Hidden Subgroup Minicourse - Representations

Gábor Ivanyos
MTA SZTAKI & TU/e

CWI Amsterdam, October 30 - November 3, 2006

Contents

1. The group algebra $\mathbb{C}G$
   - The group algebra $\mathbb{C}G$
2. Modules and representations
   - Definitions
   - Isomorphism, equivalence
   - Irreducibility
   - Unitary representations
3. Decomposition of modules
   - Complete reducibility
   - Uniqueness of the decomposition
   - Finiteness of the number of reps

The group algebra $\mathbb{C}G$

- G finite group, the group algebra $\mathbb{C}G$ is the complex vector space of dimension $|G|$, with basis G.
- In the context of quantum algorithms, a scalar product of $\mathbb{C}G$ is also used: $\mathbb{C}G$ is the complex Hilbert space (euclidean space) of dimension G, with orthonormal basis $\{|g\rangle | g \in G\}$.
- The classical HSP algorithms work over $\mathbb{C}G$:
  - $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle|0\rangle$
  - $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle|f(g)\rangle$

    Measure the second reg. observe value b:
  - $\frac{1}{\sqrt{|\mathrm{H}|}} \sum_{g:f(g)=b} |g\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |ah\rangle$, where $a \in G$ such that $f(a) = b$.

The group algebra $\mathbb{C}G$ 2.

- Multiplication in $\mathbb{C}G$: bilinear extension of the multiplication if G.
- This makes $\mathbb{C}G$ an associative ring with identity $1 = 1_G$ and $\mathbb{C}1 \cong \mathbb{C}$ in the center.
  (These are associative algebras with identity over $\mathbb{C}$.)
- The left regular representation of G: $g \in G$ acts as a unitary transformation by multiplication from the left.
  - why unitary?
- Goal: decompose $\mathbb{C}G$ into as small common invariant subspaces as possible.
- This generalizes the concept of eigenvectors/eigenspaces.

The group algebra $\mathbb{C}G$ 3.

Remark: $\mathbb{C}G$ is often viewed as the linear space of functions $G \to \mathbb{C}$.

- has another ring structure: operation defined on function values. $(f_1 + f_2)(g) = f_1(g) + f_2(g)$, $(f_1 \cdot f_2)(g) = f_1(g) \cdot f_2(g)$.
- this ring is always commutative and has a rather obvious structure.
- "our" multiplication in this context is called convolution.
- it is commutative iff G is.
- For defining Fourier transforms, this "dual" view may be more appropriate
- To me, in the quantum algorithms setting the other "direct" approach appears to be more natural.

Contents

1. The group algebra $\mathbb{C}G$
   - The group algebra $\mathbb{C}G$
2. Modules and representations
   - Definitions
   - Isomorphism, equivalence
   - Irreducibility
   - Unitary representations
3. Decomposition of modules
   - Complete reducibility
   - Uniqueness of the decomposition
   - Finiteness of the number of reps

Definitions

- A **linear representation** (or just representation) on the complex vector space V is a homomorphism $\rho : G \to GL(V)$.
- linear action: write gv instead $\phi(g)v$. Satisfies:
  - $(gh)v = g(hv)$
  - $g(\alpha v + \beta w) = \alpha gv + \beta gw$.
- G**-module:** a vector scape V together with a linear action of G on V s.t. 1_G act as the identity on V.

  Condition on 1_G assures that we have a homomorphis into the group $GL(V)$. Without this we would allow actions like $gv = 0$, which do not give homomorphisms into groups.
- In this course, modules are finite dimensional.
- by fixing a basis of V, obtain a **matrix representation**, a homomorphism $\Phi : G \to M_n(\mathbb{C})$ for $n = \dim V$.

Examples

regular representation

- module: $\mathbb{C}G$, action: lin. ext. of $x \mapsto gx$.
- matrix representation in the basis G:
$$\Phi(g)_{xy} = \begin{cases} 1 & \text{if } x = gy \\ 0 & \text{otherwise} \end{cases}$$

permutation representation from an action on $\{1, \ldots, n\}$

- module: $\mathbb{C}^n$ with basis $|1\rangle, \ldots, |n\rangle$
action: lin. ext. of $\omega \mapsto g\omega$.
- matrix representation:
$$\Phi(g)_{ij} = \begin{cases} 1 & \text{if } i = gj \\ 0 & \text{otherwise} \end{cases}$$

Examples 2.

One-dimensional reps of $\mathbb{Z}_n$ $\omega = \sqrt[n]{1}$, say $e^{2\pi i/n}$.

- $\rho_j(k) = \omega^{jk}$
- module: $\mathbb{C}$, action of k: mult. by ω^{jk}.
- matrix $\Phi_j(k)$ of $\rho_j(k)$: 1×1 ω^{jk}.

Two-dimensional rep of $\mathbb{Z}_n$ $\alpha = 2\pi/n$, $\omega = e^{\alpha i}$,

- in the $x - y$ basis:

$$\Phi(k) = \begin{pmatrix} \cos(k\alpha) & -\sin(k\alpha) \\ \sin(k\alpha) & \cos(k\alpha) \end{pmatrix}$$

- in the eigenbasis:

$$\Phi(k) = \begin{pmatrix} \omega^k & 0 \\ 0 & \omega^{-k} \end{pmatrix}$$

Examples 3.

