MATH457 - Algebra 4

Representation Theory; Galois Theory

Based on lectures from Winter 2025 by Prof. Henri Darmon.
Notes by Louis Meunier

Contents

1 Representation Theory 2
1.1 Introduction 2
1.2 Maschke's Theorem 3
1.3 Characters 6
1.4 Fourier Analysis on Finite Abelian Groups 10
1.4.1 Application to Computing Particular Infinite Series 12
1.5 Fourier Analysis on Non-Abelian Finite Groups 13
1.5.1 Random Products in Groups 13
1.6 Character Tables of S_4, A_5 and $\mathrm{GL}_3(\mathbb{F}_5)$ 14
1.6.1 S_4 14
1.6.2 A_5 15
1.6.3 $\mathrm{GL}_3(\mathbb{F}_2)$ 15
1.7 Induced Representations 16

% ! 01-06

§1 Representation Theory

§1.1 Introduction

↪**Definition 1.1** (Linear Representation): A *linear representation* of a group G is a vector space V over a field $\mathbb{F}$ equipped with a map $G \times V \to V$ that makes V a G-set in such a way that for each $g \in G$, the map $v \mapsto gv$ is a linear homomorphism of V.

This induces a homomorphism

$$\rho : G \to \mathrm{Aut}_{\mathbb{F}}(V),$$

or, in particular, when $n = \dim_{\mathbb{F}} V < \infty$, a homomorphism

$$\rho : G \to \mathrm{GL}_n(\mathbb{F}).$$

Alternatively, a linear representation V can be viewed as a module over the group ring $\mathbb{F}[G] = \left\{\sum_{g \in G} : \lambda_g g : \lambda_g \in \mathbb{F}\right\}$ (where we require all but finitely many scalars λ_g to be zero).

↪**Definition 1.2** (Irreducible Representation): A linear representation V of a group G is called *irreducible* if there exists no proper, nontrivial *subspace* $W \subsetneq V$ such that W is G-stable.

⊛ **Example 1.1**:

1. Consider $G = \mathbb{Z}/2 = \{1, \tau\}$. If V a linear representation of G and $\rho : G \to \mathrm{Aut}(V)$. Then, V uniquely determined by $\rho(\tau)$. Let $p(x)$ be the minimal polynomial of $\rho(\tau)$. Then, $p(x) \mid x^2 - 1$. Suppose $\mathbb{F}$ is a field in which $2 \neq 0$. Then, $p(x) \mid (x-1)(x+1)$ and so $p(x)$ has either $1, -1$, or both as eigenvalues and thus we may write

$$V = V_+ \oplus V_-,$$

where $V_\pm := \{v \mid \tau v = \pm v\}$. Hence, V is irreducible only if one of V_+, V_- all of V and the other is trivial, or in other words τ acts only as multiplication by 1 or -1.

2. Let $G = \{g_1, ..., g_N\}$ be a finite abelian group, and suppose $\mathbb{F}$ an algebraically closed field of characteristic 0 (such as $\mathbb{C}$). Let $\rho : G \to \mathrm{Aut}\,(V)$ and denote $T_j := \rho\left(g_j\right)$ for $j = 1, ..., N$. Then, $\{T_1, ..., T_N\}$ is a set of mutually commuting linear transformations. Then, there exists a simultaneous eigenvector, say v, for $\{T_1, ..., T_N\}$, and so span (v) a G-stable subspace of V. Thus, if V irreducible, it must be that $\dim_{\mathbb{F}} V = 1$.

↪**Theorem 1.1**: If G a finite abelian group and V an irreducible finite dimensional representation over an algebraically closed field of characteristic 0, then $\dim V = 1$.

Proof. Let $\rho : G \to \mathrm{Aut}(V)$, label $G = \{g_1, ..., g_N\}$ and put $T_j := \rho\left(g_j\right)$ for $j = 1, ..., N$. Then, $\{T_1, ..., T_N\}$ a family of mutually commuting linear transformations on V. Then, there is a simultaneous eigenvector v for $\{T_1, ..., T_N\}$ and thus $\operatorname{span}(v)$ is $T_1, ..., T_N$-stable and so $V = \operatorname{span}(v)$. ■

↪**Lemma 1.1**: Let V be a finite dimensional vector space over $\mathbb{C}$ and let $T_1, ..., T_N : V \to V$ be a family of mutually commuting linear automorphisms on V. Then, there is a simultaneous eigenvector for $T_1, ..., T_N$.

↪**Proposition 1.1**: Let $\mathbb{F}$ a field where $2 \neq 0$ and V an irreducible representation of S_3. Then, there are three distinct (i.e., up to homomorphism) possibilities for V.

Proof. Let $\rho : G \to \operatorname{Aut}(V)$ and let $T = \rho((23))$. Then, notice that $p_T(x) \mid \left(x^2 - 1\right)$ so T has eigenvalues in $\{-1, 1\}$.

If the only eigenvalue of T is -1, we claim that V one-dimensional.

If T has 1 as an eigenvalue. ■

↪**Proposition 1.2**: D_8 has a unique faithful irreducible representation, of dimension 2 over a field F in which $0 \neq 2$.

Proof. Write $G = D_8 = \left\{1, r, r^2, r^3, v, h, d_1, d_2\right\}$ as standard. Let ρ be our irreducible, faithful representation and let $T = \rho\left(r^2\right)$. Then, $p_T(x) \mid x^2 - 1 = (x-1)(x+1)$ and so $V = V_+ \oplus V_-$, the respective eigenspaces for $\lambda = +1, -1$ respectively for T. Then, notice that since r^2 in the center of G, both V_+ and V_- are preserved by the action of G, hence one must be trivial and the other the entirety of V. V can't equal V_+, else $T = I$ on all of V hence ρ not faithful so $V = V_-$.

Next, it must be that $\rho(h)$ has both eigenvalues 1 and -1. Let $v_1 \in V$ be such that $hv_1 = v_1$ and $v_2 = rv_1$. We claim that $W := \operatorname{span}\{v_1, v_2\}$, namely $V = W$ 2-dimensional.

