagram

$$\begin{array}{ccc} V & \xrightarrow{h} & W \\ {\scriptstyle f}\uparrow & & \downarrow{\scriptstyle g} \\ V & \xleftarrow[h^{-1}]{} & W \end{array}$$

must commute, hence $h^*(f) = h \circ f \circ h^{-1}$.

Proposition 3. *h^* is a group isomorphism.*

Proof. To prove that h^* is bijective, it suffices to find an inverse for each element $g \in \mathrm{GL}(W)$. The commutative diagram above implies that $h^{-1} \circ g \circ h \in \mathrm{GL}(V)$ is the inverse: indeed, we have $h^*(h^{-1} \circ g \circ h) = h \circ (h^{-1} \circ g \circ h) \circ h^{-1} = g$. To show that h^* is a group homomorphism, note that $h^*(f) \circ h^*(g) = (h^{-1} \circ f \circ h) \circ (h^{-1} \circ g \circ h) = h^{-1} \circ (f \circ g) \circ h = h^*(f \circ g)$, as required. $\square$

Date: 17 April 2016.

Corollary 1. *If* $\dim(V) = n$, *then* $\mathrm{GL}(V) \cong \mathrm{GL}(\mathbb{C}^n)$.

Proof. Apply Proposition 3 and the fact that $V \cong \mathbb{C}^n$. $\square$

Recall the correspondence between linear operators on V and n-by-n matrices over $\mathbb{C}$ (classical linear algebra fact!). Given an $n \times n$ matrix $M \in \mathrm{M}_n(\mathbb{C})$, define $L_M : \mathbb{C}^n \to \mathbb{C}^n$ be the linear operator represented by the matrix M (with respect to the standard basis, WLOG), i.e., $L_M(v) = Mv$. Recall also that L_M is linear and invertible if and only if M is an invertible matrix. Note that, to show that $\mathrm{GL}_n(\mathbb{C}) \cong V$ for any V with $\dim_{\mathbb{C}} V = n$, we need to have $\mathrm{GL}_n(\mathbb{C}) \cong \mathrm{GL}(\mathbb{C}^n)$. And this relationship between the linear operators and the matrices gives us the group isomorphism we are looking for.

Proposition 4. *Let* $L : \mathrm{GL}_n(\mathbb{C}) \to \mathrm{GL}(\mathbb{C}^n)$ *be the map defined as* $M \mapsto L_M$. *Then* L *is a group isomorphism from* $\mathrm{GL}_n(\mathbb{C})$ *to* $\mathrm{GL}(\mathbb{C}^n)$.

Proof. First we show that L is bijective by explicitly constructing its inverse, L^{-1}. Let $\mathscr{E} = \{e_1, e_2, \ldots, e_n\}$ be the standard basis of $\mathbb{C}^n$. Given $f \in \mathrm{GL}(\mathbb{C}^n)$, we define

$$M_f := \begin{pmatrix} \uparrow & \uparrow & \uparrow & \cdots & \uparrow \\ f(e_1) & f(e_2) & f(e_3) & \cdots & f(e_n) \\ \downarrow & \downarrow & \downarrow & \cdots & \downarrow \end{pmatrix},$$

which is the matrix representing f, with respect to the standard basis. Note that M_f is unique (up to a basis), since M_f's action is determined entirely by its action on each basis element. Define $L^{-1} : \mathrm{GL}(\mathbb{C}^n) \to \mathrm{GL}_n(\mathbb{C})$ as $f \mapsto M_f$. Now we prove that L is a group homomorphism. This follows from the fact that $L_{MN} = L_M \circ L_N$, i.e., $L(MN) = L_{MN} = L_M \circ L_N = L(M) \circ L(N)$, as required. $\square$

Corollary 2. *If* $\dim_{\mathbb{C}} V = n$, *then* $\mathrm{GL}_n(\mathbb{C}) \cong \mathrm{GL}(V)$.

Proof. Follows from Propositions 3 and 4. $\square$

Definition 5. Let G be a group.

(i) A *linear representation* of G is a pair (V, ρ) where:

  (a) V is a vector space (over $\mathbb{C}$); and

  (b) ρ is a group homomorphism from G to $\mathrm{GL}(V)$.

(ii) The *degree of a representation* is $\dim(V)$.

For the sake of notational cleanness, we shall write $\rho(g)$ as ρ_g for each $g \in G$.

Observe that Definition 5 formulates a linear representation from the perspective of an "action" of a group on the space of linear operators. The following alternate definition of linear representations focuses on the behaviour of the map ρ itself:

Definition 6. A *linear representation of* G is a vector space over $\mathbb{C}$ together with a family of linear bijections $(\rho_g = g \in G)$ such that if $g_1 g_2 = g$, then $\rho_{g_1} \circ \rho_{g_2} = \rho_g$.

Proposition 7. *Definitions 5 and 6 are equivalent.*

Proof. $(6 \Rightarrow 5)$ This is immediate, since $g_1 g_2 = g \Rightarrow \rho_{g_1} \circ \rho_{g_2} = \rho_g$ implies that ρ is a group homomorphism.
$(5 \Rightarrow 6)$ Since ρ is a group homomorphism, we have $\rho(g_1 g_2) = \rho(g_1) \circ \rho(g_2)$, as desired. That each ρ_g is a linear bijection follows from the fact that ρ_g is a invertible linear operator for all $g \in G$. $\square$

2. September 9

2.1. Examples of representations.

Example 1. Consider C_6, cyclic group of order 6. In this example we will construct a representation of degree 2. Start off with a linear map $L : \mathbb{C}^2 \to \mathbb{C}^2$ which maps $\binom{1}{0} \mapsto \binom{0}{1}$ and $\binom{0}{1} \mapsto \binom{-w}{-w^2}$, where w denotes a primitive cubic root of unity. Thus the matrix representation of L (call it M_L) is

$$M_L := \begin{pmatrix} 0 & -w \\ 1 & -w^2 \end{pmatrix}.$$

One can calculate that $M_L^3 = I$, hence $L^3 = \mathrm{id}_{\mathbb{C}^2}$. Hence, the map ρ satisfying the following forms a C_6-representation $(\mathbb{C}^2, \rho)$ (one can verify that ρ is indeed a group homomorphism):

$$\begin{aligned} 0, 3 &\mapsto \mathrm{id}_{\mathbb{C}^2} \\ 1, 4 &\mapsto L \\ 2, 5 &\mapsto L^2. \end{aligned}$$

Alternatively, one can write this representation in the following way: $(\mathbb{C}^2, (\mathrm{id}, L, L^2, \mathrm{id}, L, L^2))$.

Example 2. In this example, we consider a permutation group S_3. For each $\pi \in S_3$, define $\rho_\pi : \mathbb{C}^3 \to \mathbb{C}^3$ by

$$\rho_\pi(z_1, z_2, z_3) := (z_{\pi^{-1}(1)}, z_{\pi^{-1}(2)}, z_{\pi^{-1}(3)}).$$

Observe that ρ_π is indeed a linear map: ρ_π can be expressed using a matrix, namely the identity matrix with columns permuted by π^{-1}. For instance, if $\pi = (123)$, then we have $\rho_\pi(z_1, z_2, z_3) = (z_3, z_1, z_2)$ and

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix} = \begin{pmatrix} z_3 \\ z_1 \\ z_2 \end{pmatrix},$$

which is what we would expect. As we would expect from the matrices, each ρ_π is invertible. Now it remains to show that $(\mathbb{C}^3, (\rho_\pi : \pi \in S_3))$ is a representation of S_3. That is, we need to show that ρ is a group homomorphism from S_3 to $\mathrm{GL}(\mathbb{C}^3)$.

It is helpful to think of each element of $z \in \mathbb{C}^3$ as a map $z : \{1, 2, 3\} \to \mathbb{C}$ (for instance, $(1, 2, 3) \mapsto (z_1, z_2, z_3)$). We claim that $\rho_\pi \circ z = z \circ \pi^{-1}$. Indeed, in the case of $\pi = (123)$, we have $\rho_\pi(z)(1) = \rho_\pi(z_1, z_2, z_3)(1) = (z_3, z_1, z_2)(1) = z_3$ and $z \circ \pi^{-1}(1) = (z_1, z_2, z_3)(3) = z_3$, as desired. Do this for other elements and each π to verify the claim.

Now for any $\lambda, \pi \in S_3$ and $z \in \mathbb{C}^3$, we need to prove that $\rho_{\lambda\circ\pi} = \rho_\lambda \circ \rho_\pi$, which is enough to show that ρ is a group homomorphism. Indeed, we have $\rho_{\lambda\circ\pi}(z) = z \circ (\lambda \circ \pi)^{-1} = z \circ \pi^{-1} \circ \lambda^{-1} = (z \circ \pi^{-1}) \circ \lambda^{-1} = \rho_\pi(z) \circ \lambda^{-1} = \rho_\lambda(\rho_\pi(z)) = (\rho_\lambda \circ \rho_\pi)(z)$, as required.

Definition 8. Suppose (V, ρ) and (W, λ) are two representation of the same group G. Then *a morphism* (also called *an intertwining* or *a G-linear map*) from (V, ρ) to (W, λ) is a linear map $h : V \to W$ which preserves the operators ρ_g and σ_g in the following sense: for each $g \in G$ and for all $v \in V$, we have $h \circ \rho_g(v) = \sigma_g \circ h(v)$ for all $g \in G$. Also, if h is an isomorphism, then we define $h^* : \mathrm{GL}(V) \to \mathrm{GL}(W)$ as $\rho_g \mapsto h \circ \rho_g \circ h^{-1} = \sigma_g$.

Definition 9. A bijective homomorphism is called *an isomorphism.*

Lemma 1. *Suppose (V, ρ) is a representation of G and $h : V \cong W$ is some vector space isomorphism. Suppose $h^* : \mathrm{GL}(V) \to \mathrm{GL}(W)$ is the "conjugation" isomorphism. Then:*

(1) $(W, h^* \circ \rho)$ is a representation of G.

(2) $(V, \rho) \cong (W, h^* \circ \rho =: \sigma)$.

Proof. The first part follows from the fact that h^* is an isomorphism, as it implies that $h^* \circ \rho$ is a group homomorphism. As for the second part, we start with h isomorphism. First, observe that $\sigma_g = h^* \circ \rho(g) = h^*(\rho_g)$. For any $g \in G$, we have $\sigma_g \circ h = h^*(\rho_g) \circ h = (h \circ \rho_g \circ h^{-1}) \circ h = h \circ \rho_g$, as required. □

Corollary 3. *Every representation (V, ρ) of degree n is isomorphic to $(\mathbb{C}^n, \sigma)$ for some σ.*

Proof. Use the linear map $f_{\mathscr{B}} : V \to \mathbb{C}^n$ for basis $\mathscr{B}$ and apply the previous lemma. □

3. September 11

Definition 10. Suppose (V, ρ) is a representation of G and $W \leq V$. Then

(i) W is G-invariant or G-stable if $\rho_g(W) \subseteq W$ for all $g \in G$.

(ii) If W is G-invariant, then $\rho|_W$ denotes the map with domain G given by $(\rho|_W)(g) = \rho_g|_W$.

Lemma 2. *If (V, ρ) of G and W is a G-invariant subspace of V, then $(W, \rho|_W)$ is a representation of G.*

Proof. We need to prove that $\rho|_W : G \to \mathrm{GL}(W)$ is a homomorphism. For this, we need to verify the multiplicativity of $\rho|_W$. (Need to fill in the details!)

To prove that $\rho|_W$ is bijective, we note that ρ_g is a bijection, so $\rho_g|_W$ is injective. For subjectivity, use the fact that W is G-invariant, and that $g^{-1} \in G$: $\rho_{g^{-1}}(W) \subset W$, hence $W \subset \rho_g(W)$. Thus, $\rho_g(W) = W$, as required. □

4. September 15 & 16: Proof of Maschke's theorem and irreducible representations

Recall that if $(W_0, \rho), (W_1, \sigma)$ are representations of G, then $(W_0, \rho) \oplus (W_1, \sigma)$ is the representation $(V, \rho \oplus \sigma)$ where:

- $V = W_0 \oplus W_1$
- $(\rho \oplus \sigma)_g = \rho_g \oplus \sigma_g : V \to V$ given by $(\rho_g \oplus \sigma_g)(w_0 + w_1) = \rho_g(w_0) + \sigma_g(w_1)$ where $w_i \in W_i$.

Example 3 (Representation of $\mathbb{Z}/6\mathbb{Z}$). $(\mathbb{C}^2, \rho) = (\mathbb{C}^2, (\mathrm{id}_{\mathbb{C}^2}, L, L^2, \mathrm{id}_{\mathbb{C}^2}, L, L^2))$ where $L : \mathbb{C}^2 \to \mathbb{C}^2$ defined by

$$\begin{pmatrix} 0 & -\omega \\ 1 & -\omega^2 \end{pmatrix},$$

where $\omega = e^{2\pi i/3}$. In fact, this matrix is diagonalizable, with eigenvalues 1 and ω. If E_1 and E_ω are the eigenspaces, then $\mathbb{C}^2 \cong E_1 \oplus E_\omega$, and E_1 and E_ω are $\mathbb{Z}/6\mathbb{Z}$-invariant. This gives us the decomposition

$$(\mathbb{C}^2, \rho) = (E_1, \rho|_{E_1}) \oplus (E_\omega, \rho|_{E_\omega}). \tag{1}$$

We want to know what $(E_1, \rho|_{E_1})$ and $(E_\omega, \rho|_{E_\omega})$ signify. To start off, examine each map. Then $\rho|_{E_1}$ maps $(0, 1, 2, 3, 4, 5) \mapsto (\mathrm{id}_{E_1}, L|_{E_1}, L^2|_{E^1}, \mathrm{id}_{E^1}, L|_{E_1}, L^2|_{E_1})$. But since $L|_{E_1} = L^2|_{E^1} = \mathrm{id}_{E_1}$, we see that $(E_1, \rho|_{E_1})$ is the trivial representation, i.e., $\cong (\mathbb{C}, \tau)$.

As for $\rho|_{E_\omega}$, we see that $\rho|_{E_\omega}$ is a multiplication map (by ω). Thus $(E_\omega, \rho|_{E_\omega}) \cong (\mathbb{C}, \sigma)$ where $\sigma(a) =$ multiplication map by $\omega^{a \bmod 3}$. Thus $(\mathbb{C}^2, \rho) \cong (\mathbb{C}, \tau) \oplus (\mathbb{C}, \sigma)$.

Note that (1) can be stated in a more general way:

Lemma 3. *Suppose that (V, ρ) is a representation of G. If $V = W_0 \oplus W_1$ and both W_0, W_1 are G-invariant. Then $(V, \rho) = (W_0, \rho|_{W_0}) \oplus (W_1, \rho|_{W_1})$.*

Definition 11. A representation (V, ρ) of G is *irreducible* if $V \neq \{0\}$ and V has no non-trivial G-invariant subspaces. If it is not irreducible, then that representation is called *reducible.*

Lemma 4. *Suppose p is a projection of V onto W and $h \in \mathrm{GL}(V)$. Then $h^*(p) := h \circ p \circ h^{-1}$ is also a projection of V onto $h(W)$.*

Proof. We need to show two things:

(i) $h^*(p)(V) = h(W)$
Since h is an isomorphism, it follows $h^*(p)(V) = (h \circ p \circ h^{-1})(V) = (h \circ p)(V) = h(W)$, as required.

(ii) For all $x \in h(W)$, we have $h^*(p)(x) = x$.
Let $x \in h(W)$, say, $x = h(w)$ for some $w \in W$. Then $h^*(p)(X) = h^*(p)(h(w)) = (h \circ p \circ h^{-1})(h(w)) = h(w) = x$.

Thus $h^*(p)$ is a projection also. □

Theorem 1 (Maschke's Theorem)**.** *Suppose (V, ρ) is a representation of G where G is* finite*. Suppose that $W \leq V$ is G-invariant. Then W has a complement which is also G-invariant.*

Proof. It suffices to find a projection of V onto W whose kernel is G-invariant, i.e. some map $p : V \to V$ so that $p(w) = w$ for all $w \in W$ and $\mathrm{im}(p) = W$. Let f be an arbitrary projection of V onto W. Then for each $g \in G$, we have $\rho_g \in \mathrm{GL}(V)$. Let $f_g := \rho_g^*(f)$. By Lemma 4, f_g is also a projection of V onto $\rho_g(W) = W$. Define

$$\overline{f} := \frac{1}{|G|} \sum_{g \in G} f_g,$$

i.e., the "average" of all the $f_g \in \mathrm{End}(V)$. We claim that $\overline{f}$ is a projection of V onto W. Clearly, since $\overline{f}$ is composed of linear maps, $\overline{f}$ is clearly linear. For any $x \in V$, we have $\overline{f}(x) = \frac{1}{|G|} \sum_{g \in G} f_g(x)$. Note that each $f_g(w) \in W$, so $\sum f_g(x) \in W$ also. Thus $\overline{f}(x) \in W$. Also, for $w \in W$, we need $\overline{f}(w) = w$. Since

$$\overline{f}(w) = \frac{1}{|G|} \sum_{g \in G} f_g(w) = \frac{1}{|G|} \sum_{g \in G} (\rho_g \circ f \circ \rho_g^{-1})(w) = \frac{1}{|G|} \sum_{g \in G} w = w,$$

this claim follows. To finish the proof, we need to prove that $\ker(\overline{f})$ is G-invariant. Let $g \in G$ and $w \in \ker(\overline{f})$. We need to show that $\overline{f}(\rho_g(w)) = 0$. Since $\rho_g \circ \overline{f} = \overline{f} \circ \rho_g$ (see Lemma 5 for proof), we have $\overline{f}(\rho_g(w)) = (\overline{f} \circ \rho_g)(w) = (\rho_g \circ \overline{f})(w) = \rho_g(\overline{f}(w)) = \rho_g(0) = 0$. So $\ker(\overline{f})$ is our G-invariant complement to W. □

Lemma 5. *For all $g \in G$, we have $\rho_g \circ \overline{f} = \overline{f} \circ \rho_g$.*

Proof. equivalently, we have $\rho_g \circ \overline{f} \circ \rho_g^{-1} = \overline{f}$, i.e., $\rho_g^*(\overline{f}) = \overline{f}$ for all $g \in G$. Choose some $h \in G$. Then

$$\begin{aligned}
\rho_h^*(f) &= \rho_h \circ \overline{f} \circ \rho_h^{-1} \\
&= \rho_h \circ \left(\frac{1}{|G|} \sum_{g \in G} f_g \right) \circ \rho_h^{-1} \\
&= \frac{1}{|G|} \sum_{g \in G} \rho_h \circ f_g \circ \rho_h^{-1} \\
&= \frac{1}{|G|} \sum_{g \in G} \rho_h \circ \rho_g \circ f \circ \rho_g^{-1} \circ \rho_h^{-1} \\
&= \frac{1}{|G|} \sum_{g \in G} \rho_{hg} \circ f \circ \rho_{(hg)^{-1}} \\
&= \frac{1}{|G|} \sum_{g \in G} \rho_{hg}^*(f) = \frac{1}{|G|} \sum_{g \in G} \rho_g^*(f) = \overline{f}.
\end{aligned}$$

□

Corollary 4. *Suppose that G is finite, (V, ρ) is a representation of G, with $\dim(V) = n > 0$. Then (V, ρ) can be written as a direct sum of irreducible representations (of G).*

Proof. We prove by induction on n. Every representation of degree 1 is automatically irreducible, hence the base case. Now suppose that the conclusion is true for $n > 1$. If (V, ρ) is irreducible, then the conclusion is immediate, so suppose otherwise. Then there exists a proper subspace $W \leq V$ with W a G-invariant subspace. Apply Mascke's theorem to get a G-invariant complement, say V_1. Thus $V = W \oplus V_1$. Since W and V_1 are both G-invariant, it follows that $(V, \rho) = (W, \rho|_W) \oplus (V_1, \rho|_{V_1})$. Note that $W < V$, so $\dim(W) < \dim(V) = n$, and since $W \neq 0$, the dimension of W must be positive. Hence $0 < \dim(V_1) < n$ also. By the inductive hypothesis, both $(W, \rho|_W)$ and $(V_1, \rho|_{V_1})$ can be written as a direct sum of irreducible representations. □

5. September 16 & 18: Tensor products

For $\mathbb{C}^m$ and $\mathbb{C}^n$, define $\mathbb{C}^{m \times n} = \{\text{all } m \times n \text{ matrices over } \mathbb{C}\}$ as a vector space over $\mathbb{C}$. Define $\iota : \mathbb{C}^m \times \mathbb{C}^n \to \mathbb{C}^{m \times n}$ by $\iota(u, v) = uv^T$. The map ι is in fact *bilinear*: that is, ι is linear on both first and the second variables, i.e., $\iota(cx + y, v) = c\iota(x, v) + \iota(y, v)$ and $\iota(u, cx + y) = c\iota(u, x) + \iota(u, y)$.

We start with the standard basis: $\mathbb{C}^m = \text{span}\{e_1, e_2, \ldots, e_m\}$ and $\mathbb{C}^n = \text{span}\{e_1', e_2', \ldots, e_n'\}$. Now we define the *tensor product*:

Definition 12. Define $\iota(e_i, e_j') = (a_{kl})$ where $a_{kl} = 1$ only when $(k, l) = (i, j)$ and 0 otherwise. We denote $\iota(u, v)$ as $u \otimes v$. We call $\mathbb{C}^{m \times n}$ the *tensor product* of $\mathbb{C}^m, \mathbb{C}^n$ (via ι) and we denote it as $\mathbb{C}^m \otimes \mathbb{C}^n$. Also, $u \otimes v$ is called a *simple tensor*.

Remark 1. Note that not all tensor are simple, i.e., cannot be written in the form $u \otimes v$.

Proposition 13. *$\{\iota(e_i, e_j') : 1 \leq i \leq m, 1 \leq j \leq n\}$ is a basis for $\mathbb{C}^{m \times n}$.*

Proof. Observe that $\iota = \otimes : \mathbb{C}^m \times \mathbb{C}^n \to \mathbb{C}^m \otimes \mathbb{C}^n$ is a bilinear map, and that $\{e_i \otimes e'_j \mid 1 \leq i \leq m, 1 \leq i \leq n\}$ is a basis for $\mathbb{C}^m \otimes \mathbb{C}^n$. Observe also that ι is neither injective nor surjective, since $u \otimes 0 = 0 \otimes v = 0 \in \mathbb{C}^{m \times n}$ for all $u \in \mathbb{C}^m$ and $v \in \mathbb{C}^n$. ι is not surjective either since $\iota(u, v) = uv^T$ is always of rank ≤ 1, i.e., $(\mathrm{im}(\iota) = \{\text{all rank} \leq 1 \text{ matrices in } \mathbb{C}^{m \times n}\}$. It is also true that $\mathrm{span}(\mathrm{im}(\iota)) = \mathbb{C}^{m \times n} = \mathbb{C}^m \otimes \mathbb{C}^n$.

In fact, every $x \in \mathbb{C}^m \otimes \mathbb{C}^n (= \mathbb{C}^{m \times n})$ is a sum of simple tensors. Hence write $x = (m_{i,j}) \in \mathbb{C}^{m \times n}$. It is known that the matrix can be written as follows:

$$(m_{i,j}) = \sum_{i,j} m_{i,j}(e_i \otimes e'_j) = \sum_{i,j} ((m_{i,j} e_i) \otimes e'_j),$$

and $(m_{i,j} e_i) \otimes e'_j$. This completes the proof. □

5.1. **Universal property of tensor products.**

Proposition 14. *Suppose V is a $\mathbb{C}$-vector space, and fix $m, n \in \mathbb{Z}$. If $\alpha : \mathbb{C}^m \times \mathbb{C}^n \to V$ is a bilinear, then there exists a* unique linear map $\overline{\alpha} : \mathbb{C}^m \otimes \mathbb{C}^n \to V$ *such that $\overline{\alpha} \circ \iota = \alpha$.*

Proof. $\overline{\alpha} \circ \iota = \alpha$ implies that for all $(u, v) \in \mathbb{C}^m \times \mathbb{C}^n$, we have $\overline{\alpha}(u \otimes v) = \alpha(u, v)$. Uniqueness is clear from Proposition 13: recall that $\overline{\alpha}$ is determined by its actions on simple tensors, and that $\{e_i \otimes e'_j\}$ is a basis for $\mathbb{C}^m \otimes \mathbb{C}^n$. So there exists a unique linear map $\mathbb{C}^m \otimes \mathbb{C}^n \to V$ such that $e_i \otimes e'_j \mapsto \alpha(e_i, e'_j)$. Let $\overline{\alpha}$ be this map. So it remains to prove that $\alpha(u \otimes v) = \alpha(u, v)$ for all $u \in \mathbb{C}^m, v \in \mathbb{C}^n$.

Start with $u \in \mathbb{C}^m, v \in \mathbb{C}^n$. So $u = \sum u_i e_i$, $v = \sum v_j e'_j$ for some $(u_i)_{i=1}^m$ and $(v_j)_{j=1}^n$. Then

$$\begin{aligned} u \otimes v &= \left(\sum_i u_i e_i \right) \otimes \left(\sum_j v_j e'_j \right) = \sum_i u_i \left(e_i \otimes \left(\sum_j v_j e'_j \right) \right) \\ &= \sum_i u_i \left(\sum_j v_j (e_i \otimes e'_j) \right) = \sum_{i,j} u_i v_j (e_i \otimes e'_j). \end{aligned}$$

Therefore

$$\begin{aligned} \overline{\alpha}(u \otimes v) &= \overline{\alpha} \left(\sum_{i,j} u_i v_j (e_i \otimes e'_j) \right) \\ &= \sum_{i,j} u_i v_j \overline{\alpha}(e_i \otimes e'_j) = \sum_{i,j} u_i v_j \alpha(e_i, e'_j), \end{aligned}$$

so $\overline{\alpha}$ is linear. Similarly,

$$\begin{aligned} \alpha(u, v) &= \alpha \left(\sum_i u_i e_i, \sum_j v_j e'_j \right) = \sum_i u_i \alpha \left(e_i, \sum_j v_j e'_j \right) \\ &= \sum_i u_i \left(\sum_j v_j \alpha(e_i, e'_j) \right) = \sum_{i,j} u_i v_j \alpha(e_i, e'_j) = \overline{\alpha}(u \otimes v), \end{aligned}$$

as required. □

5.1.1. *One application of Proposition 14.* Let $f : \mathbb{C}^m \to \mathbb{C}^k$ and $g : \mathbb{C}^n \to \mathbb{C}^l$ linear. Let $V = \mathbb{C}^k \otimes \mathbb{C}^l$. Define $\alpha : \mathbb{C}^m \times \mathbb{C}^n \to V$ by $\alpha(u, v) = f(u) \otimes g(v)$. We claim that this is bilinear.