Natural rep of D_n in the $x - y$ basis

- $\alpha = 2\pi/n$
- rotation by α: $\Phi(r) = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & cos(\alpha) \end{pmatrix}$
- reflection w.r.t x-axis: $\Phi(t) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
- rotations:
  $\Phi(r^k) = \Phi(r)^k = \begin{pmatrix} \cos(k\alpha) & -\sin(k\alpha) \\ \sin(k\alpha) & \cos(k\alpha) \end{pmatrix}$
- reflections: $\Phi(r^k t) = \Phi(r^k)\Phi(t) =$
  $\begin{pmatrix} \cos(k\alpha) & \sin(k\alpha) \\ \sin(k\alpha) & -\cos(k\alpha) \end{pmatrix}$

Examples 4.

Natural rep of D_n in the eigenbasis for rotation.

- rotations: $\Phi'(r^k) = \begin{pmatrix} \omega^k & 0 \\ 0 & \omega^{-k} \end{pmatrix}$
- reflections: $\Phi'(r^k t) = \begin{pmatrix} 0 & \omega^k \\ \omega^{-k} & 0 \end{pmatrix}$

Isomorphism, equivalence

- isomorphism of modules: $V_1 \cong V_2$ iff there is a linear bijection $\mu : V_1 \to V_2$, such that $\mu(gv) = g(\mu v)$ for every $g \in G$ and $v \in V_1$.
- $\phi_1 : G \to GL(V_1), \phi_2 : G \to GL(V_2)$ $\phi_1(g)v_1 = gv_1$, $\phi_2(g)v_2 = gv_2$. $\mu(\phi_1(g)v) = \phi_2(g)(\mu(v))$,

$$\phi_2(g) = \mu\phi_1(g)\mu^{-1}.$$

- equivalence of linear representations: $\phi_1 : G \to GL(V_1)$ and $\phi_2 : G \to GL(V_2)$ are equivalent, if there is a lin. bijection μ as above.

  In words: the $\phi_2(g)$'s are simultaneously conjugates of the $\phi_1(g)'s$ by μ.

Isomorphisms 2.

- change of basis for matrix representations: If B is the matrix of the of the basis change then in the new basis the matrix is

$$B\Phi(g)B^{-1},$$

  where $\Phi : G \to M_n(\mathbb{C})$
- equivalence of matrix representations: dimension equality + existence of B as above.
- two linear representation equivalent, if and only if they give equivalent matrix representations.

Example 1

- the two reps

$$\Phi : r^k \mapsto \begin{pmatrix} \cos(k\alpha) & -\sin(k\alpha) \\ \sin(k\alpha) & \cos(k\alpha) \end{pmatrix}, r^k t \mapsto \begin{pmatrix} \cos(k\alpha) & \sin(k\alpha) \\ \sin(k\alpha) & -\cos(k\alpha) \end{pmatrix}$$

and

$$\Phi' : r^k \mapsto \begin{pmatrix} \omega^k & 0 \\ 0 & \omega^{-k} \end{pmatrix}, r^k t \mapsto \begin{pmatrix} 0 & \omega^k \\ \omega^{-k} & 0 \end{pmatrix}$$

of D_n are equivalent.

Example 2

- replace α by $j\alpha$ and ω by ω^j

  obtain representations of D_n

$$\Phi'_j : r^k \mapsto \begin{pmatrix} \omega^{jk} & 0 \\ 0 & \omega^{-jk} \end{pmatrix}, r^k t \mapsto \begin{pmatrix} 0 & \omega^{jk} \\ \omega^{-jk} & 0 \end{pmatrix}$$

  $Tr(\Phi'_j(r)) = \omega^j + \omega^{-j} = 2\cos(j\alpha)$,
  So $Tr(\Phi'_{j_1}(r)) \neq Tr(\Phi'_{j_2}(r))$ if $j_2 \neq \pm j_1 \pmod{n}$.
  Similar matrices have the same trace. If $j_2 \neq \pm j_1 \pmod{n}$ then Φ'_{j_1} and Φ'_{j_2} are non-equivalent.
- $\Phi'_{-j}(g) = \Phi'_j(t)\Phi'_j(g)\Phi'_j(t)$ for every $g \in D_n$,
- Φ'_{j_1} and Φ'_{j_2} are equivalent if and only if $j_2 = \pm j_1 \pmod{n}$.

Submodules, subrepresentations

- W lin. subspace of the G-module V is a submodule if $gW \leq W$ for every $g \in G$.
- submodule= common invariant subspace
- subrepresentation: action restricted to a submodule.
- In a basis that extends a basis of the submodule, the matrix rep is (simultenously) upper block triangular.
- Example. $\sum_{x \in G} x \in \mathbb{C}G$ is an eigenvector of any $g \in G$ (with eigenvalue 1), so it generates a one-dimensional submodule.

  the corresponding rep is the *trivial* (or *principal*) rep of G: $1 : g \mapsto 1 \in \mathbb{C}$.

Submodules, subrepresentations 2

- Example. The 2-dim representation Φ of $\mathbb{Z}_n$ given as

$$\Phi(k) = \begin{pmatrix} \omega^k & 0 \\ 0 & \omega^{-k} \end{pmatrix}$$

has two 1-dimensional subreps (if $n > 2$)

(If $n \leq 2$ then any vector is an eigenvector.)

Irreducible representations

- submodule = common invariant subspace.
- interested in as small submodules as possible.
- $(0) \neq V$ is **irreducible** if V has only the obvious submodules (0) and V.
- the corresponding representation is also called irreducible.
  (Irrep=IRreducible REPresentation)
- otherwise reducible
- every one-dimensional representation is irreducible.

Example for an irrep

Example. The natural representation of D_n $(n > 3)$ is irreducible.

