Contents

Definition 0.0.1. Go to Learn for the syllabus.

Remark 0.0.2. If you have 80% above for the final, then test one's weight will be moved to the final.

Chapter 1

Intro to Representations

1.1 Intro

Definition 1.1.1. In this note, when no spesification occured, then G is fintie group, V is $\mathbb{C}$ fintie dimensional vector space.

Remark 1.1.2 (Motivation)**.** Let G be a finite group of order n, say $G = \{g_1, ..., g_n\}$. Let $g \in G$ be fixed, then g induces a permutation σ in S_n. In particular, we would have $gg_i = g_{\sigma(i)}$ for $1 \leq i \leq n$. Hence, we have an embedding $\phi : G \to S_n$ and that $G \cong \phi(G) \leq S_n$. This is Cayley's theorem.

Now, let V be n-dimensional $\mathbb{C}$ vector space, let $GL(V)$ be the group of invertible linear operators of V. Now, define $\psi : S_n \to GL(V)$, where $\sigma \mapsto T_\sigma$ and $T_\sigma(b_i) = b_{\sigma(i)}$ for a fix basis $\{b_1, ..., b_n\}$ then extend by linearlity. In particular, ψ is an embedding. Thus, we have $\phi \circ \psi : G \to GL(V)$ is an embedding.

Definition 1.1.3. Let G be finite, V be finite dimensional $\mathbb{C}$ vector space. A ***representation*** of G is a group homomorphism $\rho : G \to GL(V)$.

Remark 1.1.4. Soemtimes I will write the representation as (V, ρ) to indicate the vector space.

Definition 1.1.5. The ***degree*** of a representation (V, ρ) is the dimension of V.

Remark 1.1.6. If V is $n-$dimensional vector space, then $GL(V) \cong GL_n(\mathbb{C})$ so we always talk about $\rho : G \to GL_n(\mathbb{C})$ to be representations.

Remark 1.1.7. Let ρ be a representation of G, then we write $\rho(g)(v) = \rho_g(v)$ for $g \in G, v \in V$.

Example 1.1.8.

1. Let $\rho : G \to GL(\mathbb{C}) \cong \mathbb{C}^\times$ be $\rho(g) = 1$ for all $g \in G$. This is the trivial representation (note only this degree one representation is called the trivial representation).
2. Let $\rho : G \to GL(V)$ with $\rho(g) = I$ for all $g \in G$, then this is a representation.
3. Let $\rho : S_n \to \mathbb{C}^\times$ with $\rho(\sigma) = sgn(\sigma)$, then this is a representation.
4. The representation of G afforded by Cayley's theorem is called the ***regular representation*** of G.

In particular, let $X = \{v_g : g \in G\}$ be a set of symbols, then let $V = Free(X)$, we have $\rho : G \to GL(V)$ and $\rho_g(v_h) = v_{gh}$ for all $g, h \in G$.

5. Let G be a finite group, let $X = \{x_1, ..., x_m\}$, let $V = Free(X)$. Suppose G acts on X, then we define $\rho : G \to GL(V)$ to be $\rho_g(x_i) = g \cdot x_i$. This is called the ***permutation representation***. Note the degree of this is m. Note this depends on the action of G, so it is not unique.
6. Consider a square with vertices a, b, c, d, take $X = \{a, b, c, d\}$, then we can define permutation $\rho : D_4 \to GL(V)$ where $V = Free(X)$ via the geomatric action of D_4 on the square. Note $|D_n| = 2n$ for this class.
7. Let $C_n = \langle x \rangle$ be cyclic of order n. Let $\rho : C_n \to GL(V)$ be a representation. Say we have $\rho(x) = T$, this gives a representation iff $T^n = \lambda I$.

Definition 1.1.9. Let (V, ρ) and (W, τ) be representation of G, then ρ and τ are ***isomorphic(equivalent)*** if and only if there exists isomorphism $T : V \to W$ such that $T \circ \rho_g = \tau_g \circ T$ for all $g \in G$. We write $\rho \cong \tau$ when they are isomorphic.

Example 1.1.10.
1. Let (V, ρ) be representation of G, let $T : V \to W$ be isomorphism, then let $\tau : G \to GL(W)$ to be $\tau(g) = T \circ \rho(g) \circ T^{-1}$, then $\rho \cong \tau$.
2. Let $G = \{g_1, ..., g_n\} = \{h_1, ..., h_n\}$. Fix $g \in G$, say $gg_i = g_{\alpha(i)}$ and $gh_i = h_{\beta(i)}$ where $\alpha, \beta \in S_n$. Fix a n-dimensional vector space V with basis $(b_1, ..., b_n)$. Take the two regular representations $\rho^1 : G \to GL(V)$ to be $\rho^1_g(b_i) = b_{\alpha(i)}$ and $\rho^2 : G \to GL(V)$ to be $\rho^2_g(b_i) = b_{\beta(i)}$. Let $\gamma \in S_n$ such that $h_{\gamma(i)} = g_i$ and define $T : V \to V$ by $T(b_i) = b_{\gamma(i)}$, we note T is an isomorphism.
   Note
   $$\begin{aligned} gg_i &= g_{\alpha(i)} \\ &= gh_{\gamma(i)} = h_{\beta\gamma(i)} \\ &= g_{\gamma^{-1}\beta\gamma(i)} \end{aligned}$$
   Hence, we have $\alpha = \gamma^{-1}\beta\gamma$, then, for each b_i, we have
   $$\begin{aligned} T \circ \rho^1_g \circ T^{-1}(b_i) &= T \circ \rho^1_g(b_{\gamma^{-1}(i)}) \\ &= T(b_{\alpha\gamma^{-1}(i)}) = b_{\gamma\alpha\gamma^{-1}(i)} = b_{\beta(i)} \\ &= \rho^2_g(b_i) \end{aligned}$$
   Therefore, they are indeed isomorphic.

Example 1.1.11. Let $|G| = n$, let V, W be n dimensional vector spaces with bases $(b_1, ..., b_n)$ and $(c_1, ..., c_n)$ respectively. Then, the two regular representations of V and W are isomorphic. Moreover, the regular representations of V with different bases are also isomorphic.

1.2 Subrepresentation and Irreducible Representations

Definition 1.2.1. Let (V, ρ) be a representation of G, let $W \leq V$. We say W is ***G-stable*** or $G-$***invariant*** if $\rho_g(w) \in W$ for all $g \in G, w \in W$.

Definition 1.2.2. Let (V, ρ) be a representation of G, we say $W \leq V$ is a ***subrepresentation*** if W is stable under G with the homomorphism $\rho^W : G \to GL(W)$ such that $\rho_g^W(w) = \rho_g(w)$ for all $w \in W$.

Example 1.2.3. Let (V, ρ) be the regular representation, let $G = \{g_1, ..., g_n\}$. Let $W = span\{\sum_{g \in G} v_g\}$, then W is G stable and $\rho^W : G \to GL(W)$ is the trivial representation.

Example 1.2.4. Let $\rho : S_n \to GL(V)$ be the regular representation. Let $W = span\{\sum_{\sigma \in S_n} sgn(\sigma) v_\sigma\}$, then W is $G-$stable.

Theorem 1.2.5 (Maschke's theorem)**.** *Let (V, ρ) be a representation. Let $W \leq V$ be $G-$stable. Then, there exists a $G-$stable subspace W' such that $V = W \oplus W'$.*

Proof. Let $T : V \to \mathbb{C}^n$ be an isomorphism, for $x, y \in V$, we can define $\langle x, y \rangle' := \langle T(x), T(y) \rangle_s$ where $\langle \cdot, \cdot \rangle_s$ is the standard inner product on $\mathbb{C}^n$.

Now, for $x, y \in V$, define $\langle x, y \rangle := \sum_{g \in G} \langle \rho_g(x), \rho_g(y) \rangle'$, we have $\langle x, y \rangle$ is an inner product. Then, let $x, y \in V$ and $h \in G$ be fixed. Then, $\langle \rho_h(x), \rho_h(y) \rangle = \langle x, y \rangle$ so that each ρ_h is unitary operator with this inner product. Thus, we have $\rho_h \circ \rho_h^* = I$.

Let $W \leq V$ be G stable, then take $W' = W^\perp$ with respect to the inner product $\langle \cdot, \cdot \rangle$ we defined, then we have $V = W \oplus W'$. We will show $W' = W^\perp$ is G stable.

Let $x \in W^\perp$, $w \in W$ and $g \in G$ be all arbitrary. Then, we have

$$\begin{aligned} \langle \rho_g(x), w \rangle &= \langle x, \rho_g^*(w) \rangle = \langle x, \rho_g^{-1}(w) \rangle \\ &= \langle x, \rho_{g^{-1}}(w) \rangle, \text{ note } \rho_{g^{-1}}(w) := w' \in W \\ &= \langle x, w' \rangle = 0 \end{aligned}$$

The proof follows as $\rho_g(W^\perp) \subseteq W^\perp$. ♡

Definition 1.2.6. Let (V, ρ) be a representation of G, let $V = W_1 \oplus ... \oplus W_k$ where W_i are all $G-$stable. For each $1 \leq i \leq k$, let $\rho^i = \rho^{W_i}$, then for each $v = \sum w_i \in V$, we have $\rho_g(v) = \sum \rho_g(w_i) = \sum \rho_g^i(w_i)$. In this case, we write $\rho = \rho^i \oplus ... \oplus \rho^k$ and call it a ***direct sum*** of the ρ^i's.

Remark 1.2.7. The previous definition is with respect to an ***internal direct sum*** of V.

Externally, let $W_1, ..., W_k$ be vector spaces, and representations ρ^i on W_i, respectively. We can define $\rho = (\rho^1 \oplus ... \oplus \rho^k)$ to be a representation from G to $V := W_1 \oplus ... \oplus W_k$ by $\rho_g(w_1, ..., w_k) = (\rho_g^1(w_1), ..., \rho_g^k(w_k))$.

Definition 1.2.8. Let $\rho_i : G \to GL(W_i)$ is a subrepresentation of $\rho : G \to GL(V)$, we often say W_i is a subrepresentation of V, or, I may say in this note that (W, ρ_i) is a subrepresentation of (V, ρ).

Definition 1.2.9. Let (V, ρ) be a representation, we say ρ is ***irreducible*** if $V \neq \{0\}$ and the only $G-$stable subspaces of V are $\{0\}$ and V.

Theorem 1.2.10. *Every representation (V, ρ), $V \neq \{0\}$, is a direct sum of irreducible subrepresentations.*

Proof. Immediately by Theorem 4.4.7 and induction. ♡

Example 1.2.11. Let $\rho : S_3 \to GL(\mathbb{C}^3)$ be the permutation representation with the standard basis $\{e_1, e_2, e_3\}$ by the obvious action. Let $W_1 = span(e_1 + e_2 + e_3)$, we have W_1 is $G-$stable and W_1 is isomorphic to the trivial representation. On the other hand, we have $W_1 \oplus W_2 = \mathbb{C}^3$ so that W_2 must have dimension 2. In particular, we have $W_2 = span\{e_1 - e_2, e_2 - e_3\}$.

Remark 1.2.12. Let (V, ρ) be a representation. Let $V = W_1 \oplus ... \oplus W_k$, where $dim(W_i) = 1$. Then, we have $deg(\rho^i) = 1$. Moreover, we have $\rho_{gh}(\sum w_i) = \sum \rho^i_{gh}(w_i) = \sum \rho^i_g \rho^i_h(w_i) = \sum \rho^i_h \rho^i_g(w_i) = \rho_{hg}$. Thus, we have ρ can be break up into degree 1 representation then $\rho_{gh} = \rho_{hg}$. In the previous example, $\rho_{gh} \neq \rho_{hg}$ for some $g, h \in S_3$, thus we know W_2 must be irreducible.

Example 1.2.13. Let $\rho : S_3 \to GL(V)$ be the regular representation. We try to decompose the regular representation.

Let $W_1 = span(\sum v_\sigma)$, we have W_1 is stable, this is the trivial representation. Moreover, from assignment, we have $W_2 = span(\sum sgn(\sigma) v_\sigma)$ is G-stable and isomorphic to the sign representation. We still need more vector spaces.

Consider $W_3 = \{\sum \alpha_g v_g : \alpha_e + \alpha_{(123)} + \alpha_{132} = 0 \wedge \alpha_{(12)} + \alpha_{(13)} + \alpha_{(23)} = 0\}$, we have W_3 is $G-$stable and we have $V = W_1 \oplus W_2 \oplus W_3$ as we exam the dimension. However, W_3 is not irreducible.