We simply check each element. $rv_1 = v_2$ and $rv_2 = r^2 v_1 = -v_1$ which are both in W hence r and thus $\langle r \rangle$ fixes W. Next, $hv_1 = v_1$ and $vv_2 = vrv_1 = rhv_1 = rv_1 = v_2$ (since $rhr^{-1} = v$) and so $hv_2 = -v_2$ and $vv_1 = -v_1$ and so W G-stable. Finally, d_1 and d_2 are just products of these elements and so W G-stable. ■

↪**Definition 1.3** (Isomorphism of Representations): Given a group G and two representations $\rho_i : G \to \operatorname{Aut}_{\mathbb{F}}(V_i)$, $i = 1, 2$ an isomorphism of representations is a vector space isomorphism $\varphi : V_1 \to V_2$ that respects the group action, namely

$$\varphi(gv) = g\varphi(v)$$

for every $g \in G, v \in V_1$.

§1.2 Maschke's Theorem

↪**Theorem 1.2** (Maschke's): Any representation of a finite group G over $\mathbb{C}$ can be written as a direct sum of irreducible representations, i.e.

$$V = V_1 \oplus \cdots \oplus V_t,$$

where V_j irreducible.

Remark 1.1: $|G| < \infty$ essential. For instance, consider $G = (\mathbb{Z}, +)$ and 2-dimensional representation given by $n \mapsto \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. Then, $n \cdot e_1 = e_1$ and $n \cdot e_2 = ne_1 + e_2$. We have that $\mathbb{C}e_1$ irreducible then. But if $v = ae_1 + e_2 \in W := V \setminus \mathbb{C}e_1$, then $Gv = (a+1)e_1 + e_2$ so $Gv - v = e_1 \in W$, contradiction.

Remark 1.2: $|\mathbb{C}|$ essential. Suppose $F = \mathbb{Z}/3\mathbb{Z}$ and $V = Fe_1 \oplus Fe_2 \oplus Fe_3$, and $G = S_3$ acts on V by permuting the basis vectors e_i. Then notice that $F(e_1 + e_2 + e_3)$ an irreducible subspace in V. Let $W = F(w)$ with $w := ae_1 + be_2 + ce_3$ be any other G-stable subspace. Then, by applying (123) repeatedly to w and adding the result, we find that $(a+b+c)(e_1 + e_2 + e_3) \in W$. Similarly, by applying $(12), (23), (13)$ to w, we find $(a-b)(e_1 - e_2), (b-c)(e_2 - e_3), (a-c)(e_1 - e_3)$ all in W. It must be that at least one of $a-b, a-c, b-c$ nonzero, else we'd have $w \in F(e_1 + e_2 + e_3)$. Assume wlog $a - b \neq 0$. Then, we may apply $(a-b)^{-1}$ and find $e_1 - e_2 \in W$. By applying $(23), (13)$ to this vector and scaling, we find further $e_2 - e_3$ and $e_1 - e_3 \in W$. But then,

$$2(e_1 - e_2) + 2(e_1 - e_3) = e_1 + e_2 + e_3 \in W,$$

so $F(e_1 + e_2 + e_3)$ a subspace of W, a contradiction.

↪**Proposition 1.3**: Let V be a representation of $|G| < \infty$ over $\mathbb{C}$ and let $W \subseteq V$ a sub-representation. Then, W has a G-stable complement W', such that $V = W \oplus W'$.

Proof. Denote by ρ the homomorphism induced by the representation. Let $W_{0'}$ be any complementary subspace of W and let

$$\pi : V \to W$$

be a projection onto W along $W_{0'}$, i.e. $\pi^2 = \pi, \pi(V) = W$, and $\ker(\pi) = W_{0'}$. Let us "replace" π by the "average"

$$\tilde{\pi} := \frac{1}{\#G} \sum_{g \in G} \rho(g) \pi \rho(g)^{-1}.$$

Then the following hold:

(1) $\tilde{\pi}$ G-equivariant, that is $\tilde{\pi}(gv) = g\tilde{\pi}(v)$ for every $g \in G, v \in V$.

(2) $\tilde{\pi}$ a projection onto W.

Let $W' = \ker(\tilde{\pi})$. Then, W' G-stable, and $V = W \oplus W'$. ∎

We present an alternative proof to the previous proposition by appealing to the existence of a certain inner product on complex representations of finite groups.

↪**Definition 1.4**: Given a vector space V over $\mathbb{C}$, a *Hermitian pairing/inner product* is a hermitian-bilinear map $V \times V \to \mathbb{C}$, $(v, w) \mapsto \langle v, w\rangle$ such that

- linear in the first coordinate;
- conjugate-linear in the second coordinate;
- $\langle v, v\rangle \in \mathbb{R}^{\geq 0}$ and equal to zero iff $v = 0$.

↪**Theorem 1.3**: Let V be a finite dimensional complex representation of a finite group G. Then, there is a hermitian inner product $\langle \cdot, \cdot\rangle$ such that $\langle gv, gw\rangle = \langle v, w\rangle$ for every $g \in G$ and $v, w \in V$.

Proof. Let $\langle \cdot, \cdot\rangle_0$ be any inner product on V (which exists by defining $\langle e_i, e_j\rangle_0 = \delta_i^j$ and extending by conjugate linearity). We apply "averaging":

$$\langle v, w\rangle := \frac{1}{\#G} \sum_{g \in G} \langle gv, gw\rangle.$$

Then, one can check that $\langle \cdot, \cdot\rangle$ is hermitian linear, positive, and in particular G-equivariant. ∎

From this, the previous proposition follows quickly by taking $W' = W^{\perp}$, the orthogonal complement to W with respect to the G-invariant inner product that the previous theorem provides.

From this proposition, Maschke's follows by repeatedly applying this logic. Since at each stage V is split in two, eventually the dimension of the resulting dimensions will become zero since V finite dimensional. Hence, the remaining vector spaces $V_1, ..., V_t$ left will necessarily be irreducible, since if they weren't, we could apply the proposition further.

↪**Theorem 1.4** (Schur's Lemma): Let V, W be irreducible representations of a group G. Then,

$$\mathrm{Hom}_G(V, W) = \begin{cases} 0 \text{ if } V \underset{G}{\not\cong} W \\ \mathbb{C} \text{ if } V \underset{G}{\cong} W \end{cases},$$

where $\mathrm{Hom}_G(V, W) = \{T : V \to W \mid T \text{ linear and } G - \text{equivariant}\}$.