- $\Phi' : r^k \mapsto \begin{pmatrix} \omega^k & 0 \\ 0 & \omega^{-k} \end{pmatrix}, r^k t \mapsto \begin{pmatrix} 0 & \omega^k \\ \omega^{-k} & 0 \end{pmatrix}$
- a proper submodule is generated by a common eigenvector. The rotation $\Phi'(r)$ has two distinct eigenvalues.
- The reflection $\Phi'(t)$ swaps the corresponding eigenspaces,
- So no eigenvector of $\Phi'(r)$ is an eigenvector of $\Phi'(t)$.

Unitary representations

- Assume V is equipped with a pos. def. Hermitian bilinear function $(,)$:
  - $(v_1 + v_2, w) = (v_1, w) + (v_2, w)$, $(v, w_1 + w_2) = (v, w_1) + (v, w_2)$.
  - $(\alpha v, w) = \overline{\alpha}(v, w)$ and $(v, \beta w) = \beta(v, w)$
  - $(v, w) = \overline{(w, v)}$
  - $(v, v) > 0$ whenever $v \neq 0$.
- If $v_1, \ldots, v_n$ is a basis of V then

$$(\sum_i \alpha_i v_i, \sum_j \beta_j v_j) := \sum_i \overline{\alpha_i}\beta_i = \underline{\alpha}^\dagger \underline{\beta}$$

gives a pos. def. Hermitian bilinear function on V, s.t. $v_1, \ldots, v_n$ is an orthonormal basis.

Unitary representations 2.

- Conversely, if $(,)$ is a pos. def. Hermitian bilinear function on V then $\exists$ an orthonormal basis. For every orthonormal basis $v_1, \ldots, v_n$:

$$(\sum_i \alpha_i v_i, \sum_j \beta_j v_j) := \sum_i \overline{\alpha_i}\beta_i = \underline{\alpha}^\dagger \underline{\beta}.$$

- $U(V) = \{g \in GL(V) | (gv, gw) = (v, w) \text{ for every } v, w \in V\}$.
- For $g \in GL(V)$, $g \in U(V)$ iff the matrix of g is unitary in an orthonormal basis of V.

Theorem. Every finite dimensional representation of a finite group G is equivalent to a unitary one.

Proof.

- Let V be the underlying G-module.
- Pick a pos. def. Hermitian bilinear function $\langle , \rangle$ on V.
- For every $g \in G$, $\langle , \rangle_g$ defined as $\langle v, w \rangle_g = \langle gv, gw \rangle$ is again a pos. def. Hermitian bilinear function.
- So is $(,) = \sum_{g \in G} \langle , \rangle_g$
- $(gv, gw) = \sum_{g' \in G} \langle g'gv, g'gw \rangle$

$$g'' = g'g.$$

- $(gv, gw) = \sum_{g'' \in G} \langle g''v, g''w \rangle = (v, w)$
- Every g is unitary w.r.t $(,)$.
- In an orthonormal basis for $(,)$, the matrix rep is unitary.

Contents

1 The group algebra $\mathbb{C}G$
- The group algebra $\mathbb{C}G$

2 Modules and representations
- Definitions
- Isomorphism, equivalence
- Irreducibility
- Unitary representations

3 Decomposition of modules
- Complete reducibility
- Uniqueness of the decomposition
- Finiteness of the number of reps

Complete reducibility

- A G-module V is called **completely reducible** if V is a direct sum of irreducible submodules.
- Matrix representation of direct sums: block diagonal (in appropriate bases).
- **Theorem.** Every finite dim representation of a finite group G is completely reducible
    - W submodule of V. Then $W^{\perp}$ is also a submodule:
      If $w' \in W^{\perp}$ and $w \in W$ then $(gw', w) = (gw', g(g^{-1}w) = 0$ since $g^{-1}w \in W$.
      Hence $gw' \in W^{\perp}$.
    - $V = W \oplus W^{\perp}$
    - refine until we get irred. modules.

Uniqueness of the decomposition

- Example. $V \oplus V = \{(v,0)|v \in V\} \oplus \{(0,v)|v \in V\}$ $= \{(v,v)|v \in V\} \oplus \{(v,v)|v \in V\}^{\perp}$
- Uniqueness only by means of the numbers of isomorphic irreducible components.
- V, W G-mod. A linear map $\phi : V \to W$ is a homomorphism of G-modules (notation $\phi \in Hom_G(V,W)$) if $\phi g = g\phi$ for every $g \in G$.
- If V, W are irreducible G-modules and $V \not\cong W$, then $Hom_G(V,W) = (0)$.

  The image of the homomorphism is either zero or a submodule of W isomorphic to V. The latter is impossible.

Uniqueness 2.

- If V, W_i are irreducible G-modules and $V \not\cong W_i$ $(i = 1, \ldots, n)$ then $Hom_G(V, \bigoplus_{i=1}^n W_i) = 0$.
  - Consider $\psi_i : \bigoplus_{i=1}^n W_i \to W_i$ projection. If $\phi \in Hom_G(V, \bigoplus_{i=1}^n W_i)$ then $\phi\psi_i \in Hom_G(V, W_i) = (0)$ $(i = 1, \ldots, n)$.
- **Notation.** V arbitrary, W irreducible G-mod.

$$V_W = \sum_{W \cong W' \leq V} W',$$

  the submodule generated by all the submodules isomorphic to W.
- **Theorem.** $V = \bigoplus_{i=1}^n W_i$, W_i and W irreducible $(i = 1, \ldots n)$. Then

$$V_W = \bigoplus_{i | W_i \cong W} W_i.$$

Proof of the theorem

- Let $V'_W = \bigoplus_{i|W'_i \not\cong W}$. Then $Hom_G(W, V'_W) = 0$.
- Assume $W \cong W' \leq V$ and $W' \not\leq U = \bigoplus_{i|W'_i \cong W} W_i$.
- Then composing the embedding with $V/U \cong V'_W$, we obtain a nonzero element of $Hom_G(W, V'_W)$, a contradiction with the previous statement.
- Thus $V_W \leq \bigoplus_{i|W'_i \cong W} W_i$.
- The other inclusion is obvious.