Claim. α is bilinear.

Proof. α is linear on the first variable:

$$\begin{aligned}\alpha(x+y, v) &= f(x+y) \otimes g(v) = (f(x) + f(y)) \otimes g(v) \ (f \text{ is linear})\\ &= f(x) \otimes g(v) + f(y) \otimes g(v) \ (\otimes \text{ is bilinear})\\ &= \alpha(x, v) + \alpha(y, v).\end{aligned}$$

We can apply the same argument on the second variable as well to prove the claim. □

Now apply Proposition 14. Thus, there exists a linear map $\overline{\alpha} : \mathbb{C}^m \times \mathbb{C}^n \to V$ so that $\overline{\alpha} \circ \iota = \alpha$. We call this $\overline{\alpha} = f \otimes g$. Therefore, with $f : \mathbb{C}^m \to \mathbb{C}^k$ and $g : \mathbb{C}^n \to \mathbb{C}^l$, one can form $f \otimes g : \mathbb{C}^m \otimes \mathbb{C}^n \to \mathbb{C}^k \otimes \mathbb{C}^l$ satisfying $(f \otimes g)(u \otimes v) = f(u) \otimes g(v)$. In particular, if $k = m$ and $l = n$ and both f and g are invertible, then so is $f \otimes g$ (See Assignment 2.). In other words, given $f \in \mathrm{GL}(\mathbb{C}^m), g \in \mathrm{GL}(\mathbb{C}^n)$, we get $f \otimes g \in \mathrm{GL}(\mathbb{C}^m \otimes \mathbb{C}^n)$.

5.2. **Tensor product and representation.**

Definition 15. Suppose that $(\mathbb{C}^m, \rho), (\mathbb{C}^n, \sigma)$ are representations of G. Define $\rho \otimes \sigma : G \to \mathrm{GL}(\mathbb{C}^m \otimes \mathbb{C}^n)$ given by $(\rho \otimes \sigma)_g = \rho_g \otimes \sigma_g$. Then $\rho \otimes \sigma$ is a group homomorphism. Therefore, $(\mathbb{C}^m \otimes \mathbb{C}^n, \rho \otimes \sigma)$ is a representation of G. $(\mathbb{C}^m \otimes \mathbb{C}^n, \rho \otimes \sigma)$ is called the *tensor product of* $(\mathbb{C}^m, \rho), (\mathbb{C}^n, \sigma)$.

Example 4. Let $(\mathbb{C}^3, \rho)$ be the representation of S_3 from Example 2. We want to compute $(\mathbb{C}^3, \rho) \otimes (\mathbb{C}^3, \rho) = (\mathbb{C}^3 \otimes \mathbb{C}^3, \rho \otimes \rho)$. First, "find" $\rho_{(123)} \otimes \rho_{(123)} = (\rho \times \rho)_{(123)}$. Let $z \in \mathbb{C}^3 \otimes \mathbb{C}^3 = \mathbb{C}^{3\times 3}$. Then

$$(\rho_{(123)} \otimes \rho_{(123)})(e_i \otimes e_j) = \rho_{(123)}(e_i) \otimes \rho_{(123)}(e_j) = e_{i+1} \otimes e_{j+1}.$$

Thus the given tensor map shifts the entries to the right by one unit and then down by one unit, i.e.,

$$(\rho_{(123)} \otimes \rho_{(123)}) \left(\begin{pmatrix} z_{11} & z_{12} & z_{13} \\ z_{21} & z_{22} & z_{23} \\ z_{31} & z_{32} & z_{33} \end{pmatrix} \right) = \begin{pmatrix} z_{33} & z_{31} & z_{32} \\ z_{13} & z_{11} & z_{12} \\ z_{23} & z_{21} & z_{22} \end{pmatrix}$$

More generally, we have $(\rho_\pi \otimes \rho_\pi)([z_{ij}]) = [z_{\pi^{-1}(i), \pi^{-1}(j)}]$. Thus

$$(\mathbb{C}^3, \rho)^{\otimes 2} = (\mathbb{C}^3, \rho) \otimes (\mathbb{C}^3, \rho)$$

"is" the space of 3-by-3 matrices, with S_3 acting on rows and columns.

Definition 16 (for this example). We define $\mathrm{Sym}^2(\mathbb{C}^3)$ and $\mathrm{Alt}^2(\mathbb{C}^3)$ as follows:
$\mathrm{Sym}^2(\mathbb{C}^3) = \{x \in \mathbb{C}^3 \otimes \mathbb{C}^3 : x = x^T\}, \mathrm{Alt}^2(\mathbb{C}^3) = \{x \in \mathbb{C}^3 \otimes \mathbb{C}^3 : x^T = -x\}$.

Both $\mathrm{Sym}^2(\mathbb{C}^3)$ and $\mathrm{Alt}^2(\mathbb{C}^3)$ are subspaces of $\mathbb{C}^3 \otimes \mathbb{C}^3$, and that $(\mathbb{C}^3)^{\otimes 2} = \mathrm{Sym}^2(\mathbb{C}^3) \otimes \mathrm{Alt}^2(\mathbb{C}^3)$. Also, both Sym^2 and Alt^2 are S_3-invariant.

6. September 22

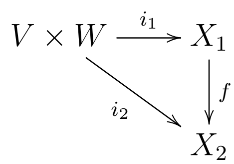
Definition 17. Given V, W complex vector spaces, a *tensor product* of V with W is a pair (i, X) where:

(i) X is a complex vector space

(ii) $i : V \times W \to X$ is bilinear.

(iii) If $\alpha : V \times W \to Y$ is any bilinear map, then there exists a unique linear map $\overline{\alpha} : X \to Y$ such that $\overline{\alpha} \circ i = \alpha$.

Proposition 18. *If (i_1, X_1) and (i_2, X_2) are tensor product for V with W, then there exists a unique isomorphism $X_1 \cong X_2$ such that*



i.e., for any $(v, w) \in V \times W$, we have $(f \circ i_1)(v, w) = i_2(v, w)$.

Denote any tensor product of V with W by $X := V \otimes W$ and write $v \otimes w := i(v, w)$. Recall from last week that there exists a tensor product of $\mathbb{C}^m$ with $\mathbb{C}^n$ ($X = \mathbb{C}^{m \times n}, i(v, w) = v \otimes w = vw^T$.).

In general, if V, W are finite-dimensional spaces (say $\dim_{\mathbb{C}} V = n, \dim_{\mathbb{C}} W = n$ by choosing bases, we can identify $V \sim \mathbb{C}^m$ and $W \sim \mathbb{C}^n$, and $V \otimes W \sim \mathbb{C}^m \otimes \mathbb{C}^n = \mathbb{C}^{m \times n}$. Thus $V \otimes W$ exists for all finite-dimensional spaces.

Proposition 19. *For any finite-dimensional V, W, X:*

(i) $V \otimes W \cong W \otimes V$

(ii) $V \otimes (W \otimes X) \cong (V \otimes W) \otimes X$

(iii) $V \otimes (W \oplus X) \cong (V \otimes W) \oplus (V \otimes X)$.

Proof of (i). Say $\dim V = m, \dim W = n$. Then $\dim(V \otimes W) = \dim(V) \dim(W) = mn = \dim(W \otimes V)$. However, what is more important is that there is a *natural* isomorphism. Namely, we have an isomorphism sending $v \otimes w \mapsto w \otimes v$. In concrete case: this would be a transpose map. In general, we call the isomorphism $V \otimes W \cong W \otimes V$ the *transpose*, denoted with T. □

As in the concrete case, if $f : V_1 \to V_2, g : W_1 \to W_2$ are linear, then there exists a unique linear map $f \otimes g : V_1 \otimes W_1 \mapsto V_2 \otimes W_2$ such that $v \otimes w \mapsto f(v) \otimes g(w)$. So given $f \in \mathrm{GL}(V_1)$ and $g \in \mathrm{GL}(V_2)$, get $f \otimes g \in \mathrm{GL}(V_1 \otimes V_2)$. Thus, given a finite group G, with representations $(V, \rho), (W, \sigma)$, get a representation $(V \otimes W, \rho \otimes \sigma) = (V, \rho) \otimes (W, \sigma)$ with $(\rho \otimes \sigma)_g = \rho_g \otimes \sigma_g$.

Definition 20. Suppose that V is a finite-dimensional vector space. Then

$$\mathrm{Sym}^2(V) = \{x \in V \otimes V : x^T = x\}$$
$$\mathrm{Alt}^2(V) = \{x \in V \otimes V : x^T = -x\}.$$

Lemma 6. *For any V and any $f \in \mathrm{GL}(V)$, both $\mathrm{Sym}^2(V)$ and $\mathrm{Alt}^2(V)$ are $f \otimes f$-invariant.*

Proof (for $\mathrm{Alt}^2(V)$). Let $x \in \mathrm{Alt}^2(V)$. So $x \in V \otimes V, x^T = -x$, i.e., $x + x^T = 0$. Write

$$x = \sum_{i=1}^{n} (u_i \otimes v_i).$$

Then

$$x^T = \left(\sum_{i=1}^{n} (u_i \otimes v_i) \right)^T = \sum_{i=1}^{n} (u_i \otimes v_i)^T = \sum_{i=1}^{n} v_i \otimes u_i.$$

We are also given that

$$\sum (u_i \otimes v_i) + (v_i \otimes u_i) = 0. \tag{2}$$

Let $y = (f \otimes f)(x)$. We must show that $y \in \mathrm{Alt}^2(V)$. Then we have

$$\begin{aligned} y = (f \otimes f)(x) = (f \otimes f) \left(\sum_{i=1}^{n} u_i \otimes v_i \right) &= \sum_{i=1}^{n} (f \otimes f)(u_i \otimes v_i) \\ &= \sum_{i=1}^{n} f(u_i) \otimes f(v_i). \end{aligned}$$

Thus

$$y^T = \sum_{i=1}^{n} f(v_i) \otimes f(u_i).$$

Now apply $f \otimes f$ to (2):

$$\begin{aligned} 0 = (f \otimes f)(0) &= (f \otimes f) \left(\sum (u_i \otimes v_i) + (v_i \otimes u_i) \right) \\ &= \sum_{i=1}^{n} f(u_i) \otimes f(v_i) + \sum_{i=1}^{n} f(v_i) \otimes f(u_i) \\ &= y + y^T. \end{aligned}$$

□

Corollary 5. *If G is a finite group and (V, ρ) a representation of G (of finite degree), then:*
(i) $\mathrm{Sym}^2(V), \mathrm{Alt}^2(V)$ *are G-invariant with respect to $(V, \rho) \otimes (V, \rho)$.*
(ii) $(V, \rho) \otimes (V, \rho) = (\mathrm{Sym}^2(V), (\rho \otimes \rho)|_{\mathrm{Sym}^2(V)}) \oplus (\mathrm{Alt}^2(V), (\rho \times \rho)|_{\mathrm{Sym}^2(V)})$.

Example 5. Let $(\mathbb{C}^3, \rho)$ be a representation of S_3 (as in Example 2). Then from Assignment #1, we know that $(\mathbb{C}^3, \rho) \cong \mathbf{B} \oplus \mathbf{1}$, where $\mathbf{B} := (\mathbb{C}^2, \sigma)$ and $\mathbf{1} := (\mathbb{C}, \tau)$ as defined in the solution to Assignment #1. Consider

$$\begin{aligned} (\mathbb{C}^3, \rho) \otimes (\mathbb{C}^3, \rho) &\cong (\mathbf{B} \oplus \mathbf{1}) \otimes (\mathbf{B} \oplus \mathbf{1}) \\ &\cong (\mathbf{B} \otimes \mathbf{B}) \oplus (\mathbf{B} \otimes \mathbf{1}) \oplus (\mathbf{1} \otimes \mathbf{B}) \oplus (\mathbf{1} \otimes \mathbf{1}) \\ &\cong (\mathbf{B} \otimes \mathbf{B}) \oplus \mathbf{B} \oplus \mathbf{B} \oplus \mathbf{1}. \end{aligned}$$

Recall also that

$$\mathbf{B} \otimes \mathbf{B} = (\mathrm{Sym}^2(\mathbb{C}^2), \sigma|_{\mathrm{Sym}^2(\mathbb{C}^2)}) \oplus (\mathrm{Alt}^2(\mathbb{C}^2), \sigma|_{\mathrm{Alt}^2(\mathbb{C})}).$$

For notational simplicity, let

$$(\mathrm{Sym}^2(\mathbb{C}^2), \sigma|_{\mathrm{Sym}^2(\mathbb{C}^2)}) =: \mathbf{Sym}, (\mathrm{Alt}^2(\mathbb{C}^2), \sigma|_{\mathrm{Alt}^2(\mathbb{C})}) =: \mathbf{Alt}. \tag{3}$$

Note that **Sym** is of degree 3 while **Alt** is of degree 1. Thus **Alt** is an irreducible representation.

First, examine **Alt**. Since $\mathrm{Alt}^2(\mathbb{C}^2)$ is a set of all skew-symmetric matrices, the basis is

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Meanwhile, σ acts on $\mathbb{C}^2$ via matrices:

$$M_{(12)} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, M_{(123)} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}.$$

$\sigma \otimes \sigma$ acts on $\mathbb{C}^2 \otimes \mathbb{C}^2$. Use basis $e_{11}, e_{12}, e_{21}, e_{22}$. Computations show that $\sigma \otimes \sigma$ acts by matrices

$$M_{(12)}^{\otimes 2} = \left(\begin{array}{cc|cc} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ \hline 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{array}\right) \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \\ 1 \\ 0 \end{pmatrix}$$

This shows that

$$(\sigma \otimes \sigma)\left(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) = -\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Hence $(\sigma \otimes \sigma)(x) = -x$ for all $x \in \mathrm{Alt}^2(\mathbb{C}^2)$. Thus, **Alt** $\neq$ trivial rep.

7. September 23: Introduction to character theory

7.1. Some linear algebra review.

Definition 21. Let $M = (a_{ij})$ be a $n \times n$ matrix over $\mathbb{C}$.

(i) The *characteristic polynomial* of M is $p(x) = \det(xI_n - M)$.

(ii) The *roots* of the characteristic polynomial are the eigenvalues of M (up to multiplicity).

(iii) $p(x) = (x - \lambda_1)(x - \lambda_2) \times \cdots \times (x - \lambda_n)$. Hence constant coeff $= (-1)^n \lambda_1 \cdots \lambda_n$, and coeff of $x^{n-1} = -(\lambda_1 + \cdots + \lambda_n)$.

(iv) $\lambda_1 \ldots \lambda_n = \det(M)$, $\lambda_1 + \cdots + \lambda_n = \mathrm{tr}(M)$.

(iv) If M, N are similar (i.e., there exists invertible Q such that $N = QMQ^{-1}$, then M, N have the same characteristic polynomial, and hence same eigenvalues, determinant, and trace.

If V is finite-dimensional ($\dim(V) = n$) and $f : V \to V$ linear map, then by choosing a basis for V, one can identify f with a matrix; then we can get char. poly., determinant, eigenvalues, and trace for f. By (v) in Definition 21, they are independent of basis. Let $\det(f)$ be the determinant of f and $\mathrm{tr}(f)$ the trace of f.

Definition 22. Let (V, ρ) be a finite-dimensional representation of a finite group G. The *character* of (V, ρ) is the function $\chi : G \to \mathbb{C}$ given by $\chi(g) = \mathrm{tr}(\rho_g)$.

Example 6. Let $(\mathbb{C}^2, \rho) = \mathbf{B}$ as in Example 4. Each σ_π is given by a matrix M_π:

$$M_{\text{id}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, M_{(12)} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$M_{(13)} = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}, M_{(23)} = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}$$
$$M_{(123)} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, M_{(132)} = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

The character of $\mathbf{B}$ is map $\chi : S_3 \to \mathbb{C}$ given by

π	id	(12)	(13)	(23)	(123)	(132)
$\chi(\pi)$	2	0	0	0	-1	-1

Proposition 23. *Let (V, ρ) be a representation of degree n of a finite group G. Let χ be its character. Then*

(1) $\chi(1) = n$.
(2) $\chi(g^{-1}) = \overline{\chi(g)}$ for all $g \in G$.
(3) χ is constant on conjugacy classes of G, i.e., $\chi(aga^{-1}) = \chi(g)$ for all $a, g \in G$.

Proof. For (1), pick a basis for V so that $[\rho_1] = I_n$. So $\chi(1) = \text{tr}(\rho_1) = \text{tr}(I_n) = n$.

As for (2), consider ρ_g and $\rho_{g^{-1}} = (\rho_g)^{-1}$. Let $\lambda_1, \ldots, \lambda_n$ be the eigenvalues of ρ_g. Then $\lambda_1^{-1}, \ldots, \lambda_n^{-1}$ are the eigenvalues of $(\rho_g)^{-1}$. It is known (by assignment #2) that

$$|\lambda_i| = 1, \text{ so } \lambda_1^{-1} = \overline{\lambda_i}.$$

Therefore,

$$\chi(g^{-1}) = \text{tr}(\rho_{g^{-1}}) = \text{tr}((\rho_g)^{-1}) = \sum_{i=1}^{n} \lambda_i^{-1} = \sum_{i=1}^{n} \overline{\lambda_i} = \overline{\sum_{i=1}^{n} \lambda_i}.$$

Finally, to prove (3), we start by picking $a, g \in G$. So $\rho_{aga^{-1}} = \rho_a \circ \rho_g \circ (\rho_a)^{-1}$. Pick a basis for V. And let $M = [\rho_g]$ and $N = [\rho_{aga^{-1}}]$. Note that M and N are similar: let $N = QMQ^{-1}$ and $Q = [\rho_a]$. So $\rho(g) = \text{tr}(\rho_g) = \text{tr}(M) = \text{tr}(N) = \text{tr}(\rho_{aga^{-1}}) = \chi(aga^{-1})$. ☐

For any two matrices, we have $\text{tr}(AB) = \text{tr}(BA)$. Thus, $\text{tr}(\rho_{ag}) = \text{tr}(\rho_a \circ \rho_g) = \text{tr}(\rho_g \circ \rho_a) = \text{tr}(\rho_{ga})$.

Definition 24. Let G be a finite group. A *class function* on G is any function $\alpha : G\ to \mathbb{C}$ which is constant on conjugacy classes. We write

$$\text{ClaFun}(G) := \{\text{all class functions on } G\}.$$

Observe that ClaFun(G) is closed under:

(1) pointwise addition. That is, if $\alpha, \beta \in \text{ClaFun}(G)$, then $(\alpha + \beta)(g) = \alpha(g) + \beta(g)$.
(2) pointwise multiplication, i.e. $(\alpha \cdots \beta)(G) = \alpha(G) \cdot \beta(G)$.
(3) complex scalar multiplication, i.e., $(c\alpha)(g) = c(\alpha(g))$.

Proposition 25. *Suppose that G is finite, and (V, ρ) and (W, σ) are finite-degree representations of G. Let χ_ρ, χ_σ be their characters.*

(1) $\chi_\rho + \chi_\sigma$ is the character of $(V, \rho) \oplus (W, \sigma)$.
(2) $\chi_\rho \cdot \chi_\sigma$ is the character of $(V, \rho) \otimes (W, \sigma)$.

Proof. Let $\mathbf{e} = (e_1, \dots, e_m)$ and $\mathbf{e}' = (e'_1, \dots, e'_n)$ be bases for V and W. Then we see that $\mathbf{e} \wedge \mathbf{e}'$ is a basis for $V \otimes W$. For any $g \in G$, we have

$$[(\rho \oplus \sigma)_g]_{\mathbf{e}\wedge\mathbf{e}'} = \left(\begin{array}{c|c} [\rho_g]_{\mathbf{e}} & 0 \\ \hline 0 & [\sigma_g]_{\mathbf{e}'} \end{array} \right).$$

Let χ be the character of $(V, \rho) \oplus (W, \sigma) = (V \oplus W, \rho \oplus \sigma)$. Then we have

$$\begin{aligned} \chi(g) = \operatorname{tr}((\rho \oplus \sigma)_g) &= \operatorname{tr}\left(\left(\begin{array}{c|c} [\rho_g]_{\mathbf{e}} & 0 \\ \hline 0 & [\sigma_g]_{\mathbf{e}'} \end{array} \right) \right) \\ &= \operatorname{tr}([\rho_g]_{\mathbf{e}}) + \operatorname{tr}([\sigma_g]_{\mathbf{e}'}) = \operatorname{tr}(\rho_g) + \operatorname{tr}(\sigma_g) = \chi_\rho(g) + \chi_\sigma(g). \end{aligned}$$

□

8. September 25: Continuation of character theory

Proposition 26. *Suppose G is finite and $(V, \rho), (W, \sigma)$ are representations of G (finite degree), with characters χ_ρ, χ_σ. Then:*

(1) The character of $(V, \rho) \oplus (W, \sigma)$ is $\chi_\rho + \chi_\sigma$.
(2) The character of $(V, \rho) \otimes (W, \sigma)$ is $\chi_\rho \cdot \chi_\sigma$.

Proof. Fix $g \in G$. Let $\mathbf{e} = (e_1, e_2, \dots e_m)$ be a basis for V and $\mathbf{e}' = (e'_1, \dots, e'_n)$ be a basis for W. Let $[\rho_g]_{\mathbf{e}} = (a_{ij})$ and $[\sigma_g]_{\mathbf{e}'} = M$. Recall that $(e_i \otimes e'_j)$ is a basis for $V \otimes W$, where $1 \le i \le m, 1 \le j \le n$. And

$$[\rho_g \otimes \sigma_g] = \begin{bmatrix} a_{11}M & a_{12}M & \cdots & a_{1m}M \\ a_{21}M & a_{22}M & \cdots & a_{2m}M \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}M & a_{m2}M & \cdots & a_{mm}M \end{bmatrix}.$$

Thus if χ is the character of $(V, \rho) \otimes (W, \sigma)$, then

$$\begin{aligned} \chi(g) &= \operatorname{tr}((\rho \otimes \sigma)_g) = \operatorname{tr}(\rho_g \otimes \sigma_g) \\ &= \operatorname{tr}([\rho_g \otimes \sigma_g]) = \sum_{i=1}^{m} a_{ii} \operatorname{tr}(M) \\ &= \operatorname{tr}((a_{ij})) \cdot \operatorname{tr}(M) = \operatorname{tr}([\rho_g]_{\mathbf{e}}) \cdot \operatorname{tr}([\sigma_g]_{\mathbf{e}'}) \\ &= \operatorname{tr}(\rho_g) \cdot \operatorname{tr}(\sigma_g) = \chi_\rho(g) \cdot \chi_\sigma(g). \end{aligned}$$

□

Proposition 27. *Suppose that (V, ρ) is a finite-degree representation of a finite group G. Let χ be its character, χ_S the char of $(\mathrm{Sym}^2(V), \rho^{\otimes 2}|_{\mathrm{Sym}^2(V)}) \le (V, \rho)^{\otimes 2}$, and χ_A the char of $(\mathrm{Alt}^2(V), \rho^{\otimes 2}|_{\mathrm{Alt}^2(V)}) \le (V, \rho)^{\otimes 2}$. Then for all $g \in G$:*

(1) $\chi_S(g) = \frac{1}{2}(\chi(g)^2 + \chi(g^2))$
(2) $\chi_A(g) = \frac{1}{2}(\chi(g)^2 - \chi(g^2))$
(3) $\chi_S(g) + \chi_A(g) = \chi(g)^2$.

Proof. Note that (3) follows from Proposition 26. Fix $g \in G$. Then ρ_g is diagonalizable (i.e., there exists a basis for V consisting of eigenvectors for ρ_g. See also Assignment #3). Let $\beta = (e_1, \dots, e_n)$ be a basis for V consisting of eigenvectors for ρ_g. Let $\lambda_1 \in \mathbb{C}$ be such that

$\rho_g(e_i) = \lambda_i e_i$. So $\mathrm{tr}(\rho_g) = \lambda_1 + \cdots + \lambda_n$. Also, ρ_{g^2} is also diagonalized by β, and $\rho_{g^2}(e_i) = \lambda_i^2 e_i$ and $\mathrm{tr}(\rho_{g^2}) = \sum_{i=1}^{n} \lambda_i^2$.

$$\beta_S := \{e_i \otimes e_j + e_j \otimes e_i : i \leq j\}$$

is a basis for $\mathrm{Sym}^2(V)$. Then we claim that $\rho_g^{\otimes 2}|_{\mathrm{Sym}^2(V)}$ is diagonalizable with respect to β_S. Observe that

$$\begin{aligned}\rho_g^{\otimes 2}(e_i \otimes e_j + e_j \otimes e_i) &= (\rho_g \otimes \rho_g)(e_i \otimes e_j + e_j \otimes e_i)\\ &= \rho_g(e_i) \otimes \rho_g(e_j) + \rho_g(e_j) \otimes \rho_g(e_i)\\ &= \lambda_i e_i \otimes \lambda_j e_j + \lambda_j e_j \otimes \lambda_i e_i\\ &= \lambda_i \lambda_j (e_i \otimes e_j + e_j \otimes e_i).\end{aligned}$$

This shows that

$$\mathrm{tr}(\rho_g^{\otimes 2}|_{\mathrm{Sym}^2(V)}) = \sum_{i \leq j} \lambda_i \lambda_j.$$

Thus,

$$\begin{aligned}\chi_S(g) = \mathrm{tr}(\rho_g^{\otimes 2}|_{\mathrm{Sym}^2(V)}) &= \sum_{i \leq j} \lambda_i \lambda_j\\ &= \sum_i \lambda_i^2 + \lambda_{i<j} \lambda_i \lambda_j\\ &= \frac{1}{2}\left(\left(\sum_i \lambda_i\right)^2 + \sum_i \lambda_i^2\right) = \frac{1}{2}(\chi(g)^2 + \chi(g^2)),\end{aligned}$$

as required. (2) can be proved in a similar manner. □

Example 7. Let $\mathbf{B} = (\mathbb{C}^2, \sigma)$ be a degree-two irreducible representation of S_3. Recall that

$$M_{(12)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad M_{(123)} = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix},$$

and

π	id	$(a\,b)$	$(a\,b\,c)$
$\chi(\pi)$	2	0	-1

So χ^2 should be the character of $\mathbf{B} \otimes \mathbf{B}$:

π	id	$(a\,b)$	$(a\,b\,c)$
$\chi^2(\pi)$	4	0	1

Recall that

$$\mathbf{B} \otimes \mathbf{B} = \mathbf{Sym} \oplus \mathbf{Alt}$$

(Refer to (3) for the definitions of **Sym** and **Alt**.). Apply Proposition 27 to get the character tables for **Sym** and **Alt**. For **Sym**:

$$\chi_S(\text{id}) = \frac{1}{2}(\chi(\text{id})^2 + \chi(\text{id}^2)) = \frac{4+2}{2} = 3$$
$$\chi_S(a\,b) = \frac{1}{2}(\chi(a\,b)^2 + \chi((a\,b)^2)) = \frac{0+2}{2} = 1$$
$$\chi_S(a\,b\,c) = \frac{1}{2}(\chi(a\,b\,c)^2 + \chi((a\,b\,c)^2)) = \frac{1-1}{2} = 0.$$

π	id	$(a\,b)$	$(a\,b\,c)$
$\chi_S(\pi)$	3	1	0

In a similar manner, one can obtain the following table for **Alt**:

π	id	$(a\,b)$	$(a\,b\,c)$
$\chi_A(\pi)$	1	-1	1

Finally, we claimed on Monday that $\mathbf{Sym} = \mathbf{B} \oplus \mathbf{1}$. Verify that $\chi_S = \chi + \chi_1$.