A basis of W_3 is $\begin{cases} e_1 = v_e - v_{(123)} \\ e_2 = v_e - v_{(132)} \\ e_3 = v_{(12)} - v_{(13)} \\ e_4 = v_{(12)} - v_{(23)} \end{cases}$ Note $S_3 = \langle (12), (123) \rangle$, thus it suffice to show subspaces are $G-$stable if we have the generator stable. In particular, we have $\rho_{(12)}$ maps $e_1 \mapsto e_4$, $e_2 \mapsto e_3$, $e_3 \mapsto e_2$ and $e_4 \mapsto e_1$. On the other hand, we have $\rho_{(123)}$ maps $e_1 \mapsto e_2 - e_1$, $e_2 \mapsto -e_1$, $e_3 \mapsto e_4 - e_3$ and $e_4 \mapsto -e_3$.

Let $U_1 = span(e_1 - e_4, e_2 + e_3 - e_1)$ as we see $e_1 \mapsto e_4$ and $e_4 \mapsto e_1$ under $\rho_{(12)}$, and then we apply $\rho_{(123)}$ to $e_1 - e_4$. Moreover, we have $U_2 = span(e_2 - e_3, e_3 - e_4 - e_1)$. Both U_1, U_2 are G stable as they are stable under (12) and (123). Moreover, we have $W_3 = U_1 \oplus U_2$ and we would see (by character theory) that U_1, U_2 are irreducible.

1.2.1 Tensor

Remark 1.2.14. The motivation of this chapter is to extend a vector space V over F into a ring with $(T(V), +, \otimes)$.

Thus, we want, for $x, y, z \in V$ and $\alpha \in F$,

1. $x \otimes (y+z) = x \otimes y + x \otimes z$ and $(y+z) \otimes x = y \otimes x + z \otimes x$
2. $\alpha(x \otimes y) = (\alpha x) \otimes y = x \otimes (\alpha y)$

Definition 1.2.15. Let X be a set of symbols, we define the ***free vector space*** on X by $V = Free(X) = \{\sum_{i=1}^{n} a_i x_i : a_i \in F, x_i \in X, n \in \mathbb{N}\}$ with addition defined to be

$$\sum \alpha_i x_i + \sum \beta_i x_i = \sum (\alpha_i + \beta_i) x_i$$

and $\alpha(\sum \alpha_i x_i) = \sum (\alpha \alpha_i x_i)$.

Remark 1.2.16. By construction, X is a basis for $Free(X)$.

Definition 1.2.17. Let V, W be fintie dimensional vector space over F, and let $X = V \times W$ to be a set of symbols. Let S be the set of vectors in $Free(X)$ of the form

$$\begin{cases} (x+y,z) - (x,z) - (y,z) \\ (z,x+y) - (z,x) - (z-y) \\ \alpha(x,y) - (\alpha x, y) \\ \alpha(x,y) - (x, \alpha y) \end{cases}$$

Then, we define the ***tensor product*** of V and W to be $V \otimes W = Free(X)/span(S)$.

Definition 1.2.18. We define $v \otimes w := \overline{v, w} = (v,w) + span(S) = \overline{(v,w)}$ where $v \in V$ and $w \in W$ and call them ***pure tensor***.

Remark 1.2.19. First, note $(v+w) \otimes z - v \otimes z - w \otimes z = 0 \otimes 0 = 0$, and so $(v+w) \otimes z = v \otimes z + w \otimes z$. Also, $\alpha(v \otimes w) = (\alpha v) \otimes w = v \otimes (\alpha w)$.

A typical element of $V \otimes W$ looks like

$$\alpha_1(v_1 \otimes w_1) + ... + \alpha_n(v_n \otimes w_n)$$

Example 1.2.20. Consider $\mathbb{C}^2 \otimes \mathbb{C}^3$(or $\mathbb{C}^2 \otimes_{\mathbb{C}} \mathbb{C}^3$ where $\otimes_{\mathbb{C}}$ indicate the underlying field), consider

$$\begin{bmatrix} 1 \\ 2 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$$

Let the standard basis for $\mathbb{C}^2$ be $\sigma_2 = \{a_1, a_2\}$ and the standard basis for $\mathbb{C}^3$ be $\sigma_3 = \{b_1, b_2, b_3\}$. Then, we have

$$\begin{aligned} \begin{bmatrix} 1 \\ 2 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} &= (a_1 + 2a_2) \otimes (b_1 + 2b_2 + 3b_3) \\ &= a_1 \otimes (b_1 + 2b_2 + 3b_3) + 2(a_2 \otimes (b_1 + 2b_2 + 3b_3)) \\ &= a_1 \otimes b_1 + 2(a_1 \otimes b_2) + 3(a_1 \otimes b_3) \\ &\quad + 2(a_2 \otimes b_1) + 4(a_2 \otimes b_2) + 6(a_2 \otimes b_3) \end{aligned}$$

Example 1.2.21. Note $2 \otimes 2 = 2(1 \otimes 2) = 4(1 \otimes 1)$.

Proposition 1.2.22. *Let V, W be finite dimensional F vector space. Let $\{v_1, ..., v_n\}$ be a basis of V, $\{w_1, ..., w_m\}$ be a basis of W. A basis for $V \otimes_F W$ is*

$$\{v_i \otimes w_j : 1 \leq i \leq n, 1 \leq j \leq m\}$$

In particular, we have $dim(V \otimes_F W) = nm = dim(V) \cdot dim(W)$.

Proof. Let $x \in A$ and $y \in B$, then $x \otimes y \in A \otimes B$. In particular, note every element of $A \otimes B$ is the sum of some pure tensors. Thus, $x = \sum_{i=1}^{n} t_i a_i$ and $y = \sum_{j=1}^{m} l_j b_j$, we have

$$\begin{aligned} x \otimes y &= (\sum_{i=1}^{n} t_i a_i) \otimes (\sum_{j=1}^{m} l_j b_j) \\ &= \sum_{i=1}^{n} \left(t_i a_i \otimes (\sum_{j=1}^{m} l_j b_j) \right) \\ &= \sum_{i=1}^{n} \left(\sum_{j=1}^{m} t_i a_i \otimes l_j b_j \right) \\ &= \sum_{i=1}^{n} \sum_{j=1}^{m} t_i l_j (a_i \otimes b_j) \in span(W) \end{aligned}$$

Hence, $A \otimes B \subseteq span(W)$ as every pure tensor is in the span of W. Next, we show W is linear independent.

Suppose $\sum_{i,j} d_{ij}(a_i \otimes b_j) = 0$. Let $f_k \in A^*$ be $f_k(a_k) = 1$ and $f_k(a_l) = 0$ for $1 \leq l \leq n$ and $k \neq l$. Let $F_k : A \times B \to B$ be $F_k(a, b) = f_k(a)b$, then F_k is bilinear. Hence, there exists a linear mapping T_k (by universal property) from $A \otimes B \to B$ such that $T_k(a \otimes b) = f_k(a)b$. Thus, for all $1 \leq k \leq n$,

$$\begin{aligned} 0 &= T_k(\sum_{i,j} d_{ij}(a_i \otimes b_j)) \\ &= \sum_{i,j} d_{ij} f_k(a_i) b_j \\ &= \sum_{j=1}^{n} d_{kj} b_j \end{aligned}$$

and since $\{b_1, ..., b_m\}$ is linear independent, we have $d_{kj} = 0$ for all $1 \leq j \leq m$. Since this hold for all $1 \leq k \leq n$, we have $d_{ij} = 0$ for all $1 \leq i \leq n$ and $1 \leq j \leq m$. Therefore, $\{(a_i \otimes b_j) : 1 \leq i \leq n, 1 \leq j \leq m\}$ is a basis of $A \otimes B$. ♡

Lemma 1.2.23. *Suppose V and W are vector spaces over F and $T : V \to W$ is linear. Let S be a subspace of V. Then there exists a linear transformation $\mathfrak{T} : V/S \to W$ such that $\mathfrak{T}(x + S) = T(x)$ for all $x \in V$ if and only if $T(s) = 0$ for all $s \in S$.*

Moreover, if $\mathfrak{T}$ exists, it is unique, and every element in $L(V/S, W)$ arises in this way from a unique T.

Proof. Suppose $\mathfrak{T}$ exists. Then for all $s \in S$, we have $T(s) = \mathfrak{T}(s+S) = \mathfrak{T}(0) = 0$.

Now, suppose $T(s) = 0$ for all $s \in S$. We must show that $\mathfrak{T}(x+S) = T(x)$ makes $\mathfrak{T}$ well-defined. In other words, we must show that $v, v' \in V$ are such that $v+S = v'+S$, then $\mathfrak{T}(v+S) = \mathfrak{T}(v'+S)$. Now, note $v+S = v'+S$ then $v - v' \in S$ and so $\mathfrak{T}((v-v')+S) = \mathfrak{T}(v+S) - \mathfrak{T}(v'+S) = 0$. Thus $\mathfrak{T}(v+S) = \mathfrak{T}(v'+S)$ and so $\mathfrak{T}$ is well-defined.

Next, we only need to show $\mathfrak{T}$ is lienar. Indeed, consider $x+S, y+S \in V/S$ and $a \in F$, we have $\mathfrak{T}(a(x+S)+(y+S)) = \mathfrak{T}((ax+y)+S) = T(ax+y) = aT(x)+T(y) = a\mathfrak{T}(x+S) + \mathfrak{T}(y+S)$. Hence $\mathfrak{T}$ is linear.

The final remarks are clear, since the statement $\mathfrak{T}(x+S) = T(x)$ uniquely determines either of T, $\mathfrak{T}$ from the other. Indeed, let T, U be lienar and they induce the same linear transformation $\mathfrak{T}$ on $V/S \to W$, we see that $\mathfrak{T}(x+S) = T(x) = U(x)$ for all $x \in V$ and so $T = U$. ♡

Theorem 1.2.24 (Universal Property of Tensor Product)**.** *Let V, W, Z be F vector spaces. Let $\phi : V \times W \to Z$ be bilinear, i.e. $\phi(\alpha x + y, z) = \alpha\phi(x,z) + \phi(y,z)$ and $\phi(x, \alpha z_1 + z_2) = \alpha\phi(x, z_1) + \alpha(x, z_2)$. Then, there exists a unique linear transformation $T : V \otimes W \to Z$ such that $T(v \otimes w) = \phi(v, w)$. Moreover, all linear transformation from $V \otimes W \to Z$ can be constructed in this way.*

Proof. Let $X = V \times W$. We first show ϕ induce a unique linear mapping Φ from $Free(X) \to Z$. Note $V \times W$ is a basis for $Free(X)$, thus, let $x = \sum_{i=1}^{n} a_i(v_i, w_i) \in Free(X)$ where $(v_i, w_i) \in X$. Define $\Phi(x) = \sum_{i=1}^{n} a_i\phi(v_i, w_i) \in Z$, first note this Φ is indeed unique (this Φ only depends on how ϕ maps all the elements of $V \times W$ to Z, and thus every ϕ uniquely induce the Φ), then we will show it is linear. Let $x = \sum_{i=1}^{n} a_i(v_i, w_i)$ and $y = \sum_{i=1}^{n} b_i(v_i, w_i)$, and $k \in F$, we have $\Phi(kx+y) = \Phi(\sum_{i=1}^{n}(ka_i+b_i)(v_i, w_i)) = \sum_{i=1}^{n}(ka_i+b_i)\phi(v_i, w_i) = \sum_{i=1}^{n} ka_i\phi(v_i, w_i) + \sum_{i=1}^{n} b_i\phi(v_i, w_i) = k\Phi(x) + \Phi(y)$. Hence, Φ is indeed linear and since it is essentially the same as ϕ, we will call it ϕ and specify it is a linear mapping from $Free(X) \to Z$(instead of bilinear function from $V \times W \to Z$).

Next, we will show $\phi(s) = 0$ for all $s \in span(S)$ where $S \subseteq Free(X)$ is the set of all vectors in the following form

$$\begin{cases} (x_1 + y_1, z_2) - (x_1, z_2) - (y_1, z_2) \\ (z_1, x_2 + y_2) - (z_1, x_2) - (z_1, y_2) \\ \alpha(x_1, y_2) - (\alpha x_1, y_2) \\ \alpha(x_1, y_2) - (x_1, \alpha y_2) \end{cases}$$

where $x_1, y_1, z_1 \in V, x_2, y_2, z_2 \in W, \alpha \in F$.