- **Corollary.** The multiplicity of W in any decomposition of V is dim $V_W/dimW$.

Finitely many irreps.

- Already know, that a specific finite dimensional module contains only finitely many non-isomorphic irreducible submodules.
- In particular the (left) regular module $\mathbb{C}G$ contains finitely many irreducible submodules.
- **Theorem.** Any irreducible G-module is isomorphic to a submodule of $\mathbb{C}G$.
  - V irred. G-module. Let $V \ni v \neq 0$.. Then $V = \{\sum \alpha_g gv | \underline{\alpha} \in \mathbb{C}^{|G|}\}$. If $\mathbb{C}G \ni x = \sum \alpha_g g$, then define $xv = \sum_{g \in G} \alpha_g gv$. Then for the map $\phi : x \mapsto xv$, $\phi \in Hom_G(\mathbb{C}G, V)$. As the image is V, $V \cong \mathbb{C}G / \ker \phi \cong (\ker \phi)^\perp$.

Contents

4. Basic orthogonalities
   - Shur's lemma
   - Orthogonality of the matrix elements
   - The Inverse Fourier transform
5. The structure of the group algebra
   - Decomposition of the group algebra
   - Consequences of the structure theorem
   - Misc
6. Characters
   - Character basics
   - Scalar product of characters
7. Tensor products
   - Tensor products of matrices
   - Irreps of direct products.
   - Tensor products of representations

Schur's lemma

Shur's lemma. V, W irred. G-modules. Then

$$Hom_G(V,W) = \begin{cases} \mathbb{C}\psi & \text{if } V \cong W \text{ (and } \psi \text{ arbitrary iso)} \\ 0 & \text{if } V \ncong W \end{cases}$$

(The (easy) case $V \ncong W$ has been established earlier.)

- Obviously, $\mathbb{C}\psi \subseteq Hom_G(V,W)$.
- Multiplying by ψ^{-1}, we may assume $W = V$ and $\psi = I$.
- Let $\phi \in Hom_G(V,V)$: ϕ is a linear transformation of V with $\phi\rho(g) = \rho(g)\phi$ for every $g \in G$.
- Let λ be an eigenvalue of ϕ. Then $(\phi - \lambda I)V < V$ is subspace of V.
- Also, $\rho(g)(\phi - \lambda I)V = (\phi - \lambda I)\rho(g)V = (\phi - \lambda I)V$, so it is a submodule.
- As V is irred and $V > (\phi - \lambda I)V$, $(\phi - \lambda I)V = (0)$, so $\phi = \lambda I$.

Orthogonality

Orthogonality of the matrix elements

Let ρ, ρ' be two irreducible unitary matrix representations of G such that either $\rho = \rho'$ or ρ and ρ' are non-equivalent. $i, j \le d_\rho = \dim \rho$, $i', j'; \le d_{\rho'} = \dim \rho'$. Then

$$\frac{1}{|G|} \sum_{g \in G} \rho(g)_{ij} \overline{\rho'(g)_{i'j'}} = \begin{cases} \frac{1}{d_\rho} & \text{if } \rho = \rho', i = i', j = j' \\ 0 & \text{otherwise} \end{cases}$$

Orthogonality - proof 1.

- Modules: $V_\rho = \mathbb{C}^{d_\rho}$, $V_{\rho'} = \mathbb{C}^{d'_\rho}$.
- Consider the $d_\rho \times d_{\rho'}$ elementary matrix $E_{k\ell}$. (Everywhere 0 except in pos. $k\ell$, where 1.)
- $E_{k\ell} : V_\rho \to V_{\rho'}$ linear map.
- Claim: $A^{k\ell} = \frac{1}{|G|}\sum_{g\in G} \rho'(g)^{-1} E_{k\ell}\rho(g) \in Hom_G(V_\rho, V_{\rho'})$

$$\begin{aligned}
\rho'(x)^{-1}A^{k\ell}\rho(x) &= \frac{1}{|G|}\sum_{g\in G}\rho'(gx)^{-1}E_{k\ell}\rho(gx) \\
&\qquad y = gx \\
&= \frac{1}{|G|}\sum_{y\in G}\rho'(y)^{-1}E_{k\ell}\rho(y) = A^{k\ell}, \text{so} \\
A^{k\ell}\rho(x) &= \rho'(x)A^{k\ell}
\end{aligned}$$

Orthogonality - proof 2.

- $A^{k\ell} = \frac{1}{|G|}\sum_{g\in G} \rho'(g)^{-1}E_{k\ell}\rho(g) \in Hom_G(V_\rho, V_{\rho'})$
- By Schur's lemma, $A^{k\ell} = 0$ if $\rho \neq \rho'$. and $A^{k\ell} = \alpha I$ if $\rho = \rho'$.
- $\left(\rho'(g)^{-1}E_{i'i}\rho(g)\right)_{j'j} = (\rho'(g)^{-1})_{j'i'}\rho(g)_{ij} = \overline{\rho(g)_{i'j'}}\rho(g)_{ij}$
- $\left(A^{i'i}\right)_{j'j} = \frac{1}{|G|}\sum_{g\in G} \rho(g)_{ij}\overline{\rho'(g)_{i'j'}}$

  Therefore:
- $\frac{1}{|G|}\sum_{g\in G} \rho(g)_{ij}\overline{\rho'(g)_{i'j'}} = 0$ if $\rho' \neq \rho$.
- $\frac{1}{|G|}\sum_{g\in G} \rho(g)_{ij}\overline{\rho(g)_{i'j'}} = 0$ if $j \neq j'$.