9. September 29

Definition 28. Let G be a finite group. Define

(1) $\mathbb{C}^G :=$ the set of all functions $G \to \mathbb{C}$

(2) If $\alpha, \beta \in \mathbb{C}^G$, then
$$(\alpha \mid \beta) = \frac{1}{|G|}\sum_{g\in G} \alpha(g)(\beta(g))^*,$$
where z^* denotes the complex conjugate of z.

(3) If $\alpha, \beta \in \mathbb{C}^G$, then
$$\langle \alpha, \beta\rangle = \frac{1}{|G|}\sum_{g\in G} \alpha(g)\beta(g)^{-1}$$
$$= \frac{1}{|G|}\sum_{g\in G} \alpha(g^{-1})\beta(g) = \langle \beta, \alpha\rangle.$$

(4) If $\beta \in \mathbb{C}^G$, then $\hat{\beta} \in \mathbb{C}^G$, where $\hat{\beta}(g) := \beta(g^{-1})^*$. Obviously, $\hat{\beta}(g^{-1}) = \beta(g)^*$.

Remark 2. We can make the following observations:

(1) $\mathbb{C}^G$ "is" $\mathbb{C}^{|G|} = \mathbb{C}^n$, where $G = \{g_1, g_2, \ldots, g_n\}$.

(2) $\mathbb{C}^G$ is a complex vector space of dim $n = |G|$.

(3) $\mathbb{C}^G$ is a ring (with pointwise addition and multiplication).

(4) $\text{ClaFun}(G) \subseteq \mathbb{C}^G$.

(5) $(\ \mid\ )$ is a complex inner product on $\mathbb{C}^G$, i.e.,
$$(\alpha_1 + \alpha_2 \mid \beta) = (\alpha_1 \mid \beta) + (\alpha_2 \mid \beta)$$
$$(c\alpha \mid \beta) = c(\alpha \mid \beta) \quad (c \in \mathbb{C})$$
$$(\beta \mid \alpha) = (\alpha \mid \beta)$$
$$(\alpha \mid \beta) \in \mathbb{C}$$
$$(\alpha \mid \alpha) \geq 0 \quad ((\alpha \mid \alpha) = 0 \Leftrightarrow \alpha = 0)$$

Suppose that $(\alpha \mid \alpha) = 0$. Then we have $\sum\limits_{g \in G} \alpha(g)\alpha(g)^* = 0$, or $\sum |\alpha(g)|^2 = 0$. Therefore, one has $|\alpha(g)| = 0$ so $\alpha = 0$.

Remark 3.

$$\begin{aligned}(\alpha \mid \beta) &= \frac{1}{|G|} \sum_{g \in G} \alpha(g)\beta(g)^* \\ &= \frac{1}{|G|} \sum_{g \in G} \alpha(g)\hat{\beta}(g^{-1}) = \langle \alpha, \hat{\beta} \rangle\end{aligned}$$

Remark 4. Which β satisfied $\beta = \hat{\beta}$? We need β to satisfy $\beta(g) = \beta(g^{-1})^*$ for all $g \in G$. This is equivalent to saying that $\beta(g^{-1}) = \beta(g)^*$. Characters have this property (see Proposition 23). So $\hat{\chi} = \chi$ for all characters χ. Thus, for all characters the relation $(\alpha \mid \chi) = \langle \alpha, \chi \rangle$ holds true, for all $\alpha \in \mathbb{C}^G$ and all characters χ.

Suppose that (V, ρ) is a finite-degree representation of finite group G. Let χ be its character and $\bar{e}$ a basis for V. Then for all $g \in G$, we get $[\rho_g]_{\bar{e}} = (r_{ij}(g))$. Thus we get a bunch of functions $r_{ij} : G \to \mathbb{C}$, i.e. $r_{ij} \in \mathbb{C}^G$.

For any character χ,

$$\chi(g) = \operatorname{tr}(\rho_g) = \operatorname{tr}([\rho_g]_{\bar{e}}) = \operatorname{tr}(r_{ij}(g)) = \sum_{i=1}^{n} r_{ii}(g) \Rightarrow \chi = \sum_{i=1}^{n} r_{ii} \in \mathbb{C}^G.$$

This proves:

Theorem 2 (Fundamental Observation). *If (V, ρ) is a finite-degree representation of a finite group G and χ is its character, and $(r_{ij}(g))$ gives the family matrices representing the ρ_g's with respect to some basis, then $\chi = r_{11} + r_{22} + \cdots + r_{nn}$.*

Lemma 7 (Schur's Lemma). *Suppose G is a finite group, and $(V, \rho), (W, \sigma)$ are* irreducible *representations. Suppose also that $f : (V, \rho) \to (W, \sigma)$ is a morphism.*

(1) f is either an isomorphism or the constant zero map.
(2) If $(W, \sigma) = (V, \rho)$, then f is a scalar map, i.e., there exists $\lambda \in \mathbb{C}$ such that $f(v) = \lambda v$ for all $v \in V$.

Proof. (Part (1)) Assume that f is not the constant zero map. Let $X = \ker(f)$. We know that X is G-invariant subspace of V. Since $f \neq 0$, $X \neq V$. Since (V, ρ) is irreducible, it follows $X = \{0\}$ so f is injective. Now let $Y := \operatorname{im}(f)$. We know that Y is G-invariant subspace of W. Since f is injective, $Y \neq \{0\}$. Since Y is irreducible, we must have $Y = W$.

(Part (2)) Assume that $(W, \sigma) = (V, \rho)$. So for $f : V \to V$, we can choose an eigenvalue λ of f, say with eigenvector v. Let $g : V \to V$ be $g = f - \lambda \operatorname{id}_V$, i.e., $d(v) = f(v) - \lambda v$. Then g is a morphism from (V, ρ) to itself. By (1), g is either an isomorphism or the constant zero map. Observe that if $v \neq 0$, then $g(v) = 0$, so g must be the constant zero map. Hence $f(v) = \lambda v$, as required. ☐

10. September 30

Definition 29. For $\alpha, \beta \in \mathbb{C}^G$, we have $\langle \alpha, \beta \rangle = \frac{1}{|G|} \sum_{g \in G} \alpha(g^{-1})\beta(g)$.

Corollary 6. *Let G be finite, and $(V,\rho),(W,\sigma)$ irreducible representations of G and $f: V\to V$ be a linear map. Define $f^0 : V\to W$ by*

$$f^0 = \frac{1}{|G|}\sum_{g\in G}\sigma_{g^{-1}}\circ f\circ \rho_g.$$

Then:

(1) *If $(V,\rho)\ncong(W,\sigma)$ then $f^0\equiv 0$.*
(2) *If $(V,\rho)=(W,\sigma)$, then $f^0(v)=\lambda v$, where $\lambda=\frac{\mathrm{tr}(f)}{\dim V}$.*

Proof. Main step: prove that f^0 is a morphism of representations, i.e., $f^0(\rho_g(v))=\sigma_g(f^0(v))$ for all $v\in V, g\in G$. Fix $g\in G$. Then we have

$$\begin{aligned}\sigma_g^{-1}\circ f^0\circ\sigma_g &= \sigma_g^{-1}\circ\left(\frac{1}{|G|}\sum_{h\in G}\sigma_{h^{-1}}\circ f\circ\rho_h\right)\circ\rho_g\\ &= \frac{1}{|G|}\sum_{h\in G}\sigma_{g^{-1}}\sigma_{h^{-1}}f\rho_h\rho_g = \frac{1}{|G|}\sum_{h\in G}\sigma_{(hg)^{-1}}f\rho_{hg} = f^0.\end{aligned}$$

Now apply Schur to f^0:

(1) Assume $(V,\rho)\ncong(W,\sigma)$. Then f^0 is not an isomorphism. Apply Schur, then we get $f^0\equiv 0$.
(2) Now assume $(V,\rho)=(W,\sigma)$. Then by Schur, we get that $f^0(v)=\lambda v$ for some λ.

On the first and, $\mathrm{tr}(f^0)=\lambda\dim(V)$. On the other hand,

$$\begin{aligned}\mathrm{tr}(f^0) &= \mathrm{tr}\left(\frac{1}{|G|}\sum_{g}\rho_{g^{-1}}f\rho_g\right) = \frac{1}{|G|}\sum_{g\in G}\mathrm{tr}(\rho_g^{-1}f\rho_g)\\ &= \frac{1}{|G|}\sum_{g\in G}\mathrm{tr}(\rho_{g^{-1}}\rho_g f) = \frac{1}{|G|}\,\mathrm{tr}(f) = \mathrm{tr}(f).\end{aligned}$$

□

Let $\dim V=m,\dim W=n$. Let $\mathbf{e}=(e_1,e_2,\ldots,e_m)$ be a basis for V and $\mathbf{e}'$ a basis for W. Define $[\rho_g]_{\mathbf{e}}=(r_{kl}(g))_{m\times m}$ and $[\sigma_g]_{\mathbf{e}'}=(s_{ij}(g))_{n\times n}$. Suppose $h:V\to W$ is a linear map, and we can write $[h]_{\mathbf{e}}^{\mathbf{e}'}=(x_{jk})_{n\times m}$. Note that $r_{kl},s_{ij}\in\mathbb{C}^G$.

Define f^0 as before. Then what is $[f^0]_{\mathbf{e}'}^{\mathbf{e}'}$? Define $[f^0]_{\mathbf{e}}^{\mathbf{e}'}:=(c_{il})_{n\times m}$. Formula for c_{il}. Start with $f^0=\frac{1}{|G|}\sum_g\sigma_{g^{-1}}f\rho_g$ So

$$[f^0]=\frac{1}{|G|}\sum_{g\in G}[\sigma_{g^{-1}}][f][\rho_g]$$

$$(c_{il})=\frac{1}{|G|}\sum_{g\in G}(s_{ij}(g^{-1}))(x_{jk})(r_{kl})$$

For each (i,l), we have

$$c_{il} = \frac{1}{|G|}\sum_{g\in G}\left(\sum_{j,k} s_{ij}(g^{-1})x_{jk}r_{kl}(g)\right) = \sum_{j,k}\left(\frac{1}{|G|}\sum_{g} s_{ij}(g^{-1})r_{kl}(g)\right)x_{jk}$$
$$= \sum_{j,k}\left(\frac{1}{|G|}\sum_{g} s_{ij}(g^{-1})r_{kl}(g)\right)x_{jk} = \sum_{j,k}\langle s_{ij}, r_{kl}\rangle x_{jk}.$$

If $(V,\rho)\not\cong(W,\sigma)$, then $f^0=0$. Thus (c_{il}) is the zero matrix. That is, the sum

$$\sum_{j,k}\langle s_{ij}, r_{kl}\rangle x_{jk} = 0.$$

This is true for all f, or for all (x_{jk}). Hence $\langle s_{ij}, r_{kl}\rangle = 0$ for all i,j,k,l. Thus we proved

Corollary 7. *If $(V,\rho),(W,\sigma)$ are irreducible representations, then $[\rho_g] = (r_{kl}(g)), [\sigma_g] = (s_{ij}(g))$ with respect to some basis. If $(V,\rho)\not\cong(W,\sigma)$, then $\langle s_{ij}, r_{kl}\rangle = 0$ for all i,j,k,l.*

Next, assume that $(V,\rho) = (W,\sigma)$. And let $[\rho_g] = (r_{kl}) = (r_{ij}), [f] = (x_{kl}), [f^0] = (c_{il})$. So $c_{il} = \sum_{j,k}\langle r_{ij}, r_{kl}\rangle x_{jk}$. By Corollary 6, $f^0(v) = \lambda v$ where $\lambda = \frac{\mathrm{tr}(f)}{m}$. Thus c_{il} is λ if $i=l$ and 0 otherwise. Thus

$$\mathrm{tr}(f) = \sum_j x_{jj} = \sum_{j,k}\delta_{jk}x_{jk}.$$

So $c_{il} = \delta_{il}(\frac{\mathrm{tr}(f)}{m}) = \frac{1}{m}\delta_{il}\sum_{j,k}\delta_{jk}x_{jk} = \sum_{j,k}(\frac{1}{m}\delta_{il}\delta_{jk})x_{jk}$. Thus, for all i,l,

$$\sum_{j,k}\langle r_{ij}, r_{kl}\rangle x_{jk} = \sum_{j,k}\left(\frac{1}{m}\delta_{il}\delta_{jk}\right)x_{jk}.$$

Since this is true for all f (= for all (x_{jk})), it follows $\langle r_{ij}, r_{kl}\rangle = \frac{1}{m}\delta_{il}\delta_{jk}$ for all i,j,k,l. Hence this proves

Corollary 8. *If (V,ρ) an irreducible representation and $[\rho_g] = (r_{kl}(g))$, then for all i,j,k,l,*

$$\langle r_{ij}, r_{kl}\rangle = \frac{1}{m}\delta_{il}\delta_{jk} = \begin{cases}\frac{1}{m} & (i=l, j=k)\\ 0 & \textit{otherwise}\end{cases}.$$

11. October 2

Corollary 9. *$(V,\rho),(W,\sigma)$ irreducible and $[\rho_g] = (r_{kl})_g, [\sigma_g] = (s_{ij}(g))$ then $\langle s_{ij}, r_{kl}\rangle = 0$ for all i,j,k,l.*

Corollary 10. *Let (V,ρ) be irreducible and $[\rho_g]] = (r_{kl}(g))$. Then*

$$\langle r_{ij}, r_{kl}\rangle = \begin{cases}\frac{1}{\dim V} & \textit{if } i=l, j=k\\ 0 & \textit{otherwise.}\end{cases}$$

Corollary 11. *Suppose $(V,\rho),(W,\sigma)$ are representations with characters χ,χ', respectively. If $(V,\rho)\cong(W,\sigma)$ then $\chi\equiv\chi'$.*

Theorem 3. *If G is a finite group, then*

(1) if χ is the character of an irreducible representation of G, then $(\chi \mid \chi) = 1$.
(2) If χ, χ' are the characters of irreducible representations $(V, \rho), (W, \sigma)$ of G and $(V, \rho) \neq (W, \sigma)$, then $(\chi \mid \chi') = 0$.

Proof. For part (1), start with χ, the character of (V, ρ). Pick a basis β for V. Write $[\rho_g]_\beta = (r_{ij}(g))$. Recall that $\chi = r_{11} + \cdots + r_{nn}$ where $n = \dim V$. Then $(\chi \mid \chi) = \langle \chi, \chi \rangle = \langle \sum_i r_{ii}, \sum_i r_{ii} \rangle = \sum_{i,j} \langle r_{ii}, r_{jj} \rangle = \sum_{i,j} \frac{\delta_{ij}}{n} = \sum_{i=1}^{n} \frac{1}{n} = 1$.

As for part (2), write $[\sigma_g]_{\beta'} = (s_{ij}(g))$ and $\chi' = s_{11} + \cdots + s_{mm}$, where $m = \dim W$. Then we have $(\chi \mid \chi') = \langle \chi, \chi' \rangle = \sum_{i,j} \langle r_{ii}, s_{jj} \rangle = 0$. □

Theorem 4. *Let (V, ρ) be a finite-degree representation of G, with φ its character. Suppose that (V, ρ) can be decomposed to*

$$(V, \rho) \cong (V_1, \rho_1) \oplus \cdots \oplus (V_k, \rho_k)$$

where each (V_i, ρ_i) is an irreducible representation of G. Let χ_i be the character of (V_i, ρ_i). Let (W, σ) be any irreducible representation of G with character χ. Then

$$(\varphi \mid \chi) = |\{i : (V_i, \rho_i) \cong (W, \sigma)\}|.$$

Proof. We know that $\varphi = \chi_1 + \chi_k$. So

$$\begin{aligned}(\varphi \mid \chi) &= (\chi_1 + \cdots + \chi_k \mid \chi) \\ &= (\chi_1 \mid \chi) + \cdots + (\chi_k \mid \chi) \\ &= |\{i : (\chi_i \mid \chi) = 1\}| = |\{i : \chi_i = x\}| \\ &= |\{i : (V_i, \rho_i) \cong (W, \rho)\}|.\end{aligned}$$ □

Corollary 12. *Let (V, ρ) be a finite-degree representation of G. Any two decompositions of $(V,\ rho)$ as direct sums of irreducible representations, are the "same" up to rearrangements and isomorphism of the individual summands.*

Proof. For each irreducible (W, σ) and char χ, we have

$$(\varphi \mid \chi) = (\#\text{ of times } (W, \rho) \text{ appears in any decomposition}).$$ □

Corollary 13. *If $(V, \rho), (W, \sigma)$ are the finite-degree representations of G, with the characters φ, φ', then $(V, \rho) \cong (W, \sigma) \Leftrightarrow \varphi \equiv \varphi'$.*

Proof. ($\Leftarrow$) Assume $\varphi = \varphi'$. Look at the direct sums of decompositions for (V, ρ) and (W, σ). By Theorem 4, for any irreducible (X, τ) (with character χ), the number of times (X, τ) occurs in either decompositions is $(\varphi \mid \chi) = (\varphi' \mid \chi)$. So, up to isomorphism, (V, ρ) and (W, σ) have the same decompositions. So $(V, \rho) \cong (W, \sigma)$.

($\Rightarrow$) This direction is immediate. □

Let (V, ρ) be a finite-degree representation, and suppose that

$$(V, \rho) = \left(\bigoplus_{m_1} (w_1, \rho_1)\right) \oplus \left(\bigoplus_{m_2} (W_2, \rho_2)\right) \oplus \cdots \oplus \left(\bigoplus_{m_k} (W_k, \rho_k)\right).$$

Let φ be a character of (V,ρ) and χ_i the character of (W_i,ρ_i). So $\varphi = m_1\chi_1 + \cdots + m_k\chi_k$, and

$$(\chi \mid \chi) = \left(\sum_{i=1}^{k} m_i\chi_i \mid \sum_{j=1}^{k} m_j\chi_j \right) = \sum_{i,j} m_i m_j \,(\chi_i \mid \chi_j) = \sum_i m_i^2.$$

Theorem 5. *Let (V,ρ) be a finite-degree representation and φ its character. Then $(\varphi \mid \varphi)$ is a positive integer. Moreover, $(\varphi \mid \varphi) = 1$ if and only if (V,ρ) is irreducible.*

Example 8. Let $\mathbf{B} = (\mathbb{C}^2, \sigma)$ be the irreducible representation of S_3, and let χ be its character. The character table is as follows:

π	id	(12)	(13)	(23)	(123)	(132)
$\chi(\pi)$	2	0	0	0	-1	-1

12. October 6

Definition 30. An *irreducible character* of G is a character of an irreducible representation of G.

Recall that if G is a finite group, then the set of irreducible characters of G is an orthonormal set of $\mathrm{ClaFun}(G)$. This proves that G has only finitely many irreducible representations, up to isomorphism. In particular, the number is bounded by $\dim(\mathrm{ClaFun}(G))$, which is the number of conjugacy classes of G.

Example 9. S_3 has 3 conjugacy classes; hence S_3 has at most 3 irreducible representations, up to isomorphism. We have already seen 3: namely $\mathbf{1}$ and $\mathbf{S}$ of degree 1 and $\mathbf{B}$ of degree 2. Thus we have found them all.

Let (V,ρ) be a finite-degree representation of G with character φ. Let (W,σ) be an irreducible representation of degree G with character χ. Let

$$(V,\rho) = (V_1,\rho_1) \oplus \cdots \oplus (V_k,\rho_k)$$

be the (essentially unique) direct-sum decomposition of (V,ρ) into a sum of irreducible representations.

Definition 31. We say that (W,ρ) *occurs in* (V,ρ) if $(W,\sigma) \cong (V_i,\rho_i)$ for some i. The *multiplicity of* (W,ρ) *in* (V,ρ) is $|\{i : (V,\rho_i) \cong (W,\sigma)\}|$ (which may equal 0).

Remark 5. The multiplicity of (W,σ) in (V,ρ) is $(\varphi|\chi)$.

Definition 32. Given a finite group G, let V be a complex vector space of dimension $|G|$ with basis $\mathscr{E} = \{e_g : g \in G\}$ indexed by the elements of G. For each $g \in G$ define $\rho_g \in \mathrm{GL}(V)$ by setting $\rho_g(e_h) = e_{gh}$, and extending linearly to all of V. Then (V,ρ) is called the *regular representation of* G, and we shall denote this character by r_G.

Clearly, we have $r_G(1) = \dim(V) = |G|$. Let $g \neq 1$. Then for each $h \in G$, we have

$$\rho_g(e_h) = e_{gh} = 0 \cdot e_1 + \cdots + 0 \cdot e_h + \cdots + 1 \cdot e_{gh} + \cdots .$$

Hence $[\rho_g]_{\mathscr{E}}$ has a 0 in the (h,h) position. Since h is arbitrary, it follows that all the diagonal entries of $[\rho_g]_{\mathscr{E}}$ are 0. Thus $\mathrm{tr}(\rho_g) = 0$, so we proved the following proposition:

Proposition 33. *The character r_G of the regular representation of a finite group G is*

$$r_G(g) = \begin{cases} |G| & (g = 1) \\ 0 & \textit{otherwise.} \end{cases}$$

Corollary 14. *Let G be finite and let (V, ρ) be its regular representation. Every irreducible representation (W, σ) of G occurs in (V, ρ), with multiplicity $\dim(W)$.*

Proof. Let χ be the character of (W, σ). Then the multiplicity of (W, σ) in (V, ρ) is

$$(r_G \,|\, \chi) = \frac{1}{|G|} \sum_{g \in G} r_G(g)\chi(g)^* = \frac{1}{|G|} r_G(1)\chi(1) = \frac{\dim(W) \cdot |G|}{|G|} = \dim(W),$$

as required. □

Suppose that $(W_1, \sigma_1), \ldots, (W_k, \sigma_k)$ are the distinct irreducible representations of G, and let $n_i = \dim(W_i)$ for each i. If χ_i denotes the character of $(W_i \sigma_i)$, then by the above corollary the regular representation decomposes as

$$(V, \rho) = n_1(W_1, \sigma_1) \oplus \cdots \oplus n_k(W_k, \sigma_k).$$

Hence $r_G = n_1\chi_1 + \cdots + n_k\chi_k$.

Corollary 15. *The following are true:*

(1) $\displaystyle\sum_{i=1}^{k} n_i^2 = |G|$.

(2) For all $g \neq 1$, $\displaystyle\sum_{i=1}^{k} n_i\chi_i(g) = 0$.

Proof. Evaluating the displayed equation at $g = 1$, we get $\dim(V) = n_1 \dim(W_1) + \cdots + n_k \dim(W_k) = n_1^2 + \cdots + n_k^2$ as required. The second part also follows from the second equation when $g \neq 1$. □

13. October 7

Recall that

- $\dim(\text{ClaFun}(G)) =$ # of conjugate classes of G
- $\{$irreducible characters for $G\}$ is an orthonormal set in $\text{ClaFun}(G)$.

Today, we show that the set of irreducible characters spans $\text{ClaFun}(G)$.

Fix $\alpha \in \text{ClaFun}(G)$. For each finite-degree representation (V, ρ) of G, define

$$f_\alpha^\rho : V \to V$$

by

$$f_\alpha^\rho(v) = \frac{1}{|G|} \sum_{g \in G} \alpha(g)\rho_g(v).$$

Clearly, f_α^ρ is linear. In fact,

Claim. f_α^ρ is a morphism from (V, ρ) to itself.

Proof. Must show that $\rho_g f = f\rho_g$ for all $g \in G$. Consider

$$\begin{aligned}\rho_g^{-1} f \rho_g &= \rho_g^{-1}\left(\frac{1}{|G|}\sum_h \alpha_h \rho_h\right)\rho_g \\ &= \frac{1}{|G|}\sum_h \alpha(h)\cdot \rho_g^{-1}\rho_h\rho_g = \frac{1}{|G|}\sum_h \alpha(h)\rho_{g^{-1}hg}.\end{aligned}$$

Let $u = g^{-1}hg \Leftrightarrow h = gug^{-1}$. Then

$$\begin{aligned}\frac{1}{|G|}\sum_h \alpha(h)\rho_{g^{-1}hg} &= \frac{1}{|G|}\sum_u \alpha(gug^{-1})\rho_u \\ &= \frac{1}{|G|}\sum_u \alpha(u)\rho_u = f.\end{aligned}$$

□

What is $\operatorname{tr}(f)$?

$$\begin{aligned}\operatorname{tr}\left(\frac{1}{|G|}\sum_{g\in G}\alpha(g)\rho_g\right) &= \frac{1}{|G|}\sum_{g\in G}\alpha(g)\operatorname{tr}(\rho_g) \\ &= \frac{1}{|G|}\sum_{g\in G}\alpha(g)\cdot\varphi(g) = (\alpha \mid \varphi^*).\end{aligned}$$

Proposition 34. *Suppose (V, ρ) is a degree n irreducible representation with χ its character, and if $\alpha \in \operatorname{ClaFun}(G)$, then f_α^ρ is a scalar mp ("multiplication by λ"), where $\lambda = \frac{1}{n}(\alpha \mid \chi^*)$.*

Proof. f_α^ρ is a morphism from (V, ρ) to itself. By Schur's lemma, f_α^ρ is scalar for some λ. With respect to any basis for V, we have

$$[f_\alpha^\rho] = \begin{pmatrix} \lambda & & 0 \\ & \ddots & \\ 0 & & \lambda \end{pmatrix}$$

so $\operatorname{tr}(f_\alpha^\rho) = n\lambda$. But $\operatorname{tr}(f_\alpha^\rho) = (\alpha \mid \chi^*) = n\lambda$. Thus $\lambda = \frac{1}{n}(\alpha \mid \chi^*)$, as required. □

What if (V, ρ) is not irreducible? Time to consider that case. Decompose $(V, \rho) = (W_1, \sigma_1) \oplus \cdots \oplus (W_k, \sigma_k)$, where each (W_i, σ_i) is irreducible.

Let $n = \dim V, m_i = \dim W_i$. Let χ_i be the character of (W_i, σ_i). Fix $\alpha \in \operatorname{ClaFun}(G)$. We have $f_\alpha^\rho : V \to V$, and for each i, $f_\alpha^{\sigma_i} : W_i \to W_i$, define $f_\alpha^{\sigma_i}(w) = \lambda_i w$.