Let $\phi : V \times W \to Z$ be bilinear. Then $\phi(\alpha x_1 + y_1, z_2) = \alpha\phi(x_1, z_2) + \phi(y_1, z_2)$ and $\phi(z_1, \alpha x_2 + y_2) = \phi(z_1, x_2) + \alpha(z_1, y_2)$ for all $x_1, y_1, z_1 \in V, x_2, y_2, z_2 \in W, \alpha \in F$. In particular, it suffice to show each vector in the above form in S is equal zero under the linear mapping ϕ as $span(S)$ is linear combinations of the above forms. Let

$0_F \in F$, $0_V \in V$, and $0_W \in W$.

$$\begin{aligned}
\phi((x_1 + y_1, z_2) - (x_1, z_2) - (y_1, z_2)) &= \phi(x_1 + y_1, z_2) - \phi(x_1, z_2) - \phi(y_1, z_2) \\
&= \phi(x_1 + y_1 - x_1, z_2) - \phi(y_1, z_2) \\
&= \phi(y_1, z_2) - \phi(y_1, z_2) \\
&= 0
\end{aligned}$$

$$\phi((z_1, x_2 + y_2) - (z_1, x_2) - (z_1, y_2)) = 0$$

$$\begin{aligned}
\phi(\alpha(x_1, y_2) - (\alpha x_1, y_2)) &= \alpha\phi(x_1, y_2) - \phi(\alpha x_1, y_2) \\
&= \phi(\alpha x_1, y_2) - \phi(\alpha x_1, y_2) \\
&= 0
\end{aligned}$$

$$\phi(\alpha(x_1, y_2) - (x_1, \alpha y_2)) = 0$$

Thus, by the above Lemma, we have a linear transformation from $V \otimes W \to Z$ induced by ϕ as $V \otimes W = (Free(X))/S$ and ϕ is a linear mapping on $Free(X)$.

Then, we show the uniqueness. Let ϕ and ψ be two bilinear functions on $V \times W$ to Z and suppose they induce the same lienar transformation from $Free(X) \to Z$, say T. Then, since T exists, it is uniquely determined by ϕ and by ψ. In particular, we must have $T(x + S) = \phi(x) = \psi(x)$ for all $x \in Free(V \times W)$ and so $\phi = \psi$. Thus, if T exists, the bilinear function that induces T is unqiue and every T gives us an bilinear function on $V \times W$ to Z. ♡

Remark 1.2.25. Let V be finite dimensional F vector space, $V^* = \{T : V \to F : T \text{ is linear}\}$ is called the ***dual space of V***. Then, let $\{v_1, ..., v_n\}$ be a basis for V, then let $v_i^* \in V^*$ to be $v_i^*(v_j) = \delta_{ij}$, and $\{v_1^*, ..., v_n^*\}$ is a basis for V^*.

Definition 1.2.26. Let V, W be finite dimensional F vector space, we define

$$L(V, W) := \{T : V \to W : T \text{ is linear}\} =: Hom(V, W)$$

Note $L(V, W)$ is a F vector space.

Example 1.2.27. Let V, W be finite dimensional F vector space, show $V^* \otimes_F W \cong L(V, W)$.

Solution. Define $\phi : V^* \times W \to L(V, W)$ by $\phi(f, w)(v) = f(v)w$. We can show ϕ is bilinear and well-defined. Thus, by the Universal property, there is a unique linear transformation $T : V^* \otimes W \to L(V, W)$ such that $T(f \otimes W) = \phi(f, w)$.

We will show T is an isomorphism by finding the inverse. Define $U : L(V, W) \to V^* \otimes W$ by $U(F) = \sum_{j=1}^{m} w_i^* F \otimes w_i$ where $\{w_1, ..., w_m\}$ is a basis for W and $\{w_1^*, ..., w_m^*\}$ is a basis for W^*.

Then, let $v \in V$ be arbitrary. Suppose $F(v) = \sum_{i=1}^{m} \alpha_i w_i$.

$$\begin{aligned}
U \circ U(F)(v) &= T(\sum w_i^* \circ F \otimes w_i)(v) \\
&= \sum T(w_i^* \circ F \otimes w_i)(v) \\
&= \sum w_i^* \circ F(v) \times w_i \\
&= \sum w_i^*(\alpha_1 w_1 + ... + \alpha_m w_m) w_i \\
&= \sum \alpha_i w_i \\
&= F(v)
\end{aligned}$$

♠

Definition 1.2.28. Let F be a field, an ***F-Algebra*** is a vector space A over F equipped with a multiplication map such that, for all $a, b, c \in A$, $\alpha \in F$, we have

1. $a(bc) = (ab)c$
2. $a(b + c) = ab + ac$
3. $(b + c)a = ba = ca$
4. $\alpha(ab) = (\alpha a)b = a(\alpha b)$

Let V be an F vector space. For $K \in \mathbb{N}$, we define $T^k(V) = \bigotimes_{i=1}^{k} V = V \otimes V \otimes ... \otimes V$. The elements in $T^k(V)$ is called a $k-$tensor. We also define $T^0(V) = F$.

Aside, let V be F vector space, and $\{W_i\}$ be countable many subspaces of V. The direct product

$$\prod_{i=1}^{\infty} W_i = \{(a_1, a_2, ...) : a_i \in W_i\}$$

The direct sum

$$\bigoplus_{i=1}^{\infty} W_i = \{(a_1, a_2, ...) : a_i \in W_i, \text{ where } a_i = 0 \text{ for all but infinite many } i\}$$

We then define the ***tensor algebra*** of V by $T(V) = \bigoplus_{i=0}^{\infty} T^i(V)$.

Example 1.2.29. Let $x, y \in V$, $F = \mathbb{R}$, then an element in $T(V)$ would like

$$3 + 2(x \otimes y) - \frac{1}{7}(x \otimes x \otimes y) + 87(x \otimes x \otimes x \otimes y \otimes x) \in T(V)$$

Here, in $T(V)$, multiplication is given by $(v_1 \otimes ... \otimes v_k)(u_1 \otimes ... \otimes u_l) = v_1 \otimes ... \otimes v_k \otimes u_1 \otimes ... \otimes u_l$ and extend by distributivity.

Chapter 2

Character Theory

2.1 Intro

Definition 2.1.1. Let $\rho : G \to GL(V)$ be a representation. The ***character*** of ρ is $\chi : G \to \mathbb{C}$ given by

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

Remark 2.1.2.

1. Let $A(g) = [\rho_g]_\beta$ where β is a basis of V, then $\chi(g) = Tr(A(g))$, which is the sum of diagonal entries.
2. We have $Tr(AB) = Tr(BA)$ and $Tr(ABA^{-1}) = Tr(B)$.
3. Suppose $\rho \cong \tau$, then we have $Tr(\rho_g) = Tr(\tau_g)$. In particular, we have $\chi_\rho = \chi_\tau$
4. We remark $\chi(g)$ is the sum of eigenvalues of ρ_g.
5. We have $\chi(e) = n$ where n is the degree of representation.

Proposition 2.1.3. *Let (V, ρ) be a representation of G, then for every $g \in G$, the eigenvalues of $\rho(g)$ have norm 1. In particular, $\chi(g^{-1}) = \overline{\chi(g)}$.*

Proof. Let $n = |G|$. We note $\rho(g)^n = \rho(g^n) = I$, thus $\lambda^n - 1 = 0$ and so $|\lambda| = 1$.

Next, note $\chi(g) = \sum \lambda_i$ where λ_i are all eigenvalues of $\rho(g)$. Thus, we have

$$\begin{aligned}\overline{\chi(g)} &= \overline{\sum \lambda_i} = \sum \overline{\lambda_i} \\ &= \sum \lambda_i^{-1} \\ &= \chi(g^{-1})\end{aligned}$$

♡

Proposition 2.1.4. *Let (V, ρ) and (W, τ) be two representations of G. Then we have $\chi_{\rho\oplus\tau} = \chi_\rho + \chi_\tau$ and $\chi_{\rho\otimes\tau} = \chi_\rho \cdot \chi_\tau$.*

Proof. Let $\beta_1 = \{v_1, ..., v_n\}$ be a basis of V and $\beta_2 = \{w_1, ..., w_m\}$ be a basis of W. Then, we have $\beta = \{(v_1, 0), ..., (0, w_1), ...\}$ is a basis of $V \oplus W$. Then, we have

$[(\rho \oplus \tau)(g)]_\beta$ is a block matrix that equals $diag\{[\rho(g)]_{\beta_1}, [\tau(g)]_{\beta_2}\}$. Thus we have $\chi_{\rho\oplus\tau} = \chi_\rho + \chi_\tau$ as desired.

For the tensor, we have $\gamma = \{v_i \otimes w_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ to be lexicographic order, i.e. $v_1 \otimes w_1, v_1 \otimes w_2, ..., v_1 \otimes w_m, v_2 \otimes w_1, ...$ and so on.

Let $g \in G$ be fixed. Let $A = [\rho(g)]_{\beta_1}$ and $B = [\tau(g)]_{\beta_2}$. Fix $v_i \otimes w_j \in \gamma$. Then,

$$\begin{aligned}(\rho \otimes \tau)(g)(v_i \otimes w_j) &= \rho(g)(v_i) \otimes \tau(g)(w_j) \\ &= (\sum_{k=1}^{n} a_{ki} v_i) \otimes (\sum_{k=1}^{m} b_{kj} w_j) \\ &= ... + (a_{ii} b_{jj})(v_i \otimes w_j) + ...\end{aligned}$$

Therefore, we have $Tr([(\rho \otimes \tau)(g)]_\gamma) = \sum_{i,j} a_{ii} b_{jj} = Tr(A) \cdot Tr(B)$.

Hence, $\chi_{\rho\otimes\tau} = \chi_\rho(g) \cdot \chi_\tau(g)$. ♡

Example 2.1.5. Let $\rho : S_n \to GL(\mathbb{C}^n)$ be the permutation representation with $\{e_1, ..., e_n\}$. Then, we have $\chi(\sigma) = |\{1 \leq i \leq n : \sigma(i) = i\}| = fix(\sigma)$.

Now, recall Burnside's lemma, we have $1 = \frac{1}{|S_n|} \sum_{\sigma \in S_n} |fix(\sigma)|$ so

$$|S_n| = \sum_{\sigma \in S_n} \chi(\sigma)$$

Example 2.1.6. Let (V, ρ) be the regular representation of G. Then, $g \neq e$, then $\forall h \in G, gh \neq h$. Thus, we have

$$\chi(g) = \begin{cases} 0, & g \neq e \\ |G|, & g = e \end{cases}$$

Example 2.1.7. Let $\rho : S_3 \to GL(V)$ be the regular representation. Then we have $V = W_1 \oplus W_2 \oplus U_1 \oplus U_2$ where W_1 is the trivial representation and W_2 is the sign representation. Let χ_1 be the character of W_1, χ_2 be of W_2, χ_3 of U_1 and χ_4 of U_4. Since $S_3 = \langle (12), (123) \rangle$, so it suffice to know what χ_i maps (12) and (123) to.

Remark 2.1.8. Let (V, ρ) be a representation of G. Then, for all $g, h \in G$, we have

$$\rho(hgh^{-1}) = \rho(g)\rho(h)\rho(g^{-1})$$

In particular, this gives us

$$Tr(\rho(ghg^{-1})) = Tr(h)$$

Thus, we have $\chi(ghg^{-1}) = \chi(h)$, i.e. χ is constant on the conjugacy classes.

Theorem 2.1.9. *[Schur's lemma] Let (V, ρ) and (W, τ) be two irreducible representations of G. Moreover, suppose $T \in Hom(V, W)$ such that $\forall g \in G$, we have $\tau(g) \circ T = T \circ \rho(g)$, note we call this T* ***intertwine****. Then T is isomorphism or $T = 0$. In particular, if $V = W$ and $\rho = \tau$, then T is a scalar multiple of the identity.*

Proof. If $T = 0$, then we are done.

Suppose $T \neq 0$. We first claim T is injective. Let $v \in Ker(T)$, then, for any $g \in G$, we have $T(\rho_g(v)) = \tau_g(T(v)) = \tau_g(0) = 0$. Thus, we have $\rho_g(v) \in Ker(T)$ and so $Ker(T)$ is G stable with respect to ρ. However, since ρ is irreducible, we have $Ker(T) = \{0\}$.

Next, we claim T is surjective. Let $v \in Range(T)$, say $v = T(x)$ for some $x \in V$. Then, $\forall g \in G$, we have $\tau_g(v) = \tau_g(T(x)) = T(\rho_g(x)) \in Range(T)$. Thus $Range(T)$ is G stable with respect to τ. Hence, $Range(T)$ must be W as τ is irreducible and T is non-zero.