Orthogonality - proof 3.

- For $i \neq i'$:

$$\begin{aligned}\frac{1}{|G|}\sum_{g\in G}\rho(g)_{ij}\overline{\rho(g)_{i'j'}} &= \frac{1}{|G|}\sum_{g\in G}\rho(g^{-1})_{ij}\overline{\rho(g^{-1})_{i'j'}} \\ &= \frac{1}{|G|}\sum_{g\in G}\overline{\rho(g)_{ji}}\rho(g)_{j'i'} \\ &= 0 \quad \text{if } i \neq i'.\end{aligned}$$

Orthogonality - proof 4.

- For $\rho = \rho', i = i', j = j'$
- $\frac{1}{|G|} \sum_{g \in G} \rho(g)_{ij} \overline{\rho(g)_{ij}} = \left(A^{ii}\right)_{jj} = \alpha$, where $A^{ii} = \alpha I_{d_\rho}$.
- So

$$\begin{aligned}
\frac{1}{|G|} \sum_{g \in G} \rho(g)_{ij} \overline{\rho(g)_{ij}} &= \frac{1}{d_\rho} Tr(A^{ii}) \\
&= \frac{1}{d_\rho |G|} \sum_{g \in G} Tr(\rho(g)^{-1} E_{ii} \rho(g)) \\
&= \frac{1}{d_\rho}
\end{aligned}$$

The Inverse Fourier transform

- $\hat{G}$ = set of representatives of the equivalence classes of irreps of G, a finite set. We view each $\rho \in \hat{G}$ as a unitary matrix representation of dimension d_ρ
- Consider the linear space $R = \bigoplus_{\rho \in \hat{G}} M_{d_\rho}(\mathbb{C})$.
- R has orthonormal basis $\{E^\rho_{ij} | \rho \in \hat{G}, 1 \leq i,j \leq d_\rho\}$, where E^ρ_{ij} is the appropriate elementary matrix in the ρth component.

Inverse Fourier transform

linear extension of

$$E^\rho_{ij} \mapsto \frac{\sqrt{d_\rho}}{\sqrt{|G|}} \sum_{g \in G} \overline{\rho(g)_{ij}} g$$

The Inverse Fourier transform 2.

- Inverse Fourier transform: linear extension of

$$E_{ij}^{\rho} \mapsto \frac{\sqrt{d_\rho}}{\sqrt{|G|}} \sum_{g \in G} \overline{\rho(g)_{ij}} g$$

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

$$\Phi^{-1} : \sum_{\rho,i,j} \alpha_{\rho,i,j} E_{ij}^{\rho} \mapsto \sum_{g \in G} \sum_{\rho,i,j} \frac{\sqrt{d_\rho}}{\sqrt{|G|}} \alpha_{\rho,i,j} \overline{\rho(g)_{ij}} g.$$

- Orthogonality of the matrix elements

$$\frac{1}{|G|} \sum_{g \in G} \rho_{ij}(g) \overline{\rho'_{i'j'}(g)} = \begin{cases} \frac{1}{d_\rho} & \text{if } \rho = \rho', i = i', j = j' \\ 0 & \text{otherwise} \end{cases}$$

$$\Updownarrow$$

$\{\Phi^{-1} E_{ij}^{\rho} | \rho \in \hat{G}, 1 \leq i,j \leq d_\rho\}$ is an orthonormal set vectors in $\mathbb{C}G$.

Φ^{-1} as a module homomorphism

- R is a G-module under the action $g : \sum_{\rho\in\hat{G}} M_\rho \mapsto \sum_{\rho\in\hat{G}} \rho(g)M_\rho$.
- **Theorem.** Φ^{-1} is a module homomorphism from R to $\mathbb{C}G$.
- Proof.

$$
\begin{aligned}
\Phi^{-1}(gE_{ij}^{\rho}) &= \Phi^{-1}(\rho(g)E_{ij}^{\rho}) = \\
&= \Phi^{-1}\left(\sum_{k=1}^{d_\rho} \rho(g)_{ki}E_{kj}^{\rho}\right) \\
&= \sum_{k=1}^{d_\rho} \sqrt{\frac{d_\rho}{|G|}} \sum_{x\in G} \rho(g)_{ki}\overline{\rho(x)_{kj}}x
\end{aligned}
$$

Module homomorphism - Proof 2.

$$\begin{aligned} g\Phi^{-1}(E_{ij}^{\rho}) &= \sqrt{\frac{d_\rho}{|G|}}\sum_{x\in G}\overline{\rho(x)_{ij}}gx \\ &= \sqrt{\frac{d_\rho}{|G|}}\sum_{y\in G}\overline{\rho(g^{-1}y)_{ij}}y \\ &= \sqrt{\frac{d_\rho}{|G|}}\sum_{y\in G}\sum_{k=1}^{d_\rho}\overline{\rho(g^{-1})_{ik}\rho(y)_{kj}}y \\ &= \sqrt{\frac{d_\rho}{|G|}}\sum_{y\in G}\sum_{k=1}^{d_\rho}\rho(g)_{ki}\overline{\rho(y)_{kj}}y \\ &= \Phi^{-1}(gE_{ij}^{\rho}) \end{aligned}$$

The related algebra map

- R is an algebra (matrix multiplication component-wise) and Φ^{-1} is related to another map, the linear extension Ψ of

$$E_{ij}^{\rho} \mapsto \frac{d_\rho}{|G|}\sum_{g\in G}\overline{\rho(g)_{ij}}g$$

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

$$\Psi : \sum_{\rho,i,j}\alpha_{\rho,i,j}E_{ij}^{\rho} \mapsto \sum_{g\in G}\sum_{\rho,i,j}\frac{d_\rho}{|G|}\alpha_{\rho,i,j}\overline{\rho(g)_{ij}}g.$$

- $\Psi E_{ij}^{\rho} = \frac{\sqrt{d_\rho}}{\sqrt{|G|}}\Phi^{-1}E_{ij}^{\rho}$.
- **Theorem.** Ψ is an algebra homomorphism.