Claim. $f_\alpha^\rho = f_\alpha^{\sigma_1} \oplus \cdots \oplus f_\alpha^{\sigma_k}$.

Proof of Claim. Need to check that, for $v \in V$, we can write $v = w_1 + \cdots w_k$ with $w_i \in W_i$.

$$\begin{aligned} f_\alpha^\rho(v) &= \frac{1}{|G|}\sum_{g\in G}\alpha(g)\rho_g(v) \\ &= \frac{1}{|G|}\sum_{g\in G}\alpha(g)((\sigma_1)_g(w_1) + \cdots + (\sigma_k)_g(w_k)) \\ &= \sum_{i=1}^{k}\frac{1}{|G|}\sum_{g\in G}\alpha(g)(\sigma_i)_g(w_i) = \sum_{i=1}^{k} f_\alpha^{\sigma_i}(w_i) \\ &= (f_\alpha^{\sigma_1}\oplus\cdots\oplus f_\alpha^{\sigma_k})(v). \end{aligned}$$ □

In general, for $\alpha \in \operatorname{ClaFun}(G)$ and with representation (V, ρ) with

$$(V,\rho) = (W_1,\sigma_1)\oplus\cdots\oplus(W_k,\sigma_k) \text{ and } v = w_1 + \cdots + w_k, w_i \in W_i,$$

we have

$$f_\alpha^\rho(v) = \sum_{i=1}^{k}\lambda_i w_i,$$

where $\lambda_i = \frac{1}{m_i}(\alpha \mid \chi_i^*), m_i = \dim W_i, \chi_i = \text{char of } (W_i, \sigma_i)$.

Theorem 6. *The irreducible characters of G span* $\operatorname{ClaFun}(G)$.

Proof. Let $\chi_1, \ldots, \chi_k$ be irreducible characters of G. Suffices to show that

$$\beta \in \operatorname{ClaFun}(G), (\chi_i \mid \beta) = 0 \ \forall i = 1, 2, \ldots, k,$$

then $\beta = 0$.

Suppose that $\beta \in \operatorname{ClaFun}(G)$ and $(\chi_i \mid \beta) = 0$ for all i. Let $\alpha = \beta^*$. It suffices to show that $\alpha = 0$. It is already known that $(\chi_i \mid \alpha^*) = (\alpha \mid \chi_i^*) = 0$ for all $i = 1, 2, \ldots, k$. By our analysis, for any finite-degree representations (V, ρ) of G, we have $f_\alpha^\rho = 0$. □

Apply this to the regular representations (V, ρ) of G, where V has basis $e_g, g \in G$ such that $\rho_g(e_h) = e_{gh}$. We get $f_\alpha^\rho = 0$. in particular, $f_\alpha^\rho(e_1) = 0$. Calculate this using definition:

$$f_\alpha^\rho(e_1) = \frac{1}{|G|}\sum_{g\in G}\alpha(g)\cdot\rho_g(e_1) = \frac{1}{|G|}\sum_{g\in G}\alpha(g)\cdot e_g = 0.$$

Thus $\alpha(g) = 0$ for all $g \in G$, so $\alpha \equiv 0$.

Theorem 7. *If G is finite, then the number of irreducible representations of G (up to isomorphism) is equal to the number of conjugacy classes of G.*

Here is one neat consequence of Theorem 6: Let G be a finite group, and pick $s \in G$ and let θ_s be its conjugacy class. Define $\alpha : G \to \mathbb{C}$ such that

$$\alpha(g) = \begin{cases} 1 & (g \in \theta_s) \\ 0 & \text{otherwise.} \end{cases}$$

By Theorem 6, α is a linear combination of irreducible characters of G. Let $\chi_1, \ldots, \chi_k$ be the irreducible characters of G. Write $\alpha = c_1\chi_1 + \cdots + c_k\chi_k$, with $c_i = (\alpha \mid \chi_i)$. (to be continued...)

14. October 9

Fix G and $\chi_1, \dots, \chi_k$ irreducible characters. Fix $s \in G$. Let θ_s be the conjugacy class of s. Define

$$f_s : G \to \mathbb{C}$$

to be

$$f_s(g) = \begin{cases} 1 & (g \in \theta_s) \\ 0 & \text{otherwise} \end{cases}.$$

Write

$$f_s = \sum_{i=1}^{k} a_i \chi_i.$$

Note that $(f_s \mid \chi_i) = \left(\sum_{j=1}^{k} a_j \chi_j \mid \chi_i\right) = \sum_{j=1}^{k} a_j \left(\chi_j \mid \chi_i\right) = a_i$. Also,

$$\begin{aligned}(f_s \mid \chi_i) &= \frac{1}{|G|} \sum_{g \in G} f_s(g) \chi_i(g)^* \\ &= \frac{1}{|G|} \sum_{g \in \theta_s} 1 \cdot \chi_i(g)^* \\ &= \frac{|\theta_s|}{|G|} \chi_i(g)^* = a_i.\end{aligned}$$

Thus

$$f_s = \sum_{i=1}^{k} \left(\frac{|\theta_s|}{|G|} \chi_i(s)^* \right) \chi_i.$$

Evaluate at s:

$$1 = f_s(s) = \frac{|\theta_s|}{|G|} \sum_{i=1}^{k} \chi_i(s)^* \chi_i(s) = \frac{|\theta_s|}{|G|} \sum_{i=1}^{k} |\chi_i(s)|^2.$$

Now suppose $t \in G \setminus \theta_s$. Evaluate at t:

$$0 = f_s(t) = \frac{|\theta_s|}{|G|} \sum_{i=1}^{k} \chi_i(s)^* \chi_i(t).$$

Thus we proved the following proposition:

Proposition 35. *Let $\chi_1, \dots, \chi_k$ be the irreducible characters of G, and let $s \in G$.*

(1) $\sum_{i=1}^{k} |\chi_i(s)|^2 = \frac{|G|}{|\theta_s|}$

(2) If $t \in G \setminus \theta_s$, then $\sum_{i=1}^{k} \chi_i(s)^* \chi_i(t) = 0$.

Example 10. Let's verify Proposition 35 when $s = 1$. Then $\chi_i(1) = n_i$, where n_i is the degree of representations for χ_i. Then we observe that

(1) $\sum_{i=1}^{k} n_i^2 = |G|$

(2) If $t \in G \setminus \{1\}$, then $\sum_{i=1}^{k} n_i\chi_i(t) = 0$.

Note that we saw this already, from $r_G = n_1\chi_1 + \cdots + n_k\chi_k$.

Example 11. Let's find the irreducible characters of D_5 (the dihedral group of order 10):

$$\begin{aligned} D_5 &= \langle r, s \mid r^5 = 1 = s^2, rs = sr^{-1} \rangle \\ &= \langle r \rangle \cup s\langle r \rangle \\ &= \{1, r, r^2, r^3, r^4\} \cup \{s, sr, sr^2, sr^3, sr^4\}. \end{aligned}$$

Conjugacy classes of D_5: $\{1\}, \theta_s = \{s, sr^{-2}, sr, sr^2, sr^4\}, \theta_r = \{r, r^{-1}\}, \theta_{r^2} = \{r^2, r^3\}$. Thus, D_5 has four irreducible characters, call them $\chi_1, \chi_2, \chi_3, \chi_4$, say of degrees n_1, n_2, n_3, n_4 respectively. Without loss of generality, let $n_1 \leq n_2 \leq n_3 \leq n_4$. There is only solution, namely $(n_1, n_2, n_3, n_4) = (1, 1, 2, 2)$. Time for some character table. Let χ_1 be the trivial character and χ_2 the sign character:

	1	s	r	r^2
χ_1	1	1	1	1
χ_2	1	-1	1	1
χ_3	2	a	c	e
χ_4	2	b	d	f

SInce $(\chi_3 \mid \chi_i) = 0$ for $i = 1, 2$, we have

$$\begin{aligned} (\chi_3 \mid \chi_1 - \chi_2) = 0 &= \frac{1}{|D_5|} \sum_{g \in D_5} \chi_3(g) \cdot ((\chi_1 - \chi_2)(g))^* \\ &= \frac{1}{10}(2 \cdot 0^* + 5(a \cdot 2^*) + 2(c \cdot 0^*) + 2(e \cdot 0^*) + 2(f \cdot 0^*)) = a. \end{aligned}$$

Similar calculation shows that $a = b = 0$. Now from $(\chi_3 \mid \chi_1) = 0$, we have

$$0 = \frac{1}{10}\left(2 \cdot 1 * + 5(0 \cdot 1^*) + 2(c \cdot 1^*) + 2(e \cdot 1^*)\right) = 2 + 2c + 2e,$$

so $e = -c - 1$. Similarly, we have $f = -d - 1$. Recall that $n_1^2 + n_2^2 + n_3^2 + n_4^2 = 10$. Thus since $n_1\chi_1(r) + \cdots + n_4\chi_4(r) = 0$, we have $2c + 2d = 0$, so $d = -c - 1$.

By (2) from Proposition 35,

$$\sum_{i=1}^{4} \chi_i(r)^*\chi_i(r^2) = 0,$$

so $1 + 1 + c^*(-c - 1) + (-c - 1)^*c = 0$. Simplify this to get $|c|^2 + \mathrm{Re}(c) = 1$. We also have

$$\sum_{i=1}^{4} |\chi_i(r)|^2 = \frac{|D_5|}{|\theta_r|} = 5,$$

so $1 + 1 + |c|^2 + |c + 1|^2 = 5$. Solve for c to get $c = \frac{-1 \pm \sqrt{5}}{2} = 2\cos\frac{2\pi}{5}$.

15. October 14

Fix:

- finite group G
- $(W_1, \sigma_1), \ldots, (W_k, \sigma_k)$ the list of irreducible representations (up to isomorphism)
- χ_i = character of (W_i, σ_i)
- $n_i = \dim(W_i) = \chi_i(1)$.

Let (V, ρ) be a finite-degree representation of G. How can we find G-invariant subspaces $U_1, \ldots, U_m$ of V so that

$$(V, \rho) = (U_1, \rho|_{U_1}) \oplus \cdots \oplus (U_m, \rho|_{U_m})$$

with each $(U_j, \rho|_{U_j})$ irreducible?

Assume that we have such

$$(V, \rho) = (U_1, \rho|_{U_1}) \oplus \cdots \oplus (U_{r(1)}, \rho_{U_{r(1)}}) \oplus (U_{r(1)+1}, \rho|_{U_{r(1)+1}}) \oplus \cdots \oplus$$
$$(U_{r(2)}, \rho|_{U_{r(2)}} \oplus \cdots \oplus (U_{r(k)}, \rho|_{U_{r(k)}}),$$

where we define $(V_i, \rho|_{V_i}) = (U_{r(i)+1}, \rho_{U_{r(i)+1}}) \oplus \cdots \oplus (U_{r(i+1)}, \rho|_{U_{r(i+1)}}) \cong (W_i, \sigma_i)$ for all i.

Theorem 8. *The subspaces $V_1, \ldots, V_k$ do not depend on the particular decomposition $V = U_1 \oplus \cdots \oplus U_m$ from which they arose.*

Proof. Start with a finite group of order $|G| = p_1^{n_1} \cdots p_k^{n_k}$. Then $G = H_1 \oplus \cdots \oplus H_k$ such that $|H_i| = p_i^{n_i}$, and fix some $i = 1, 2, \ldots, k$. Let χ_i be the character of (W_i, σ_i). Define $p_i : V \to V$ by

$$p_i = \frac{n_i}{|G|} \sum_{g \in G} \chi_i(g)^* \rho_g.$$

Note that p_i depends only on (V, ρ) and χ_i.

Define $\alpha \in \mathrm{ClaFun}(G)$ by $\alpha = n_i \chi_i^*$. Note also that

$$\rho_i = \frac{1}{|G|} \sum_{g \in G} \alpha(g) \rho_g = f_\alpha^\rho.$$

Note also that

$$p_i|_{U_j} = f_\alpha^\rho|_{U_j} = f_\alpha^{\rho|_{U_j}} : U_j \to U_j.$$

If $(U_j, \rho|_{U_j}) \cong (W_l, \sigma_l)$ for some l, then:

- the character of $(U_j, \rho|_{U_j})$ is χ_l
- $\dim(U_j) = n_l$
- By Proposition 34, $f_\alpha^{\rho|_{U_j}}$ is a scalar map, namely by
$$\lambda = \frac{1}{n_l} (\alpha \mid \chi_l^*) = (n_i \chi_i^* \mid \chi_l^*)$$
$$= n_i (\chi_i \mid \chi_l)^* = \begin{cases} n_i & \text{if } l = i \\ 0 & \text{otherwise,} \end{cases}$$
by orthogonality.

Hence p_i is the identity function on V_i, and is the zero function on all other V_l with $l \neq i$. So p_i is the projection map onto V_i with respect to $V = V_1 \oplus \cdots \oplus V_k$.

Thus $V_i = \mathrm{im}(p_i)$, and hence is determined intrinsically, as desired. □

Definition 36. The decomposition

$$(V,\rho) = (V_1, \rho|_{V_1}) \oplus \cdots \oplus (V_k, \rho|_{V_k})$$

is called the *canonical decomposition of* (V,ρ).

We still want to further decompose each of $(V_i, \rho|_{V_i})$.

15.1. **How to further decompose.** Here we outline methods on how to further decompose each of $(V_i, \rho|_{V_i})$.

(1) Fix i
(2) Have (W_i, σ_i), and choose a basis $\mathbf{e} = (e_1, \ldots, e_n)$ for W_i. Note that $n = n_i$ in this case.
(3) Let $[(\sigma_i)_g]_{\mathbf{e}} = (r_{st}(g))_{n\times n}$. This gives us $r_{st} \in \mathbb{C}^G$, where $1 \le s, t \le n$.
(4) Note that $\chi_i = r_{11} + \ldots r_{nn}$, and by Corollary 8,

$$\langle r_{st}, r_{uv}\rangle = \begin{cases} \frac{1}{n_i} & \text{if } s = v, t = u \\ 0 & \text{otherwise.} \end{cases}$$

Definition 37. For any representation (U,τ) of G, define, for $1 \le s, t \le n$,

$$p^\tau_{st} : U \to U$$

by

$$p^\tau_{st} = \frac{n_i}{|G|}\sum_{g\in G} r_{ts}(g^{-1})\tau_g.$$

Suppose that (U,τ) is irreducible but not isomorphic to (W_i,σ_i). Pick a basis $\mathbf{e}' = (e'_1, \ldots, e'_n)$ for U.

$$[\tau_g]_{\mathbf{e}'} = (\tilde{r}_{uv}(g))_{m\times m}.$$

Then for each e'_u,

$$p^\tau_{st}(e'_u) = \frac{n_i}{|G|}\sum_{g\in G} r_{ts}(g^{-1})\tau_g(e'_u).$$

Then we have

$$[\tau_g]_{\mathbf{e}'} = \begin{pmatrix} \tilde{r}_{11}(g) & \cdots & \tilde{r}_{im}(g) \\ \vdots & \ddots & \vdots \\ \tilde{r}_{m1}(g) & \cdots & \tilde{r}_{mm}(g) \end{pmatrix} e'_u = \begin{pmatrix} \tilde{r}_{1u}(g) \\ \vdots \\ \tilde{r}_{mu}(g) \end{pmatrix} \sim \sum_{v=1}^m \tilde{r}_{vu}(g).$$

Then for each e'_u, we have

$$p^\tau_{st}(e'_u) = \frac{n_i}{|G|}\sum_{g\in G} r_{ts}(g^{-1})\tau_g(e'_u) \tag{4}$$

$$= \frac{n_i}{|G|}\sum_{g\in G} r_{ts}(g^{-1})\sum_{v=1}^m \tilde{r}_{vu}(g)e'_v \tag{5}$$

$$= n_i\sum_{v=1}^m\left(\frac{1}{|G|}\sum_{g\in G} r_{ts}(g^{-1})\tilde{r}_{vu}(g)\right)e'_v, \tag{6}$$

and $\langle r_{ts}, \tilde{r}_{vu}\rangle = 0$. Thus (6) becomes 0. By Corollary 7, since true for all e'_i, we have $p^\tau_{st} \equiv 0$.

16. October 16

Suppose G is finite, and $(W_1, \sigma_1), \dots, (W_k, \sigma_k)$ irreducible representations. Suppose $\chi_1, \dots, \chi_k$ their characters. Let (V, ρ) be some random representation (finite-degree). Fix some $1 \le i \le k$, and let $n_i := \dim W_i$. Choose basis $\mathbf{e} = (e_1, \dots, e_n)$ for W_i. Write $[(\sigma_i)_g]_{\mathbf{e}} = (r_{st}(g))_{n\times n}$.

Given a rep (U, τ) and $1 \le s, t \le n$, define

$$p_{st}^{\tau} = \frac{n}{|G|} \sum_{g\in G} r_{ts}(g^{-1})\tau_g : U \to U.$$

Last time, we claimed that if (U, τ) is irreducible and $\ncong (W_i, \sigma_i)$ then all p_{st}^{τ} is 0.

Proof. Let $\mathbf{e}'$ be a basis for U. For each e'_u, we have

$$p_{st}^{\tau}(e'_u) = n_i \sum_{v=1}^{n} \langle r_{ts}, \tilde{r}_{vu}\rangle e'_v.$$

Repeat this calc, but when $(U, \tau) = (W_i, \sigma_i)$, then let $\mathbf{e}' = \mathbf{e}$. Then $(\tilde{r}_{uv}(g))_{n\times n} = [(\sigma_i)_g]_{\mathbf{e}} = (r_{uv}(g))$. Get:

$$\begin{aligned} p_{st}^{\sigma_i}(e_u) &= n_i \sum_{v=1}^{n} \langle r_{ts}, r_{vu}\rangle e_v \\ &= n_i \sum_{v=1}^{n} \left(\frac{1}{n_i}\delta_{tu}\delta_{sv}\right) e_v \quad \text{(by Corollary 8)} \\ &= \delta_{tu} \sum_{v=1}^{n} \delta_{sv} e_v = \delta_{tu} e_s. \end{aligned}$$

When $t \neq u$, then we have $p_{st}^{\sigma_i}(e_u) = 0$; if $t = u$, then $p_{st}^{\sigma_i}(e_t) = e_s$. So (on W_i), $p_{st}^{\sigma_i}$ sends e_t to e_s, and every other basis elements e_u to 0. □

Recall that our main goal is to decompose (V, ρ). Suppose hat we know a decomposition:

$$(V,\rho) = \underbrace{(U_1, \rho|_{U_1}) \oplus \cdots \oplus (U_{r(1)}, \rho|_{U_{r(1)}})}_{=:V_1 \cong (W_1,\sigma_1)} \oplus \cdots \oplus \underbrace{(U_{l+1}, \rho|_{l+1}) \oplus \cdots \oplus (U_{l+m}, \rho|_{U_{l+m}})}_{=V_i \cong (W_i,\sigma_i)} \oplus \cdots.$$

We can find $V_1, \dots, V_k$. Goal : find candidates for $U_{l+1}, \dots, U_{l+m}$. Let $p_{st} = p_{st}^{\rho} : V \to V$. From calculations, we have:

1. $p_{st}|_{U_r}$ with $(U_r, \rho|_{U_r}) \cong (W_i, \sigma_i) \Rightarrow p_{st}^{\rho|_{U_r}} = 0$.
2. Hence $p_{st}|_{V_j} = 0$ if $j \neq i$.

As for $p_{st}|_{V_i}$, write $V_i = U_{l+1} \oplus U_{l+m}$, with each $(U_{l+j}, \rho|_{U_{l+j}} \cong (W_i, \sigma_i)$. Let $e_1^{(j)}, \dots, e_n^{(j)} \in U_{l+j}$ be the image of $e_1 \dots, e_n \in W_i$ under an isomorphism.

Observe that, on U_{l+j}, we have $p_{st}(e_t^{(j)}) = e_s^{(j)}$, and $p_{st}(e_u^{(j)}) = 0$ if $u \neq t$. Hence, p_{11} is a projection from V to $\operatorname{span}(e_1^{(1)}, e_1^{(2)}, \dots, e_1^{(m)}) = V_{i,1}$, and p_{22} a projection from V to $\operatorname{span}(e_2^{(1)}, \dots, e_2^{(m)}) = V_{i,2}$, etc. Reverse-engineer this: Start with (V, ρ). Fix a basis $\mathbf{e}$ for W_i. Have $(r_{st}(g))_{n\times n} = [(\sigma_i)_g]_{\mathbf{e}}$, so $p_{st} = p_{st}^{\rho} : V \to V$. Let $V_{i,1} = \operatorname{range}(p_{11})$. Next, pick a basis for $V_{i,1}$, say $e_1^{(1)}, \dots, e_1^{(m)}$. For $s = 2, \dots, n$, define

$$e_s^{(j)} = p_{s1}(e_1^{(j)}) \in \operatorname{range}(p_{ss}) = V_{i,s}.$$

Now define $U_{l+1} := \text{span}(e_1^{(1)}, \ldots, e_n^{(1)}$, and define $U_{l+2}, \ldots$ in a similar manner. We need to check that:

- each U_{l+j} is G-invariant;
- $V_i = U_{l+1} \oplus \cdots \oplus U_{l+m}$;
- Each $(U_{l+j}, \rho|_{U_{l+j}}) \cong (W_i, \sigma_i)$.

17. October 20

17.1. **Subgroups and products.** Suppose that (V, ρ) is a representation of G. So $\rho : G \to \text{GL}(V)$. Let $H \leq G$. Then $\rho|_H : H \to \text{GL}(V)$, so $(V, \rho|_H =: \rho_H)$ is a representation of H.

Proposition 38. *Suppose that $H \leq G$. Let k be the maximum degree of irreducible representations of H. Then every irreducible representation of G has degree $\leq k \cdot [G : H]$.*

Proof. Let (V, ρ) be an irreducible representation of G. Then (V, ρ_H) is a representation of H. Pick an irreducible subrepresentation $(W, \rho_H|_W)$ of (V, ρ_H). Note that $\dim(W) \leq k$. Look at all images of $\rho_g(W)$ for all $g \in G$. Note also that if $h \in H$, then $\rho_H(W) = W$. If $g_1 H = g_2 H$, then in particular $g_2 = g_1 h$ for some $h \in H$. Thus $\rho_{g_2}(W) = \rho_{g_1 h}(W) = (\rho_{g_1} \circ \rho_h)(W) = \rho_{g_1}(W)$, since $\rho_h(W) = W$. Then the number of different $\rho_g(W)$ is at most $[G : H]$. Let $V' = \text{span}\left(\bigcup_{g \in G} \rho_g(W)\right) \leq V$. "Clearly", V' is a G-invariant subspace of V, and $\dim V' \geq 1$. But (V, ρ) is irreducible, so $V' = V$. So

$$\begin{aligned} \dim(V) = \dim(V') &\leq \sum_{\rho_g(W)} \underbrace{\dim(\rho_g(W))}_{=\dim(W)} \\ &= \dim(W) \cdot (\#\text{ of distinct } \rho_g(W)\text{'s}) \\ &\leq k \cdot [G : H]. \end{aligned}$$

□

Corollary 16. *Suppose that G has an* abelian *subgroup $A \leq G$. Then every irreducible representation of G has degree at most $[G : A]$.*

Proof. This follows from the fact that every irreducible representation of A has degree 1. □

One application: if D_n is a dihedral group of order $2n$, then D_n has a cyclic subgroup of order n. Thus every irreducible representation of D_{2n} has degree ≤ 2.

17.2. **Direct products.** Suppose that $G = G_1 \times G_2$, and let $(V_1, \rho^1), (V_2, \rho^2)$ representations of G_1 and G_2, respectively. Let π_1, π_2 to be canonical projections from G onto G_1 and G_2, respectively. By Assignment #4, $(V_1, \rho^1 \circ \pi_1$ and $(V_2, \rho^2 \circ \pi_2)$ are representations of G. Take their tensor product: $(V_1 \otimes V_2, (\rho^1 \circ \pi_1) \oplus (\rho^2 \circ \pi_2))$. Write $\rho^1 \boxtimes \rho^2 := (\rho^1 \circ \pi_1) \otimes (\rho^2 \circ \pi_2)$. So $(V_1 \otimes V_2, \rho^1 \boxtimes \rho^2)$.

Note. If $g = (g_1, g_2)$, then on simple tensors,

$$\begin{aligned} (\rho^1 \boxtimes \rho^2)_g (v_1 \otimes v_2) &= ((\rho^1 \circ \pi_1)_g \otimes (\rho^2 \circ \pi_2)_g)(v_1 \otimes v_2) \\ &= (\rho^1_{g_1} \otimes \rho^2_{g_2})(v_1 \otimes v_2) = \rho^1_{g_1}(v_1) \otimes \rho^2_{g_2}(v_2). \end{aligned}$$

Let χ_1 and χ_2 be the characters of (V_1, ρ^1) and (V_2, ρ^2) respectively. Then:

- $(V_1, \rho^1 \circ \pi_1)$ has character $\chi_1 \circ \pi_1$
- $(V_2, \rho^2 \circ \pi_2)$ has character $\chi_2 \circ \pi_2$.

Thus $(V_1 \otimes V_2, \rho^1 \boxtimes \rho^2)$ has character $(\chi_1 \circ \pi_1) \cdot (\chi_2 \circ \pi_2)$.

Let $\varphi = (\chi_1 \circ \pi_1) \cdot (\chi_2 \circ \pi_2)$, and $\varphi : G \to \mathbb{C}$. If $g = (g_1, g_2) \in G$, then $\varphi(g) = (\chi_1 \circ \pi_1)(g) \cdot (\chi_2 \circ \pi_2)(g) = \chi_1(g_1) \cdot \chi_2(g_2)$.