Proof. Suppose $V \underset{G}{\not\cong} W$ and let $T \in \mathrm{Hom}_G(V, W)$. Then, notice that $\ker(T)$ a subrepresentation of V (a subspace that is a representation in its own right), but by assumption V irreducible hence either $\ker(T) = V$ or $\{0\}$.

If $\ker(T) = V$, then T trivial, and if $\ker(T) = \{0\}$, then this implies $T : V \to \operatorname{im}(T) \subset W$ a representation isomorphism, namely $\operatorname{im}(T)$ a irreducible subrepresentation of W. This implies that, since W irreducible, $\operatorname{im}(T) = W$, contradicting the original assumption.

Suppose now $V \underset{G}{\cong} W$. Let $T \in \operatorname{Hom}_G(V, W) = \operatorname{End}_G(V)$. Since $\mathbb{C}$ algebraically closed, T has an eigenvalue, λ. Then, notice that $T - \lambda I \in \operatorname{End}_G(V)$ and so $\ker(T - \lambda I) \subset V$ a, necessarily trivial because V irreducible, subrepresentation of V. Hence, $T - \lambda I = 0 \Rightarrow T = \lambda I$ on V. It follows that $\operatorname{Hom}_G(V, W)$ a one-dimensional vector space over $\mathbb{C}$, so namely $\mathbb{C}$ itself. ■

↪**Corollary 1.1**: Given a general representation $V = \bigoplus_{j=1}^{t} V_j^{m_j}$,

$$m_j = \dim_{\mathbb{C}} \operatorname{Hom}_G\left(V_j, V\right).$$

↪**Definition 1.5** (Trace): The trace of an endomorphism $T : V \to V$ is the trace of any matrix defining T. Since the trace is conjugation-invariant, this is well-defined regardless of basis.

↪**Proposition 1.4**: Let $W \subseteq V$ a subspace and $\pi : V \to W$ a projection. Then, $\operatorname{tr}(\pi) = \dim(W)$.

↪**Theorem 1.5**: If $\rho : G \to \operatorname{Aut}_{\mathbb{F}}(V)$ a complex representation of G, then

$$\dim\left(V^G\right) = \frac{1}{\#G} \sum_{g \in G} \operatorname{tr}(\rho(g)),$$

where $V^G = \{v \in V : gv = v \,\forall\, g \in G\}$.

Proof. Let $\pi = \frac{1}{\#g} \sum_{g \in G} \rho(g)$. Then, notice that $\operatorname{im}(\pi) = V^G$ and $\pi^2 = \pi$ hence a projection from V onto V^G. Using the previous proposition and linearity of the trace completes the proof. ■

§1.3 Characters

↪**Definition 1.6**: Let $\dim(V) < \infty$ and G a group. The *character* of V is the function

$$\chi_V : G \to \mathbb{C}, \qquad \chi_V(g) := \operatorname{tr}(\rho(g)).$$

↪**Proposition 1.5**: Characters are class functions, namely constant on conjugacy classes.

↪**Theorem 1.6**: If V_1, V_2 are 2 representations of G, then $V_1 \underset{G}{\cong} V_2 \Leftrightarrow \chi_{V_1} = \chi_{V_2}$.

↪**Proposition 1.6**: Given two representations V, W of G, there is a natural action of G on $\mathrm{Hom}(V, W)$ given by $g * T = g \circ T \circ g^{-1}$. Then,

$$\mathrm{Hom}(V, W)^G = \{T : V \to W \mid g * T = T\},$$

so

$$\mathrm{Hom}(V, W)^G = \mathrm{Hom}_G(V, W).$$

↪**Proposition 1.7**: Suppose $V = V_1^{m_1} \oplus \cdots \oplus V_t^{m_t}$ a representation of G written in irreducible form. Then,

$$\mathrm{Hom}_G\left(V_j, V\right) = \mathbb{C}_j^m.$$

Proof. "Hom is linear with respect to $\oplus$". ■

↪**Proposition 1.8**: If V, W are two representations, then so is $V \oplus W$ with point-wise action, and $\chi_{V \oplus W} = \chi_V + \chi_W$.

↪**Theorem 1.7**: $\chi_{\mathrm{Hom}(V,W)} = \overline{\chi_V} \chi_W$.

Proof. Use an eigenbasis for V, W respectively to define a corresponding eigenbasis for $\mathrm{Hom}(V, W)$ such as to write any $g \in G$ as a diagonal matrix. The entries will contain an expression depending solely on the eigenvalues for g acting on V, W. ■

↪**Theorem 1.8** (Orthogonality of Irreducible Group Characters): Suppose $V_1, ..., V_t$ is a list of irreducible representations of G and $\chi_1, ..., \chi_t$ are their corresponding characters. Then, the χ_j's naturally live in the space $L^2(G) \simeq \mathbb{C}^{\#G}$, which we can equip with the inner product

$$\langle f_1, f_2 \rangle : \frac{1}{\#G} \sum_{g \in G} \overline{f_1(g)} f_2(g).$$

Then,

$$\langle \chi_i, \chi_j \rangle = \delta_i^j.$$

Proof.

$$\begin{aligned}\langle \chi_i, \chi_j \rangle &= \frac{1}{\#G} \sum_{g \in G} \overline{\chi_i(g)} \chi_j(g) \\ &= \frac{1}{\#G} \sum_{g \in G} \chi_{\mathrm{Hom}(V_i, V_j)}(g) \\ &= \dim_{\mathbb{C}} \left(\mathrm{Hom}\left(V_i, V_j\right)^G \right) \\ &= \begin{cases} \dim_{\mathbb{C}}(\mathbb{C}) i = j \\ \dim_{\mathbb{C}}(0) i \neq j \end{cases} = \delta_i^j. \end{aligned}$$

■

↪**Corollary 1.2**: $\chi_1, ..., \chi_t$ orthonormal vectors in $L^2(G)$.

↪**Corollary 1.3**: $\chi_1, ..., \chi_t$ linearly independent, so in particular $t \leq \#G = \dim L^2(G)$.

↪**Corollary 1.4**: $t \leq h(G) := \#$ conjugacy classes.