Algebra homomorphism - proof 1.

- To show multiplicativity, it is sufficient to check $\Psi^{-1}(ab) = \Psi(a)\Psi(b)$ on a basis of R.
- We do this for the basis E_{ij}^{ρ}
- Observe

$$\Psi(E_{ij}^{\rho} E_{k\ell}^{\rho'}) = \begin{cases} \Psi(E_{i\ell}^{\rho}) & \text{if } \rho = \rho' \text{ and } k = j \\ 0 & \text{otherwise} \end{cases}$$

Algebra homomorphism - proof 2.

$$\Psi(E_{ij}^{\rho})\Psi(E_{k\ell}^{\rho'}) = \frac{d_\rho d_{\rho'}}{|G|^2} \sum_{g,g' \in G} \overline{\rho(g)_{ij}\rho'(g')_{k\ell}} gg'$$

$$x = gg'$$

$$= \frac{d_\rho d_{\rho'}}{|G|^2} \sum_{x \in G} \left(\sum_{g \in G} \overline{\rho(g)_{ij}\rho'(g^{-1}x)_{k\ell}} \right) x$$

$$\rho'(g^{-1}x)_{k\ell} = \sum_{r=1}^{d_{\rho'}} \rho'(g^{-1})_{kr}\rho'(x)_{r\ell}$$

$$= \frac{d_\rho d_{\rho'}}{|G|^2} \sum_{x \in G} \left(\sum_{r=1}^{d_{\rho'}} \sum_{g \in G} \overline{\rho(g)_{ij}\rho'(g^{-1})_{kr}\rho'(x)_{r\ell}} \right) x$$

Algebra homomorphism - proof 3.

$$\Psi(E^{\rho}_{ij})\Psi(E^{\rho'}_{k\ell}) = \frac{d_\rho d_{\rho'}}{|G|^2}\sum_{x\in G}\left(\sum_{r=1}^{d_{\rho'}}\sum_{g\in G}\overline{\rho(g)_{ij}}\rho'(g)_{rk}\overline{\rho'(x)_{r\ell}}\right)x$$

Orthogonality for $\frac{1}{|G|}\sum_{g\in G}\overline{\rho(g)_{ij}}\rho'(g)_{rk}$

$$= \begin{cases} \frac{d_\rho}{|G|}\sum_{x\in G}\overline{\rho(x)_{i\ell}}x & \text{if } \rho=\rho',\ k=j \\ 0 & \text{otherwise} \end{cases}$$

$$= \Psi(E^{\rho}_{ij}E^{\rho'}_{k\ell}) \quad \text{by the observation.}$$

Contents

4 Basic orthogonalities
- Shur's lemma
- Orthogonality of the matrix elements
- The Inverse Fourier transform

5 The structure of the group algebra
- Decomposition of the group algebra
- Consequences of the structure theorem
- Misc

6 Characters
- Character basics
- Scalar product of characters

7 Tensor products
- Tensor products of matrices
- Irreps of direct products.
- Tensor products of representations

Decomposition of the group algebra

- $R = \bigoplus_{\rho \in \hat{G}} M_{d_\rho}(\mathbb{C})$.
- $\Psi : R \to \mathbb{C}G$ injective algebra homomorphism (maps a basis of R into a linearly independent set).
- For every irrep $\rho : G \to M_{d_\rho}(\mathbb{C})$, extend ρ linearly to $\mathbb{C}G$.
- The extension, also denoted by ρ, is an algebra homomorphism $\mathbb{C}G \to M_{d_\rho}(\mathbb{C})$ (linear and multiplicative on a basis).
- The direct sum map $\Xi = \bigoplus_\rho \rho$ is a homomorphism from $\mathbb{C}G$ to R.

Decomposition of the group algebra

- Claim: Ξ is injective.
  - If $\mathbb{C}G \ni x \in \ker \Xi$ then $\rho(x) = 0$ (equivalently, $xV_\rho = 0$) for every $\rho \in \hat{G}$,
    As $\mathbb{C}G$ as a G-module is isomorphic to a direct sum of copies of V_ρ's:
  - $x\mathbb{C}G = 0$, in particular
  - $x = x1_G = 0$.
- Thus $\dim R \leq \dim \mathbb{C}G \leq \dim R$, so both Ψ and Ξ are algebra isomorphisms.
- Remark: Φ^{-1} is an orthogonal G-module isomorphism.

Structure of the group algebra

$$\mathbb{C}G \cong \bigoplus_{\rho \in \hat{G}} M_{d_\rho}(\mathbb{C}).$$

Consequences of the structure theorem

- $\mathbb{C}G \cong \bigoplus_{\rho\in\hat{G}} M_{d\rho}(\mathbb{C})$.
- $|G| = \sum_{\rho\in\hat{G}} d_\rho^2$. (dimension)
- $Center(\mathbb{C}G) = \{x \in \mathbb{C}G | xy = yx \text{ for every } y \in \mathbb{C}G\}$
  $= \{x \in \mathbb{C}G | xg = gx \text{ for every } g \in G\}$
- $\sum_{g\in G} \alpha_g \in Center(\mathbb{C}G)$ iff $\alpha_{g^y} = \alpha_{ygy^{-1}} = \alpha_g$ for every $y \in G$.