Theorem 9. *Suppose $G = G_1 \times G_2$. If (V_1, ρ^1) and (V_2, ρ^2) are irreducible representations of G_1, G_2, then $(V_1 \otimes V_2, \rho^1 \boxtimes \rho^2)$ is an irreducible representation of G.*

Proof. Let χ_i be the character of (V_i, ρ^i), and φ the character of $(V_1 \otimes V_2, \rho^1 \boxtimes \rho^2)$. It suffices to show that $(\varphi \mid \varphi) = 1$.

$$\begin{aligned}
(\varphi \mid \varphi) &= \frac{1}{|G|} \sum_{g \in G} |\varphi(g)|^2 = \frac{1}{|G|} \sum_{(g_1, g_2) \in G_1 \times G_2} |\chi_1(g_1)\chi_2(g_2)|^2 \\
&= \frac{1}{|G|} \sum_{\substack{g_1 \in G_1 \\ g_2 \in G_2}} |\chi_1(g_1)|^2 \cdot |\chi_2(g_2)|^2 \\
&= \frac{1}{|G|} \left(\sum_{g_1 \in G_1} |\chi_1(g_1)|^2 \right) \left(\sum_{g_2 \in G_2} |\chi_2(g_2)|^2 \right) \\
&= \left(\frac{1}{|G_1|} \sum_{g_1 \in G_1} |\chi_1(g_1)|^2 \right) \left(\frac{1}{|G_2|} \sum_{g_2 \in G_2} |\chi_2(g_2)|^2 \right) \\
&= (\chi_1 \mid \chi_1) \cdot (\chi_2 \mid \chi_2) = 1,
\end{aligned}$$

so $(\chi_1 \mid \chi_1) = (\chi_2 \mid \chi_2) = 1$. □

Remark 6. If $(V_1, \rho^1), (V_2, \rho^2)$ are arbitrary representations and $(V_1 \otimes V_2, \rho^1 \boxtimes \rho^2)$ is irreducible, then each (V_i, ρ^i) must be irreducible.

18. October 21

Suppose $G = G_1 \times G_2$, and (V_1, ρ^1) representations of G_1 with char χ_1; similarly, (W_1, σ^1) a representation of G_2 with character χ_2. Then $(V_1 \otimes W_1, \rho^1 \boxtimes \sigma^1)$ is a representation of G with character χ.

(1) $\chi(g) = \chi_1(g_1) \cdot \chi_2(g_2)$ for $g = (g_1, g_2) \in G$
(2) $(\chi \mid \chi) = (\chi_1 \mid \chi_1) \cdot (\chi_2 \mid \chi_2)$
(3) χ is irreducible if and only if χ_1, χ_2 irreducible.

Define (V_2, ρ^2) to be a second representation of G_1 with character φ_1 and (W_2, σ^2) a second representation of G_2 with character φ_2. Same recipe gives $(V_2 \otimes W_2, \rho^2 \boxtimes \sigma^2)$ with character φ. And we can also get

$$(\chi \mid \varphi) = (\chi_1 \mid \varphi_1) \cdot (\chi_2 \mid \varphi_2) .$$

Lemma 8. *In this situation, assume that $(V_1, \rho^1), (V_2, \rho^2), (W_1, \sigma^1), (W_2, \sigma^2)$ are irreducible. Then*

$$(V_1 \otimes W_1, \rho^1 \boxtimes \sigma^1) \cong (V_2 \otimes W_2, \rho^2 \boxtimes \sigma^2)$$

if and only if

$$(V_1, \rho^1) \cong (V_2, \rho^2) \text{ and } (W_1, \sigma^1) \cong (W_2, \sigma^2).$$

Proof. (⇒) We prove the contrapositive. Assume without loss of generality that $(V_1, \rho^1) \not\cong (V_2, \rho^2)$, with characters χ_1, φ_1. By irreducibility, we have $(\chi_1 \mid \varphi_1) = 0$. Then $(\chi \mid \varphi) = (\chi_1 \mid \varphi_1) \cdot (\chi_2 \mid \varphi_2) = 0$. Therefore $(V_1 \otimes W_1, \cdot) \not\cong (V_2 \otimes W_2, \cdot)$, as desired.

(⇐) This part is immediate. □

Theorem 10. *Suppose that $G = G_1 \times G_2$. Every irreducible representation of G is of the form (= is isomorphic to) $(V_1 \otimes W_1, \rho^1 \boxtimes \sigma^1)$, for some (V_1, ρ^1) irreducible representation of G_1 and (W_1, σ^1) irreducible representation of G_2.*

Proof. Let (V_i, ρ^i) be the irreducible representations of G_1 for $1 \leq i \leq k$ with character φ_1. Similarly, let (W_j, σ^j) be the irreducible representation of G_2 for $1 \leq j \leq l$ with character φ_2. Our recipe gives kl non-isomorphic irreducible representations of G of the form $(V_i \otimes W_j, \rho^i \boxtimes \sigma^j)$. Let $m_i = \dim(V_i), n_j = \dim(W_j)$. We know that $m_1^2 + \cdots + m_k^2 = |G_1|$ and $n_1^2 + \cdots + n_l^2 = |G_2|$. So $\sum(\text{degree of irreducible representation of } G)^2 = |G|$.

Looking at the irreducible representation of G that we know,

$$\begin{aligned} |G| \geq \sum_{\substack{1\leq i \leq k \\ 1 \leq j \leq l}} \dim(V_i \otimes W_j)^2 &= \sum_{i,j} (m_i n_j)^2 \\ &= \left(\sum_i m_i^2\right)\left(\sum_j n_j^2\right) \\ &= |G_1| \cdot |G_2| = |G|. \end{aligned}$$

Thus, there are no other "room" for any other irreducible representations of G. □

18.1. **Induced representations.** If H is a subgroup of G and (V, ρ) is a representation of G, then (V, ρ_H) is the corresponding representation of H. Let W be an H-invariant subspace. Get $(W, \rho_H|_W)$ a representation of H. Let $\theta = \rho_H|_W : H \to \mathrm{GL}(W)$. Now, for each $g \in G, \rho_g(W) \leq V$. As on Monday, if $g_1 H = g_2 H$, then $\rho_{g_1}(W) = \rho_{g_2}(W)$. Let $G/H = \{\text{all left cosets of } H\}$. For each $gH \in G/H$, define $W_{gH} := \rho_g(W)$. Note that this operation is well-defined.

Definition 39. Let $(V, \rho), H, W, \theta$ be as above. We say (W, θ) *induces* (V, ρ) if V is the direct sum of $(W_{gH} : gH \in G/H)$. In other words, we have bases $\mathbf{e}_{gH}$ for each W_{gH} such that:

(1) $\mathbf{e}_{gH}, \mathbf{e}_{g'H}$ are disjoint if $gH \neq g'H$.
(2) The union of the $\mathbf{e}_{gH}$ is a basis for V.

Example 12. Let (V, ρ) be the regular representation of G, i.e., we have a basis $\{e_g : g \in G\}$ for V, and $\rho_g(e_h) = e_{gh}$. Given $H \leq G$, let $W = \mathrm{span}(\{e_h : h \in H\}) \leq V$.

What are the W_{gH}?

$$\begin{aligned} W_{gH} = \rho_g(W) &= \rho_g(\mathrm{span}\{e_h : h \in H\}) \\ &= \mathrm{span}\{\rho_g(e_h) : h \in H\} \\ &= \mathrm{span}\{e_{gh} : h \in H\}. \end{aligned}$$

If $\theta = \rho_H|_W$, then (W, θ) induces (V, ρ).

19. October 23

Question 1. If $G = G_1 \times G_2, (V, \rho)$ an irreducible representation of G, then $(V, \rho) \cong (X \otimes Y, \sigma \boxtimes \tau)$ for some irreducible representation (X, σ) of G_1 and (Y, τ) of G_2. How can we find $(X, \sigma), (Y, \tau)$?

Answer 1. Say $(X_1, \sigma^1), \ldots, (X_k, \sigma^k)$ be a list of the irreducible representations of G_1, and let $(Y_1, \tau_1), \ldots, (Y_l, \tau_l)$ be a list of representations of G_2. Say $\chi_i = \text{char}(X_i, \sigma_i), \varphi_j = (Y_j, \tau_j)$. Let $\theta = \text{char}(V, \rho)$. Then

$$\theta((g_1, g_2)) = \chi_i(g_1) \cdot \varphi_j(g_2) = \text{character for } (X_i \otimes Y_j, \sigma^i \boxtimes \tau^j).$$

Question 2 (Real question!)**.** How do I find the isomorphism between (V, ρ) and $(X_i \otimes Y_j, \sigma^i \boxtimes \tau^j)$?

Answer 2. More generally, given irreducible representations $(V, \rho), (W, \sigma)$ of G, plus a promise they are isomorphic. How can we find an isomorphism?

Fact 1. $\text{Hom} := \text{Hom}((V, \rho), (W, \sigma)) = \{\text{set of all morphisms from } (V, \rho) \text{ to } (W, \sigma)\}$ is a l-dimensional vector space over $\mathbb{C}$, consisting of

- constant zero map.
- continuum-many isomorphisms.

Proof. Pick an isomorphism $\varphi : (W, \sigma) \cong (V, \rho)$. Given $h \in \text{Hom}$, the map $\varphi \circ h : (V, \rho) \to (V, \rho)$ is scalar, say, $(\varphi \circ h)(v) = \lambda_h v$. Now, randomly pick a linear map $f : V \to W$. Use recipe from Corollary 6. Namely, define $f^0 : (V, \rho) \to (W, \sigma)$ such that

$$f^0 = \frac{1}{|G|} \sum_{g \in G} \sigma_{g^{-1}} \circ f \circ \rho_g.$$

Then $f^0 \in \text{Hom}$. And "probably" $f^0 \neq 0$, and if so, we have that f^0 is an isomorphism from (V, ρ) to (W, σ). $\square$

Recall from the October 21 lecture that if

- (V, ρ) a representation of G
- $H \leq G$
- H-invraitn subspace W of V

then (V, ρ_H) is a representation of H. Let $(W, \rho_H|_W) = (W, \theta)$ is a subrepresentation. Now we define the following notion:

Definition 40. We say that (W, θ) *induces* (V, ρ) if V is the direct sum of $W_{gH}\,(gH \in G/H)$ where $W_{gH} = \rho_g(W)$. Also, if (V, ρ) is the *regular representation of* G (i.e., basis for $V = \{e_g : g \in G\}$) and $W := \text{span}\left(\{e_h : h \in H\}\right)$ and $\theta = \rho_H|_W$ then (W, θ) *induces* (V, ρ).

Remark 7. If $H \leq G$, then the regular representation of H induces the regular representation of G.

19.1. **Universal property of induced representations.**

Lemma 9. *Suppose that (V, ρ) is a representation of G and $H \leq G$. Let W be an H-invariant subspace of V, and $(W, \theta := \rho_H|_W)$ induces (V, ρ). Then for all representation (X, σ) of G and for all morphism $f : (W, \theta) \to (X, \sigma_H)$, there exists a* unique *morphism $F : (V, \rho) \to (X, \sigma)$ extending f.*

Proof. We first start with uniqueness. Suppose that $F_1, F_2 : (V,\rho) \to (X,\sigma)$. Suppose also that $F_1|_W = F_2|_W = f$. To prove that $F_1 = F_2$, enough to prove that

$$F_1|_{W_{gH}} = F_2|_{W_{gH}}$$

for all gH. Fix an arbitrary gH. Consider $W_{gH} = \rho_g(W)$. Let $x \in W_{gH}$. THen $x = \rho_g(w)$ for some $w \in W$. Thus we have

$$\begin{aligned} F_1(x) &= F_1(\rho_g(w)) = \sigma_g(F_1(w)) \quad (\because F_1 \text{ a morphism}) \\ &= \sigma_g(f(w)) \quad (\because F_1|_W = f) \\ &= F_2(x). \end{aligned}$$

Now we move on to proving the existence. For this, it is sufficient to define $F|_{W_{gH}}$. Fix gH. For $x \in W_{gH}$, choose $w \in W$ so that $x = \rho_g(w)$. Define $F(x) = \sigma_g(f(w))$. We need to verify first if $(F|_{W_{gH}})$ is well-defined, i.e. must not depend on g or w. Assume $g_1H = g_2H$ and $w_1, w_2 \in W$ so that $x = \rho_{g_1}(w_1) = \rho_{g_2}(w_2)$. We must show that $\sigma_{g_1}(f(w_1)) = \sigma_{g_2}(f(w_2))$. Let $h = g_2^{-1}g_1 \in H$. Then $\theta_h(w_1) = \rho_h(w_1) = \rho_{g_2^{-1}g_1}(w_1) = (\rho_{g_2})^{-1}(\rho_{g_1}(w)) = \rho_{g_2}^{-1}(x) = w_2$. So $f(w_2) = f(\theta_h(w_1)) = (\sigma_H)_h(f(w_1)) = \sigma_h(f(w_1))$. Therefore, $\sigma_{g_2}(f(w_2)) = \sigma_{g_2}(\sigma_h(f(w_1))) = \sigma_{g_1}(f(w_1))$. ∎

20. October 27

Theorem 11. *Assume $H \leq G$. Let (W,θ) be a representation of H. Then there exists a representation (V,ρ) of G induced by (W,θ) and (V,ρ) is unique up to isomorphism.*

Proof. For existence, we need the following lemmas:

Lemma 10 (Lemma A)**.** *Suppose that (W,θ) induces (V,ρ) and W_1 is an H-invariant subspace of W. Let $V_1 := \sum_{gH \in G/H} \rho_g(W_1)$ (hence a subspace of V). Then:*

(1) V_1 is G-invariant.
(2) $(W_1, \theta|_{W_1})$ induces $(V_1, \rho|_{V_1})$.

Lemma 11 (Lemma B)**.** *Suppose (W_1,θ^1) and (W_2,θ^2) are representations of H. Suppose also that (W_i,θ^i) induces (V_i,ρ^i) for $i = 1,2$. Then $(W_1,\theta^1) \oplus (W_2,\theta^2)$ induces $(V_1,\rho^1) \oplus (V_2,\rho^2)$.*

Now let (W,θ) be a representation of H. Consider the following cases:

Case 1. (W,θ) is irreducible. Then (W,θ) is isomorphic to a subrepresentation of $(\overline{W},\overline{\theta})$ of R_H. Recall that R_H induces R_G. Then by Lemma A, $(\overline{W},\overline{\theta}) \cong (W,\theta)$ induces some representation of G.

Case 2. (W,θ) is not irreducible. Write $(W,\theta) = (W_1,\theta^1) \oplus \cdots \oplus (W_k,\theta^k)$, with each (W_i,θ^i) irreducible. By applying Lemma B and Case 1, we get that (W,θ) induces some representation of G.

For uniqueness, suppose that (W,θ) is a representation of H and it induces (V,ρ) and (V',ρ'). Note that $W \subseteq V$ and $W \subseteq V'$. Also, we have $\dim(V) = [G:H]\dim(W) = \dim(V')$. Let $\iota : W \to V'$ be the inclusion map $\iota(w) = w$. As (W,θ) is a subrepresentation of (V,ρ_H), $\iota : (W,\theta) \to (V,\rho_H)$ is a morphism. Since (V,ρ) is induced by (W,θ), the universal property gives that there is a morphism $F : (V,\rho) \to (V',\rho')$ extending i (so if $w \in W$ then $F(w) = \iota(w)$).

Claim. For all $gH \in G/H$, we have $\rho'_g(W) \subset \operatorname{im}(F)$.

Proof. Let $x \in \rho'_g(W)$, so $x = \rho'_g(w), w \in W$. Then $x = \rho'_g(w) = \rho'_g(F(w)) = F(\rho_g(w))$. $\square$

Since
$$V' = \sum_{gH \in G/H} \rho'_g(W),$$
it impiles that F is surjective hence is an isomorphism. $\square$

Definition 41. Given $H \leq G$, a representation (W, θ) of H, let $\operatorname{Ind}_H^G(W, \theta)$ denote *the representation of G induced by* (W, θ).

Example 13. Define $G = S_3, H = \langle(123)\rangle$. Let (C, θ) be this representation of H:
$$\begin{aligned}\theta_{\text{id}} &= (x \mapsto x)\\ \theta_{(123)} &= (x \mapsto \omega x)\\ \theta_{(132)} &= (x \mapsto \omega^2 x).\end{aligned}$$
What is $\operatorname{Ind}_H^{S_3}(\mathbb{C}, \theta)$? We know that $[S_3 : H] = 2$. So the underlying subspace of $\operatorname{Ind}_H^{S_3}(\mathbb{C}, \theta)$ will have the form $\mathbb{C} \oplus \underbrace{\rho_{(12)}(\mathbb{C})}_{\mathbb{C}'}$. Since $\rho_{(12)}^2 = \text{id}$, we can choose $\mathbb{C}'(= \rho_{(12)}(\mathbb{C}))$, an isomorphic copy of $\mathbb{C}$ such that $\rho_{(12)}(z) = z', \rho_{(12)}(z') = z$ and $V = \mathbb{C} \oplus \mathbb{C}'$ with $\rho_{(123)}|_{\mathbb{C}} = \theta_{(123)} = (x \mapsto \omega x)$. As for $\rho_{(123)}|_{\mathbb{C}'}$, if $x' \in \mathbb{C}'$ then $x' = \rho_{(12)}(x)$ $(x \in \mathbb{C})$. So $\rho_{(123)}(x') = \rho_{(123)}(\rho_{(12)}(x)) = \rho_{(12)}(\rho_{(132)}(x)) = \rho_{(12)}(w^2 x) = w^2 x'$. Thus $\rho_{(123)}|_{\mathbb{C}'} = (x' \mapsto \omega^2 x')$.

Thus, if $\mathbf{e} = (1, 1')$, a basis for $V = \mathbb{C} \oplus \mathbb{C}'$, then
$$\begin{aligned}[\rho_{(12)}]_{\mathbf{e}} &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\\ [\rho_{(123)}]_{\mathbf{e}} &= \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}.\end{aligned}$$
By Assignment #3 Problem #6, we have $(V, \rho) \cong \mathbf{B}$, the unique irreducible representation of S_3 of degree 2.

21. October 28

As usual, suppose $H \leq G$, and let (W, θ) representation of H and $(V, \rho) := \operatorname{Ind}_H^G(W, \theta)$. Let $R \subseteq G$ be a set of representatives of the left cosets of H (assume $1 \in R$. Then $|R| = [G : H], RH = G$. As usual, we have $W \leq V$. For $r \in R$, define $W_r = \rho_r(W)$ (for 1, let $W_1 = \rho_1(W) = W$).

Let $\mathbf{e}_1 = (e_1, \ldots, e_k)$ be a basis for W_1. For $r \in R$, define $\mathbf{e}_r = (\rho_r(e_1), \ldots, \rho_r(e_k))$, a basis for W_r. By definition, we have
$$V = \bigoplus_{r \in R} W_r.$$
For $g \in G$, ρ_g acts on W_r's, and let $\mathbf{e} = \bigcup_{r \in R} \mathbf{e}_r$, which is a basis for V. Fix $g \in G, r \in R$. Then g acts on the left cosets of H. Then g permutes R, i.e., $g(rH) = sH$, where $s \in R$. If

$gr \in g(rH)$, then $gr \in sH$, thus $gr = sh$ for some $h \in H$. Take $w' \in W_r = \rho(W)$, and write $w' = \rho_r(w)$ for some $w \in W$. Then we have

$$\begin{aligned}\rho_g(w') &= \rho_g(\rho_r(w)) = \rho_s(\rho_h(w)) \\ &= \rho_s(\theta_h(w)) \quad (\text{since } \rho_H|_W = \theta) \\ &= \rho_s(\underbrace{\theta_h(\underbrace{\rho_r^{-1}(w')}_{\in W})}_{\in W}) \in W_s.\end{aligned}$$

Hence, $\rho_g(W_r) \subseteq W_s$. Thus,

$$\rho_g|_{W_r} = (\rho_s|_W) \circ \theta_h \circ (\rho_r|_W)^{-1}.$$

This means that $[\rho_g]_{\mathbf{e}}$ is a block-form matrix (row-blocks, column-blocks indexed by R). That is, if $\rho_g(W_r) = W_s$, then

$$[\rho_g]_{\mathbf{e}} = \begin{pmatrix} 0 \\ 0 \\ [\theta_h]_{\mathbf{e}_1} \\ 0 \\ 0 \end{pmatrix},$$

where the block $[\theta_h]_{\mathbf{e}_1}$ is located in the "r-th" block column and "s-th" block row (note that we assume $gr = sh$). Each row-block and each column-block have exactly one non-zero block. If we have a non-zero block in row s, column r, then the block is $[\theta_h]_{\mathbf{e}_1}$, where $h \in H, s^{-1}gr = h$.

Let χ_θ be the character of (W, θ). Similarly, let χ_ρ be the character of (V, ρ). Fix $g \in G$. Recall that

$$\begin{aligned}\chi_\rho(g) = \operatorname{tr}(\rho_g) = \operatorname{tr}([\rho_g]_{\mathbf{e}}) &= \sum_{\substack{r \in R \\ r^{-1}gr = h \in H}} \overbrace{\operatorname{tr}([\theta_h]_{\mathbf{e}_1})}^{\chi_\theta(h)} \\ &= \sum_{\substack{r \in R \\ r^{-1}gr \in H}} \chi_\theta(r^{-1}gr) = \frac{1}{|H|} \sum_{\substack{a \in G \\ a^{-1}ga \in H}} \chi_\theta(a^{-1}ga)\end{aligned}$$

(Note that if $a \in rH$ and $r^{-1}gr \in H$, then $a^{-1}ga \in H$, and in this case, they are conjugate in H.)

Let $\theta(g)$ = conjugacy classes of g (in G). If $\theta(g) \cap H = \emptyset$, then $\chi_\rho(g) = 0$. Else, pick $h \in \theta(g) \cap H$.

Claim. $\{a \in G : a^{-1}ga = h\}$ is a right coset of $C_G(g) = \{h \in G : gh = hg\}$, the centralizer of g.

So

$$\chi_\rho(g) = \frac{1}{|H|} \sum_{\substack{h \in H \cap \theta(g) \\ a \in \{a \in G : a^{-1}ga = h\}}} \chi_\theta(h)$$

$$= \frac{|C_G(g)|}{|H|} \sum_{h \in H \cap \theta(g)} \chi_\theta(h)$$

$$= \frac{|G|}{|H| \cdot |\theta(g)|} \sum_{h \in H \cap \theta(g)} \chi_\theta(h). \quad (|C_G(g)| = |G|/|\theta(g)|)$$

Example 14. If $G = S_3, H = \langle (123) \rangle$, and the representation has degree 1 (say $(\mathbb{C}, \theta)$), then the character table for $\chi_\theta(h)$ is

h	id	(123)	(132)
$\chi_\theta(h)$	1	ω	ω^2

Let $(V, \rho) = \mathrm{Ind}_H^{S_3}(\mathbb{C}, \theta) = \mathbf{B}$ with the character χ_ρ. Using the formula, we get

g	id	(abc)	(ab)
$\chi_\rho(g)$	?	?	?

Let $g = \mathrm{id}$. Then $\theta(g) = \{id\}$, so $\theta(g) \cap H \neq \emptyset$. Thus

$$\chi_\rho(\mathrm{id}) = \frac{6}{3 \cdot 1} \chi_\theta(\mathrm{id}) = 2.$$

As for $(123) = g$, we have $\theta(g) = \{(123), (132)\}$. $H \cap \theta(g) \neq \emptyset$, so we use the given formula again:

$$\chi_\rho((123)) = \frac{6}{3 \cdot 2} (\chi_\theta((123)) + \chi_\theta((132))) = w + w^2 = -1.$$

Similarly, since the $\theta(g) \cap H = \emptyset$ for $g = (12)$, we have $\chi_\rho(g) = 0$.

22. October 30

To start off, let's find all irreducible representation of A_5, with 1 identity, 20 three-cycles, 24 five-cycles, and 15 elements of the form $(ab)(cd)$. There are five conjugacy classes: $\{\mathrm{id}\}, \{\text{all 3-cycles}\}, \theta((12345)), \theta((21345)), \{\text{all } (ab)(cd)\}$. Now we need two character tables, one for irreducible representations and another for other representations.

We denote $\mathbf{1}$ the trivial representation of degree 1, with character χ_1. Then χ_1 is the trivial character. Define $\mathbf{P} := (\mathbb{C}^5, \rho)$ with $e_1, e_2, \ldots, e_5$ the standard basis such that $\rho_g(e_i) := e_{g(i)}$. Thus, so far we have

	$\{\mathrm{id}\}$	(abc)	$(ab)(cd)$	(12345)	(21345)
χ_1	1	1	1	1	1

	$\{\mathrm{id}\}$	(abc)	$(ab)(cd)$	(12345)	(21345)
$\chi_{\mathbf{P}}$	5	2	1	0	0

Note that, if

	$\{\mathrm{id}\}$	(abc)	$(ab)(cd)$	(12345)	(21345)
φ	a	b	c	d	e
ψ	a'	b'	c'	d'	e'

we have $(\varphi \mid \varphi) = \frac{1}{60}(|a|^2 + 20|b|^2 + 15|c|^2 + 12|d|^2 + 12|e|^2)$, and since $(\chi_{\mathbf{P}} \mid \chi_{\mathbf{P}}) = 2$, $\mathbf{P}$ is not irreducible! But since $(\chi_{\mathbf{P}} \mid \chi_{\mathbf{1}}) = 1$, we have $\mathbf{P} = \mathbf{1} \oplus \mathbf{Q}$ with $\mathbf{Q}$ some irreducible representation, so $\chi_{\mathbf{P}} = \chi_{\mathbf{1}} + \chi_{\mathbf{Q}}$. Use this to compute $\chi_{\mathbf{Q}}$.