Proof. We have that $L_c^2(G) \subseteq L^2(G)$, where $L_c^2(G)$ is the space of $\mathbb{C}$-valued functions on G that are constant on conjugacy classes. It's easy to see that $\dim_{\mathbb{C}}\left(L_c^2(G)\right) = h(G)$. Then, since $\chi_1, ..., \chi_t$ are class functions, the live naturally in $L_c^2(G)$ and hence since they are linearly independent, there are at most $h(G)$ of them. ■

Remark 1.3: We'll show this inequality is actually equality soon.

↪**Theorem 1.9** (Characterization of Representation by Characters): If V, W are two complex representations, they are isomorphic as representations $\Leftrightarrow \chi_V = \chi_W$.

Proof. By Maschke's, $V = V_1^{m_1} \oplus \cdots \oplus V_t^{m_t}$ and hence $\chi_V = m_1 \chi_1 + \cdots + m_t \chi_t$. By orthogonality, $m_j = \langle \chi_V, \chi_j \rangle$ for each $j = 1, ..., t$, hence V completely determined by χ_V.
■

↪**Definition 1.7** (Regular Representation): Define

$$\begin{aligned} V_{\mathrm{reg}} &:= \mathbb{C}[G] \text{ with left mult.} \\ &\simeq L^2(G) \text{ with } (g * f)(x) := f\left(g^{-1} x\right), \end{aligned}$$

the "regular representation" of G.

↪**Proposition 1.9**: $\chi_{\text{reg}}(g) = \begin{cases} \#G & \text{if } g = \text{id} \\ 0 & \text{else} \end{cases}.$

Proof. If $g = \text{id}$, then g simply acts as the identity on V_{reg} and so has trace equal to the dimension of V_{reg}, which has as basis just the elements of G hence dimension equal to $\#G$. If $g \neq \text{id}$, then g cannot fix any basis vector, i.e. any other element $h \in G$, since $gh = h \Leftrightarrow g = \text{id}$. Hence, g permutes every element in G with no fixed points, hence its matrix representation in the standard basis would have no 1s on the diagonal hence trace equal to zero. ■

↪**Theorem 1.10**: Every irreducible representation of V, V_j, appears in V_{reg} at least once, specifically, with multiplicity $\dim_{\mathbb{C}}(V_j)$. Specifically,

$$V_{\text{reg}} = V_1^{d_1} \oplus \cdots \oplus V_t^{d_t},$$

where $d_j := \dim_{\mathbb{C}}(V_j)$.

In particular,

$$\#G = d_1^2 + \cdots + d_t^2.$$

Proof. Write $V_{\text{reg}} = V_1^{m_1} \oplus \cdots \oplus V_t^{m_t}$. We'll show $m_j = d_j$ for each $j = 1, ..., t$. We find

$$\begin{aligned} m_j &= \langle \chi_{\text{reg}}, \chi_j \rangle \\ &= \frac{1}{\#G} \sum_{g \in G} \overline{\chi_{\text{reg}}(g)} \chi_j(g) \\ &= \frac{1}{\#G} \#G \chi_j(\text{id}) = \chi_j(\text{id}) = d_j, \end{aligned}$$

since the trace of the identity element acting on a vector space is always the dimension of the space. In particular, then

$$\begin{aligned} \#G = \dim_{\mathbb{C}}(V_{\text{reg}}) &= \dim_{\mathbb{C}}\left(V_1^{d_1} \oplus \cdots \oplus V_t^{d_t}\right) \\ &= d_1 \cdot \dim_{\mathbb{C}}(V_1) + \cdots + d_t \cdot \dim_{\mathbb{C}}(V_t) \\ &= d_1^2 + \cdots + d_t^2. \end{aligned}$$

■

↪**Theorem 1.11**: $t = h(G)$.

Proof. Remark that $\mathbb{C}[G]$ has a natural ring structure, combining multiplication of coefficients in $\mathbb{C}$ and internal multiplication in G. Define a group homomorphism

$$\underline{\rho} = (\rho_1, ..., \rho_t) : G \to \text{Aut}(V_1) \times \cdots \times \text{Aut}(V_t),$$

collecting all the irreducible representation homomorphisms into a single vector. Then, this extends naturally by linearity to a ring homomorphism

$$\underline{\rho} : \mathbb{C}[G] \to \mathrm{End}_{\mathbb{C}}(V_1) \oplus \cdots \oplus \mathrm{End}_{\mathbb{C}}(V_t).$$

By picking bases for each $\mathrm{End}_{\mathbb{C}}\left(V_j\right)$, we find that $\dim_{\mathbb{C}}\left(\mathrm{End}_{\mathbb{C}}\left(V_j\right)\right) = d_j^2$ hence $\dim_{\mathbb{C}}(\mathrm{End}_{\mathbb{C}}(V_1) \oplus \cdots \oplus \mathrm{End}_{\mathbb{C}}(V_t)) = d_1^2 + \cdots + d_t^2 = \#G$, as we saw in the previous theorem. On the other hand, $\dim_{\mathbb{C}}(\mathbb{C}[G]) = \#G$ hence the dimensions of the two sides are equal. We claim that $\underline{\rho}$ an isomorphism of rings. By dimensionality as $\mathbb{C}$-vector spaces, it suffices to show $\underline{\rho}$ injective.

Let $\theta \in \ker\left(\underline{\rho}\right)$. Then, $\rho_j(\theta) = 0$ for each $j = 1, \ldots, t$, i.e. θ acts as 0 on each of the irreducibles $V_1, \ldots, V_t$. Applying Maschke's, it follows that θ must act as zero on every representation, in particular on $\mathbb{C}[G]$. Then, for every $\sum \beta_g g \in \mathbb{C}[G]$, $\theta \cdot \left(\sum \beta_g g\right) = 0$ so in particular $\theta \cdot 1 = 0$ hence $\theta = 0$ in $\mathbb{C}[G]$. Thus, $\underline{\rho}$ has trivial kernel as we wanted to show and thus $\mathbb{C}[G]$ and $\mathrm{End}_{\mathbb{C}}(V_1) \oplus \cdots \oplus \mathrm{End}_{\mathbb{C}}(V_t)$ are isomorphic as rings (moreover, as $\mathbb{C}$-algebras).