Therefore, we indeed have T is isomorphism.

Now we suppose $V = W$ and $\rho = \tau$. Let $\lambda \in \mathbb{C}$ be an eigenvalue of T. Consider $T' = T - \lambda I$. Now, note that for $g \in G$, $\rho(g) \circ T' = T' \circ \rho(g)$. Since $Ker(T') \neq \{0\}$, we have T' cannot be isomorphism, and by what we have done, we must have $T' = 0$. Thus $T = \lambda I$ as desired. ♡

Corollary 2.1.9.1. *Let (V, ρ) and (W, τ) be two irreducible representations of G. Let $T \in Hom(V, W)$, then we let*

$$T' = \frac{1}{|G|} \sum_{g \in G} \tau(g)^{-1} \circ T \circ \rho(g)$$

Then, we have:

1. *If $T \neq 0$ then $\rho \cong \tau$ via T',*
2. *If $V = W$ and $\rho = \tau$, then $T' = \frac{Tr(T)}{dim(V)} I$*

Proof. We need to show T' is intertwine. We first note T' is linear. Then, for $h \in G$, we have

$$\begin{aligned}
\tau(h)T' &= \tau(h)\frac{1}{|G|}\sum_{g} \tau(g^{-1})T\rho(g) \\
&= \frac{1}{|G|}\sum_{g} \tau(hg^{-1})T\rho(g), \quad \text{let } t^{-1} = hg^{-1} \\
&= \frac{1}{|G|}\sum_{t} \tau(t^{-1})T\rho(th) \\
&= \frac{1}{|G|}\sum_{t} \tau(t^{-1})T\rho(t)\rho(h) \\
&= T'\rho(h)
\end{aligned}$$

If $W = V$ and $\rho = \tau$ then $T' = \alpha T$. Thus, we have

$$Tr(T') = \frac{1}{|G|} Tr(T) \cdot |G| = \alpha \cdot dim(V) \Rightarrow \alpha = \frac{Tr(T)}{dim(V)}$$

Thus, we have all the desired results. ♡

Remark 2.1.10. Now, let's say (V, ρ) and (W, τ) are both irreducible and $T : V \to W$ is linear. Let β be a basis of V and γ be a basis of W.

For $g \in G$, say $[\rho(g)]_\beta = (a_{ij}(g))$, $[\tau(g)]_\beta = (b_{kl}(g))$ and $[T]_\beta^\gamma = (x_{ki})$. Moreover, we let $[T']_\beta^\gamma = (x'_{ki})$. By matrix multiplication, we have

$$x'_{ki} = \frac{1}{|G|} \sum_g \sum_{j,l} b_{kl}(g^{-1}) x_{lj} a_{ji}(g)$$

If $\rho \ncong \tau$, then $T' = 0$. By viewing the RHS as a polynomial with x_{lj}, we have

$$\frac{1}{|G|} \sum_g b_{kl}(g^{-1}) a_{ji}(g) = 0 \tag{2.1}$$

for any k, l, i, j

If $\rho = \tau$, then $T' = \lambda I$ where $\lambda = \frac{Tr(T)}{dim(V)}$. Therefore, we have

$$\begin{aligned} x'_{kl} &= \frac{1}{|G|} \sum_g \sum_{j,l} b_{kl}(g^{-1}) x_{lj} a_{ji}(g) \\ &= \frac{1}{|G|} \sum_g \sum_{j,l} a_{kl}(g^{-1}) x_{lj} a_{ji}(g) \\ &= \lambda \delta_{ki} = \frac{1}{dim(V)} \sum_{j,l} \delta_{ki} \delta_{jl} x_{lj} \end{aligned}$$

By equating coefficients of x_{lj}, we have

$$\frac{1}{|G|} \sum_g a_{kl}(g^{-1}) a_{ji}(g) = \frac{1}{dim(V)} \delta_{ki} \delta_{jl} \tag{2.2}$$

Remark 2.1.11. Let G be a finite group, consider the vector space of all functions $\phi : G \to \mathbb{C}$. For any ϕ and ψ, we can define an ***inner product*** to be

$$\langle \phi, \psi \rangle := \frac{1}{|G|} \sum_{g \in G} \phi(g) \overline{\psi(g)}$$

In particular, χ_1, χ_2 are characters of G, then we have

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{|G|} \sum_g \chi_1(g) \overline{\chi_2(g)} = \frac{1}{|G|} \sum_g \chi_1(g) \chi_2(g^{-1})$$

Definition 2.1.12. If χ is the character of an irreducible representation, we say χ is ***irreducible***. If ρ and τ are isomorphic representations, we say χ_ρ and χ_τ are ***isomorphic***.

Remark 2.1.13. We remark that if two representations are isomorphic then their character is the same.

Theorem 2.1.14 (Orthogonality Relation I)**.**

1. *If χ is a irreducible character then*

$$\langle \chi, \chi \rangle = 1$$

2. *If χ_1 and χ_2 non-isomorphic irreducible characters of G then*

$$\langle \chi_1, \chi_2 \rangle = 0$$

Proof. We proof part one first. Say $[\rho(g)]_\beta = (a_{ij}(g))$ where ρ is an irreducible representation with character χ. Thus, we have

$$\begin{aligned}
\langle \chi, \chi \rangle &= \frac{1}{|G|} \sum_g \chi(g)\chi(g^{-1}) = \frac{1}{|G|} \sum_g \chi(g^{-1})\chi(g) \\
&= \frac{1}{|G|} \sum_g \sum_{i,j} a_{ii}(g^{-1}) a_{jj}(g) \\
&= \sum_{i,j} \left(\frac{1}{|G|} \sum_g a_{ii}(g^{-1}) a_{jj}(g) \right) \\
&= \sum_i \left(\frac{1}{|G|} \sum_g a_{ii}(g^{-1}) a_{ii}(g) \right), \text{ by equation (2.2)} \\
&= \sum_i \frac{1}{dim(V)} = 1, \text{ by equation (2.2)}
\end{aligned}$$

Then, we will show part two. Consider $\langle \chi_1, \chi_2 \rangle$. Then, we have

$$\begin{aligned}
\langle \chi_1, \chi_2 \rangle &= \frac{1}{|G|} \sum_g \chi_1(g)\chi_2(g^{-1}) \\
&= \frac{1}{|G|} \sum_g \sum_{i,j} a_{ii}(g) b_{jj}(g^{-1}) \\
&= \sum_{i,j} \left(\frac{1}{|G|} \sum_g a_{ii}(g) b_{jj}(g^{-1}) \right) \\
&= \sum_{i,j} 0 = 0, \text{ by equation (2.1)}
\end{aligned}$$

♡

Second Proof. Let χ_1 be of $\rho_1 : G \to GL(V)$ and χ_2 be of $\rho_2 : G \to GL(W)$ with basis $\{v_1, ..., v_m\}$ for V and $\{w_1, ..., w_n\}$ for W. Note for all $T \in Hom(U, U)$ where $U = span(u_1, ..., u_q)$ is $\mathbb{C}$ vector space (where $\{u_i\}$ is orthonormal basis) we have $Tr(T) = \sum_{i=1}^q \langle u_i, T(u_i) \rangle_U$ with the standard inner product on U. Observe that (we will omit the subscript(i.e. $\langle \cdot, \cdot \rangle_V$) for the inner product):

$$\begin{aligned}
\langle \chi_1, \chi_2 \rangle &= \frac{1}{|G|} \sum_g \chi_1(g)\overline{\chi_2(g)} \\
&= \frac{1}{|G|} \sum_{g \in G} Tr(\rho_1(g)) \cdot Tr(\rho_2(g^{-1})) \\
&= \frac{1}{|G|} \sum_{g \in G} \sum_{i=1}^{m} \sum_{j=1}^{n} \langle v_i, \rho_1(g)(v_i) \rangle \cdot \langle w_j, \rho_2(g^{-1})(w_j) \rangle \\
&= \frac{1}{|G|} \sum_{g \in G} \sum_{i=1}^{m} \sum_{j=1}^{n} \langle w_j, \overline{\langle v_i, \rho_1(g)(v_i) \rangle} \cdot \rho_2(g^{-1})(w_j) \rangle \\
&= \frac{1}{|G|} \sum_{g \in G} \sum_{i=1}^{m} \sum_{j=1}^{n} \langle w_j, \langle \rho_1(g)(v_i), v_i \rangle \cdot \rho_2(g^{-1})(w_j) \rangle
\end{aligned}$$

Note $W \otimes V^* \cong Hom(V, W)$ with $w \otimes f(v) = f(v)w$ and so $w \otimes f$ can be viewed as a linear operator from V to W. In particular, for each $v_0 \in V$, we can define $v_0* \in V^*$ to be $v_0^*(v) = \langle v, v_0 \rangle$ and so for each $w \in W$ and each $v_0 \in V$, we have $w \otimes v_0^*$ is a linear operator from V to W defined for all $v \in V$ by

$$(w \otimes v_0^*)(v) = \langle v, v_0 \rangle w$$

Next, note for each $1 \leq i \leq m$, $1 \leq j \leq n$, consider the linear operator $\rho_2(g^{-1})(w_j \otimes v_i^*)\rho_1(g)$ and we have

$$\begin{aligned}
\rho_2(g^{-1})(w_j \otimes v_i^*)\rho_1(g)(v) &= \rho_2(g^{-1})(\langle \rho_1(g)(v), v_i \rangle w_j) \\
&= \langle \rho_1(g)(v), v_i \rangle \cdot \rho_2(g^{-1})(w_j)
\end{aligned}$$

Therefore, we have

$$\begin{aligned}
\langle \chi_1, \chi_2 \rangle &= \frac{1}{|G|} \sum_{g \in G} \sum_{i=1}^{m} \sum_{j=1}^{n} \langle w_j, \langle \rho_1(g)(v_i), v_i \rangle \cdot \rho_2(g^{-1})(w_j) \rangle \\
&= \sum_{i=1}^{m} \sum_{j=1}^{n} \langle w_j, \frac{1}{|G|} \sum_{g \in G} \rho_2(g^{-1})(w_j \otimes v_i^*)\rho_1(g)(v_i) \rangle
\end{aligned}$$

We remark that for each fixed v_i, we have $w \otimes v_i^* : V \to W$ and so the linear operator $\frac{1}{|G|} \sum_{g \in G} \rho_2(g^{-1})(w_j \otimes v_i^*)\rho_1(g)$ is an intertwiner by Corollary 2.1.9.1.

Therefore, if $V \not\cong W$, we have

$$\langle \chi_1, \chi_2 \rangle = \sum_{i=1}^{m} \sum_{j=1}^{n} \langle w_j, \frac{1}{|G|} \sum_{g \in G} \rho_2(g^{-1})(w_j \otimes v_i^*)\rho_1(g)(v_i) \rangle = \sum_{i=1}^{m} \sum_{j=1}^{n} \langle w_j, 0 \rangle = 0$$

On the other hand, if $V \cong W$, then

$$\frac{1}{|G|} \sum_{g \in G} \rho_2(g^{-1})(v_j \otimes v_i^*)\rho_1(g) = \frac{Tr((v_j \otimes v_i^*))}{dim(V)} I$$

To see the trace of $v_j \otimes v_i^*$, note $(v_j \otimes v_i^*)(v_k) = \langle v_k, v_i \rangle v_j = \delta_{ki} v_j$ for all $1 \leq k \leq m$. If $i = j$ then we will have 1 non-zero entry on the diagonal, and the value is 1. If not, then the diagonal has all zero. Thus

$$\begin{aligned}
\langle \chi_1, \chi_1 \rangle &= \sum_{i=1}^{m} \sum_{j=1}^{m} \langle v_j, \frac{Tr((v_j \otimes v_i^*))}{dim(V)} v_i \rangle \\
&= \sum_{i=1}^{m} \sum_{j=1}^{m} \langle v_j, \frac{\delta_{ij}}{dim(V)} v_i \rangle \\
&= \sum_{i=1}^{m} \langle v_i, \frac{1}{dim(V)} v_i \rangle \\
&= \frac{\sum_{i=1}^{m} \langle v_i, v_i \rangle}{dim(V)} = \frac{dim(V)}{dim(V)} = 1
\end{aligned}$$

♡

Corollary 2.1.14.1. *Let $\rho : G \to GL(V)$ be a representation with character χ. Say $V = W_1 \oplus W_2 \oplus ... \oplus W_k$ is an irreducible decomposition of V. If $\tau : G \to GL(W)$ is an irreducible representation of G with character ϕ. Then, the number of W_i isomorphic to W(i.e. the number of ρ_i isomorphic to τ) is $\langle \chi, \phi \rangle$.*

Proof. Say $\chi = n_1\chi_1 + ... + n_l\chi_l$ where χ_i are pairwise non-isomorphic. Then, $\langle \chi, \chi_i \rangle = n_i$. In particular, ϕ could be isomorphic to any of χ_i so we are done. ♡

Corollary 2.1.14.2. *If two representations of a group G have the same character, then they are isomorphic.*

Proof. If they have the same character, then they have the same irreducible decomposition and we are done. ♡

Corollary 2.1.14.3. *Let (V, ρ) be a representation, and let χ be the character of ρ. We have $\langle \chi, \chi \rangle \in \mathbb{N}$ and $\langle \chi, \chi \rangle = 1$ if and only if χ is irreducible.*

Proof. Let $\chi_1, ..., \chi_k$ be all the distinct irreducible characters of G in χ. Then, we have $\chi = \sum n_i \chi_i$ where $n_i \in \mathbb{N}$. Then, we have $\langle \chi, \chi \rangle = n_1^2 + ... + n_k^2 \in \mathbb{N}$. Moreover, $\langle \chi, \chi \rangle = 1$ if and only if $k = 1$ and $n_1 = 1$ if and only if $\chi = \chi_1$ is irreducible. ♡

Remark 2.1.15. The above tells us that the irreducible decomposition of a representation is unique up to isomorphism of the irreducible components and re-ordering, i.e. there is only one way to decompose a representation up to isomorphism and re-ordering.

