Misc Notes in Algebra

1. THE STANDARD REPRESENTATION

Let M_σ be the permutation matrix corresponding to $\sigma \in S_n s$ and let M_{S_n} be the span of the M_σ.

LEMMA 1.1. *The Standard Representation of S_n is irreducible. Equivalently, $dim(M_{S_n}) = n^2 - 2n + 2$*

PROOF. Let M_σ be the permutation matrix corresponding to $\sigma \in S_n$.

1. $dim(M_{S_n}) \leq n^2 - 2n + 2$

   PROOF. The permutations decompose into $\begin{bmatrix} 1 & 0 \\ 0 & M'_\sigma \end{bmatrix}$ in a suitable basis. Alternate argument see next item. □

2. $dim(M_{S_n}) \geq n^2 - 2n + 2$

   PROOF. Define Generalized Stochastic matrices, $\mathbb{S}^{n\times n}$, as $\mathbb{R}^{n\times n}$ matrices whose row and column sums are all equal (but not necessarily 1)

   (a) $span(\{M_\sigma\}) \subseteq \mathbb{S}^{n\times n}$

   (b) Positive matrices in $\mathbb{S}^{n\times n} \subseteq span(\{M_\sigma\})$ via Birkhoff-Von Neumann. They span $\mathbb{S}^{n\times n}$. Hence,
   $$\mathbb{S}^{n\times n} \subseteq span(\{M_\sigma\})$$

   (c) $dim(\mathbb{S}^{n\times n}) = (n-1)^2 + 1$. Easy isomorphism $R^{(n-1)^2+1} \leftrightarrow \mathbb{S}^{n\times n}$

□

2. WEDDERBURN'S THEOREM

THEOREM 2.1. *Every finite division ring is a field*

PROOF. Let C_0 be the centre of R. Let $q = |C_0| \geq 2$. Let $C_1, \ldots C_k$ be the conjugacy classes of $(R\backslash 0, \cdot)$.

1. C_0 is a field and R is a vector space over C_0 with finite dimension, say n. It follows that $|R| = q^n$. We want to show that $n = 1$.

2. For any $a \in R$ the centralizer $N(a) = \{x : xa = ax\}$ is a vector space over C_0. It follows that the size of the conjugacy class containing a is $q^{n(a)}$ where $n(a) = |N(a)|$.

3. $N(a)\backslash 0$ is a subgroup of $(R\backslash 0, \cdot)$. It follows that the class equation can be written as
   $$q^n - 1 = (q-1) + \sum_{i=1}^{k} \frac{q^n - 1}{q^{n_i} - 1} \text{ (where } n_i | n)$$

4. Clearly $\Phi_n(q)$ (Φ_n is nth cyclotomic polynomial), divides all terms above except $q-1$ so for some polynomial p with integer coefficients
   $$\begin{aligned} q - 1 &= \Phi_n(q)p(q) \\ \implies |q-1| &\geq |\Phi_n(q)| \\ &\geq \prod |q - \theta_i| \end{aligned}$$
   where θ_i are the primitive nth roots of 1. Clearly this is a contradiction if $n > 1$ and $q > 1$.

□

3. STRUCTURE OF ABELIAN GROUPS

THEOREM 3.1. *Every finite abelian group G of order p^n can be uniquely decomposed into a product of cyclic groups of order $p^{n_1}, \ldots, p^{n_k}$ where $n_1 \geq \ldots \geq n_k$*

PROOF. For any $s||G|$ let $G(s) = \{g \in G : g^s = 1\}$. If G is cyclic then there is nothing to prove. Otherwise:

1. Pick an element g_1 in G of largest order and construct $G_1 = G/\langle g_1 \rangle$. Iterate till G_k is cyclic.

2. $|G(s)| = p^{m_s}$ where $m_s = \sum_{i=1}^{k} \min(s, n_i)$

3. If there are distinct decompositions then there exists an s such that $|G(s)|$ will be different for the two decompositions.

□

4. CONJUGACY CLASSES

We summarize some facts for the basic groups:

4.1 Dihedral Group

$D_{2n} = \langle a, b \rangle$, where $a^n = 1$ and $b^{-1}ab = a^{-1}$

5. AVERAGING PRINCIPLE

THEOREM 5.1. **(Averaging Principle)** *Suppose $\rho : G \to GL(V)$ is a representation of a* **finite** *group G and $v \in V$ any vector. The vector*
$$\frac{1}{|G|} \sum_{g \in G} \rho(g)v$$
is fixed by the action of G. In fact if $V_1 \subseteq V$ is the subspace of all fixed vectors for the action of G then the endomorphism
$$A = \frac{1}{|G|} \sum_{g \in G} \rho(g)$$
is a projection onto V_1.