We look now at the centers of the two rings, since they are (in general) noncommutative. Namely,

$$Z(\mathbb{C}[G]) = \left\{\sum \lambda_g g \mid \left(\sum \lambda_g g\right)\theta = \theta\left(\sum \lambda_g g\right) \ \forall\, \theta \in \mathbb{C}[G]\right\}.$$

Since multiplication in $\mathbb{C}$ is commutative and "factors through" internal multiplication, it follows that $\sum \lambda_g g n Z(\mathbb{C}[G])$ iff it commutes with every group element, i.e.

$$\begin{aligned}\left(\sum \lambda_g g\right)h = h\left(\sum \lambda_g g\right) &\Leftrightarrow \sum_g \left(\lambda_g h^{-1} g h\right) = \sum_g \lambda_g g \\ &\Leftrightarrow \sum_g \lambda_{h^{-1}gh} g = \sum_g \lambda_g g \\ &\Leftrightarrow \lambda_{h^{-1}gh} = \lambda_g \ \forall\, g \in G.\end{aligned}$$

Hence, $\sum \lambda_g g \in Z(\mathbb{C}[G])$ iff $\lambda_{h^{-1}gh} = \lambda_g$ for every $g, h \in G$. It follows, then, that the induced map $g \mapsto \lambda_g$ a class function, and thus $\dim_{\mathbb{C}}(Z(\mathbb{C}[G])) = h(G)$.

On the other hand, $\dim_{\mathbb{C}}\left(Z\left(\mathrm{End}_{\mathbb{C}}\left(V_j\right)\right)\right) = 1$ (by representing as matrices, for instance, one can see that only scalar matrices will commute with all other matrices), hence $\dim_{\mathbb{C}}(Z(\mathrm{End}_{\mathbb{C}}(V_1) \oplus \cdots \oplus \mathrm{End}_{\mathbb{C}}(V_t))) = t$. $\underline{\rho}$ naturally restricts to an isomorphism of these centers, hence we conclude justly $t = h(G)$. ■

§1.4 Fourier Analysis on Finite Abelian Groups

↪**Definition 1.8**: For a finite group G, let

$$L^2(G) = \{\text{square integrable functions } G \to \mathbb{C}\},$$

equipped with the L^2-norm, $\|f\|^2 = \frac{1}{\#G} \sum_{g \in G} |f(g)|^2$. This is a vector space isomorphic to $\mathbb{C}^{\#G}$. We make the space a Hilbert space by defining

$$\langle f_1, f_2 \rangle = \frac{1}{\#G} \sum_{g \in G} \overline{f_1(g)} f_2(g).$$

↪**Definition 1.9**: Denote by $\hat{G} = \{\chi_1, ..., \chi_N\}$ the set of irreducible characters of G. Then, $\hat{G}$ an orthonormal family of functions in $L^2(G)$.

We suppose for now G abelian. In this case, $\#\hat{G} = \#G$ so $\hat{G}$ is an orthonormal basis for $L^2(G)$ (comparing dimensions).

↪**Definition 1.10**: Given $f \in L^2(G)$, the function $\hat{f} : \hat{G} \to \mathbb{C}$ is defined by

$$\hat{f}(\chi) = \frac{1}{\#G} \sum_{g \in G} \overline{\chi}(g) f(g),$$

called the *Fourier transform* of f over G. Then,

$$f = \sum_{\chi \in \hat{G}} \hat{f}(\chi) \chi,$$

is called the *Fourier inversion formula*.

⊛ **Example 1.2**: Consider $G = \mathbb{R}/\mathbb{Z}$. $L^2(G)$ space of $\mathbb{C}$-valued periodic functions on $\mathbb{R}$ which are square integrable on $[0,1]$. Then, $\hat{G}$ abstractly isomorphic to $\mathbb{Z}$. Write $\hat{G} = \{\chi_n \mid n \in \mathbb{Z}\}$. Then, remark that

$$\chi_n : \mathbb{R}/\mathbb{Z} \to \mathbb{C}^\times, \qquad \chi_n(x) = e^{2\pi i n x}$$

gives the characteristic function for any integer n. More precisely, its not hard to see that the map $\mathbb{R} \to \mathbb{C}^\times, x \mapsto e^{2\pi i n x}$ factors through (is constant on integer multiples) $\mathbb{Z}$.

To speak about orthogonality of members of $\hat{G}$, we must define a norm. We can identity $\mathbb{R}/\mathbb{Z}$ with $[0,1]$, and so write

$$\langle f_1, f_2 \rangle := \int_0^1 \overline{f_1(x)} f_2(x) \, \mathrm{d}x.$$

Then, its not hard to see

$$\langle \chi_n, \chi_m \rangle = \int_0^1 e^{-2\pi i (m-n) x} \, \mathrm{d}x = \delta_m^n.$$

⊛ **Example 1.3**: Let $G = \mathbb{Z}/N\mathbb{Z}$ under addition. Note that G then a subgroup of $\mathbb{R}/\mathbb{Z}$, and in particular,

$$\hat{G} = \{\chi_0, \chi_1, ..., \chi_{N-1}\}, \qquad \chi_j(k) := e^{2\pi ijk/N}.$$

Then, one notices

$$\chi_{j_1} \cdot \chi_{j_2} = \chi_{j_1+j_2},$$

so there is indeed a natural group structure on $\hat{G}$. Then, the Fourier transform in this case gives, for $f \in L^2(\mathbb{Z}/N\mathbb{Z})$,

$$\hat{f}(n) = \frac{1}{N} \sum_{k=0}^{N-1} e^{-2\pi ink/N} f(k).$$

1.4.1 Application to Computing Particular Infinite Series

We consider an application of the theory we've developed on $G = \mathbb{Z}/N\mathbb{Z}$ to study particular infinite summations. Its well know that the harmonic series $1 + \frac{1}{2} + \frac{1}{3} + \cdots$ diverges. A natural extension is to study modified such series, for instance $1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots$ and to ask if this series converges, and if it does, to what?