Proposition 2.1.16. *Every irreducible representation of G occurs as a subrepresentation of the regular representation of G with the multiplicity equal to its degree.*

Proof. Let χ be an irreducible character of G and χ_{reg} be the character of the regular representation of G.

Then, we have $\langle \chi, \chi_{reg} \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\chi_{reg}(g)} = \frac{1}{|G|}(\chi(e) \cdot \overline{\chi_{reg}(e)}) = \chi(e)$ where $\chi(e)$ is the degree of the regular representation. The proof follows. ♡

Corollary 2.1.16.1. *Let $\chi_1, ..., \chi_k$ be all the distinct irreducible representations of G. Say $deg(\chi_i) := \chi_i(e) = n_i$. Then, we have $\sum n_i^2 = |G|$ and for $g \neq 1$, we have $\sum_{i=1}^k n_i \chi_i(g) = 0$.*

Proof. We have $\chi_{reg} = n_1\chi_1 + ... + n_k\chi_k$. Plug in e, we have $\chi_{reg}(e) = |G| = n_1\chi_1(e) + ... + n_k\chi_k(e) = \sum n_i^2$.

Plug in $g \neq e$, then we have $\chi_{reg}(g) = 0 = \sum n_i \chi_i(g)$, the proof follows. ♡

Definition 2.1.17. Let G be a group. A function $f : G \to \mathbb{C}$ is called a ***class function*** if f is constant on each conjugacy class, i.e. $\forall a, b \in G, f(a) = f(bab^{-1})$.

Proposition 2.1.18. *Let $f : G \to \mathbb{C}$ be a class function, let $\rho : G \to GL(V)$ be a representation with character χ. Let $\rho_f = \sum_{g \in G} f(g)\rho(g)$, then ρ_f is linear on V. Moreover, if ρ is irreducible of degree n then $\rho_f = \lambda I$ where λ is equal $\frac{|G|}{n}\langle f, \overline{\chi}\rangle$.*

Proof. Let h be fixed in G. We have (note we used re-indexing at the second line)

$$\begin{aligned}
\rho_f \circ \rho(h) &= \sum_{g \in G} f(g)\rho(g)\rho(h) = \sum_{g \in G} f(g)\rho(gh) \\
&= \sum_{g \in G} f(hgh^{-1})\rho(hg) = \sum_{g \in G} f(g)\rho(h)\rho(g) \\
&= \rho(h) \circ \rho_f
\end{aligned}$$

Thus, we have ρ_f is intertwine and so $\lambda = \frac{Tr(\rho_f)}{n}$. However, we also have $Tr(\rho_f) = Tr(\sum_{g \in G} f(g)\rho(g)) = \sum_{g \in G} f(g)\chi(g) = |G|\langle f, \overline{\chi}\rangle$ and the proof follows. ♡

Proposition 2.1.19. *Let G be a group. The irreducible characters of G form an orthonormal basis for the vector space V of class functions on G.*

Proof. Let $\beta = \{\chi_1, ..., \chi_k\}$ be the irreducible characters of G. Then β is orthonormal hence linear independent.

Let $W = span(\beta)$, to show $W = V$, we will show $W^\perp = \{0\}$. Let $f \in W^\perp$, suppose $\rho : G \to GL(V)$ is irreducible. By Assignment 2, we have $\overline{\chi_1}, ..., \overline{\chi_k}$ are all irreducible characters of G. Thus $\rho_f = \sum_{g \in G} f(g)\rho_g = 0$ by above Proposition. Hence, by consider irreducible decomposition, we have $\rho_f = 0$ for all representations.

When ρ is the regular representation, we have

$$0 = \rho_f(v_e) = \sum_{g \in G} f(g)\rho_g(v_e) = \sum_{g \in G} f(g)v_g$$

where $\{v_g : g \in G\}$ is linear independent. This force $f(g) = 0$ for all $g \in G$. Thus f is the zero function and $W = V$ as desired. ♡

Corollary 2.1.19.1. *The number of irreducible characters is the number of conjugacy classes.*

Proof. Let $c_1, ..., c_k$ are the distinct conjugacy classes, then define

$$\phi_i(g) = \begin{cases} 1, g \in c_i \\ 0, g \notin c_i \end{cases}$$

for all $1 \leq i \leq k$. Clearly ϕ_i span the vector space of class functions and are linear independent. Hence, we must have this many (k) irreducible characters as well. ♡

Proposition 2.1.20 (Orthogonality Relation II). *Let G be a group and $g \in G$. Let O_g be the conjugacy class of g. Let $\chi_1, ..., \chi_k$ be all the irreducible characters of G. Then,*

1. $\sum_{i=1}^{k} |\chi_i(g)|^2 = \frac{|G|}{|O_g|}$
2. *If $h \notin O_g$ then* $\sum_{i=1}^{k} \chi_i(g)\overline{\chi_i(h)} = 0$

Proof. Let ϕ be the indicator function on O_g, i.e. $\phi(x) = 1$ if $x \in O_g$ and $x \notin O_g$ then $\phi(x) = 0$. Therefore, since ϕ is class function, we have

$$\phi = \sum_{i=1}^{k} \lambda_i \chi_i$$

where $\lambda_i = \langle \phi, \chi_i \rangle = \frac{1}{|G|} \sum_{x \in G} \phi(x)\overline{\chi_i(x)} = \frac{|O_g|}{|G|}\overline{\chi_i(g)}$

Therefore, we have

$$\phi(x) = \frac{|O_g|}{|G|} \sum_{i=1}^{k} \overline{\chi_i(g)}\chi_i(x)$$

Then, we have $\phi(g) = 1 = \frac{|O_g|}{|G|} \sum_{i=1}^{k} |\chi_i(g)|^2$ and if $h \notin O_g$ then $\phi(h) = 0$ and the proof follows. ♡

Remark 2.1.21. For character tables, we always have orthogonal columns, and if we list all elements of G on the top, we would have orthogonal row as well. This is due to orthogonality.

Example 2.1.22. The character table of S_3.

Solution. We know the number of degree 1 representations are 2, where $2 = [S_3, A_3]$. Moreover, the number of irreducible characters is equal 3 as we have three conjugacy classes, i.e. $\{e, (12), (123)\}$.

Moreover, we have $|S_3| = 1^2 + 1^2 + n_3^2$ so that $n_3 = 2$. Thus, we know the last irreducible representation must have degree 2.

	ε	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	a	b

Note the columns of character table are orthogonal so that we must have $a = 0$ and $b = -1$. ♠

Proposition 2.1.23. *G is abelian if and only if all irreducible representations of G has degree 1.*

Proof. Let G be abelian, then we have $|G|$ many non-isomorphic degree 1 representations. Since G has $|G|$ many conjugacy classes, the degree 1 representations are all the irreducible representations of G.

Suppose G is a group with all irreducible representations to be degree 1 representations, say we have k many of them. Then, we have $k = |G|$ many such degree 1 representations as $|G| = \sum_{i=1}^{k} 1^2 \Rightarrow k = |G|$. Thus G has $|G|$ many conjugacy classes, and so G is abelian. ♡

Proposition 2.1.24. *Let H be an abelian subgroup of G, then any irreducible representation of G has degree at most $[G : H]$.*

Proof. Let $p : G \to GL(V)$ be an irreducible representation of G. Consider the restriction $\tau : H \to GL(V)$, let $W \leq V$ be an irreducible subrepresentation of τ. Since H is abelian, we have $dim(W) = 1$. Say $W = span(x)$, let $W' = span(\{\rho_g(x) : g \in G\})$ so that V' is $G-$stable, then we have $V' = V$.

Take $g \in G$ and $h \in H$, we have $\rho_{gh}(x) = \rho_g(\rho_h(x)) = \alpha\rho_g(x)$ where $\alpha \in \mathbb{C}$. Say $g_1, ..., g_m$ are coset representatives of H in G, then

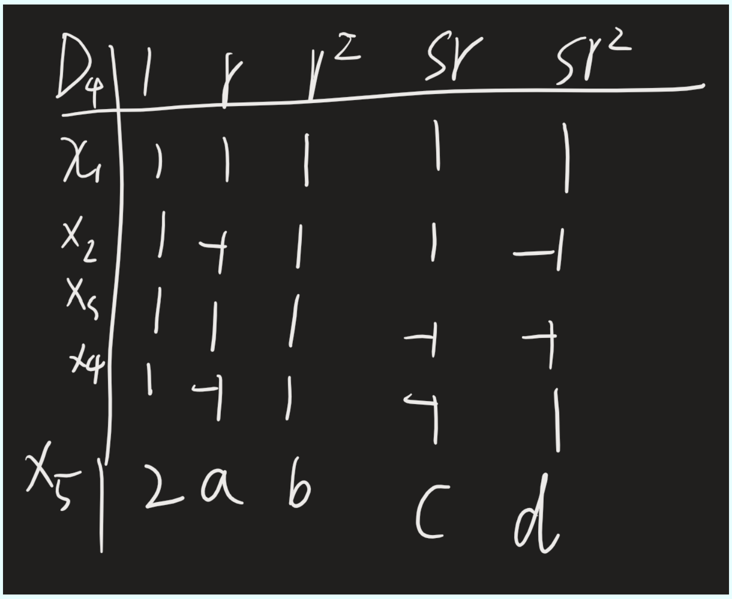
$$V = V' = span(\{\rho_{g_i}(x) : 1 \leq i \leq m\})$$

Therefore, we see $dim(V) \leq m = [G : H]$ and the proof follows. ♡

Example 2.1.25. Let's make the character table of D_4. Note $[D_4, \langle r^2 \rangle] = 4$, we know we have 4 degree 1 irreducibles.

Next, the conjugacy classes of D_4 are $[e], [r], [r^2], [s], [rs]$ and so there are five irreducible representations. In particular, note $1^2 + 1^2 + 1^2 + 1^2 + n^2 = 8$ and so $n = 2$ and so the last irreducible representation must be degree 2.

Hence, we get



D_4	1	r	r^2	sr	sr^2
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	1	1	1	-1	-1
χ_4	1	-1	1	-1	1
χ_5	2	a	b	c	d

Then, we have $1 - 1 + 1 - 1 + 2\overline{a} = 0$ and so $a = 0$. We have $4 + 2b = 0$ so $b = -2$ and $c = 0$ and $d = 0$.

Example 2.1.26. Let's make the character table of S_4. Note we have $[S_4 : A_4] = 2$ many degree one representations, i.e. the trivial one and the sgn representation.

Next, the conjugacy classes are

$$[e], [(12)], [(12)(34)], [(123)], [1234]$$

Thus the number of irreducible representations is equal 5. Thus we have

$$24 = 1^2 + 1^2 + n_3^2 + n_4^2 + n_5^2 \Rightarrow n_3^2 + n_4^2 + n_5^2 = 22$$

Hence, the only possibilities is $n_3 = 2, n_4 = n_5 = 3$. Therefore,

S_4	e	(12)	$(12)(34)$	(123)	(1234)
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	2				
χ_4	3		?		
χ_5	3				

Let $K = \{e, (12)(34), (13)(24), (14)(23)\} \trianglelefteq S$, $H = \{1, (12), (13), (123), (132), (23)\}$ and we have

$$S_4 = KH$$

where $H \cong S_3$.