PROOF. $\rho(hg) = \rho(h)\rho(g)$. The first claim follows. For the second claim,

1. $Im(A) = V_1$

2. If $M^2 = M$, it is a projection operator onto $Im(M)$

   PROOF. $v = (v - Mv) + Mv$. $(v - Mv) \in Ker(M)$. Hence, $V = Ker(M) + Im(M)$.
   Also, $u = Mv$ and $Mu = 0 \implies M^2 v = 0 = Mv = u$.
   Hence, $V = Ker(M) \oplus Im(M)$ □

LEMMA 5.2. *If the minimal polynomial of M has no repeated roots then M is diagonalizable.*

PROOF. M is diagonalizable $\Leftrightarrow$ M has an eigenbasis.

1. Any set of eigenvectors with distinct eigenvalues is linearly independent.

2. The direct sum of the eigenspaces is the entire space.

3. Pick a basis for each eigenspace of M.

□

COROLLARY 5.3. *If G is finite and $\rho : G \to GL(V)$ is a representation then $\forall g \in G$, $\rho(g)$ is diagonalizable.*

5.1 G-action on Hom(V,W)

Definition Let V, W be G-modules. We define the G action on $Hom(V, W)$ as follows:

$$\begin{tikzcd} V \arrow[r, "\phi"] & W \arrow[d, "g"] \\ V \arrow[u, "g^{-1}"] \arrow[r, "g \cdot \phi"'] & W \end{tikzcd}$$

This turns $Hom(V, W)$ into a G-module.

THEOREM 5.4. *The averaging operator:*

$$A(\phi) = \frac{1}{|G|} \sum_{g \in G} g \cdot \phi$$

projects $Hom(V, W)$ onto $Hom_G(V, W)$.

PROOF. The space of fixed points of the above G-action is $Hom_G(V, W)$.

$$\begin{aligned} g\phi g^{-1} = \phi &\iff g\phi = \phi g \\ &\iff \forall (v \in V),\ g \cdot \phi(v) = \phi(g \cdot v) \\ &\iff \phi \in Hom_G(V, W) \end{aligned}$$

It follows from the averaging principle, that the operator A is a projection onto $Hom_G(V, W)$ $\square$

Note the different objects types:

1. G-modules V, W
2. Vector space $Hom(V, W)$
3. G-module $Hom(V, W)$ using the G-action defined
4. Vector subspace $Hom_G(V, W)$ of $Hom(V, W)$. G acts trivially on this.

5.2 G-invariant inner product

LEMMA 5.5. *If G is a group and $\rho : G \to GL(V)$ is a finite dimensional representation. Then $\exists$ an inner product on V that is preserved by the action of G.*

PROOF. Choose any basis $\mathbb{B} = (v_1, \ldots, v_n)$ of V and let $\langle , \rangle_{\mathbb{B}}$ be the corresponding inner product. We define

$$[v_1, v_2]_{\mathbb{B}} = \frac{1}{|G|} \sum_{g \in G} \langle gv_1, gv_2 \rangle_{\mathbb{B}}$$

Clearly,

$$\begin{aligned} [hv_1, hv_2]_{\mathbb{B}} &= \frac{1}{|G|} \sum_{g \in G} \langle ghv_1, ghv_2 \rangle_{\mathbb{B}} \\ &= \frac{1}{|G|} \sum_{g \in G} \langle gv_1, gv_2 \rangle_{\mathbb{B}} \\ &= [v_1, v_2]_{\mathbb{B}} \end{aligned}$$

$\square$

5.3 R-module complements

Let R be a ring and $N \leq M$ be left R-modules. The following lemma shows that a complement of N in M is simply a system of coset representatives of M/N that is itself an R-module:

LEMMA 5.6. *R-module complements of N, if they exist, are unique up to isomorphism. In fact if,*

$$M = N \oplus N_1 = N \oplus N_2$$

then,

$$N_1 \cong N_2 \cong M/N \textit{ canonically}$$

PROOF. Consider the restriction $\phi|_{N_1}$ of the canonical map $\phi : M \to M/N$ to N_1. Clearly,

$$Ker(\phi|_{N_1}) = N \cap N_1 = \{0\} \text{ hence } \phi|_{N_1} \text{ is injective}$$