To approach this question, we more generally consider, for $f \in L^2(\mathbb{Z}/N\mathbb{Z})$ (i.e. a complex-valued N-periodic function defined on the integers), the series

$$S(f) := \sum_{n=1}^{\infty} \frac{f(n)}{n},$$

when the summation exists. Remark then that $f \mapsto S(f)$ is linear. So, it suffices to consider the value of $S(f)$ on a basis of $L^2(\mathbb{Z}/N\mathbb{Z})$, which we've derived in the previous example, namely $\hat{G} = \left\{\chi_j : j = 0, ..., N-1\right\}$. We can explicitly compute $S(\chi_j)$:

$$\begin{aligned} S(\chi_j) &= \sum_{n=1}^{\infty} \frac{\chi_j(n)}{n} \\ &= \sum_{n=1}^{\infty} \frac{x^n}{n}, \qquad x := e^{\frac{2\pi ij}{N}} \\ &= -\log(1-x), \end{aligned}$$

where the final sequence converges on the unit circle in the complex plane centered at the $1 + 0i$.

In particular, if $j = 0$, $S(\chi_0)$ diverges. Otherwise, each χ_j maps onto the roots of unity hence the convergence is well-defined. In particular, then, we find

$$S(\chi_j) = \begin{cases} -\log\left(1 - e^{2\pi i\frac{j}{N}}\right) & \text{if } j \neq 0 \\ 0 & \text{else} \end{cases}.$$

Now, for a general function $f \in L^2(\mathbb{Z}/N\mathbb{Z})$, we find by the Fourier inversion formula

$$S(f) = S\left(\hat{f}(0)\chi_0 + \cdots + \hat{f}(N-1)\chi_{N-1}\right),$$

which certainly diverges if $\hat{f}(0) \neq 0$. Otherwise, we find by linearity

$$S(f) = \sum_{j=1}^{N-1} \hat{f}(j)(-\log(1-x)).$$

So, returning to our original example, we can define $f \in L^2(\mathbb{Z}/4\mathbb{Z})$ by $f(n) = \begin{cases} 0 & \text{if } n \text{ even} \\ 1 & \text{if } n{=}1{+}4k \\ -1 & \text{if } n{=}3{+}4k \end{cases}$. Then, we find

$$\begin{aligned} 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \cdots &= S(f) \\ &= \frac{1}{2i}(S(\chi_1) - S(\chi_3)) \\ &= \frac{1}{2i}(-\log(1-i) + \log(1+i)) \\ &= \frac{1}{2i}\left(-\log\left(\sqrt{2}\right) + \frac{\pi i}{4} + \log\left(\sqrt{2}\right) + \frac{\pi i}{4}\right) = \frac{\pi}{4}. \end{aligned}$$

§1.5 Fourier Analysis on Non-Abelian Finite Groups

When G abelian, recall that $\mathbb{C}[G]$ was a commutative ring isomorphic to $\bigoplus_{\chi \in \hat{G}} \mathbb{C}$. More generally, we find an isomorphism

$$\Phi : \mathbb{C}[G] \to \oplus_{j=1}^{h} \operatorname{End}_{\mathbb{C}(V_j)} \simeq \oplus_{j=1}^{h} M_{d_j \times d_j}(\mathbb{C}),$$

where $h = h(G)$, V_j enumerate the irreducible representations of G, and $d_j := \dim_{\mathbb{C}(V_j)}$.

↪**Definition 1.11** (Fourier Transform): Given a function $f : G \to \mathbb{C}$, denote by

$$\theta_f = \sum_{g \in G} f(g) g$$

its corresponding element in $\mathbb{C}[G]$. Then, ots corresponding image under Φ in $\bigoplus \operatorname{End}\left(V_j\right)$ is called the *Fourier transform* of f, i.e.

$$\hat{f} = (T_1, \ldots, T_h) \in \bigoplus \operatorname{End}\left(V_j\right),$$

a h-tuple of matrices where T_i a $d_i \times d_i$matrix.

1.5.1 Random Products in Groups

↪**Definition 1.12** (Probability Measure on a Group): A probability measure on a group G is a function $\mu : G \to [0, \infty)$ such that $\sum_g \mu(g) = 1$. Then, we can view μ as living naturally both in $\mathbb{R}^G$ and $\mathbb{R}[G]$ through the standard identification.

One of the key properties we notice by viewing μ as living in $\mathbb{R}[G]$ is in multiplication; multiplication in $\mathbb{R}[G]$ corresponds to convolution of functions. Namely, if μ_1, μ_2 two measures on G, then

$$(\mu_1 \circledast \mu_2)(g) = \sum_{\substack{(g_1,g_2)\in G\times G,\\ g_1g_2=g}} \mu_1(g_1)\mu_2(g_2) = \mu_1 \times_{\mathbb{R}[G]} \mu_2$$
$$= \mathbb{P}(\text{getting } g \text{ from a random product of } g_1, g_2 \text{ with } g_i \text{ picked according to } \mu_i).$$

For a fixed probability measure μ, then, we wish to investigate the limiting behavior of $\mu^{\circledast N}$ (μ convolved with itself N times for large N), which corresponds to the likelihood of obtaining a particular element from large numbers of products in the group.

↪**Definition 1.13**: Define the support

$$\mathrm{supp}(\mu) = \{g \in G \mid \mu(g) \neq 0\},$$

and the 2 subgroups

$$G_\mu := \text{subgroup generated by } g \in \mathrm{supp}(\mu), G_\mu^+ := \text{subgroup generated by } \{g^{-1}h \mid g, h \in \mathrm{supp}(\mu)\}.$$

Notice then $G_\mu^+ \subset G_\mu \subset G$.

↪**Theorem 1.12**: Let μ a probability measure on G. Then, if $G_\mu^+ = G$, then $\lim_{N\to\infty} \mu^{\circledast N} = \mu_{\mathrm{unif}}$, where μ_{unif} the uniform probability distribution which assigns $\frac{1}{\#G}$ to each element in G.

§1.6 Character Tables of S_4, A_5 and $\mathrm{GL}_3(\mathbb{F}_5)$

1.6.1 S_4

For S_4, we denote the conjugacy classes by $1A, 2A, 2B, 3A, 3B, 4A$ as the conjugacy classes of elements of the form $()$, $(12)(34)$, (12), (123), (1234) respectively.