Now consider $\mathbf{Q} \otimes \mathbf{Q} = \mathbf{S} \oplus \mathbf{A}$, where $\mathbf{S} := \mathrm{Sym}^2(\mathbf{Q}), \mathbf{A} := \mathrm{Alt}^2(\mathbf{Q})$. Note that we can calculate $\chi_{\mathbf{Q}\otimes\mathbf{Q}}$ from $\chi_{\mathbf{Q}}$. Use the decomposition to calculate $\chi_{\mathbf{S}}$ and $\chi_{\mathbf{A}}$:

$$(\chi_{\mathbf{S}} \mid \chi_{\mathbf{1}}) = \frac{1}{60}(10 + 20 \cdot 1 + 15 \cdot 2) = 1$$
$$(\chi_{\mathbf{S}} \mid \chi_{\mathbf{Q}}) = \frac{1}{60}(40 + 20 \cdot 1) = 1.$$

Therefore, $\mathbf{S} = \mathbf{1} \oplus \mathbf{Q} \oplus \mathbf{T}$, so $\chi_{\mathbf{S}} = \chi_{\mathbf{1}} + \chi_{\mathbf{Q}} + \chi_{\mathbf{T}}$. Since

$$(\chi_{\mathbf{T}} \mid \chi_{\mathbf{T}}) = \frac{1}{60}(25 + 20 \cdot 1 + 15 \cdot 1) = 1.$$

Thus, $\mathbf{T}$ is irreducible. So far, our two character tables are as follows:

	$\{\mathrm{id}\}$	(abc)	$(ab)(cd)$	(12345)	(21345)
χ_1	1	1	1	1	1
$\chi_{\mathbf{Q}}$	4	1	0	-1	-1
$\chi_{\mathbf{T}}$	5	-1	1	0	0

	$\{\mathrm{id}\}$	(abc)	$(ab)(cd)$	(12345)	(21345)
$\chi_{\mathbf{P}}$	5	2	1	0	0
$\chi_{\mathbf{Q}\otimes\mathbf{Q}}$	16	1	0	1	1
$\chi_{\mathbf{S}}$	10	1	2	0	0
$\chi_{\mathbf{A}}$	6	0	-2	1	1

We need 5 irreducible representation, so we are yet to find 2 more irreducible representations. Let the two remaining representations be $\mathbf{B}$ and $\mathbf{C}$. If $m_{\mathbf{B}} = \deg(\mathbf{B})$ and $m_{\mathbf{C}} = \deg(\mathbf{C})$, then $1^2 + 4^2 + 5^2 + m_{\mathbf{B}}^2 + m_{\mathbf{C}}^2 = |A_5| = 60$. Therefore $m_{\mathbf{B}} = m_{\mathbf{C}} = 3$. Note that there is no $\mathbf{1}, \mathbf{Q}, \mathbf{T}$ in the decomposition of $\mathbf{A}$, since $(\chi_{\mathbf{A}} \mid \chi_{\mathbf{1}}) = (\chi_{\mathbf{A}} \mid \chi_{\mathbf{Q}}) = (\chi_{\mathbf{A}} \mid \chi_{\mathbf{T}}) = 0$. Hence $\chi_{\mathbf{A}} = \chi_{\mathbf{B}} + \chi_{\mathbf{C}}$ since $\mathbf{A} = \mathbf{B} \oplus \mathbf{C}$. This implies that final values are $b, c = \frac{1 \pm \sqrt{5}}{2}$. Thus the final character tables are:

	$\{\mathrm{id}\}$	(abc)	$(ab)(cd)$	(12345)	(21345)
χ_1	1	1	1	1	1
$\chi_{\mathbf{Q}}$	4	1	0	-1	-1
$\chi_{\mathbf{T}}$	5	-1	1	0	0
$\chi_{\mathbf{B}}$	3	0	-1	b	c
$\chi_{\mathbf{C}}$	3	0	-1	c	b

	$\{\mathrm{id}\}$	(abc)	$(ab)(cd)$	(12345)	(21345)
$\chi_{\mathbf{P}}$	5	2	1	0	0
$\chi_{\mathbf{Q}\otimes\mathbf{Q}}$	16	1	0	1	1
$\chi_{\mathbf{S}}$	10	1	2	0	0
$\chi_{\mathbf{A}}$	6	0	-2	1	1

Question 3. What are $\mathbf{T}, \mathbf{B}, \mathbf{C}$?

Answer 3. **T**: We need a representation of $K \lhd A_4$ of degree 1, where K is the Klein 4-subgroup.

$$\begin{aligned} A_4 &\to \mathrm{GL}(C) \\ g \in K &\mapsto \mathrm{id} \\ (123)K &\mapsto (x \mapsto \omega x) \\ \text{other cosets} &\mapsto (x \mapsto \omega^2 x) \end{aligned}$$

Call this representation (C, θ) of A_4. Then $\mathrm{Ind}_{A_4}^{A_5}(\mathbb{C}, \theta)$ is the representation of A_5 of degree 5.

As for **B** or **C**, we start with the fact that A_5 is isomorphic to the group of rigid symmetries of the dodecahedron:

$$\begin{array}{ccc} A_5 & \longrightarrow & SO_3 \leq \mathrm{GL}(\mathbb{R}^3) \\ & \searrow^{\textbf{B} \text{ or } \textbf{C}} & \downarrow \\ & & \mathrm{GL}(\mathbb{C}^3) \end{array}$$

A_5 has a nontrivial automorphism, τ, namely conjugation by (12).

Claim. G = group of rigid symmetries of dodecahedron "is" A_5.

Proof. 12 faces, and 5 rotations of a face, hence $|G| = 60$. Need to see how G acts on (some) 5-element. (Google the diagram!) □

23. November 3

23.1. **Introduction to modules.**

Definition 42. Let R be a ring (always with 1). A *(left) R-module* is an abelian group $(A, +)$ with a "scalar multiplication" operation $R \times A \to A$ defined as $(r, a) \mapsto ra$, satisfying the "usual" axioms:

- $(r + s)a = ra + sa$
- $(rs)a = r(sa)$
- $1a = a$
- $r(a + b) = ra + rb$.

We write ${}_RA$ if A is a left R-module.

Example 15. If F is a field, then every F-module is a vector space over F.

Example 16. Every abelian group $(A, +)$ can be viewed as a $\mathbb{Z}$-module, i.e., $\mathbb{Z}$-modules $\equiv$ abelian groups.

Example 17. R can be viewed as an R-module ${}_RR$.

Definition 43. Let ${}_RA$ be an R-module. Then

(1) A *submodule* is a subgroup of $(A, +)$ closed under scalar multiplication.
(2) Given $a \in A$, the *cyclic submodule generated by* a is $\{ra : r \in R\} =: Ra$.

Example 18. Some examples:

- Submodules of ${}_FV$ are exactly the subspaces of V, and $Fa = \mathrm{span}\{a\}$.
- Submodules of ${}_{\mathbb{Z}}A \equiv$ subgroups of $(A, +)$ and $\mathbb{Z}a = \langle a \rangle$

- Submodules of ${}_RR \equiv$ left ideals of R.

Definition 44. Suppose that ${}_RA$ and ${}_RB$ are R-modules. Then a *module homomorphism* from ${}_RA$ to ${}_RB$ is a homomorphism $h : (A, +) \to (B, +)$ satisfying $h(ra) = r \cdot h(a)$.

Example 19. Some selected examples of (module) homomorphisms:

(1) If F is a field, then any homomorphism from ${}_FV$ to ${}_FVW$ is a linear map.
(2) Homomorphisms from ${}_{\mathbb{Z}}A$ to ${}_{\mathbb{Z}}B$ are just group homomorphisms.
(3) Consider ${}_RR$. Let ${}_RA$ be any R-module. Given $a \in A$, define $h_a : R \to A$ by $h_a(r) = ra$.

Claim. h_a is a homomorphism from ${}_RR$ to ${}_RA$.

Proof. For $r, s \in R$:

$$\begin{aligned} h_a(r+s) &= (r+s)a \\ &= ra + sa \ (\because {}_RA \text{ is an } R\text{-module}) \\ &= h_a(r) + h_a(s). \end{aligned}$$

For any $r, s \in R$, must show $h_a(rs) = rh_a(s)$:

$$\begin{aligned} h_a(rs) &= (rs)a \\ &= r(sa) \ (\because {}_RA \text{ is an } R\text{-module}) \\ &= rh_a(s), \end{aligned}$$

as required. □

Definition 45. We define $\mathrm{Hom}_R(R, A)$ to be the set of all R-module homomorphisms from ${}_RR$ to ${}_RA$.

Fact 2. $\mathrm{Hom}_R(R, A) = \{h_a : a \in A\}$.

Fact 3. ${}_RR$ is the free R-module on one generator (1) (in the category of all R-modules). Given $h : {}_RR \to {}_RA$, left $a = h(1)$. Then $h = h_a$ (exercise!).

Definition 46. GIven ${}_RA_1, \cdots, {}_RA_k$ R-modules, their *(external) direct sum* is the group $A_1 \times \cdots \times A_k$ with scalar multiplication defined coordinate-wise:

$$r(a_1, a_2, \dots, a_k) = (ra_1, \dots, ra_k).$$

This direct sum is denoted by ${}_RA_1 \oplus \cdots \oplus {}_RA_k$ it is an R-module.

Definition 47. Given ${}_RA$ and $B_1, \dots, B_k$ submodules of A, we say that ${}_RA$ is the *internal direct sum* of $B_1, \dots, B_k$ if every $a \in A$ can be *uniquely* expressed as as $a = b_1 + \cdots + b_k$ with $b_i \in B_i$. We write in this case, ${}_RA = B_1 \oplus \cdots \oplus B_k$.

Fact 4. Usual facts about the direct sums:

(1) If ${}_RA = B_1 \oplus \cdots \oplus B_k$ (internal direct sum) then ${}_RA \cong {}_RB_1 \oplus \cdots \oplus {}_RB_k$ (external).
(2) If ${}_RA \cong {}_RA_1 \oplus \cdots \oplus {}_RA_k$ (external) then there exist submodules $B_1, \dots, B_k$ with ${}_RA = B_1 \oplus \cdots \oplus B_k$ (internal) and, for all i, ${}_RB_i \cong {}_RA_i$.

23.2. **Tensor products over noncommutative rings.**

Remark 8. Tensor products over commutative rings are easily defined and have "beautiful" properties. Unfortunately, over noncommutative rings it is messy and rather subtle. In this course we will primarily focus on noncommutative rings.

Definition 48. Given R a ring, we can also define the notion of *right R-module*, with scalar multiplication defined as $A \times R \to A$ defined as $a(rs) = (ar)s$. Other key axioms can be defined accordingly, with elements of R multiplied on the right-side rather than left.

Definition 49. Given rings R and S, an (R, S)-*bimodule* is an abelian group $(A, +)$ with two scalar multiple operations $R \times A \to A$ and $A \times S \to A$ so that A is a left R-module $({}_RA)$ and a right S-module (A_S), satisfying $r(as) = (ra)s$ for all $r \in R, s \in S, a \in A$. We write ${}_RA_S$ if A is an (R, S)-bimodule.

Example 20. If R is commutative, then every ${}_RA$ is naturally a right R-module A_R and an (R, R)-bimodule ${}_RA_R$ by $ar := ra$. To verify this, we need to verify four axioms. The only less obvious one to verify is $a(rs) = (ar)s$:

$$\begin{aligned} a(rs) &:= (rs)a = (sr)a \ (\because R \text{ is commutative}) \\ &= s(ra) = (ar)s. \end{aligned}$$

Similarly, one can check $r(as) = (ra)s$:

$$r(as) = r(sa) = (rs)a = (sr)a = s(ra) = (ra)s.$$

24. November 4

Example 21. More examples of R-modules:

(1) If R is commutative, then the left R-modules $\equiv$ right R-modules $\equiv$ (R, R)-bimodules
(2) More generally, if ${}_RA$ is a left R-module, and C is the centre of R then we can view ${}_RA$ as an (R, C)-bimodule ${}_RA_C$. Define (right-)multiplication as follows: if $a \in A, c \in C$, define $a \cdot c = ca$ (already defined). We can check that A_C is a right C-modue, i.e. $r(ac) = (ra)c$ for all $r \in R, c \in C, a \in A$. Note that $r(ac) = r(ca) = (rc)a = (cr)a = c(ra) = (ra)c$.
(3) Every ring R is an (R, R)-bimodule.
(4) If ${}_RA$ is a left R-module, then we can view it as an $(R, \mathbb{Z})$-bimodule ${}_RA_{\mathbb{Z}}$.
(5) Given a bimodule ${}_RA_S$, then for any subrings $R_1 \leq R$ and $S_1 \leq S$, we get an (R_1, S_1)-bimodule ${}_{R_1}A_{S_1}$ (by "forgetting" some scalar multiplications).

24.1. **Tensor product of modules.**

Definition 50. Let R be a ring, and let A_R be a right R-module and ${}_RB$ a left R-module. We say that F is a *free abelian group with a basis* $\{e_{(a,b)} : (a, b) \in A \times B\}$ if F consists of elements of the form $n_1 e_{(a_1,b_1)} + \cdots + n_k e_{(a_k,b_k)}$ with $k \geq 0, (a_i, b_i) \in A \times B, n_i \in \mathbb{Z}$. Let H be the smallest subgroup of F containing all:

$$\begin{aligned} e_{(a_1+a_2,b)} - e_{(a_1,b)} - e(a_2, b) &\quad (a_1, a_2 \in A, b \in B) \\ e_{(a,b_1+b_2)} - e_{(a,b_1)} - e_{(a,b_2)} &\quad (a \in A, b_1, b_2 \in B) \\ e_{(ar,b)} - e_{(a,rb)} &\quad (a \in A, b \in B, r \in R). \end{aligned}$$

Then the *tensor product of A and B*, $A \otimes_R B$, is defined as F/H.

Definition 51. For $(a, b) \in A \times B$, define $a \otimes b = e_{(a,b)} + H \in F/H$. Define $\iota : A \times B \to A \otimes_R B$ by $\iota(a, b) = a \otimes b$.

Definition 52. If C is an abelian group, and A_R right R-module and ${}_RB$ left R-module, then a function $\alpha : A \times B \to C$ is *middle R-bilinear* (or *R-balanced*) if

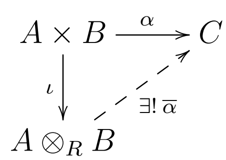
- $\alpha(a_1 + a_2, b) = \alpha(a_1, b) + \alpha(a_2, b)$
- $\alpha(a, b_1 + b_2) = \alpha(a, b_1) + \alpha(a, b_2)$
- $\alpha(ar, b) = \alpha(a, rb)$.

Claim. $\iota : A \times B \to A \otimes_R B$ is middle R-bilinear.

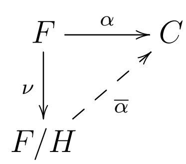
Proof. Check $\iota(ar, b) = \iota(a, rb)$. We have $\iota(ar, b) = (ar) \otimes b = e_{(ar,b)} + H$, and $\iota(a, rb) = a \otimes (rb) = e_{(a,rb)} + H$, and $e_{(ar,b)} + H = e_{(a,rb)} + H$ since $e_{(ar,b)} - e_{(a,rb)} \in H$.

Other axioms can be checked in a similar manner. □

Claim. For any abelian group C, any middle R-bilinear map $\alpha : A \times B \to C$, there exists a *unique* group homomorphism $\overline{\alpha} : A \otimes_R B \to C$ such that $\overline{\alpha} \circ \iota = \alpha$.



Namely, we want $\overline{\alpha}$ so that the diagram below commutes:



Proof. Recall that F is a free abelian group. We can define a (unique)group homomorphism $\alpha^* : F \to C$ satisfying $\alpha^*(e_{(a,b)}) = \alpha(a, b)$ for all $(a, b) \in A \times B$. Since α is middle R-bilinear, $\ker(\alpha^*)$ contains $e_{(a_1+a_2,b)} - e_{(a_1,b)} - e_{(a_2,b)}$, etc. Since

$$\alpha(a_1 + a_2, b) = \alpha(a_1, b) + \alpha(a_2, b)$$
$$\alpha^*(e_{(a_1+a_2,b)}) = \alpha(e_{(a_1,b)}) + \alpha(e_{(a_2,b)}) = \alpha(e_{(a_1,b)} + e_{(a_2,b)}).$$

Hence $\alpha^*(e_{(a_1+a_2,b)}) - e_{(a_1,b)} - e_{(a_2,b)} = 0$. Thus, $H \subseteq \ker(\alpha^*)$. □

Now we try to turn $A \otimes_R B$ into a module. Two possible methods:

Method 24.1. We will attempt to construct ${}_SA_R$ and ${}_RB$. Form $A \otimes_R B$, and define an action of S on left by $s(a \otimes b) = (sa) \otimes b$. This will turn $A \otimes_R B$ into a left S-mobule ${}_SA \otimes_R B$.

Method 24.2. We need a ring S, and R must be a subring of the centre of S. Then we need two left S-modules ${}_SA$ and ${}_SB$, and we will get a new S-submodule.

25. November 6

Let R be a ring, A_R and ${}_RB$ be modules. Then $A \otimes_R B$ is an abelian group. Now we turn $A \otimes_R B$ into a left S-module.

Method 25.1. Went A is an (S,R)-bimodule (${}_SA_B$), then for $s \in S$ declare $s(a \otimes b) = (sa) \otimes b$. Extend linearly to sums of simple tensors. Formally, given $s \in S$, define $\alpha_s : A \times B \to A \otimes_R B$ by $\alpha_s(a,b) = (sa) \otimes b$.

Claim. α_s is middle R-bilinear.

Proof. Additive in the first variable, since

$$\begin{aligned} \alpha_s(a_1 + a_2, b) &= s(a_1 + a_2) \otimes b = (sa_1 + sa_2) \otimes b \\ &= sa_1 \otimes b + sa_2 \otimes b = \alpha_s(a_1, b) + \alpha_s(a_2, b). \\ \alpha_s(ar, b) &= s(ar) \otimes b = (sa)r \otimes b \\ &= sa \otimes rb = \alpha_s(a, rb). \end{aligned}$$

By the universal property, there exists a unique group homomorphism $\overline{\alpha_s} : A \otimes_R B \to A \otimes_R B$ such that $\overline{\alpha_s} \circ \iota = \alpha_s$, i.e., $\overline{\alpha_s}(a \otimes b) = \alpha_s(a,b) = (sa) \otimes b$, where $\iota(a,b) = a \otimes b$.

Define a left action of S on $A \otimes_R B$. For $x \in A \otimes_R B$ and $sinS$, let $s \cdot x = \overline{\alpha_s}(x)$. You will show in the assignment to show that this gives a left S-module ${}_SA \otimes_R B$. □

Definition 53. ${}_SA \otimes_R B$ as defined in Method 25.1 is called the *left tensor product of* ${}_SA_R$ *with* ${}_RB$.

Method 25.2. Given ${}_SA$ and ${}_SB$, and R a subring of the centre of S, we can view ${}_SA$ as ${}_SA_R$ and ${}_SB$ as ${}_RB$. The idea is that for $s \in S$, let $s(a \otimes b) = (sa) \otimes (sb)$ (need to verify if it's well-defined) and then extend linearly.

To formalize this, define (for $s \in S$) $\beta_s : A \times B \to A \otimes_R B$ by $\beta_s(a,b) := (sa) \otimes (sb)$. Check middle R-bilinearity:

$$\begin{aligned} \beta_s(ar, b) &= s(ar) \otimes (sb) = (sa)r \otimes (sb) = (sa) \otimes r(sb) \\ &= (sa) \otimes (rs)b = (sa) \otimes (sr)b = (sa) \otimes s(rb) \\ &= \beta_s(a, rb). \end{aligned}$$

Thus ${}_SB$ is a left S-module as r is in the centre of S. Repeat this argument from Method 1 to obtain $\overline{\beta_s} : A \otimes_R B \to A \otimes_R B$ and define $s \cdot x = \overline{\beta_s}(x)$. This gives another left S-module denoted

$${}_S(A \otimes_R B).$$

Remark 9. Upon comparing the two methods, the second method is nicer, which gives the cleaner output ${}_SA \otimes_R B$, and is symmetric, i.e., ${}_S(A \otimes_R B) \cong {}_S(B \otimes_R A)$. The first method is uglier in nearly all respects, since it is not uniform and not symmetric. However, method 1 has no restrictions on R and S.

Example 22 (Application of the first method). Suppose that R and S are rings with $R \leq S$, and that ${}_RB$ is given. It will be nice if we can make this an S-module. This is called the *extension of scalars*.

Recall that we can consider S as ${}_SS_S$ and ${}_SS_R$. We can apply the first method to get ${}_SS \otimes_R B =: {}_S\overline{B}$, a left S-module. Define $\iota : B \to \overline{B}$ by $\iota(b) = 1 \otimes b$.

Claim. $\iota : {}_RB \to {}_R\overline{B}$ is an R-module homomorphism.

Proof. For addition, we have

$$\iota(b_1 + b_2) = 1 \otimes (b_1 + b_2) = 1 \otimes b_1 + 1 \otimes b_2 = \iota(b_1) + \iota(b_2).$$

As for multiplication, for $r \in R$ and the multiplication definition of S on $S \otimes_R B$.

$$\iota(rb) = 1 \otimes (rb) = 1r \otimes b = r1 \otimes b = r(1 \otimes b) = r \cdot \iota(b).$$

□

If ι is injective, then ${}_RB$ is $\cong$ to a submodule of ${}_R\overline{B}$, the restriction to R of ${}_S\overline{B}$.

Example 23. If $S = R$, then ${}_RB \cong {}_R\overline{B}$. In fact, ι serves as an isomorphism.

Example 24. If F, K are fields and $F \leq K$, and if ${}_FV$ is a vector space over F, then

$${}_FV \to {}_KK \otimes_F V = {}_K\overline{V},$$

a vector space over K of same dimension as ${}_FV$.

Example 25. Let A be a finite abelian group. Then we can view A as a left $\mathbb{Z}$-module ${}_\mathbb{Z}A$. Let $S = \mathbb{Q}$. Then ${}_\mathbb{Z}A \to {}_\mathbb{Q}\mathbb{Q} \times {}_\mathbb{Z}A = {}_\mathbb{Q}\overline{A}$. And in the assignment, you will prove that, in fact, $\left|{}_\mathbb{Q}\overline{A}\right| = 1$, the zero vector space!

26. November 10: Semisimple rings and their modules

Definition 54. Let R be a ring. An R-module ${}_RA$ is *simple* if:

- $A \neq \{0\}$
- its only submodules are $\{0\}$ and ${}_RA$.

Example 26. If $R = F$ is a field, then simple F-modules are one-dimensional vector spaces over F (only one up to isomorphism).

Example 27. $R = \mathbb{Z}$. Simple $\mathbb{Z}$-modules are simple abelian groups, i.e., $(\mathbb{Z}/p\mathbb{Z}, +)$, p prime.

Suppose that ${}_RA$ is a simple R-module. Pick $a \in A, a \neq 0$. Then

$$\{0\} \neq Ra \leq {}_RA,$$

so $A = Ra$. Since cyclic, ${}_RA \cong {}_R(R, +)/I$, for some left ideal I (by Assignment #6). The submodules of a simple module ${}_R(R, +)/I$ correspond to the left ideals of R containing I, by the correspondence theorem. Therefore I is a maximal left ideal.

Lemma 12. *Every simple* ${}_RA$ *is isomorphic to* ${}_R(R, +)/I$, *with* I *a maximal left ideal of* R.

If $R = F$ is a field, and $R = \mathrm{M}_n(F)$, then one can find all the maximal left ideals I of R. Thus one can determine, up to isomorphism, all simple R-modules. In fact, all are isomorphic to $(F, +)^n$, with R acting on this group by left-multiplication by matrices. We can also show that

Lemma 13. *Let* $R = \mathrm{M}_n(F)$. *Then* ${}_R(R, +)$ *can be written as a direct sum of simple modules.*

Proof. For $i = 1, 2, \ldots, n$, let S_i be the set of $n \times n$ matrices which are 0 everywhere except for the i-th column. We can also show that:

- each S_i is a submodule of ${}_R(R, +)$
- each S_i is isomorphic to ${}_R(F, +)^n$ (so is simple)

- ${}_R(R,+) = S_1 \oplus \cdots \oplus S_n$.

Then the claim follows. □

Definition 55. A ring R is *semisimple* if ${}_R(R,+)$ can be written as a direct sum of simple R-modules.

Theorem 12 (Wedderburn's theorem I)**.** *Suppose that R is semisimple. Then every R-module ${}_RA$ can be written as a direct sum of (possibly infinitely many) simple R-modules.*

Proof (sketch, when $R = \mathrm{M}_n(F)$). For $i = 1, 2, \ldots, n$, let e_i be matrix with 1 at (i,i)-position and 0 elsewhere. we note the following facts about e_i:

- $e_i^2 = e_i$
- $e_ie_j = 0$ for all $i \neq j$
- $e_1 + e_2 + \cdots + e_n = 1$.

Let $S_i = Re_i$. Now let ${}_RA$ be an R-module, and let $a \in A$.

Claim. Each S_ia is a submodule of ${}_RA$, and ${}_RS_ia$ is a homomorphic image of ${}_RS_i$. Therefore, S_ia is either isomorphic to ${}_RS_i$ or is $\{0\}$.

Note that $a \in S_1a + \cdots + S_na$, since $a = 1a = (e_1 + \cdots + e_n)a \in S_1a + \cdots + S_na$. Therefore, each $a \in A$ belongs to the sum of some simple submodules. Now, we apply Zorn's lemma ("Zornification (?)"). □

Remark 10. Note that everything about $\mathrm{M}_n(F)$ is true for $\mathrm{M}_n(D)$, where D is a division ring (i.e. has all the properties of fields except that it need not be commutative).

26.1. **Direct product of rings.** Suppose $R = R_1 \times R_2 \times \cdots \times R_k$. Observe that if ${}_{R_i}A$ is an R_i-module, then it is naturally an R-module, via $(r_1, r_2, \ldots, r_k) \cdot a = r_ia$. Conversely, for $i = 1, 2, \ldots, k$, let $e_i = (0, 0, \ldots, 0, 1, 0, \ldots, 0) \in R$ (i.e., 1 in the i-th entry only).

Lemma 14. *Let ${}_RA$ be an R-module. For $i = 1, 2, \ldots, k$, let $A_i = e_iA$. Then:*

(1) Each A_i is a submodule of ${}_RA$.
(2) Each A_i is naturally an R_i-module (i.e., $r_ia = (0, 0, \ldots, 0, r_i, 0, \ldots, 0)a$)
(3) ${}_RA = {}_RA_1 \oplus \cdots \oplus {}_RA_k$. (Morally, ${}_RA$ decomposes into ${}_{R_1}A_1, \ldots, {}_{R_k}A_k$.)

Definition 56. If $R = R_1 \times \cdots \times R_k$ and

$$ {}_RA = {}_RA_1 \oplus \cdots \oplus {}_RA_k, $$

then this decomposition is called the *canonical decomposition of* ${}_RA$, relative to $R = R_1 \times \cdots \times R_k$.

Corollary 17. *If R, S are semisimple, then so is $R \times S$.*

Proof. Consider the canonical decomposition of $(R \times S, +)$:

$$ {}_{R\times S}(R \times S, +) \text{“} \cong \text{”} {}_R(R,+) \oplus {}_S(S,+). $$

□

Theorem 13 (Wedderburn's theorem II)**.** *Let R be a ring. Then:*

(1) R is semisimple if and only if

$$ R \cong \mathrm{M}_{n_1}(D_1) \times \mathrm{M}_{n_2}(D_2) \times \cdots \times \mathrm{M}_{n_k}(D_k) $$

for some division rings $D_1, D_2, \ldots, D_k$ and $n_1, n_2, \ldots, n_k \geq 1$.

(2) If R is semisimple and *R has a subring F, which:*

- *is an* algebraically closed *field*
- *is contained in the centre of* R
- *and* $\dim_F(R) < \infty$,

then $D_1 = D_2 = D_3 = \cdots = D_k = F$.

27. November 11: Return to Serre (Chapter VI)!

Now that we finished the excursion, time to remind ourselves of some usual notation: let G be a finite group, and let V be the vector space in the regular representation of G with a basis $\{e_g : g \in G\}$. Define a product operation on V, and the idea was that $e_g \cdot e_h = e_{gh}$. Then we extend linearly to all the elements of V. If $G = \{g_1, g_2, \dots, g_n\}$, and every $v \in V$ can be written

$$v = \sum_{i=1}^{n} c_i e_{g_i}.$$

Formally expand the product:

$$\left(\sum_{i=1}^{n} a_i e_{g_i}\right) \cdot \left(\sum_{j=1}^{n} b_j e_{g_j}\right) = \sum_{i,j} a_i b_j e_{g_i g_j}$$

$$= \sum_{g \in G} \left(\sum_{g_i g_j = g} a_i b_j\right) e_g.$$

Definition 57. The structure $(V, +, \cdot)$ we just constructed is called the *group ring of* G *over* $\mathbb{C}$, and we write $\mathbb{C}[G]$ or $\mathbb{C}G$.