Let ρ be an irreducible representation of H of degree 2. Recall from Example 2.1.22, we have the character of ρ to be α_3 to be $e \mapsto 2, (12) \mapsto 0$ and $(123) \mapsto -1$. Then, we extend ρ to a representation of S_4 by $\rho(kh) := \rho(h)$, we have this is irreducible representation of S_4. To see this is homomorphism, we have $\rho(k_1h_1k_2h_2) = \rho(k_1k_2'h_1h_2)$ since $K \trianglelefteq S_4$ and then we indeed have ρ is irreducible representation. Hence, we know $\chi_3((12)) = 0$ just like in H and $\chi_3((123)) = -1$. In addition, we note $\rho((12)(34)) = \rho((12)(34) \circ e) = \rho(e)$ and so $\chi_3((12)(34)) = 2$, which is the degree of the representation. Similarly, we have

$$\rho((1234)) = \rho((14)(13)(12)) = \rho((14)(23)(23)(13)(12)) = \rho((14)(23) \circ (13)) = \rho(13)$$

Thus $\chi_3((1234)) = 0$.

Next, if τ is corresponds to χ_4, then consider $sgn \otimes \tau$, this is a different irreducible degree three representation, and we must have the following. Note we know a and d are not 0 because the column must add up to 4 for the second column. We know a must be real because we must have $(12)^2 = e$ so $\rho((12))$ must have real eigenvalues. In general, if $g^2 = 1$, then $\chi(g) \in \mathbb{R}$ for all group G and $g \in G$. This is because $\chi(g) = Tr(\rho_g) = \sum \lambda_i$ where each $\lambda_i = \pm 1$.

S_4	e	(12)	$(12)(34)$	(123)	(1234)
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	2	0	2	-1	0
χ_4	3	a	b	c	d
χ_5	3	$-a$	b	c	$-d$

$\to \chi_2 \otimes \chi_4$ by ass 2

We have $1+1+4+6b=0$ and $1+1-2+6c=0$ and hence $b=-1$ and $c=0$.

On the other hand, to compute a and d, we have $1^2+(-1)^2+0^2+a^2+(-a)^2=2+2a^2$ and this must equal to $\frac{|S_4|}{|O_{(12)}|}=\frac{4!}{6}=4$. Hence, we have $a^2=1$ and so $a=\pm 1$. Suppose $a=1$.

Then, with column 2 and column 5, we get $1+1+0+d+d=0$ and so $d=-1$.

Remark 2.1.27. THIS IS THE END OF TEST 1 MATERIALS.

Next Friday, 1:30-2:20, MC 2034. Assigned seating.

4 questions worth 5 marks.

1. Computation, assignment type (2 parts)
2. Character theory
3. A character table
4. A new proof

Chapter 3

Induced Representations

3.1 Intro

Remark 3.1.1. Given a subgroup $H \le G$ and a representation $\rho : H \to GL(V)$ construct a representation of G.

Let $H \le G$ and $\rho : H \to GL(V)$ be a representation. Say the cosets of H in G are $g_1 H, ..., g_m H$ where $m = [G : H]$.

For each i, let $g_i V = \{g_i v : v \in V\}$ be an isomorphic copy of V, then let $W = \bigoplus_{i=1}^{m} g_i V$ so that every $w \in W$ can be uniquely written as $w = g_1 v_1 + g_2 v_2 + ... + g_m v_m$ where each $g_i v_i \in g_i V$.

Fix $g \in G$, then there exists $\pi \in S_m$ such that for every i, we have $g g_i = g_{\pi(i)} h_i$ where $h_i \in H$. We then define the induced representation from H to G by ρ, write as $Ind_H^G(\rho) : G \to GL(W)$, to be

$$Ind_H^G(\rho)(g)(\sum g_i v_i) = \sum g_{\pi(i)} \rho(h_i) v_i$$

One should check this is actually a representation of G.

Definition 3.1.2. Remark 3.1.1 defines the induced representation.

Example 3.1.3. Consider $H := \{e\} \le G$ and $\rho : \{e\} \to GL(\mathbb{C})$ be the trivial representation. Let $G = \{g_1, ..., g_n\}$, we have $g_1, ..., g_n$ are coset representatives of $G/\{e\}$. Fix $g \in G$, we note $g g_i e = g g_i$ where $g_{\pi(i)} = g g_i$. Thus, we get

$$Ind(\rho)_g(\sum g_i \alpha_i) = \sum g g_i \rho(1)(\alpha_i) = \sum g g_i \alpha_i$$

We note $Ind(\rho)$ is isomorphic to the regular representation via the mapping $v_{g_i} \to g_i \cdot 1$

Example 3.1.4. Consider $\langle r \rangle \le D_n$. Let $\rho : \langle r \rangle \to GL(\mathbb{C})$, we map $\rho_r(1) = \zeta_n$ where $\zeta_n = e^{\frac{2\pi i}{n}}$. Then, we have the coset representatives to be e and s.

Consider $r \in D_n$, we have $re = er$ and $rs = sr^{-1}$. Consider $W = e\mathbb{C} \oplus s\mathbb{C}$. Then, we have

$$Ind(\rho) : D_n \to GL(W)$$

where

$$\begin{aligned} Ind(\rho)_r(e\alpha_1 + s\alpha_2) &= e\rho_r(\alpha_1) + s\rho_{r^{-1}}(\alpha_2) \\ &= e\zeta_n\alpha_1 + s\zeta_n^{n-1}\alpha_2 \end{aligned}$$

On the other hand, consider $s \in D_n$, we have $se = se$ and $ss = ee$. Then,

$$\begin{aligned} Ind(\rho)_s(\epsilon\alpha_1 + s\alpha_2) &= s\rho_e(\alpha_1) + e\rho_e(\alpha_2) \\ &= s\alpha_1 + e\alpha_2 \end{aligned}$$

Now, consider a basis $\beta = (\epsilon \cdot 1, s \cdot 1)$ for W, we have

$$[Ind(\rho)_r]_\beta = \begin{bmatrix} \zeta_n & 0 \\ 0 & \zeta_n^{n-1} \end{bmatrix}$$

and

$$[Ind(\rho)_s]_\beta = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Example 3.1.5. Let $\langle r \rangle \leq D_5$. Let $\rho : \langle r \rangle \to GL(\mathbb{C})$ such that $\rho_r(1) = \zeta_5$, and let $Ind(\rho)$ be just like Example 3.1.4. Then, we have $Ind(\rho)_r = \begin{bmatrix} \zeta_5 & 0 \\ 0 & \zeta_5^4 \end{bmatrix}$ and $Ind(\rho)_s = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Note the conjugacy classes of D_5 is $\{e\}, \{r, r^4\}$, $\{r^2, r^3\}$, and $\{s, sr, sr^2, sr^3, sr^4\}$. Let χ be the character of $Ind(\rho)$. Thus, we have

$$\begin{aligned} \langle \chi, \chi \rangle &= \frac{1}{10}(|\chi(e)|^2 + 2|\chi(r)|^2 + 2|\chi(r^2)| + 5|\chi(s)|^2) \\ &= \frac{1}{5}(2 + \zeta_5^2 + \zeta_5^3 + 2 + \zeta_5^2 + \zeta_5 + 2) \\ &= \frac{1}{5}(6 + \zeta_5^4 + \zeta_5^3 + \zeta_5^2 + \zeta_5^1) \\ &= \frac{1}{5}(6 - 1) = 1 \end{aligned}$$

Example 3.1.6. We now compute the character table of D_5. Consider

D_5	1	r	r^2	s
χ_1	1	1	1	1
χ_2	1	1	1	-1
χ_3	2	$\zeta_5+\zeta_5^4$	$\zeta_5^2+\zeta_5^3$	0
χ_5	2	$\underline{x}$	$\underline{y}$	0

$$\Rightarrow \quad 1+1+2(\zeta_5+\zeta_5^4)+2x=0$$

$$\Rightarrow \quad x=-1-\zeta_5-\zeta_5^4$$

$$x=\zeta_5^2+\zeta_5^3$$

and the same for $y=\zeta_5+\zeta_5^4$

Chapter 4

Module Theory

4.1 Intro

Remark 4.1.1. Let R be a ring (always unital, not always commutative).

Definition 4.1.2. A ***(left) R-module*** is an abelian group $(M,+)$ equipped with an $R-$action $\cdot : R \times M \to M$ such that for all $r_1, r_2, r \in R$ and $m, m_1, m_2 \in M$,

1. $1m = m$
2. $r(m_1 + m_2) = rm_1 + rm_2$
3. $(r_1 + r_2)m = r_1 m + r_2 m$
4. $(r_1 r_2)(m) = r_1(r_2 m)$

Example 4.1.3.
1. Let F be a field, then M is a $F-$module if and only if M is a $F-$vector space.
2. M is a $\mathbb{Z}$-module if and only if M is an abelian group.
3. R is a $R-$module with the action left multiplication.
4. Let I be a left ideal of R, then I is a $R-$module with the left multiplication.
5. Let $R = M_n(\mathbb{F})$ and $V = \mathbb{F}^n$, then V is a R-module with matrix action.
6. Let I be a left ideal of R, consider $R/I = \{a + I := \overline{a} : a \in R\}$, in this case, R/I is a R-module with the action $r \cdot \overline{a} = \overline{ra}$. Note R/I may not be a ring as we may not have I be a two sided ideal.

Definition 4.1.4. Let M be a R-module, we say a subgroup $(N,+)$ of $(M,+)$, write as $N \leq M$, is an ***R-submodule*** of M if $rn \in N$ for all $r \in R$, $n \in N$.

Definition 4.1.5. Suppose $N \leq M$ where M is R-module, then with $M/N = \{m+N : m \in M\}$, we define $(a+N)+(b+N) = (a+b)+N$ and $r(m+N) = rm+N$ is the quotient module.

Definition 4.1.6. Let $G = \{g_1, ..., g_n\}$ be a finite group, let F be a field, we define the group algebra (or group ring), denoted as $F[G]$, to be

$$F[G] = \{\sum_{i=1}^{n} \alpha_i g_i : \alpha_i \in F\}$$

equipped with

$$\sum \alpha_i g_i + \sum \beta_i g_i = \sum (\alpha_i + \beta_i) g_i$$

and

$$\alpha g_i \cdot \beta g_j = \alpha\beta g_i g_j$$

and extend by distributivity.

Example 4.1.7. Let M be a $\mathbb{C}[G]$-module. Then, it is also a $\mathbb{C}$-module. Indeed, consider the action of $\mathbb{C}$ as following: let $c \in \mathbb{C}$, then we define $c \cdot w = (ce) \cdot_a w$ where $\cdot_a$ is the action of the element ce, e being the group identity of G, on $w \in W$. In this case, let $\rho : G \to GL(W)$, where W be considered as a $\mathbb{C}$-module (i.e. a vector space since $\mathbb{C}$ is a field), to be $\rho_g(m) = gm$, where we consider $g \cdot m$ as an element in $\mathbb{C}[G]$ acts on the module. Then, this defines a valid group representation.

Indeed, ρ_g is linear, we have $\rho_g(c_1 m_1 + m_2) = gc_1 m_1 + gm_2 = c_1 g m_1 + g m_2 = c_1 \rho_g(m_1) + \rho_g(m_2)$ and clearly it is a homomorphism.

Conversely, let $\rho : G \to GL(V)$ be a representation, then V is a $\mathbb{C}[G]$-module given by the action

$$\alpha g \cdot v = \alpha \rho_g(v) = \rho_g(\alpha v)$$

Hence, we established an correspondence between $\mathbb{C}[G]$-modules and representations of G.

Remark 4.1.8. Let M be a $\mathbb{C}[G]$-module, corresponding to representation ρ. Say $N \leq M$ is a submodule of M, then for all

$$g \in G, \alpha \in \mathbb{C}, \alpha g \cdot n \in N \iff \alpha \rho_g(n) \in N \iff \rho_g(\alpha n) \in N$$

Thus, N is a subspace of M which is $G-$stable.

Definition 4.1.9. Let N, M be R-module, we say $\phi : N \to M$ is a ***(module) homomorphism*** if $\forall v \in R, \forall n_1, n_2 \in N$, we have

$$\phi(n_1 + n_2) = \phi(n_1) + \phi(n_2)$$

and

$$\phi(rn_1) = r\phi(n_1)$$

Definition 4.1.10. A homomorphism $\phi : M \to M$ is called an ***endomorphism***. The set of endomorphisms of R-module M, $End_R(M)$, is a ring under addition and composition.