	$1A$	$2A$	$2B$	$3A$	$4A$
χ_1	1	1	1	1	1
χ_2	1	1	-1	1	1
χ_3	2	2	0	-1	0
χ_4	3	-1	1	0	-1
χ_5	3	-1	-1	0	1

χ_1 is the trivial representation. χ_2 is the sign representation given by $\sigma \mapsto \mathrm{sgn}(\sigma) \in \{-1, 1\} \subseteq \mathbb{C}^x$. χ_3 comes from noticing that $K_4 = \mathbb{Z}/2 \times \mathbb{Z}/2 = 1A \sqcup 2A \subseteq S_4$ gives $S_4/K_4 \simeq S_3$. We then can find a new representation by composing the quotient map $\pi : S_4 \to S_3$ with a representation $\rho : S_3 \to \mathrm{Aut}_{\mathbb{C}}(V)$. Remember that there are three irreducible representations of S_3. The first two are the trivial and sign, already accounted for here. The last is the unique two-dimensional representation where $\chi(2A) = 0$ and $\chi(3A) = -1$ (these are the conjugacy classes in S_3 now). Under the quotient map, then, we find that

- since $1A, 2A$ contained in K_4, they are mapped to the identity in $\mathrm{Aut}(\mathbb{C}^2)$ so have trace 2;
- $2B, 4A$ must be mapped to elements of order 2 in S_3 (i.e. in $2A$) under π and thus must have trace 0;

- $3A$ must map to elements of order 3 in S_3 under π so must have trace -1.

This characterizes χ_3.

χ_4 comes from the standard representation on a 4 dimensional vector space (by permuting basis vectors), then subtracting off the trivial representation. This results in a character where each entry equals the number of fixed points each conjugacy class has, minus 1.

χ_5 comes from considering the homomorphism representation found from $V_5 = \mathrm{Hom}(V_2, V_4)$, where V_2, V_4 the vector spaces upon which χ_2, χ_4 "act". Hence, V_5 is a three dimensional representation, with $\chi_5 = \overline{\chi}_2\chi_4$.

1.6.2 A_5

For A_5, denote the conjugacy classes $1A, 2A, 3A, 5A, 5B$.

	$1A$	$2A$	$3A$	$5A$	$5B$
χ_1	1	1	1	1	1
χ_2	4	0	1	-1	-1
χ_3	5	1	-1	0	0
χ_4	3	-1	0	$1+\zeta+\zeta^{-1}$	$1+\zeta^2+\zeta^{-2}$
χ_5	3	-1	0	$1+\zeta^2+\zeta^{-2}$	$1+\zeta+\zeta^{-1}$

χ_1 trivial. χ_2 comes from the standard representation, minus the trivial. χ_3 similarly comes from the action of A_5 on the coset space S_5/F_{20}, or equivalently on A_5/D_{10}, minus the trivial again.

For the last two, we can check by dimensionality that it must be that the dimensions of both must be 3, so we are looking for representations $\rho : A_5 \to \mathrm{Aut}_{\mathbb{C}}(\mathbb{C}^3)$. Let $g \in 5A$. Notice then that g must have at most three eigenvalues, which are fifth roots of unity. But also, notice that g and g^{-1} are conjugate in A_5, and namely $g, g^{-1} \in 5A$. Hence, since a linear transformation has inverse eigenvalues of its inverse, it follows that the set of eigenvalues for g must be closed under taking inverses. So, the eigenvalues must be of the form $\{1, \zeta, \zeta^{-1}\}$ or $\{1, \zeta^2, \zeta^{-2}\}$ where ζ a primitive root of unity. It follows then that either $\mathrm{tr}(5A) = 1 + \zeta + \zeta^{-1}$ or $1 + \zeta^2 + \zeta^{-2}$, with, by symmetrical argument, gives the trace of $5B$ since $g \in 5A \Rightarrow g^2 \in 5B$.

Then, to find $\chi(3A) =: x_3$, taking the inner product with χ_2 we find

$$0 = 12 + 20x_3 - 12(1 + \zeta + \zeta^{-1}) - 12(1 + \zeta^2 + \zeta^{-2})$$

$$= 20x_3 - 12\left(\underbrace{1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4}_{=0}\right) \Rightarrow x_3 = 0.$$

From here, one can compute $\chi(2A)$ using orthogonality relations.

1.6.3 $\mathrm{GL}_3(\mathbb{F}_2)$

size:	1	21	56	42	24	24
	$1A$	$2A$	$3A$	$4A$	$7A$	$7B$
χ_1	1	1	1	1	1	1
χ_2	6	2	0	0	-1	-1

χ_3	7	−1	1	−1	0	0

χ_1 trivial. We consider χ_V given by G acting on $\mathbb{F}_2^3$ in the standard way (as three by three matrices) Then, the character is just given by the number of fixed points each element has, so in this case the number of fixed nonzero vectors.

- $1A$ 7, being the dimension
- A typical element of $2A$ looks like $\begin{pmatrix} 1 & & 1 \\ & 1 & \\ & & 1 \end{pmatrix}$ which has trace 3.
- $g \in 3A$ has minimal polynomial $(x-1)\left(x^2+x+1\right)$ so has a one-dimensional eigenspace so fixes one nonzero vector.
- $g \in 4A$ has minimal polynomial $(x-1)^3$ so by similar reasoning as $3A$ fixes a one-dimensional eigenspace.
- $g \in 7A$ or $7B$ must cyclically permute the basis vectors so fixes none so has trace 0.

In summary:

	$1A$	$2A$	$3A$	$4A$	$7A$	$7B$
χ_V	7	3	1	1	0	0

This is not irreducible by checking orthogonality relations, but we obtain χ_2 by subtracting off χ_1.

For χ_3, consider $X = \{\text{sylow} - 7 \text{ subgroups}\}$. One can check $\#X = 8$, and we have a natural action of G on X by conjugation, which is isomorphic to the action of G on $G/N(\text{Sylow} - 7)$ so $H := N(\text{Sylow} - 7)$ has cardinality 21. Then, the trace of each element is just the number of fixed cosets each element has acting on G/H. We then subtract off 1 from this number to obtain χ_3.