  I.e. the function $\alpha : g \mapsto \alpha_g$ is constant on the conjugacy classes of G.
- $\dim Center(\mathbb{C}G) = |\{\text{conj. classes of } G\}|$.
- $Center(\mathbb{C}G) = Center(\bigoplus_{\rho\in\hat{G}} M_{d_\rho}(\mathbb{C})) \cong \mathbb{C}^{|\hat{G}|}$.
- $|\hat{G}| = |\{\text{conj. classes of } G\}|$

Consequences- examples, exercises

- Exercise. G is commutative $\Leftrightarrow$ every irrep of G is one-dimensional.
- Example: Irreps of D_n

  odd n - even n
- Exercise: $|G/G'| = |\{\text{one-dimensional reps of } G\}|$

Miscellanies

- ρ an (ir)rep of G, $\ker \rho \lhd G$, ρ is an (ir)rep of $G/\ker \rho$.
- If $N \lhd G$ and $\phi : G \to G/N$ the natural map, $\tilde{\rho} : G/N$ an (ir)rep of G/N then $\rho = \tilde{\rho}\phi$ is an (ir)rep of G with N in the kernel.

Contents

4 Basic orthogonalities
- Shur's lemma
- Orthogonality of the matrix elements
- The Inverse Fourier transform

5 The structure of the group algebra
- Decomposition of the group algebra
- Consequences of the structure theorem
- Misc

6 Characters
- Character basics
- Scalar product of characters

7 Tensor products
- Tensor products of matrices
- Irreps of direct products.
- Tensor products of representations

Character basics

- ρ (finite dim!) rep of G.

$$\chi_\rho(g) = Tr(\rho(g))$$

- similar matrices have equal traces: $Tr(ab) = Tr(ba)$ (immediate),
  $Tr(dcd^{-1}) = Tr(d(cd^{-1})) = Tr((cd^{-1})d) = Tr(c)$
- Tr linear on $M_n(\mathbb{C})$
- χ_ρ extends linearly to $\mathbb{C}G$
- For equivalent ρ_1, ρ_2: $\chi_{\rho_1} = \chi_{\rho_2}$
- Soon: the converse also holds.

Character basics 2.

- Characters take constant values on conjugacy classes.
- $\chi_{\rho_1 \oplus \rho_2} = \chi_{\rho_1} + \chi_{\rho_2}$
- If ρ_1 is an irrep, $\exists e_1 \in \mathbb{C}G$ s.t $\rho_1(e_1) = I_{d_{\rho_1}}$, $\rho_2(e_1) = 0$ for any irrep ρ_2 non-equivalent to ρ_1
  - $\Psi : \mathbb{C}G \cong M_{d_{\rho_1}}(\mathbb{C}) \oplus \bigoplus_{\rho \neq \rho_1} M_{d_\rho}(\mathbb{C})$
  - $e_1 = \Psi^{-1}(I_{d_{\rho_1}}, 0, \ldots, 0)$
- If ρ_1 irrep, $V = V_\phi = V_{\rho_1}^{n_1} \oplus$ irred constituents $\ncong V_1$ then $n_1 = \chi_\rho(e_1)/d_{\rho_1}$
- ρ_1 and ρ_2 are equivalent $\Leftrightarrow \chi_{\rho_1}(g) = \chi_{\rho_2}(g)$ for every $g \in G$.

Scalar product of characters 1.

- class functions: $G \to \mathbb{C}$, constant on conjugacy classes
- characters are class functions.
- $|\hat{G}| = |\{\text{conj. classes}\}| = \dim\{\text{class functions}\}$
- $(\chi_1, \chi_2) = \frac{1}{|G|} \sum_{g \in G} \chi_1(g)\overline{\chi}_2(g)$.

Scalar product of characters 2.

- ρ_1, ρ_2 irreps.

$$(\chi_{\rho_1}, \chi_{\rho_2}) = \begin{cases} 1 & \text{if } \rho_1 \text{ and } \rho_2 \text{ are equivalent} \\ 0 & \text{otherwise} \end{cases}$$

  - May assume that ρ_1 and ρ_2 are unitary matrix reps and $\rho_1 = \rho_2$ in case they are equivalent.
  - $(\chi_{\rho_1}, \chi_{\rho_2}) = \sum_{i=1}^{d_{\rho_1}} \sum_{j=1}^{d_{\rho_2}} \frac{1}{|G|} \sum_{g \in G} \rho_1(g)_{ii} \overline{\rho_2(g)_{jj}}$
  - Recall:

$$\frac{1}{|G|} \sum_{g \in G} \rho_1(g)_{ii} \overline{\rho_2(g)_{jj}} = \begin{cases} \frac{1}{d_\rho} & \text{if } \rho_1 = \rho_2, i = j \\ 0 & \text{otherwise} \end{cases}$$

Scalar product of characters 3.

- The irred. characters form an orthonormal basis of the space of class functions.
- ϕ repr., $V_\phi = \bigoplus_\rho V_\rho^{m_\rho}$. Then $m_\rho = (\chi_\phi, \chi_\rho)$
- $(\chi_\phi, \chi_\phi) = \sum_\rho m_\rho^2$.
- ϕ rep is irrep iff $(\chi_\phi, \chi_\phi) = 1$.
- Example *reg* =regular rep. $(\chi_{reg}, \chi_{reg}) = \sum_\rho d_\rho^2 = |G|$.