Proposition 58. *A few facts about group rings:*

1. *It is a ring.*
2. *A group ring is commutative if and only if* G *is abelian.*
3. *Its identity element is* e_1.
4. $\operatorname{span}_{\mathbb{C}}(e_1) = \{ce_1 : c \in \mathbb{C}\}$ *is a subring of* $\mathbb{C}[G]$.
5. $\operatorname{span}_{\mathbb{C}}(e_1) \cong \mathbb{C}$ *(ring isomorphism).*
6. $\operatorname{span}_{\mathbb{C}}(e_1)$ *is contained in the centre of* $\mathbb{C}[G]$.

Proofs of (4) and (5). Define $f : \mathbb{C} \to \mathbb{C}[G]$ by $f(c) = ce_1$. Obviously $f(\mathbb{C}) = \operatorname{span}_{\mathbb{C}}(e_1)$. Check if f is a ring homomorphism. Clearly, $f(c+d) = (c+d)e_1 = ce_1 + de_1 = f(c) + f(d)$, and $f(cd) = (cd)e_1 = (ce_1) \cdot (de_1) = f(c) \cdot f(d)$, by the definition of product in $\mathbb{C}[G]$. Finally, we have $f(1) = 1e_1 = e_1$, which is the identity element, as required. Also, since $f \not\equiv 0$ (not constantly zero), f is injective (since $\mathbb{C}$ is a field). This proves both (4) and (5). ☐

Notational trick: we will identify each e_g with g. So, with this notational trick, elements of V have form

$$\sum_{i=1}^{n} c_i g_i,$$

and this puts $G \subseteq V$. So the identity of $\mathbb{C}[G]$ is 1. Secondly, identify each $c1 \in \operatorname{span}_{\mathbb{C}}(1)$ with c. And in doing so, this puts $\operatorname{span}_{\mathbb{C}}(1) = \mathbb{C}$, and $\mathbb{C} \subseteq \mathbb{C}[G]$. Modulo this notational trick, we can re-write some of statements in Proposition 58 as follows:

(1) $\mathbb{C}[G]$ is a ring.

(2) $G \cup \mathbb{C} \subseteq \mathbb{C}[G]$
(3) $\mathbb{C}$ is a subring sontained in the centre of $\mathbb{C}[G]$.

Now it's time to talk about $\mathbb{C}[G]$-modules. Let ${}_{\mathbb{C}[G]}W$ be a left $\mathbb{C}[G]$-module. Since $\mathbb{C} \leq \mathbb{C}[G]$, W is also a $\mathbb{C}$-module, i.e., vector space over $\mathbb{C}$. For each $g \in G$, we see that g "acts" on W (by left multiplication). Define $\rho_g : W \to W, \rho_g(w) = gw$.

Claim. $\rho_g \in \mathrm{GL}(W)$ (for each $g \in G$), and $\rho_g \circ \rho_h = \rho_{gh}$, where $g, h \in G$.

Proof. We start with proving the second part of the claim: $(\rho_g \circ \rho_h)(w) = \rho_g(\rho_h(w)) = \rho_g(hw) = g(hw) = (gh)w = \rho_{gh}(w)$. The first part is slightly more complicated, and this will be left as an exercise. □

So if $\rho : G \to \mathrm{GL}(W)$ defined by $\rho(g) = \rho_g$, then $({}_{\mathbb{C}}W, \rho)$ is a representation of G. Conversely, let (W, ρ) be some representation of G. Take $(W, +)$ and turn it into a $\mathbb{C}[G]$-module by

$$\left(\sum_{i=1}^{n} c_i g_i\right) \cdot w = \sum_{i=1}^{n} c_i \rho_{g_i}(w) \in W.$$

Claim. $(W, +)$ with the scalar multiplication as defined above is a left $\mathbb{C}[G]$-module, and there is a bijection between the set of representations of G and the set of left $\mathbb{C}[G]$-modules. This one-to-one correspondence can be characterized as: $(W, \rho) \leftrightarrow {}_{\mathbb{C}[G]}W$ and $\rho_g(w) \leftrightarrow gw$.

Now we explain why this connection is *very nice*!

Lemma 15. *Suppose $(W, \rho), (X, \sigma)$ are representations of G. Let ${}_{\mathbb{C}[G]}W$ and ${}_{\mathbb{C}[G]}X$ be their corresponding $\mathbb{C}[G]$-modules. Suppose that $f : W \to X$. Then f is a morphism from (W, ρ) to (X, σ) if and only if f is a (module) homomorphism from ${}_{\mathbb{C}[G]}W$ to ${}_{\mathbb{C}[G]}X$.*

Proof. ($\Rightarrow$) GIven f is a morphism, we need to prove that $f(w_1 + w_2) = f(w_1) + f(w_2)$, and that $f(r \cdot w) = r \cdot f(w)$ for all $w \in W, r \in \mathbb{C}[G]$. The first one is easy, since f is $\mathbb{C}$-linear. For the second claim, write

$$r = \sum_{i=1}^{n} c_i g_i.$$

Then we have

$$\begin{aligned} f(r \cdot w) &= f\left(\left(\sum_{i=1}^{n} c_i g_i\right) \cdot w\right) = f\left(\sum_i c_i \rho_{g_i}(w)\right) \\ &= \sum_i c_i f(\rho_{g_i}(w)) \text{ (by } \mathbb{C}\text{-linearity)} \\ &= \sum_i c_i \sigma_{g_i}(f(w)) \text{ (since } f \text{ is a morphism)} \\ &= \left(\sum_i c_i g_i\right) \cdot f(w) \in {}_{\mathbb{C}[G]}X \\ &= r \cdot f(w), \end{aligned}$$

as required.

($\Leftarrow$) Exercise! □

Some correspondences:

Representations of G	$\mathbb{C}[G]$-modules
morphisms	module homomorphisms
subrepresentations	submodules
direct sums	direct sums
tensor products	symmetric tensor product over $\mathbb{C}$ $({}_{\mathbb{C}[G]}(W \otimes_{\mathbb{C}} X))$
irreducible representations	simple modules
regular representations	${}_{\mathbb{C}[G]}(\mathbb{C}[G], +)$

Theorem 14. *Let G be a finite group. Then $\mathbb{C}[G]$ is semisimple.*

Proof. Let $R = \mathbb{C}[G]$. Consider $(R, +)$ as a left R-module ${}_R(R, +)$, i.e., the module corresponding to the regular representation of G. The regular representation is of finite degree, so it decomposes as a direct sum of irreducible representations. Thus, by our correspondence, ${}_R(R, +)$ decomposes as a direct sum of simple modules. □

28. November 13

Recall that, if G is a finite group, then the group ring $\mathbb{C}[G]$ is a semisimple ring, and that $\mathbb{C}$ is contained in the centre of $\mathbb{C}[G]$. Additionally, $\dim_{\mathbb{C}}(\mathbb{C}[G]) = |G| < \infty$. By Wedderburn's theorem, $\mathbb{C}[G] \cong \prod \mathrm{M}_{n_i}(\mathbb{C})$. We hope to discover this isomorphism.

We explore the "real story" in the translation from (W, ρ) to ${}_{\mathbb{C}[G]}W$. Suppose that (W, ρ) is a representation of degree n. So $\rho : G \to \mathrm{GL}(W)$ is a group homomorphism preserving $\cdot$ and 1.

Remark 11. Some facts:

(1) $\mathrm{GL}(W) \subseteq \mathrm{End}(W) := \mathrm{Hom}_{\mathbb{C}}(W, W)$
(2) $\mathrm{End}(W)$ is naturally a ring $(\mathrm{End}(W), +, \circ)$ and is a vector space over $\mathbb{C}$ with dimension n^2.
(3) $\mathrm{End}(W) \cong \mathrm{M}_n(\mathbb{C})$ (both as a ring and as a vector space)

For any $\rho : G \to \mathrm{GL}(W)$, extend ρ to $\tilde{\rho} : \mathbb{C}[G] \to \mathrm{End}(W)$ additively, i.e.,

$$r = \sum_{g \in G} c_g g \Rightarrow \tilde{\rho}(r) = \sum_{g \in G} c_g \rho_g$$

Lemma 16. *$\tilde{\rho}$ is a ring homomorphism and a $\mathbb{C}$-linear map.*

Proposition 59 (Prop A)**.** *Suppose that (W, ρ) is irreducible. Then $\tilde{\rho} : \mathbb{C}[G] \to \mathrm{End}(W)$ is surjective.*

Proof (sketch). Recall that the dual representation (W^*, ρ^*) (as from Assignment #5) is irreducible. Thus $(W \otimes w^*, \rho \boxtimes \rho^*)$ is an irreducible representation of $G \times G$. Note that $W^* = \mathrm{Hom}(W, \mathbb{C})$ and $\rho^*_g : W^* \to W^*$ is defined as $\rho^*_g(L) = L \circ \rho_{g^{-1}}$.

$\mathrm{End}(W)$ supports a representation $(\mathrm{End}(W), \tau)$ of $G \times G$ given $(h, k) \in G \times G$, where $\tau_{(h,k)} : \mathrm{End}(W) \to \mathrm{End}(W)$ defined as $\tau_{(h,k)}(f) = \rho_h \circ f \circ \rho_{k^{-1}}$.

Claim. $(\mathrm{End}(W), \tau)$ is a representation of $G \times G$.

Recall from Assignment #5 that for any finite-dimensional V, we have

$$V \otimes W \cong \mathrm{Hom}(V^*, W)$$

Also, naturally, we have $V^{**} \cong V$. So $W \otimes V^* = V^* \otimes W \cong \operatorname{Hom}(V, W)$, and particularly $W \otimes W^* \cong \operatorname{End}(W)$. In fact, we have

$$(W \otimes W^*, \rho \boxtimes \rho^*) \cong (\operatorname{End}(W), \tau),$$

as representations of $G \times G$. Hence $(\operatorname{End}(W), \tau)$ is irreducible also.

Claim. $\operatorname{im}(\tilde{\rho})$ is a $G \times G$-invariant subspace of $(\operatorname{End}(W), \tau)$.

Clearly a subspace. If we let

$$r = \sum_{g \in G} c_g g \in \mathbb{C}[G],$$

then

$$\tilde{\rho}(r) = \sum_{g \in G} c_g \rho_g.$$

Pick $(h, k) \in G$; then we have

$$\tau_{(h,k)} \left(\sum_{g \in G} c_g \rho_g \right) = \rho_h \circ \left(\sum_{g \in G} c_g \rho_g \right) \circ \rho_{k^{-1}} = \sum_{g \in G} c_g \rho_{hgk^{-1}} \in \operatorname{im}(\tilde{\rho}).$$

Clearly, $\operatorname{im}(\tilde{\rho}) \neq \{0\}$, since $\tilde{\rho}(1) = \rho_1 = \mathrm{id}_W$. Hence $\operatorname{im}(\tilde{\rho}) = \operatorname{End}(W)$. □

Proposition 60 (Prop B)**.** *Suppose that (W, ρ) is irreducible. Let χ be its character. Suppose that*

$$r = \sum_{g \in G} \alpha(g) g,$$

where $\alpha \in \operatorname{ClaFun}(G)$. Then $\tilde{\rho}(r)$ is a scalar multiplication by

$$\frac{|G|}{\dim(W)} (\alpha \mid \chi^*).$$

Proof. Recall

$$\tilde{\rho}(r) = \sum_{g \in G} \alpha(g) \rho_g,$$

and by Proposition 34,

$$\frac{1}{|G|} \sum_{g \in G} \alpha(g) \rho_g$$

is scalar multiplication by

$$\frac{1}{\dim(W)} (\alpha \mid \chi^*),$$

as desired. □

Corollary 18. *Suppose that (W_1, ρ_1) is an irreducible representation of G. Then there exists $e \in \mathbb{C}[G]$ such that for every irreducible representation (W, ρ),*

$$\tilde{\rho}(e) = \begin{cases} 1 & \text{if } (W, \rho) \cong (W_1, \rho_1) \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let χ_1 be the character of (W_1, ρ_1). Define

$$\alpha := \frac{\dim(W_1)}{|G|}\chi_1^* \in \mathrm{ClaFun}(G).$$

Let

$$e = \sum_{g \in G} \alpha(g) g \in \mathbb{C}[G],$$

and let (W, ρ) be an irreducible representation with character χ. By Proposition 60, $\tilde{\rho}(e)$ is a scalar multiplication by

$$\begin{aligned} \frac{|G|}{\dim(W)} (\alpha \mid \chi^*) &= \frac{|G|}{\dim(W)} \cdot \frac{\dim(W_1)}{|G|} (\chi_1^* \mid \chi^*) \\ &= \frac{\dim W_1}{\dim W} (\chi \mid \chi_1) \\ &= \begin{cases} 0 & \text{if } (W, \rho) \ncong (W_1, \rho_1) \\ 1 & \text{otherwise.} \end{cases} \end{aligned}$$

Now, let $(W_1, \rho_1), \dots, (W_k, \rho_k)$ be a list of irreducible representations of G. Define $h : \mathbb{C}[G] \to \mathrm{End}(W_1) \times \cdots \times \mathrm{End}(W_k)$ by $h(r) = (\tilde{\rho}_1(r), \dots, \tilde{\rho}_k(r))$. It is easy to show that h is a ring homomorphism and a $\mathbb{C}$-linear map. So the dimension of $\prod \mathrm{End}(W_i)$ is $n_1^2 + \cdots + n_k^2$ where $\dim W_i = n_i$ whereas $\dim_{\mathbb{C}}(\mathbb{C}[G]) = |G|$. But then it is already known that $|G| = \sum n_i^2$. So it suffices to show that h is surjective. □

29. November 17

Let G be a finite group, and (W_i, ρ_i) be the irreducible representations of G, for $1 \leq i \leq k$, and as usual, suppose $\mathbb{C}[G]$ is the group ring of G. For $i = 1, 2, \dots, k$, let $\rho_i : G \to \mathrm{GL}(W_i)$, and extend this map so that $\tilde{\rho}_i = \mathbb{C}[G] \to \mathrm{End}(W_i)$. Define

$$h : \mathbb{C}[G] \to \prod_{i=1}^{k} \mathrm{End}(W_i)$$

by

$$h(r) = (\tilde{\rho}_1(r), \dots, \tilde{\rho}_k(r))$$

a ring homomorphism and a vector space homomorphism.

Proposition 61. *h is a ring isomorphism.*

Proof. Since h is a ring homomorphism, it is enough to show that h is surjective (injectivity follows from surjectivity). Let's recall some facts:

(1) By Proposition 59, each $\tilde{\rho}_i$ is surjective.
(2) We also know that the k-tuples of the form $(1, 0, 0, \dots, 0)$, $(0, 1, 0, \dots, 0)$, $(0, 0, 1, 0, \dots, 0)$, $(0, 0, \dots, 0, 1)$ are in range(h). In other words, there exists $e_1, \dots, e_k \in \mathbb{C}[G]$ such that

$$h(e_i) = (\tilde{\rho}_i(e_i), \dots, \tilde{\rho}_k(e_i)) = (0, 0, \dots, 0, 1, 0, \dots, 0)$$

(1 in the i-th entry), according to Corollary 18.

Now surjectivity is "obvious". Let's see why it is. To prove that h is surjective, start off by choosing

$$(f_1, f_2, \dots, f_k) \in \prod_{i=1}^{k} \mathrm{End}(W_i).$$

Each $\tilde{\rho}_i$ is surjective, so there exists $r_1 \in \mathbb{C}[G]$ such that $\tilde{\rho}_1(r_1) = f_1$. Thus the first entry of $h(r_1)$ is f_1, so we have

$$h(e_1 r_1) = h(e_1)h(r_1) = (1, 0, \dots, 0) \cdot (f_1, *, \dots, *) = (f_1, 0, 0, \dots, 0).$$

Similarly, for all i we can get r_i so that

$$h(e_i r_i) = (0, 0, 0, \dots, f_i, 0, \dots, 0).$$

So we can construct $e_1 r_1 + \dots, e_k r_k$ so that

$$h(e_1 r_1 + \dots + e_k r_k) = (f_1, f_2, \dots, f_k).$$

Therefore h is surjective. □

Remark 12. Therefore, Proposition 61 shows that

$$\mathbb{C}[G] \cong \mathrm{End}(W_1) \times \dots \times \mathrm{End}(W_k) \cong \mathrm{M}_{d_1}(\mathbb{C}) \times \dots \times \mathrm{M}_{d_k}(\mathbb{C}),$$

hence verifying Wedderburn's theorem.

Note that this sheds light on the canonical decomposition of the regular representation of G, i.e.,

$$(V, \rho) \cong \bigoplus_{i=1}^{k} \left(\underbrace{(W_i, \rho_i) \oplus \dots \oplus (W_i, \rho_i)}_{d_i (\text{canonical component})} \right),$$

and $V = (\mathbb{C}[G], +)$. The i-th canonical component of (V, ρ) is

$$h^{-1}(\{0\} \times \dots \times \{0\} \times \mathrm{End}(W_i) \times \{0\} \times \dots \times \{0\}),$$

or to put in another way,

$$\{r \in \mathbb{C}[G] : h(e_i r) = h(r)\}.$$

29.1. **More about induced representations (well, not exactly...)**

(1) Chapter VII in Serre
(2) Frobenius reciprocity
(3) Mackey's criterion

One fact about induced representations:

Remark 13. Suppose $H \leq G$. Let (W, θ) be a representation of H and (V, ρ) the representation of G induced by (W, θ), i.e. $(V, \rho) = \mathrm{Ind}_H^G(W, \theta)$. Then clearly $\mathbb{C}[H] \leq \mathbb{C}[G]$, and if we let ${}_{\mathbb{C}[H]}W$ is a $\mathbb{C}[H]$-module corresponding to (W, θ) and ${}_{\mathbb{C}[G]}V$ a $\mathbb{C}[G]$-module corresponding to (V, ρ), then ${}_{\mathbb{C}[G]}V$ is the extension of scalars of ${}_{\mathbb{C}[H]}W$. In other words, we have

$${}_{\mathbb{C}[G]}V = {}_{\mathbb{C}[G]}\mathbb{C}[G] \otimes_{\mathbb{C}[H]} W,$$

by Method 25.1.

We won't talk about induced representations anymore, but we *will* talk about some subtle arithmetical information about G that can be deduced from $\mathbb{C}[G]$.

29.2. **Characterization of the centre of $\mathbb{C}[G]$.** Start with

$$u = \sum_{g \in G} \alpha(g) g,$$

where $\alpha \in \mathbb{C}^G$. Fix $h \in G$. Then

$$hu = h\left(\sum_{g \in G} \alpha(g) g\right) = \sum_{g \in G} \alpha(g) hg = \sum_{g \in G} \alpha(h^{-1}g) g,$$

and similarly,

$$uh = \left(\sum_{g \in G} \alpha(g) g\right) h = \sum_{g \in G} \alpha(g) gh = \sum_{g \in G} \alpha(gh^{-1}) g$$

So $hu = uh$ if and only if $\alpha(h^{-1}g) = \alpha(gh^{-1})$ for all $g \in G$. Let $g' = h^{-1}g$, i.e., $\alpha(hg'h^{-1}) = \alpha(g')$ for all $g' \in G$. Therefore, $hu = uh$ if and only if α is invariant under the conjugation by h if and only if $\alpha \in \mathrm{ClaFun}(G)$. Now it's easy to see that if u commutes with all $g \in G$, then u commutes with all $x \in \mathbb{C}[G]$. This proves that the centre of $\mathbb{C}[G]$ consists of

$$u = \sum_{g \in G} \alpha(g) g,$$

where $\alpha \in \mathrm{ClaFun}(G)$.

Remark 14. If $R = Z(\mathbb{C}[G])$ (the centre of $\mathbb{C}[G]$), then:

(1) R is a commutative ring
(2) For each conjugacy class $\mathcal{O}$ of G, let $e_\theta = \sum_{g \in \theta} g = \sum_{g \in G} \alpha_\theta(g) g$, where

$$\alpha_\theta(g) = \begin{cases} 1 & \text{if } g \in \theta \\ 0 & \text{else.} \end{cases}$$

This is a class function, so $e_\theta \in R$ for all conjugacy classes θ.

Hence we can state the following: $R = \mathrm{span}_{\mathbb{C}}\{e_\theta : \theta \text{ a conjugacy class of } G\}$. In fact, these e_θ's form a $\mathbb{C}$-basis for R, and the $\dim_{\mathbb{C}}(R) = \#$ of conjugacy classes of G, as a $\mathbb{C}$-vector space.

30. November 18: More about the centre of $\mathbb{C}[G]$

Let G be a finite group, and (W, ρ) an irreducible representation of G. As usual, let $\tilde{\rho} : \mathbb{C}[G] \to \mathrm{End}(W)$ be the extension of ρ, and $R \subseteq \mathbb{C}[G]$ the centre of $\mathbb{C}[G]$. Consider $\tilde{\rho}|_R : R \to \mathrm{End}(W)$, which is also a ring homomorphism. Recall Proposition 60, which says that if $r = \sum_{g \in G} \alpha(g) g$ and $\alpha \in \mathrm{ClaFun}(G)$ (i.e., if $r \in R$), then $\tilde{\rho}(r)$ is a scalar endomorphism, say by λ_r. Then we have

$$\lambda_r = \frac{|G|}{\dim(W)} \left(\alpha \mid \chi^*\right),$$

with $\chi = \mathrm{char}(W, \rho)$.

Define $w_\rho : R \to \mathbb{C}$ with $w_\rho(r) = \lambda_r$. And this is a ring homomorphism. Note that:

$$(\alpha \mid \chi^*) = \frac{1}{|G|} \sum_{g \in G} \alpha(g) \cdot \chi(g)$$

$$\therefore w_\rho(r) = \lambda_r = \frac{|G|}{\dim(W)} \cdot \frac{1}{|G|} \sum_{g \in G} \alpha(g)\chi(g).$$

Hence, we have:

Proposition 62. *Let R be the centre of $\mathbb{C}[G]$. Let (W, ρ) be an irreducible representation of G. Then the map*

$$w_\rho : R \to \mathbb{C}, w_\rho\left(\sum_{g \in G} \alpha(g) g\right) = \frac{1}{d} \sum_{g \in G} \alpha(g)\chi(g) \quad (\alpha \in \text{ClaFun}(G))$$

is a ring homomorphism.

Proof. Only need to check that $w_\rho(1) = 1$. But then $w_\rho(1) = \chi(1)/d$, and since $\chi(d)$ is the dimension of W, it follows that $w_\rho(1) = 1$. □

31. November 18: some algebraic number theory

Definition 63. Let R be a commutative ring containing $\mathbb{Z}$ and $u \in R$.

(1) u is *algebraic over* $\mathbb{Z}$ if u is a root of some nonzero polynomial $p(x) \in \mathbb{Z}[x]$.
(2) u is *integral over* $\mathbb{Z}$ if u is a root of some *monic* polynomial $p(x) \in \mathbb{Z}[x]$.
(3) If $R = \mathbb{C}$, then $u \in \mathbb{C}$ is an *algebraic integer* if it is integral over $\mathbb{Z}$.

Example 28. Examples of integral elements:

(1) Every integer $n \in \mathbb{Z}$ is integral over $\mathbb{Z}$.
(2) $c/d \in \mathbb{Q}$ is integral over $\mathbb{Z}$ if and only if $c/d \in \mathbb{Z}$.

Proof. Suppose that c/d is a root of a monic polynomial with integer coefficients. Say $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $a_i \in \mathbb{Z}$. If $f(c/d) = 0$, then $(c/d)^n + a_{n-1}(c/d)^{n-1} + \cdots + a_1(c/d) + a_0 = 0$, or

$$c^n + \underbrace{a_{n-1}c^{n-1}d + \cdots + a_1 cd^{n-1} + a_0 d^n}_{\text{divisible by } p} = 0.$$

Assume that c/d is in lowest terms. If $c/d \in \mathbb{Z}$, then there exists a prime that $p \mid d$ but $p \nmid c$. But note that $p \mid c^n$, so $p \mid c$, and this is a contradiction. □

(3) Every n-th root of 1 is integral over $\mathbb{Z}$.
(4) If R, S are commutative, then both contain $\mathbb{Z}$. So if $h : R \to S$ is a ring homomorphism and $u \in R$ and u is integral over $\mathbb{Z}$, then so is $h(u)$.

Definition 64. Let R be a commutative ring.

(1) If $u_1, \ldots, u_n \in R$ then the *span of* $\mathbb{Z}$ is

$$\text{span}_{\mathbb{Z}}(u_1, \ldots, u_n) = \{a_1 u_1 + \cdots + a_n u_n : a_1, \ldots, a_n \in \mathbb{Z}\}.$$

(2) Suppose that U is a subgroup of $(R, +)$. Then U is *finitely generated as a $\mathbb{Z}$-module* iff there exist $u_1, u_2, \ldots, u_n \in U$ such that $\text{span}_{\mathbb{Z}}(u_1, \ldots, u_n) = U$.

(3) If $u \in R$, then $\mathbb{Z}[u]$ is the subring of R generated by u. Equivalently, $\mathbb{Z}[u] = \text{span}_{\mathbb{Z}}\{1, u, u^2, u^3, \dots\} = \{f(u) : f(x) \in \mathbb{Z}[x]\}$.

Proposition 65. *Let R be a commutative ring containing $\mathbb{Z}$. Let $u \in R$. Then the following are equivalent:*

(1) u is integral over $\mathbb{Z}$
(2) $\mathbb{Z}[u]$ is finitely-generated as $\mathbb{Z}$-module
(3) there exists a subring $S \leq R$ with $u \in S$ such that S is finitely-generated as $\mathbb{Z}$-module.

But, before going into the proof, need to mention the following theorem/big fact we will use:

Theorem 15. *Submodules fo a finitely-generated $\mathbb{Z}$-module are finitely generated.*

Proof of Proposition 65. ((1) $\Rightarrow$ (2)) Assume that u is integral over $\mathbb{Z}$. So say $f(u) = 0$ for some $f(x) \in \mathbb{Z}[x]$, monic. For $m \geq n = \deg(f)$, take x^m and divide it by $f(x)$. Get quotient $q(x)$ and remainder $r(x)$ (in $\mathbb{Q}[x]$). Since $f(x)$ is monic, by the division algorithm we have $q, r \in \mathbb{Z}[x]$. Then $x^m = f(x)q(x) + r(x)$, so we have $u^m = f(u)q(u) + r(u) = r(u) \in \text{span}_{\mathbb{Z}}(1, u, u^2, \dots, u^{n-1})$. Hence $\mathbb{Z}[u] = \text{span}_{\mathbb{Z}}(1, u, u^2, \dots, u^{n-1})$.