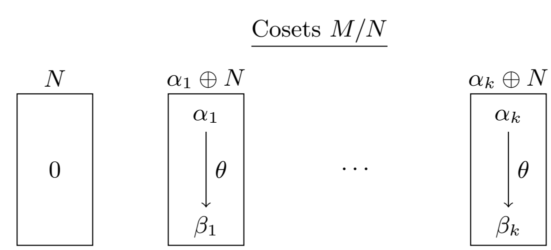
For any $\alpha \in M/N$, pick an $a \in \alpha$.

$$\begin{aligned} M = N \oplus N_1 &\implies a = n + n_1, n \in N, n_1 \in N_1 \\ &\implies \alpha = n_1 + N \\ &\implies \phi|_{N_1}(n_1) = \alpha \\ &\implies \phi|_{N_1} \text{ is surjective} \end{aligned}$$

$\square$

LEMMA 5.7. *Suppose N has an R-module complement N_α. All complements of N are in bijection with homomorphisms $\phi \in Hom_R(N_\alpha, N)$ given by $N_\phi = \{\phi(x) + x : x \in N_\alpha\}$.*

PROOF. Suppose N_β a system of coset respresentatives and $\theta : N_\alpha \to N_\beta$ as below:



Consider the map $\phi = \theta - I$. Clearly $Im(\phi) \subseteq N$.

$$\begin{aligned} M = N \oplus N_\beta &\iff \theta \in Iso_R(N_\alpha, N_\beta) \text{ (previous lemma)} \\ &\iff \phi \in Hom_R(N_\alpha, N) \end{aligned}$$

$\square$

COROLLARY 5.8. *In the above lemma*

$$(Hom_R(N_\alpha, N) = \{0\}) \iff (N_\alpha \textit{ is uniquely defined})$$

5.4 Complements in $\mathbb{C}G$

THEOREM 5.9 (MASCHKE). *Let G be a finite group and V a $\mathbb{C}G$-module. V is a direct sum $V_1 \oplus \cdots \oplus V_k$ where the V_i are simple.*

PROOF. Enough to show that for any proper submodule $U \subseteq V$ there is a decomposition $V = U \oplus W$.

1. First proof:

   (a) Extend any basis of U to a basis $\mathbb{B}$ of V.

(b) Pick $W = U^{\perp}$ wrt the inner product $[,]_{\mathbb{B}}$. It only remains to check that W is closed under G-action:

$$\begin{aligned} [w,u]_{\mathbb{B}} &= 0, \forall u \in U \\ \implies [hw,u]_{\mathbb{B}} &= \frac{1}{|G|}\sum_{g\in G}\langle ghw, gu\rangle_{\mathbb{B}} \\ &= [w, h^{-1}u]_{\mathbb{B}} \\ &= 0 \end{aligned}$$

2. Second proof:

(a) Extend any basis of U to a basis of V and define the projection ϕ onto U in this basis.

(b) The averaged operator (using the G-action in previous section), ϕ_A, is a $\mathbb{C}G$-module projection onto U.

(c) $W = Ker(\phi_A)$

□

Lemma 5.10. *For any $\mathbb{C}G$-module V, the isotypic component of the one dimensional trivial representation in V is unique.*

Proof. Let,

$$V = c_1U_1 \oplus \cdots \oplus c_kU_k$$

where c_iU_1 is the isotypic component of the 1D trivial representation, and let

$$F = \{v : v \in V \text{ and } g\cdot v = v\}$$

Clearly $v \in c_1U_1 \Rightarrow v \in F$ Now suppose $v \in F$ and

$$\begin{aligned} v &= \sum_{1\le i\le k} v_i \text{ where } 0 \neq v_i \in c_iU_i \\ \Rightarrow g\cdot v &= \sum_{1\le i\le k} g\cdot v_i, \forall g \in G \end{aligned}$$

Since G does not act trivially on c_iU_i $(i \neq 1)$there must exist $v_i \neq 0$. For this v_i there must be a $g \in G$ such that $g\cdot v_i \neq v_i$. □

Corollary 5.11. *The projection onto V_1 in the averaging principle is unique.*

Theorem 5.12. *For any $\mathbb{C}G$-module V and irreducible $\mathbb{C}G$-module U, the isotypic component of U in V is unique.*

Proof. Suppose U_1, U_2 are distinct isotypic components of U in V.