Remark 4.1.11. Let $\phi : N \to M$ be a homomorphism, where N, M are $\mathbb{C}[G]$-modules. Say M corresponds to representation ρ and N correspondss to representation τ, and write $M \sim \rho$ and $N \sim \tau$. Then, we have

$$\phi(gn) = g\phi(n) \Leftrightarrow \phi(\rho_g(n)) = \tau_g(\phi(n)) \Leftrightarrow \phi \circ \rho_g = \tau(g) \circ \phi$$

Therefore, a module homomorphism is an intertwiner.

Example 4.1.12. Let $\rho : G \to GL(V)$ be the regular representation. Let V be the span of $\{v_g, g \in G\}$. Think V as a $\mathbb{C}[G]$ module, with $g \cdot v_h = v_{gh}$. Then via the module isomorphism $v_g \mapsto g$, we have $V \cong \mathbb{C}[G]$.

4.2 From Representation to Module

Remark 4.2.1. When is $\rho : G \to GL(V)$ a faithful (injective) representation? We must have trivial kernel, thus we have

$$\begin{aligned} &\rho(g) \text{ is faithful} \\ \iff &\rho(g) = I \text{ iff } g = e \\ \iff &(\forall v, \rho_g(v) = \rho_e(v)) \text{ iff } g = 1 \\ \iff &(\forall v, g \cdot v = e \cdot v) \text{ iff } g = 1 \\ \iff &\forall v, (g - e) \cdot v = 0 \text{ iff } g - e = 0 \end{aligned}$$

Definition 4.2.2. Let M be an $R-$module, the ***annihilator*** of M is

$$Ann(M) = \{r \in R : \forall m, rm = 0\}$$

Definition 4.2.3. Let M be an R-module, we say M is ***faithful*** if $Ann(M) = \{0\}$.

Proposition 4.2.4. *Let M be an R-module, then $Ann(M)$ is a 2-sided ideal of R. Moreover, M is a faithful $R/Ann(M)$-module.*

Proof. Easy to show it is a two-sided ideal. Indeed, let $x \in R$, then $\forall m \in M, xrm = x(0) = 0$ and $rxm = r(xm) = 0$ as $xm \in M$.

Next, consider the action of $R/Ann(M)$ on M to be $\overline{r} \cdot m = rm$. We should see it is a vaild module indeed. ♡

Definition 4.2.5. Let M be a R-module, we say M is ***irreducible*** if $M \neq \{0\}$ and the only submodule of M are $\{0\}$ and M.

Definition 4.2.6. A ***division ring*** is a unital ring such that every non-zero elements is invertible.

Theorem 4.2.7 (Schur's Lemma Ver. 2)**.** *Let M be an irreducible R-module. Then $End_R(M)$ is a division ring.*

Proof. Let $\phi \in End_R(M)$ and suppose $\phi \neq 0$. Then $Range(\phi) = M$ and $Ker(\phi) = \{0\}$ by irreducibility, thus ϕ must be invertible. Thus $End_R(M)$ is indeed a division ring. ♡

Theorem 4.2.8 (First Isomorphism Theorem)**.** *Let M, N be R-modules and let $\phi : M \to N$ be a module homomorphism, then $M/Ker(\phi) \cong \phi(M) \leq N$.*

Proof. Immediately by First Isomorphism Theorem from PMATH 347. ♡

Proposition 4.2.9. *If M is an irreducible R-module, then $M \cong R/I$ where I is an maximal left ideal of R. Conversely, if I is a maximal left ideal then R/I is irreducible.*

Proof. Let M be a irreducible R-module. Fix $0 \neq m \in M$ and define $\phi : R \to M$ by $\phi(r) = rm$. Then ϕ is a module homomorphism, and by First Isomorphism Theorem, we have $R/I \cong \phi(R) \leq M$ where $I = Ker(\phi)$, however $\phi(R)$ cannot be empty (think $\phi(1) = 1m = m$), so $\phi(R) = M$ by irreducibility of M.

Thus, we are left to check that I is maximal. Let J be an left ideal of R such that $I \subsetneq J \subseteq R$. Now, $\phi(J) \leq M$ and $\phi(J) \neq 0$ as J cannot be the kernel. Thus $\phi(J) = M$. In particular, there exists $x \in J$ such that $\phi(x) = xm = m$. Thus $(x-1)m = 0$ and so $x - 1 \in Ker(\phi) = I \subseteq J$. Hence $1 \in J$ and so $J = R$. ♡

4.3 The Jacobson Radical

Definition 4.3.1. Let R be a ring, the ***Jacobson radical*** of R is

$$J(R) = \bigcap_{M \in \mathcal{M}} Ann(M)$$

where $\mathcal{M}$ is the collection of all irreducible left modules of R.

Definition 4.3.2. A left ideal I of R is called ***left quasiregular*** if $\forall a \in I$, $R(1+a) = R$.

Theorem 4.3.3. *Let R be a ring, then the following are equivalent:*

1. $a \in J(R)$
2. *Ra is left quasiregular*
3. *$a \in \bigcap_{I \in \mathcal{I}} I$ where $\mathcal{I}$ is the collection of all the maximal left ideals of R*

Proof. We first show $1 \Rightarrow 2$.

Let $a \in J(R)$ and for contradiction, assume for some $x \in R$, we have $R(1+xa) \neq R$. Thus, there exists a maximal left ideal I such that $R(1+xa) \subseteq I$. Thus R/I is an irreducible R-module. Thus, $a(R/I) = \{0\}$ as we recall a annihilates all irreducible left modules. In particular, $a \cdot \overline{1} = \overline{a} = \overline{0}$ and hence $a \in I$ imply $xa \in I$ as I is an left ideal and so $1 \in I$ as $1 + xa \in I$ and thus we obtained a contradiction.

Then, we show $2 \Rightarrow 3$.

Assume Ra is left quasiregular. Assume for a contradiction that there exists a maximal left ideal I such that $a \notin I$. Again, we have R/I is irreducible. Then, $(I + Ra)/I$ is a submodule of R/I. In particular, note $(I + Ra)/I$ is not empty so by irreducibility, we have $(I + Ra)/I = R/I$ and hence, there exists $x \in R$ such that $\overline{x} \cdot \overline{a} = \overline{-1}$ and hence $\overline{1} + \overline{xa} = \overline{0}$ and hence $1 + xa \in I$. Thus $I = R$ as Ra is left quasiregular imply $1 + xa$ is a unit, we get a contradiction.

We show $3 \Rightarrow 1$.

Assume $A = \bigcap_{I \in \mathcal{I}} I$. Assume there exists an irreducible module M such that $AM \neq \{0\}$ for a contradiction. Hence, there exists $0 \neq m \in M$ such that $Am \neq \{0\}$.

Note that Am is a left R-submodule of M. Therefore, we have $Am = M$. Hence, there exists $a \in A$ such that $am = -m$. Thus $am + m = 0$ and then $(a+1)m = 0$. Note if $1+a$ is left-invertible, then m must be zero[1], a contradiction. If $1+a$ is a not left invertible, then it is in a maximal left ideal[2], then $1+a-a$ is in that maximal ideal as well as a is in all left maximal ideal. Therefore we have a contradiction as every maximal ideal must be proper.

♡

Remark 4.3.4. We have

$$J(R) = \bigcap_{M \in \mathcal{M}} Ann(M) = \bigcap_{I \in \mathcal{I}} I = \sum_{a \in \mathcal{R}} Ra$$

where $\mathcal{R}$ is the subset of R such that $a \in \mathcal{R}$ imply Ra is left-quasiregular.

Remark 4.3.5. Let $a \in J(R)$ and $x \in R$. Suppose $R(1+ax) \neq R$. Then $R(1+ax) \subseteq I$ where $I \in \mathcal{I}$. Thus R/I is irreducible. Hence, we have $a(x+I) = a\overline{x} = \overline{ax} = \overline{0}$ by definition of annihilator. Therefore, we have $ax \in I$ and so $1 \in I$ and so a contradiction. Therefore, we have $R(1+ax) = R$, i.e. we have $a \in J(R)$ then aR is left quasiregular.

Remark 4.3.6. Take $a \in J(R)$, then there exists $b \in R$ such that $b(1+a) = -a$ as $a \in Ra$ where Ra is left quasiregular and $R(1+a) = R$. Therefore, we have $a + b + ba = 0$. Thus, $b \in J(R)$ as $a, ba \in J(R)$.

In particular, we have $c(1+b) = -b$ and so $b + c + cb = 0$. Then, by multiply c from left on $a + b + ba = 0$ and a from right on $b + c + cb = 0$, we get

$$ca + cb + cba = 0, ba + ca + cba = 0$$

Subtract one equation with another, we get $cb = ba$ and so $a + b = b + c$ and so $a = c$.

Therefore, we have $(1+a)b = b + ab = b + cb = -c = -a$. Hence, we have $(1+a)b = -a$ and so

$$(1+a)R = R$$

Indeed, note $b \in R$ so $(1+a)b = -a \in (1+a)R$. In addition, we have $1+a \in (1+a)R$ so $1 + a - a = 1 \in (1+a)R$ and so $(1+a)R = R$ as $(1+a)R$ is an right ideal.

Therefore, we have $J(R)$ is the sum of right quasiregular aR. By the exact same proof, we would get $J(R) = \cap I = \cap Ann(M)$ where this time we are intersecting maximal right ideals and annihilator of irreducible right submodules.

Hence, we have $J(R)$ is two-sided ideal.

Remark 4.3.7. We also see that since $Ann(M)$ is two-sided ideals of R, so that $J(R) = \cap Ann(M)$ must also be two-sided ideal.

Definition 4.3.8. A ring is ***semiprimitive*** if $J(R) = \{0\}$.

---

[1] if $1+a$ is a unit, say $y(1+a) = 1$, then $y(1+a)m = y0 = 0$ so that $1m = m = 0$, hence $m = 0$

[2] It can form a proper left ideal, and hence contained in a left maximal ideal

Example 4.3.9.

1. $J(\mathbb{Z}) = \bigcap_{p \text{ be prime}} \langle p \rangle = \{0\}$
2. $J(F[[x]]) = \langle x \rangle$
3. $J(\mathbb{Z}_{12}) = \langle 2 \rangle \cap \langle 3 \rangle = \langle 6 \rangle$

Definition 4.3.10. Let R be a ring, we say $a \in R$ is ***nilpotent*** if $\exists n \in \mathbb{N}$ such that $a^n = 0$.

Definition 4.3.11. An ideal (left, right, or both) is ***nil*** if every element is nilpotent.

An (left,right, or both) ideal I is ***nilpotent*** if there exist $n \in \mathbb{N}$ such that $I^n = \{0\}$, i.e. $\forall a_1, ..., a_n \in I$, we have $a_1 a_2 ... a_n = 0$.

Proposition 4.3.12. *Every nil left ideal of R is contained in $J(R)$.*

Proof. Let I be nil and $a \in I$, we will show $(1 + a)$ is left invertible. Note we have $a^n = 0$ and so

$$(1 + a)(1 - a + a^2 - a^3 + ... + (-1)^{n-1} a^{n-1}) = (1 - a + ... + (-1)^{n-1} a^{n-1})(1 + a) = 1$$

Thus Ra is left quasiregular as $Ra \subseteq I$ where I is a left ideal and so $I \subseteq J(R)$ as desired. ♡

Proposition 4.3.13. *We have $J(R/J(R)) = \{0\}$, i.e. $R/J(R)$ is semiprimitive.*

Proof. Consider $J(R/J(R))$, and we have this is the intersection of $I/J(R)$ where I is maximal in R and $J(R) \subseteq I$. This is the same as the intersection of $\frac{I}{J(R)}$ where I is maximal in R. Indeed, this is because $J(R) \subseteq I$ for all maximal left ideal I by definition.

Therefore, we have $J(R/J(R)) = \frac{J(R)}{J(R)} = \{0\}$ as desired. ♡

4.4 Artin-Wedderburn Theory and the Fore-play

Definition 4.4.1. A ring R is (left) ***Artinian*** if whenever $I_1 \supseteq I_2 \supseteq I_3 \supseteq ...$ is a descending chain of left ideals then there exists $N \in \mathbb{N}$ such that $I_k = I_N$ for all $k \geq N$.

Equivalently, R is Artinian if every non-empty set of left ideal has a minimal element.

Example 4.4.2. $\mathbb{Z}$ is not Artinian, as we have $\langle 2 \rangle \supseteq \langle 4 \rangle \supseteq \langle 8 \rangle \supseteq ....$

Remark 4.4.3. We will assume the following fact without proof it.