((2) $\Rightarrow$ (1)) Assume that $\mathbb{Z}[u] = \text{span}_{\mathbb{Z}}(v_1, \dots, v_k)$ is finitely-generated as $\mathbb{Z}$-module. Each $v_i \in \mathbb{Z}[u] = \text{span}_{\mathbb{Z}}(1, u, u^2, \cdots)$, so there exists N such that $v_1, \dots, v_k \in \text{span}_{\mathbb{Z}}(1, u, u^2, \dots, u^N)$. Thus we have $u^{N+1} \in \mathbb{Z}[u] = \text{span}_{\mathbb{Z}}(1, u, u^2, \dots, u^N)$, and this gives $p(x) \in \mathbb{Z}[x]$, monic of degree $N+1$ such that $p(u) = 0$.

((2) $\Rightarrow$ (3)) This is immediate: just let $S = \mathbb{Z}[u]$.

((3) $\Rightarrow$ (2)) Given $u \in S$, finitely-generated as a $\mathbb{Z}$-module, then $\mathbb{Z}[u] \leq S$. Thus $\mathbb{Z}[u]$ is a subgroup of $(S, +)$. Since S is finitely-generated, it follows that $\mathbb{Z}[u]$ is finitely-generated also, by Theorem 15. ☐

32. November 20

Some consequences of Proposition 65:

Corollary 19. *Suppose that R is a commutative ring containing $\mathbb{Z}$ and R is finitely-generated as a $\mathbb{Z}$-module. Then every $u \in R$ is integral over $\mathbb{Z}$.*

Proof. Apply statement (3) of Proposition 65 with $S = R$. ☐

Corollary 20. *Suppose R is commutative containing $\mathbb{Z}$. The set $\{u \in R : u \text{ integral over } \mathbb{Z}\} = S$ is a subring of R.*

Proof. Obviously $1 \in S$. Let $u, v \in S$. So u, v are integral over $\mathbb{Z}$ so $\mathbb{Z}[u] = \text{span}_{\mathbb{Z}}(1, u, u^2, \dots, u^{n-1})$ and $\mathbb{Z}[v] = \text{span}_{\mathbb{Z}}(1, v, v^2, \dots, v^{m-1})$ for some m and N. Must show that $u \pm v$ and uv are integral over $\mathbb{Z}$. Let $T = \text{span}_{\mathbb{Z}}(\{u^i v^j : i < n, j < m\}$. Then T is a finitely-generated submodule of $(R, +)$. We claim (without proof) that T is a subring of R. By the previous corollary, every element of T is integral over $\mathbb{Z}$. Thus $u \pm v, uv$ are integral over $\mathbb{Z}$. ☐

Now we return to the representation (Section 6.5 in Serre):

Proposition 66. *Let χ be the character of (V, ρ) of G of finite degree. Then $\chi(g)$ is an algebraic integer for all $g \in G$.*

Proof. If $|G| = n$, then $\chi(g) = \text{tr}(\rho_g) =$ sum of eigenvalues of ρ_g, which are n-th roots of unity. Every n-th root of unity is integral over $\mathbb{Z}$, so their sum is integral over $\mathbb{Z}$ also. $\square$

Let $R = Z(\mathbb{C}[G])$, the centre of $\mathbb{C}[G]$, i.e., a commutative ring containing $\mathbb{Z}$.

Definition 67. We define

$$\mathbb{Z}[G] := \left\{ \sum_{g \in G} n_g g : n_g \in \mathbb{Z} \right\} \subset R.$$

Note that $\mathbb{Z}[G]$ is a subring of $\mathbb{C}[G]$.

Lemma 17. *Every element of $R \cap \mathbb{Z}[G]$ is integral over $\mathbb{Z}$.*

Proof. $\mathbb{Z}[G]$ is a ring, finitely-generated as a $\mathbb{Z}$-module. $R \cap \mathbb{Z}[G]$ is a subring of both, so is a commutative ring. Also it is a submodule of $\mathbb{Z}[G]$. By Theorem 15, $R \cap \mathbb{Z}[G]$ is finitely-generated as a $\mathbb{Z}$-module. Thus by Corollary 19, every $r \in R \cap \mathbb{Z}[G]$ is integral over $\mathbb{Z}$. $\square$

Example 29. Let C be the set of conjugacy classes of G. For $\theta \in C$,

$$e_\theta = \sum_{g \in \theta} g.$$

Lemma 18. *Each e_θ is integral over $\mathbb{Z}$.*

Proposition 68. *Let G be a finite group, and $\alpha \in \text{ClaFun}(G)$ such that each $\alpha(g)$ is an algebraic integer (i.e., integral over $\mathbb{Z}$). Let*

$$u = \sum_{g \in G} \alpha(g) g \in R.$$

Then u is integral over $\mathbb{Z}$.

Proof. For each $\theta \in C$, let b_θ be the constant value $\alpha(g), g \in \theta$. Then

$$\begin{aligned} u &= \sum_{\theta \in C} \left(\sum_{g \in \theta} \alpha(g) g \right) = \sum_{\theta \in C} \left(\sum_{g \in \theta} b_\theta g \right) \\ &= \sum_{\theta \in C} b_\theta \left(\sum_{g \in \theta} g \right) = \sum_{\theta \in C} b_\theta e_\theta. \end{aligned}$$

Recall that b_θ is an algebraic integer and e_θ is integral over $\mathbb{Z}$, and that all b_θ, e_θ are in R and integral over $\mathbb{Z}$. Hence $\sum b_\theta e_\theta$ is also integral over $\mathbb{Z}$, by Corollary 20. $\square$

Now let (W, ρ) be an irreducible representation of G. Let $\tilde{\rho} : \mathbb{C}[G] \to \text{End}(W)$, and let $w_\rho : R \to \mathbb{C}$ be a ring homomorphism. Recall that $\chi := \text{char}(W, \rho)$ and $d = \dim(W)$. THen

$$w_\rho \left(\sum_{g \in G} \alpha(g) g \right) = \frac{1}{d} \sum_{g \in G} \alpha(g) \chi(g).$$

As w_ρ is a ring homomorphism, we have

Corollary 21. *Suppose $\alpha \in \operatorname{ClaFun}(G)$ such that each $\alpha(g)$ is an algebraic integer. Let (W, ρ) be an irreducible representation of G with character χ. Then*

$$\frac{1}{d}\sum_{g\in G}\alpha(g)\chi(g)$$

is an algebraic integer where d is the degree of (W, ρ).

Fix irreducible representation (W, ρ) with degree d and character χ. Define $\alpha \in \operatorname{ClaFun}(G)$ by $\alpha(g) = \chi(g^{-1}) \in \operatorname{ClaFun}(G)$. Then all values of α are algebraic integers. Note that

$$\begin{aligned}\frac{1}{d}\sum_{g\in G}\alpha(g)\chi(g) &= \frac{1}{d}\sum_{g\in G}\chi(g^{-1})\chi(g) \\ &= \frac{|G|}{d}\left(\frac{1}{|G|}\sum_{g\in G}\chi(g^{-1})\chi(g)\right) = \frac{|G|}{d}\langle\chi,\chi\rangle \\ &= \frac{|G|}{d}(\chi \mid \chi) = \frac{|G|}{d},\end{aligned}$$

so it is an algebraic integer. So $|G|/d \in \mathbb{Z}$, i.e., $d \mid |G|$. Hence we proved:

Theorem 16 (Lagrange-like theorem)**.** *If (W, ρ) is an irreducible representation, then $\dim(W)$ divides $|G|$.*

33. November 24

Suppose that G is a finite group and (W, ρ) is an irreducible representation of G and $\dim(W) = D$. Then we know that

(1) d divides $|G|$ (Theorem 34)
(2) If G has an abelian normal subgroup, say A, then $d \leq [G : A]$. (Corollary 16)

Proposition 69 (Mackey)**.** *Let G be a finite group and let $Z(G)$ be the centre of G. If (W, ρ) is an irreducible representation, then $\dim(W) \mid [G : Z(G)]$.*

Proof. Let $d = \dim(W), n = |G|$ and $k = |Z(G)|$. We will show that $dk \mid n$. Let $h \in Z(G)$ and observe that ρ_h commutes with ρ_g for all $g \in G$. This means that $\rho_h : (W, \rho) \to (W, \rho)$ is a morphism. By Schur's lemma (Lemma 7), ρ_h is multiplication by some λ_h. This gives a homomorphism $\lambda : Z(G) \to \mathbb{C}^*$ defined as $h \mapsto \lambda_h$.

Fix $m \geq 1$. By Theorem 9, the representation

$$(\underbrace{W \otimes \cdots \otimes W}_{m}, \underbrace{\rho \boxtimes \cdots \boxtimes \rho}_{m})$$

is an irreducible representation of G^m. Recall that if $g = (g_1, g_2, \ldots, g_m) \in G^m$, then $(\rho^m)_g(v_1 \otimes \cdots \otimes v_m) = \rho_{g_1}(v_1) \otimes \cdots \otimes \rho_{g_m}(v_m)$. If $h = (h_1, h_2, \ldots, h_m) \in (Z(G))^m$ then

$$\begin{aligned}(\rho^m)_h(v_1 \otimes \cdots \otimes v_m) &= \rho_{h_1}(v_1) \otimes \cdots \otimes \rho_{h_m}(v_m) \\ &= \lambda_{h_1}(v_1) \otimes \cdots \otimes \lambda_{h_m}(v_m) \\ &= (\lambda_{h_1}\lambda_{h_2}\cdots\lambda_{h_m})(v_1 \otimes \cdots \otimes v_m).\end{aligned}$$

Let $H = \{(h_1, h_2, \ldots, h_m) \in Z(G) : h_1 \cdot \cdots \cdot h_m = 1\}$. Thus $H \leq (Z(G))^m$ hence $H \triangleleft G^m$. By the above calculation, we have $(\rho^m)_h = \mathrm{id}$ for any $h \in H$, since $\lambda_{h_1} \cdot \cdots \cdot \lambda_{h_m} = 1$. Therefore

$H \subseteq \ker(\rho^m)$. This means that we get a well-defined homomorphism $\overline{\rho} : G^m/H \to \mathrm{GL}(W^{\otimes m})$ defined by $gH \mapsto (\rho^m)_g$. Thus $(W^{\otimes m}, \overline{\rho})$ is a representation of G^m/H. In fact this is also irreducible. If $V \leq W^{\otimes m}$ is G^m/H-invariant, then it is also G^m-invariant. Thus by Theorem 34, $d^m \mid |G^m/H|$, since $d^m = \deg((W^{\otimes m}, \overline{\rho}))$ and $|H| = k^{m-1}$. So we have d^m divides $\frac{n^m}{k^{m-1}}$, or $d^m k^{m-1} \mid n^m$ for all m. This implies that $dk \mid n$. To see why, suppose that $p^{\alpha(p)} \parallel d$. Similarly, define $\beta(p)$ and $\gamma(p)$ so that $p^{\beta(p)} \parallel k$ and $p^{\gamma(p)} \parallel n$. Then we have $m\alpha(p) + (m-1)\beta(p) \leq m\gamma(p)$ for all m, or $m(\alpha(p) + \beta(p) - \gamma(p)) \leq \beta(p)$ for all m, so $\alpha(p) + \beta(p) - \gamma(p) \leq 0$, as required. □

Definition 70. A representation (V, ρ) is *isotypical* if it is a direct sum of isomorphic irreducible representations.

Example 30. If (V, ρ) is an arbitrary representation of finite degree and

$$(V, \rho) = (V_1, \rho_1) \oplus \cdots \oplus (V_k, \rho_k)$$

is its canonical decomposition, then (V_i, ρ_i) is isotypical.

Suppose that G is finite and $N \lhd G$ and (V, ρ) is a representation. Let (V, ρ_N) be the representation restricted to N. Let

$$(V, \rho_N) = (V_1, \rho_1) \oplus \cdots \oplus (V_k, \rho_k)$$

be its canonical decomposition into isotypical components. Consider (V_1, ρ_1). It decomposes as

$$(V_1, \rho_1) = (U_1', \sigma_1') \oplus \cdots \oplus (U_{k_1}', \sigma_{k_1}')$$

where the (U_i, σ_i') are all isomorphic and irreducible. In Assignment #7 Problem #1, we will prove that ρ_g maps $U_1', \ldots, U_{k_1}'$ to isomorphic subrepresentations. We are applying this claim here. The point is that ρ_g maps them all to the same isotypical component. Thus $\rho_g(V_1) \subseteq V_j$ for some j. With some calculations, we can actually show that $\rho_g(V_1) = V_j$. Note that 1 is not special in this argument, so we have the following lemma.

Lemma 19. *If G is a finite group and $N \lhd G$ and (V, ρ) is a representation of G of finite degree, then for each $g \in G$, ρ_g permutes the isotypical components of (V, ρ_N).*

34. November 25

Suppose G is a finite group, and $N \lhd G$, and (V, ρ) is a representation of finite degree. On November 24 we talked about how G acts on $V_1, V_2, \ldots, V_k$, the isotypical components of (V, ρ_N) by permuting them. Suppose that (V, ρ) is irreducible. Then the action of G on $\{V_1, V_2, \ldots, V_k\}$ is transitive. Say, if θ is the orbit of V_1 for every $g \in G$ and $\rho_g(V_1) = V_{i_g}$ for some i_g. Then $\bigoplus_{g \in G} V_{i_g}$ is G-invariant.

Pick one of the components, say V_1, and let $H \leq G$ be the stabilizer of V_1 under this action.i.e., $H = \{g \in G : \rho_g(V_1) = V_1\}$. By the orbit-stabilizer theorem, $[G : H] = k$ and the left cosets of H senD V_1 to distinct V_i.

Let $\theta = \rho_H|_{V_1}$, so that (V_1, θ) is the representation of H obtained from (V, ρ) by restricting to H and V_1. Thus the previous discussion shows that distinct left cosets of H send V_1 to distinct V_i, and since V is the direct sum of the V_i, we have that (V_1, θ) induces (V, ρ). Also, note that $N \leq H$ since V_1 is N-invariant.

Proposition 71. *Suppose G is a finite group, N a normal subgroup, and (V,ρ) is an irreducible representation. Then either one of the following claims holds:*

(1) There exists:
  (a) a proper *subgroup $H < G$ with $N \leq H$*
  (b) an irreducible representation (W,θ) of H such that $(V,\rho) = \operatorname{Ind}_H^G(W,\theta)$

(2) The restriction (V,ρ_N) of (V,ρ) to N is isotypical.

Proof. Let $(V_1,\rho_1)\oplus\cdots\oplus(V_k,\rho_k)$ be the canonical decomposition of (V,ρ_N) into isotypical components. If $k=1$, then the second claim holds. So we will show that if $k>1$, then the first claim will hold. If $k>1$, then the H constructed in the preceding discussion is proper. So we need only show that (W,θ) is irreducible.

Suppose that V_1 has a proper invariant space X. Define

$$X^* = \sum_{g\in G}\rho_g(X).$$

But since X^* is G-invariant, we have

$$\rho_h(X^*) = \rho_h\left(\sum_{g\in G}\rho_g(X)\right) = \sum_{g\in G}\rho_h\rho_g(X) = \rho_{hg}(X) = \sum_{g\in G}\rho_g(X).$$

Note that $X^*\subseteq X\oplus V_2\oplus\cdots\oplus V_k$ since X is properly contained in V_1, and that $\rho_g(X)\subseteq X$ if $g\in H$. Also,

$$\rho_g(X)\subseteq\begin{cases} V_i & (i>1)\\ \rho_g(V_1)=V_i & \text{otherwise,}\end{cases}$$

so (V,ρ) is not irreducible. □

Corollary 22. *Suppose G is a finite group and $A\triangleleft G$ is abelian. If (V,ρ) is an irreducible representation of degree d then $d \mid [G:A]$.*

Proof. We prove it by induction on $|G|$. If $|G|=1$, then let $K=\ker(\rho)$.

Case 0. $|K|>1$

Let $\overline{G}=G/K$. Then (V,ρ) naturally gives an irreducible representation $(V,\overline{\rho})$ on $\overline{G}$. Then $\overline{A}:=AK/K$ is a normal subgroup of $\overline{G}$. Since, by the Second Isomorphism Theorem, $\overline{A}=AK/K\cong A/(A\cap K)$, it follows that $\overline{A}$ is abelian. Since $k>1$, we have $|\overline{G}|<|G|$, and we can apply induction to get

$$d \mid [\overline{G}:\overline{A}] = [G:AK] = \frac{[G:A]}{[AK:A]},$$

so the claim follows.

If $|K|=1$, then ρ is faithful/one-to-one.

Case 1. There exists $H<G$ with $A\leq H$, and an irreducible representation (W,θ) of H such that $(V,\rho)=\operatorname{Ind}_H^G(W,\theta)$. Note that $A\triangleleft H$, so by induction, $|H|<|G|$. We get that $\dim(W)$ divides $[H:A]$. Since $\dim(V)=d=\dim(W)\cdot[G:H]$, we have $d\mid[G:H][H:A]=[G:A]$.

Case 2. (V,ρ_A) is isotypical. Then $(V,\rho_A)=(U_1,\sigma_1)\oplus\cdots\oplus(U_k,\sigma_k)$ with the (U_i,σ_i) all isomorphic to (U,σ). (U,σ) has degree 1, since A is abelian. So $\sigma_a=\lambda_a$ for each $a\in A$. The same is strue for (U_i,σ_i) so ρ_A is just multiplication by λ_a. It follows that ρ_a commutes with ρ_g for all $g \in G$. Since ρ is injective as a homomorphism from G to $\mathrm{GL}(V)$, $A \leq Z(G)$. Then by Theorem , $d \mid [G : Z(G)]$, so $d \mid [G : A]$ since $[G : A] = [G : Z(G)][Z(G) : A]$. □

35. November 27

Lemma 20. *Suppose that G is a finite group, (W, ρ) an irreducible representation of degree d, and χ is its character. Suppose G has a conjugacy class θ whose size is coprime to d. Then for all $g \in \theta$, either $\chi(g) = 0$ or ρ_g is scalar.*

Proof. Fix $c = |\theta|$ and $g \in G$ and assume that $\chi(g) \neq 0$. By Corollary 21, we know that if $\alpha : G \to \mathbb{C}$ is a class function whose values are algebraic integers, then

$$\frac{1}{d} \sum_{h \in G} \alpha(h)\chi(h)$$

is an algebraic integer.

Let α be the class function

$$\alpha(h) = \begin{cases} 1 & \text{if } h \in \theta; \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$\frac{1}{d} \sum_{h \in \theta} \chi(h) = \frac{c}{d}\chi(g)$$

is an algebraic integer. Choose $s, t \in \mathbb{Z}$ such that $sc + td = 1$, and $sc\chi(g) + td\chi(g) = \chi(g)$. Divide by d:

$$s\left(\frac{c}{d}\chi(g)\right) + t\chi(g) = \frac{\chi(g)}{d}.$$

Thus $\chi(g)d^{-1}$ is an integral linear combination of algebraic integers, making $\chi(g)d^{-1}$ an algebraic integer also. Let $a_1 := \chi(g)/d$. Then $a_1 = \lambda_1 + \lambda_2 + \cdots + \lambda_d$ where the λ_i are the eigenvalues of ρ_g. ρ_g satisfies the equation $x^{|G|} - I = O$, so each λ_i is an n-th root of unity where $n = |G|$. So

$$|a_1| = \frac{|\lambda_1 + \cdots + \lambda_d|}{d} \leq \frac{|\lambda_1| + \cdots + |\lambda_n|}{d} = 1.$$

Since a_1 is an algebraic integer, we can find a monic $p(x) \in \mathbb{Z}[x]$ which is the minimal polynomial for a_1. Let $a_1, \ldots, a_k \in \mathbb{C}$ be the roots of $p(x)$ and $\zeta_n = e^{2\pi i/n}$ be a primitive n-th root of unity, and let $F = \mathbb{Q}(a_1, \ldots, a_k, \zeta_n)$. Then F is the splitting field of $p(x)(x^n - 1)$. Galois theory tells us that there is an automorphism of F (say σ_i) satisfying $\sigma(a_i) = a_i$, hence $\sigma_i(a_1) = \sigma_i((\lambda_1 + \cdots + \lambda_d)/d) = \left(\sum_{i=1}^{d} \sigma_i(\lambda_i)\right)/\sigma_i(d)$. Thus $\sigma_i(\lambda_j)^n = \sigma_i(\lambda_j^n) = \sigma_i(1) = 1$. So $\sigma_i(\lambda_i)$ is an n-th root of unity, so $|\sigma_i(\lambda_j)| = 1$. Thus the same argument as before shows that $|a_i| \leq 1$ for all i.

Since $\chi(g) \neq 0$ and $a_i = \chi(g)/d \neq 0$, so $a_i = \sigma_i(a_i) \neq 0$. Hence $a_1 a_2 \ldots a_k \neq 0$, but $\pm a_1 a_2 \ldots a_k = cp(x)$ for some constant coefficient c, whichever is an integer. So $|a_1 a_2 \cdots a_k| \geq 1$, but we also have $|a_1 a_2 \cdots a_k| \leq 1$, hence $|a_1 a_2 \ldots a_k| = 1$. If $|a_i| < 1$ then $|a_{i'}| > 1$ for some i', so $|a_i| = 1$ for all i. Hence $|\chi(g)| = |a_1 d| = d$. And since $|\lambda_1 + \cdots + \lambda_d| = d$, and each $|\lambda_1| \leq 1$, we have $\lambda_1 = \lambda_2 = \cdots = \lambda_d$. Hence ρ_g is a scalar. Thus, in a suitable basis we have

$$\rho_g \begin{bmatrix} \lambda_1 & & & 0 \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_d \end{bmatrix} = \lambda_1 I,$$

as required. □

36. December 1

Lemma 21. *If G is a finite group and (W, ρ) irreducible rep such that $d = \dim(W)$ and $\chi = \mathrm{char}(W, \rho)$ and θ a conjugacy class of G satisfying $\gcd(|\theta|, d) = 1$, then for all $g \in \theta$ either $\chi(g) = 0$ or ρ_g is scalar.*

Corollary 23. *Suppose that G is a finite non-abelian* simple *group, and suppose also that θ is a conjugacy class such that $\theta \neq \{1\}$. Then $|\theta|$ is not a prime power.*

Proof. Since G is non-abelian simple group, we have $Z(G) = \{1\}$. Assume also that $|\theta| = p^c$ where p is a prime and $c > 0$. Let r_G be the character of the regular representation of G. We know that

$$r_G = \sum_{i=1}^{k} d_i \chi_i,$$

where $(W_1, \rho_1), \ldots, (W_k, \rho_k)$ are the irreducible representations $\dim(W_i) = d_i$ and $\mathrm{char}(W_i, \rho_i) = \chi_i$. Also,

$$r_G(g) = \begin{cases} |G| & \text{if } g = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Assume that (W_1, ρ_1) is these trivial representation of degree 1. So $d_1 = 1$ and $\chi_1 \equiv 1$. Fix $g \in \theta$. Then

$$0 = r_G(g) = 1 + \sum_{i=2}^{k} d_i \chi_i(g).$$

So either $p \mid d_i$ or $\chi_i(g) = 0$.

Claim. For $i = 2, 3, \ldots, k$, if $\chi_i(g) \neq 0$ then $p \mid d_i$.

Proof of the claim. Assume that $p \nmid d_i$. Note that $\gcd(|\theta|, d_i) = 1$ since $|\theta| = p^c$. So by Lemma 21, either $\chi_i(g) = 0$ or $(\rho_i)_g$ is a scalar. Assume that $\chi_i(g) \neq 0$. Then $(\rho_i)_g$ is scalar. So $(\rho_i)_g$ commutes with $(\rho_i)_h$ for all $h \in G$.

Consider $(\rho_i)_g : G \to W_i$, and let $N = \ker(\rho_i)_g$. Note that $N \neq G$, since (W_i, ρ_i) is not the trivial representation. So these simplicity implies that $N = \{1\}$. Hence $(\rho_i)_g : G \cong \mathrm{im}(\rho_i)_g$. Since $(\rho_i)_g$ commutes with $(\rho_i)_h$, we see that g commutes with all $h \in G$, hence $g \in Z(G) = \{1\}$. Hence $g \notin \theta$, a contradiction. The claim follows. □

The claim implies that if $p \nmid d_i$ then $\chi_i(g) = 0$. Equivalently, if $\chi_i(g) \neq 0$ then $p \mid d_i$.

$$-1 = \sum_{i=2}^{k} d_i \chi_i(g) = \sum_{\substack{2 \leq i \leq k \\ \chi_i(g) \neq 0}} d_i \chi_i(g) = \sum_{\chi_i(g) \neq 0} p e_i \chi_i(g),$$

where $e_i := d_i/p \in \mathbb{Z}$. Divide by p to get

$$-\frac{1}{p} = \sum_{\chi_i(g) \neq 0} e_i \chi_i(g),$$

so the right-hand side is an integral combination of an algebraic integer, but the left-hand side is not an algebraic integer, a contradiction. This completes the proof. □

Theorem 17 (Burnside's pq theorem, version I)**.** *If $|G| = p^a q^b$ for p, q distinct primes, then G is not a simple group.*

Proof. Suppose G is simple. Let $P \leq G$ be a Sylow p-subgroup. Then $|P| = p^a$. We know that $Z(P) \neq \{1\}$. Pick a non-identity element $g \in Z(P)$. Let $\mathcal{O}$ be the conjugacy class of g in G. By the orbit-stabilizer theorem, $|\theta| = [G : C_G(g)]$, where $C_G(g) := \{h \in G : hg = gh\} \supseteq P$ denotes the centralizer of g in G. Thus $[G : P] = q^b$ so $[G : C_G(g)] = q^\gamma$ for some $\gamma \leq \beta$. Therefore $[G : C_G(g)] = |\theta|$ and this contradicts Corollary 23. □

Definition 72. A finite group G is *solvable* if there exists a chain of subgroups $G = N_0 \triangleright N_1 \triangleright \cdots \triangleright N_m = \{1\}$ such that N_i/N_{i+1} is abelian for all i.

Theorem 18 (Burnside's pq theorem, version II)**.** *If $|G| = p^a q^b$ with p and q primes, then G is solvable.*

Proof. The proof is by induction on $|G|$. G is not simple, so there exists at least one N such that $\{1\} < N \triangleleft G$ such that $N \neq G$. By induction, N and G/N are both solvable. □

Department of Pure Mathematics, University of Waterloo, 200 University Avenue West, Waterloo, ON, Canada N2L 3G1
E-mail address: hsyang@uwaterloo.ca