Scalar product of characters 4.

Example. permutation character

- ρ linear extension of a permutation representation
- In the basis indexed by elements of the G-set Ω each $\rho(g)$ is a permutation matrix.
- $\chi_\rho(g) = Tr(\rho(g)) = |\{\text{diag elements of } \rho(g)\}| = |\{\text{fixed points of } g\}|$
- Burnside's lemma: For a permutation repr. ρ,

$$(\chi_\rho, 1) = |\{\text{orbits}\}|.$$

Scalar product of characters 4.

Exercise. A permutation representation π of G is 2-transitive on Ω ($|\Omega| > 1$), iff
any pair $\omega_1 \neq \omega_2 \in \Omega$ can be moved to an arbitrary pair $\omega_1' \neq \omega_2' \in \Omega$:
$\exists g \in G$ s.t. $\pi(g)(\omega_1) = \omega_1'$ and $\pi(g)(\omega_2) = \omega_2'$

Prove that G is 2-transitive iff $\chi_\pi = 1 + \chi_\psi$, where ψ is an irrep.

Contents

4 Basic orthogonalities
- Shur's lemma
- Orthogonality of the matrix elements
- The Inverse Fourier transform

5 The structure of the group algebra
- Decomposition of the group algebra
- Consequences of the structure theorem
- Misc

6 Characters
- Character basics
- Scalar product of characters

7 Tensor products
- Tensor products of matrices
- Irreps of direct products.
- Tensor products of representations

Tensor products of matrices

- If $A : V \to V, B : W \to W$ lin. transformations, then $A \otimes B$ is the unique linear transformation $A \otimes B : V \otimes W \to V \otimes W$ such that

  $$(A \otimes B)(v \otimes w) = Av \otimes Aw$$

  for every $v \in V, w \in W$. If (a_{ij}) is the matrix of A and $(b_{k\ell})$ is the matrix of B in certain bases, then in the product basis the matrix of $A \otimes B$ is $c_{ik,jl} = a_{ij} b_{kl}$.
- $Tr(A \otimes B) = Tr(A)Tr(B)$
  - $Tr(A \otimes B) = \sum_{i,k} c_{ik,ik} = \sum_{i,k} a_{ii} b_{kk} = Tr(A)Tr(B)$

- If ρ_1 is a rep of G_1 on V_1 and ρ_2 is a rep of G_2 on V_2 then $\rho_1 \otimes \rho_2$ is a rep of $G_1 \otimes G_2$.
- If ρ_1 is an irrep of G_1 on V_1 and ρ_2 is an irrep of G_2 on V_2, then $\rho_1 \otimes \rho_2$ (defined on $G_1 \times G_2$ as $\rho_1(g_1) \otimes \rho_2(g_2)$) is an irrep of $G_1 \times G_2$.
    - $\chi_{\rho_1\otimes\rho_2}(g_1, g_2) = \chi_{\rho_1}(g_1)\chi_{\rho_2}(g_2)$
    - $(\chi_{\rho_1\otimes\rho_2}, \chi_{\rho_1\otimes\rho_2}) = \frac{1}{|G_1||G_2|}\sum_{g_1\in G_1}\sum_{g_2\in G_2}\chi_{\rho_1}(g_1)\chi_{\rho_2}(g_2)\overline{\chi_{\rho_1}(g_1)\chi_{\rho_2}(g_2)} = (\frac{1}{|G_1|}\sum_{g_1\in G_1}\chi_{\rho_1}(g_1)\overline{\chi_{\rho_1}(g_1)})(\frac{1}{|G_2|}\sum_{g_2\in G_2}\chi_{\rho_2}(g_2)\overline{\chi_{\rho_2}(g_2)}) = 1$
- conjugacy classes of $G_1 \times G_2$ are $C_1 \times C_2$, where C_1 is a class of G_1 and C_2 is a class of G_2
- These are all the irreps of $G_1 \times G_2$.

Irreps of abelian groups

$$G = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r} = \{\underline{z} = (z_1, \ldots, z_r) \mid z_i \bmod m_i\}$$

$$m = LCM(m_1, \ldots, m_r), \quad \omega = \sqrt[m]{1} (= e^{2\pi i/m})$$

$$G^* = \{\chi_{\underline{u}} \mid \underline{u} \in G\}$$

$$\chi_{\underline{u}}(\underline{z}) = \omega^{\sum_{i=1}^{r} \frac{m}{m_i} u_i z_i} = \omega^{\underline{u} \cdot \underline{z}}$$

$$\underline{u} \cdot \underline{z} = \sum_{i=1}^{r} \frac{m}{m_i} u_i z_i \bmod m$$

Tensor products of representations

- If ρ_1, ρ_2 are reps of G, then $\rho_1 \otimes \rho_2$ is a rep not only for $G \times G$, but also for G: $g \mapsto \rho_1(g) \otimes \rho_2(g)$

  (Say, composed form the diagonal embedding $G \to G \times G$ and $\rho_1 \times \rho_2 \to GL(V_1 \otimes V_2)$.
- $\chi_{\rho_1 \otimes \rho_2} = \chi_{\rho_1} \chi_{\rho_2}$
- If ρ_i are one-dimensional, then $\rho_1 \otimes \rho_2$ is just $\rho_1 \rho_2$.
- In general, the $\rho_1 \otimes \rho_2$ is rarely irreducible, even if ρ_1, ρ_2 are.
- Exercise. If ρ_1 is one-dimensional and ρ_2 is irred, then $\rho_1 \otimes \rho_2$ is irred again.
- Exercise. Decomposition of the tensor products of 2-dimensional irreps of D_n.