1. From Maschke's theorem, $V = U_1 \oplus V_1$. Consider any projection of U_2 into V_1.

2. Schur's theorem ensures that the image of this projection is $\{0\}$, hence $U_2 \subseteq U_1$.

3. Other direction is similar.

□

5.5 Inner product of characters

We start with a simple restatement of the averaging principle:

Lemma 5.13. *Let G be a group and $\mathbb{C}$ be its trivial 1D representation. For any representation U of G,*

$$dim(Hom_G(\mathbb{C}, U)) = \langle \chi_{\mathbb{C}}, \chi_U\rangle$$

Proof. Clearly, $Hom(\mathbb{C}, U) \cong U$ as vector spaces. Let $\phi_u \in Hom(\mathbb{C}, U)$ take 1 to u. The following diagram:

$$\begin{tikzcd} \mathbb{C} \arrow[r, "\phi_u"] & U \arrow[d, "g"] \\ \mathbb{C} \arrow[u, "g^{-1}"] \arrow[r, "\phi_{g\cdot u}"'] & U \end{tikzcd}$$

shows that the G-representations on $Hom(\mathbb{C}, U)$, and U are isomorphic (say ρ)

Consider the averaging operator A from theorem 5.4 acting on $Hom(\mathbb{C}, U)$:

$$\begin{aligned} dim(Hom_G(\mathbb{C}, U)) &= Tr(A) \\ &= \frac{1}{|G|}\sum_{g\in G} Tr(\rho(g)) \\ &= \frac{1}{|G|}\sum_{g\in G} \chi_U(g) \\ &= \langle \chi_{\mathbb{C}}, \chi_U\rangle \end{aligned}$$

□

The following theorem is just a generalization of the averaging principle:

Theorem 5.14. *Let U, V be representations of a group G and χ_U, χ_V their respective characters.*

$$\langle \chi_U, \chi_V\rangle = dim(Hom_G(U, V))$$

Proof. Let ρ_U, ρ_V be the representations of G in U, V respectively. Clearly, for $M \in Hom(U, V)$ and $g \in G$,

$$g\cdot M = \rho_V(g)M\rho_U(g)^{-1} = \rho_V(g)M\rho_U(g^{-1})$$

Let ρ be the representation of G in $Hom(U, V)$, χ its character and $E_{i,j}$ the standard basis of $Hom(U, V)$.

$$\begin{aligned} Tr(\rho(g)) &= \sum_{i,j}(\rho_U(g^{-1}))_{i,i}(\rho_V(g))_{j,j} \\ &= Tr(\rho_U(g^{-1}))\cdot Tr(\rho_V(g)) \\ \Rightarrow \chi_(g^{-1}) &= \chi_U(g)\cdot\chi_V(g) \end{aligned}$$

Using the previous lemma on the representation ρ,

$$\begin{aligned} dim(Hom_G(\mathbb{C}, Hom(U, V)) &= \frac{1}{|G|}\sum_{g\in G}\chi(g) \\ \Rightarrow dim(Hom(U, V)) &= \frac{1}{|G|}\sum_{g\in G}\chi_U(g^{-1})\cdot\chi_V(g) \\ &= \langle \chi_U, \chi_V\rangle \end{aligned}$$

□

6. R-MODULE HOMOMORPHISMS

Let $R \leq S$ be rings, M, N be R-modules.

1. $Hom_R(M,N)$ is an R-module iff R is commutative
2. $Hom_R(R,M) \cong M$ as abelian groups
3. Every $\phi \in Hom_R(R,S)$ is the right multiplication by $\phi(1)$.
4. $Hom_R(R,R) \cong R^{opp}$ as rings

6.1 Homomorphisms in $\mathbb{C}G$

Let $H \leq G$ be groups and U be a left $\mathbb{C}H$-submodule of $\mathbb{C}H$.