- $g \in 1A$ must have trace 8 so $\chi_3(1A) = 7$
- if $g \in 2A$, $gaH = aH \Leftrightarrow a^{-1}ga \in H$, but g of order 2 and thus so is $a^{-1}ga$, but H a group of cardinality of order 21 so such an element can't live in it.Thus g has no fixed points and $\chi_3(2A) = -1$. In particular g as a permutation looks like 4 disjoint 2 cycles.
- if $g \in 4A$, similar reasoning follows and we find $\chi_3(4A) = -1$ and g looks like 2 disjoint 4 cycles.
- $g \in 7A, 7B$ must act as a 7-cycle and so has one fixed point and thus $\chi_3(7A) = \chi_3(7B) = 0$.
- we can compute $\chi_3(3A)$ by checking the orthogonality relations by taking the inner product of it with itself. Computing this we find that $\chi_3(3A) = \pm 1$. We conclude it must be 1 by remarking that $3A$ acts on G/H either by a single 3 cycles (hence with 5 fixed points) or two three cycles (hence with 2), so it must be that the second case holds which gives us a character of 1.

§1.7 Induced Representations

Let G a finite group and $H \subseteq G$, and take $\chi \in \operatorname{Hom}(H, \mathbb{C}^\times)$ a one-dimensional representation of H. Consider the space

$$V_\chi = \{f : G \to \mathbb{C} \mid f(xh) = \chi(h) \cdot f(x)\ \forall\, h \in H\}.$$

Then,

↪**Proposition 1.10**:

1. G acts (linearly) on V_χ by the rule $gf(x) = f(g^{-1}x), \forall\, x \in G$.
2. $\dim(V_\chi) = [G : H]$

Proof.

1. We need to show $gf \in V_\chi$. We compute,
$$gf(xh) = f(g^{-1}(xh)) = f((g^{-1}x)h) = \chi(h)f(g^{-1}x) = \chi(h)(gf)(x),$$
for any $x \in G, h \in H, f \in V_\chi$, as required.
2. Let $a_1, \ldots, a_t$ be a set of coset representatives for H, i.e. $G = a_1 H \sqcup \cdots \sqcup a_t H$. Then, we claim that the map $f \mapsto (f(a_1), \ldots, f(a_t))$, $V_\chi \to \mathbb{C}^t$ a $\mathbb{C}$-vector space isomorphism.

Injective: If f in the kernel of this map, then $f(a_1) = \cdots = f(a_t) = 0$. But $f \in V_\chi$ so $f(a_j h) = \chi(h)f(a_j) = 0$ for any $h \in H, j = 1, \ldots, t$. Any element in G is in some $a_j H$ so equals $a_j h$ for some $h \in H$, so we conclude that f must be identically 0 and so this map injective.

Surjective: Given $(\lambda_1, \ldots, \lambda_t) \in \mathbb{C}^t$, define f by $f(a_j) := \lambda_j$ for each j, and "extend" naturally to behave under action of H, namely $f(a_j h) := \chi(h)f(a_j) = \chi_h \lambda_j$. ■

The representation V_χ is called the *induced* representation of χ from H to G. We sometimes write
$$V_\chi = \mathrm{Ind}_H^G \chi.$$

If H is a quotient of G, then any representation of H gives a representation of G (we've done this many times before, such as with S_4 and S_3). But in general, these aren't easy to come by. But if H just a subgroup of G, which are far more common, then we can use the induced representation technique above to look at representations of G.

Let $\psi : H \to \mathbb{C}^\times$ some one-dimensional representation of H and $V_\psi = \mathrm{Ind}_H^G \psi$. We wish to find the induced character χ_{V_ψ}.

We begin by looking for a basis for V_ψ. For any $a \in G$, define $f_a \in V_\psi$ defined by
$$f_a : G \to \mathbb{C}, \qquad f_a(g) := \begin{cases} \psi(h) \text{ if } g = ah \in aH \\ 0 \quad\;\; \text{ if } g \notin aH \end{cases}.$$

Then, if $a_1, \ldots, a_t$ coset representatives for H in G, $\beta := \{f_{a_1}, \ldots, f_{a_t}\}$ a basis for V_ψ.

Now, given $g \in G$, what is the matrix of g acting on V_ψ with respect to the basis β? We have that
$$g \cdot f_{a_j}(x) = f_{a_j}(g^{-1}x) = f_{ga_j}(x),$$

since, more precisely
$$gf_{a_j}(a_i) = \begin{cases} 0 \text{ if } g^{-1}a_i \notin a_j H \\ \psi(h) \text{ if } g^{-1} = a_j h' \end{cases}$$

and we can extend to general $g \in G$. Hence, if $a_1, ..., a_t$ are coset representatives, $ga_jH = a_iH$ for each a_j and some a_i, i.e. g permutes the coset representatives, modulo H. Hence, $ga_j = a_ih_{ij}$ for some $h_{ij} \in H$. So,

$$gf_{a_j} = f_{a_ih_{ij}} = \psi(h_{ij})f_{a_i}.$$

Write $ga_iH = a_{i'}H$ so $ga_i = a_{i'}h_i$. With this, $gf_{a_1} = \psi(h_1)f_{a_{1'}}$, etc, and so in each ith column of our matrix there is a single nonzero entry in the i'th row with entry $\psi(h_i)$.

Thus,

$$\chi_{V_\psi}(g) = \sum_{\substack{i \mid ga_i = a_ih_i, \\ h_i \in H}} \psi(h_i) = \sum_{i=1}^{t} \tilde{\psi}\left(a_i^{-1}ga_i\right),$$

namely, we only sum over the h_i's that land the in the diagonal, which are only those that come from g fixing the respective cosets. We put $\tilde{\psi}$ to be ψ on H and 0 elsewhere. In all, them, we have proven the following theorem.

↪**Theorem 1.13**: Let $H \subseteq G$ and $\psi : H \to \mathbb{C}^\times$ a one-dimensional representation of H. Then, the induced character from H to G is given by

$$\chi_{\mathrm{Ind}_H^G \psi} = \sum_{a \in G/H} \tilde{\psi}(a^{-1}ga),$$

where

$$\tilde{\psi}(g) = \begin{cases} 0 & \text{if } g \notin H \\ \psi(h) & \text{if } g \in H \end{cases}.$$