1. Any $\phi \in Hom_H(U, \mathbb{C}H)$ is given by right multiplication by some $\alpha \in \mathbb{C}H$

   Proof. By Maschke's Theorem, $\mathbb{C}H = U \oplus V$ for some $\mathbb{C}H$-submodule V. Let ψ be a projection operator, $\psi : \mathbb{C}H \to U$. $\square$

7. INDUCED REPRESENTATIONS

Let $H \leq G$ be groups and let U be a $\mathbb{C}H$-module with H action given by ρ and character χ. We give three equivalent definitions of the induced $\mathbb{C}G$-module $U \uparrow G$, equivalently the induced representation $\rho \uparrow G$ and induced character $\chi \uparrow G$

Definition I1 Choose a system of left coset representatives $g_1 = 1, \ldots, g_k$ of H in G. Extend ρ by defining $\rho(g) = 0$ whenever $g \in G \setminus H$. Similarly χ.

$$(\rho \uparrow G)(x) = \begin{bmatrix} \rho(g_1^{-1}xg_1) & \rho(g_1^{-1}xg_2) & \cdots & \rho(g_1^{-1}xg_k) \\ \rho(g_2^{-1}xg_1) & \rho(g_2^{-1}xg_2) & \cdots & \rho(g_2^{-1}xg_k) \\ \vdots & \vdots & \rho(g_i^{-1}xg_j) & \vdots \\ \rho(g_k^{-1}xg_1) & \rho(g_k^{-1}xg_2) & \cdots & \rho(g_k^{-1}xg_k) \end{bmatrix}$$

$$\begin{aligned} (\chi \uparrow G)(x) &= \sum_i \chi(g_i^{-1}xg_i) \\ &= \frac{1}{|H|}\sum_{g\in G}\chi(g^{-1}xg) \end{aligned}$$

Note that this definition allows us to extend the definition of $\chi \uparrow G$ to any class function χ.

Definition I2 Choose a system of left coset representatives $g_1 = 1, \ldots, g_k$ of H in G. Let $e_1, \ldots, e_l$ be a basis of U. We construct the vector space with basis symbols $g_i \otimes e_j$ with the following properties:

1. $h \otimes e_j = 1 \otimes he_j$, whenever $h \in H$
2. $g_i \otimes (\sum_j c_j e_j) = \sum_j c_j g_i \otimes e_j$
3. $g \cdot (g_i \otimes e_j) = g_a \otimes he_j$, where $gg_i = g_a h$

Note: Add "extension of scalars definition"

Theorem 7.1 (Frobenius' Reciprocity Theorem). *Let χ, ψ be any class functions on H, G respectively.*

$$\langle \chi \uparrow G, \psi\rangle_G = \langle \chi, \psi \downarrow H\rangle_H$$

Proof. Bilinearity of inner product ensures that it is enough to verify for arbitrarily chosen bases of the space of class functions over H, G. We choose the bases of indicators of the conjugacy classes in H, G.

Fix $h_0 \in H, g_0 \in G$ and let

$$\chi = \text{indicator of } h_0^H, \quad \psi = \text{indicator of } g_0^G$$

Suppose $x \in h_0^G$,

$$\begin{aligned} (\chi \uparrow G)(x) &= \frac{1}{|H|}\sum_{g\in G}\chi(g^{-1}xg) \\ &= \frac{|C_G(x)| \cdot |h_0^H|}{|H|} \\ &= \frac{|C_G(x)|}{|C_H(h_0)|} \\ &= \frac{|C_G(h_0)|}{|C_H(h_0)|} \end{aligned}$$

Hence we have,

$$(\chi \uparrow G)(x) = \begin{cases} \frac{|C_G(h_0)|}{|C_H(h_0)|} & \text{if } x \in h_0^G \\ 0 & \text{otherwise} \end{cases}$$

Also note,

$$(\psi \downarrow H)(x) = \begin{cases} 1 & \text{if } x \in h_0^G \\ 0 & \text{otherwise} \end{cases}$$

Finally,

$$\begin{aligned} \langle \chi \uparrow G, \psi\rangle_G &= \frac{1}{|G|}\sum_{g\in G}(\chi \uparrow G)(g)\cdot\psi(g) \\ &= \frac{1}{|G|}\cdot\frac{|C_G(h_0)|}{|C_H(h_0)|}|h_0^G| \\ &= \frac{1}{|C_H(h_0)|} \\ \langle \chi, \psi \downarrow H\rangle_H &= \frac{1}{|H|}\sum_{h\in H}\chi(h)\cdot(\psi\downarrow H)(h) \\ &= \frac{|h_0^H|}{|H|} \\ &= \frac{1}{|C_H(h_0)|} \end{aligned}$$

$\square$