We have R is Artinian then $M_n(R)$ Artinian. It is easy to see when we are working with commutative rings. Indeed, we have I be an ideal of $M_n(\mathbb{R})$ then $I = M_n(I')$ where I' is ideals of R.

We also have Artinian is stronger than Noetherian, i.e. Artinian imply Noetherian.

Definition 4.4.4. Let F be a field, a ***F-algebra*** is a ring R with bilinear scalar multiplication, i.e. $\alpha(ab) = (\alpha a)b = a(\alpha b)$.

Example 4.4.5.
1. Division rings are Artinian.
2. Let R be a F-algebra where F is a field with $dim_F(R) < \infty$, then R is Artinian. Indeed, if we have a descending chain, then the dimension is finite so it can only drop so much.
3. Let F be a field and G be a finite group. Then, we have $F[G]$ is Artinian, as we have $dim_F(F[G]) = |G| < \infty$.

Proposition 4.4.6. *If R is Artinian then $J(R)$ is nilpotent.*

Proof. Let $J = J(R)$. Consider $J \supseteq J^2 \supseteq J^3 \supseteq ....$ Thus, there exists N such that $J^k = J^N$ for $k \geq N$.

Let $I = J^N$, we claim $I = \{0\}$. Suppose $I \neq \{0\}$, let A be a minimal left ideal of R such that $IA \neq \{0\}$ (we can do this by Artinian property by taking the collection of left ideals $\{IL\}$ such that IL is not zero, then it must exists a minimal element).

Let $a \in A$ such that $Ia \neq \{0\}$, note Ia is a left ideal. Then, we have $I(Ia) = I^2a = Ia \neq 0$. By minimality, we have $Ia \subseteq A$ and hence $A = Ia$. Thus there exists $x \in I$ such that $a = xa$. Therefore, $(1 - x)a = 0$ where $1 - x$ must be left invertible as $x \in J(R)$. Hence $a = 0$, which is a contradiction. ♡

Theorem 4.4.7. *[Maschke's Theorem] Let G be a finite group. If F is a field with characteristic is 0 or p such that $p \nmid |G|$, then $F[G]$ is semiprimitive and Artinian*[3].

Proof. Since $\dim_F(F[G])$ is finite, we have $F[G]$ is Artinian. We will show it is semiprimitive. We will show $F[G]$ does not have nil ideals.

For a contradiction, suppose I is a non-zero nil ideal of $R := F[G]$. Take $0 \neq x \in I$, thus $x = \sum_{g \in G} a_g g$ where $a_h \neq 0$ for some $h \in G$. By multiply h^{-1}, we may assume $a_e \neq 0$.

For each $a \in F[G]$, define $T_a : F[G] \to F[G]$ by $T_a(v) = av$, this is a F linear operator and observe that $T_x = \sum a_g T_g$. However, note $Tr(T_x) = \sum a_g Tr(T_g)$, where if we fix the basis to be G, then we have $g \neq e$ then $Tr(T_g) = 0$ and $Tr(T_e) = |G|$. Thus, we have $Tr(T_x) = a_1|G| \neq 0$ as $char(F) = 0$ or $char(F) \nmid |G|$.

Since the trace is not 0, then T_x is not nilpotent linear operator. Therefore, we cannot possibly have x to be nilpotent, and the contradiction follows.

Thus, since R has no non-zero nil ideals and $J(R)$ is nilpotent(hence nil), we must have $J(R) = \{0\}$. ♡

Definition 4.4.8. A ring R is ***primitive*** if it has a faithful irreducible module.

Remark 4.4.9. We note primitive imply semiprimitive as we have $Ann(M) = \{0\}$ so the intersection of all $Ann(M)$ must be $\{0\}$.

[3] A R-module M is semiprimitive and Artinian if and only if M is semisimple

Example 4.4.10. 1. Let D be a division ring, then $M_n(D)$ is primitive with the module D^n. We can see this is faithful and irreducible.

2. Let R be primitive and commutative. Consider a faithful and irreducible module M, then $M \cong R/I$ for some maximal ideal I. However, note $IM = \{0\}$, and since M is faithful, we have I must be 0. Thus R must be a field.

Definition 4.4.11. A ring R is ***simple*** if R is not zero and R has no proper non-zero (two-sided) ideals.

Example 4.4.12. $M_n(D)$ is simple where D is simple. Consider $J \trianglelefteq M_n(D)$, then $J = M_n(I)$ for some ideal $I \trianglelefteq D$. Thus $I = D$ or $I = 0$, and so $J = M_n(D)$ or $J = 0$.

Remark 4.4.13. We have R is irreducible imply R is simple. Indeed, no left ideal imply no two-sided ideal.

The converse is false. Consider $M_2(\mathbb{R})$, we have $M_2(\mathbb{R})$ is simple, but $I = \{\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} : a, b \in \mathbb{R}\}$ is a non-zero left ideal.

Proposition 4.4.14. *Every simple ring is primitive.*

Proof. Let R be simple, we will show R is primitive, thus we need to find a faithful and irreducible R-module.

Let I be a maximal left ideal of R so that $M := R/I$ is irreducible. We have M is faithful as $Ann(M)$ is an two-sided ideal of R and $Ann(M) \neq R$, we must have $Ann(M) = \{0\}$ by simplicity. ♡

Definition 4.4.15. In the following, we are going to use the following notations to mean the following things.

Let R be primitive and M be faithful and irreducible. Then $D := End_R(M)$ is a division ring by Schur's lemma. Then, M is a D-module by a action via evalueation mapping, i.e. $\phi \in D$ then define the action $\phi \cdot m = \phi(m)$.

We say R ***acts densely*** on M if for all D-linearly independent $v_1, v_2, ..., v_n \in M$ and all $w_1, w_2, ..., w_n \in M$, there exists $r \in R$ such that $rv_i = w_i$ for $i = 1, 2, ..., n$.

Remark 4.4.16. In addition to above convention, assume $dim_D(M) < \infty$. Say R acts densely on M. Then, note $\{v_1, ..., v_n\}$ is a D-basis. Thus, $\forall w_1, ..., w_n \in M$, there exists $r \in R$, we have $rv_i = w_i$. Thus, r is the same as $T : M \to M$ given by $T(v_i) = w_i$, and so

$$R \cong \{T : M \to M : T \text{ is D-linear}\} \cong M_n(D)$$

Lemma 4.4.17. *If for every finite dimensional D-subspace V of M and every $m \in M \backslash V$ there exists $r \in R$ such that $rV = \{0\}$ but $rm \neq 0$ then R acts densely on M.*

Proof. Assume the above hypothesis. Let $v_1, v_2, ..., v_n$ be D-linearly independent in M. Also, let $w_1, ..., w_n$ be arbitrary in M.

For each $1 \leq i \leq n$, let

$$V_i = span(v_1, ..., v_{i-1}, v_{i+1}, ..., v_n)$$

Then, by our assumption, there exists $t_i \in R$ such that $t_i V_i = \{0\}$ but $t_i v_i \neq 0$.

Observe that $Rt_i v_i = M$ as $t_i v_i$ is not 0 and M is irreducible. Therefore, there exists $r_i \in R$ such that $r_i t_i V_i = \{0\}$ and $r_i t_i v_i = w_i$. Let

$$t = r_1 t_1 + ... + r_n t_n$$

and so we have

$$t v_i = r_i t_i v_i = w_i$$

♡

Theorem 4.4.18 (Jacobson Density Theorem)**.** *R acts densely on M. Note R and M is followed by our convention 4.4.15*

Proof. Let V be a finite dimension D-subspace of M and let $m \in M \backslash V$. We proceed by induction on $dim(V)$.

If $dim(V) = 0$, then $V = \{0\}$ and so if we take $r = 1$, then we can use the lemma 4.4.17.

Proceeding inductively, assume $dim(V) > 0$ and suppose $0 \neq w \in V$ with $V = V_0 \oplus span(w)$ where $dim(V_0) = dim(V) - 1$ and so we can use our induction hypothesis.

Set $A(V_0) = \{x \in R : xV_0 = \{0\}\}$. By induction, for every $y \notin V_0$, there exists $r \in A(V_0)$ such that $ry \neq 0$. Remember this part and we call this part 'star'.

Note $A(V_0)$ is a left ideal and since $w \notin V_0$, we have $A(V_0)w \neq \{0\}$. Then, we have $A(V_0)w$ is a non-trivial submodule of M and hence $A(V_0)w = M$ by irreducibility. We note thus, every element in M can be written as aw where $a \in A(V_0)$.

Consider $\tau : M \to M$ given by $\tau(aw) = am$ where we recall $w \in M \backslash V$ is fixed.

We first show τ is well-defined. Say we have $aw = a'w$, where $a, a' \in A(V_0)$. Thus, we have $(a - a')w = 0$ and so $(a - a')V = 0$. For contradiction, assume that if $r \in R$ and $rV = \{0\}$, then $rm = 0$. With this assumption of contradiction, we have $(a - a')m = 0$ and so $am = a'm$, therefore $\tau(aw) = \tau(a'w)$. Thus, τ is well-defined.

We notice, $\tau \in End_R(M) = D$. For all $a \in A(V_0)$, we have

$$am = \tau(aw) = a\tau(w) \Rightarrow a(m - \tau(w)) = 0$$

By 'star', we must have $m - \tau(m) \in V_0$, i.e. $m - \tau \cdot m \in V_0$ where now D is the scalars.

Therefore, we have $m \in V_0 + span_D(w) = V$, which is a contradiction as we assumed w is not in V. Therefore, by our assumption for contradiction, we showed the inductive step and hence R is indeed act densely on M by our lemma 4.4.17. ♡

Proposition 4.4.19. *If R is primitive and (left) Artinian, then $R \cong End_D(M) \cong M_n(D)$.*

Proof. It will be enough to just show $dim_D(M) < \infty$. Suppose $\{v_1, v_2, ...\}$ is infinite and is D-linear independent. For each m, let $I_m = \{r \in R : \forall 1 \leq i \leq m, rv_i = 0\}$, this is an left ideal of the ring R. Then, we have $I_1 \supseteq I_2 \supseteq I_3 ....$

By the Jacobson Density Theorem, R acts densely on M by primitivity. In particular, for every $m > 1$, there exists $r \in R$ such that $rv_1 = rv_2 = ... = rv_{m-1} = 0$ and $rv_m = v_m \neq 0$. Therefore, we have $r \in I_{m-1} \backslash I_m$. Since we can do this for all m, we get $I_1 \supset I_2 \supset I_3 ...$, which is a contradiction to the Artinian condition.

Say $\{v_1, ..., v_n\}$ is a basis for M over D, define $\phi : R \to End_D(M) \cong M_n(D)$ by

$$\phi(r)(\sum r_i v_i) = \sum r r_i v_i$$

One should check this is an isomorphism of rings, we have surjectivity by Jacobson Density Theorem and injective by faithfulness. ♡

Remark 4.4.20. With Proposition 4.4.19, we can show that every semiprimitive Artinian ring is a finite direct sum of primitive Artinian rings.

Theorem 4.4.21 (Artin-Wedderburn)**.** *Every semisimple ring*[4] *is isomorphic to a finite direct sum of matrix rings over division rings, i.e.*

$$R \cong \bigoplus_{i=1}^{k} M_{n_i}(D_i)$$

Proof. Assignment. ♡

Corollary 4.4.21.1. *Every commutative semisimple ring is isomorphic to a finite direct sum of fields.*

Remark 4.4.22. Let R be primitive F-algebra where F is a field. Let M be a faithful irreducible R module and $D = End_R(M)$. For $\alpha \in F$, consider $\phi_\alpha : M \to M$ given by $\phi_\alpha(m) = \alpha m$. Since $F \subseteq Z(R)$, we have $\phi_\alpha \in D$.

Next, consider $\psi : F \to D$ given by $\psi(\alpha) = \phi_\alpha$. This is an injective homomorphism. Also, for each $\phi \in D$, we have

$$\phi(\phi_\alpha(m)) = \phi(\alpha m) = \alpha\phi(m) = \phi_\alpha(\phi(m)) \Rightarrow \phi \circ \phi_\alpha = \phi_\alpha \circ \phi$$

Thus, we have D is an F-algebra.

Lemma 4.4.23. *Let $F = \overline{F}$ where $\overline{F}$ means the algebraic closure. If D is a division F-algebra which is algebraic over F, then $D = F$.*

[4] Note semisimple if and only if semiprimitive and Artinian

Proof. Take $a \in D$, we will show $a \in F$, then we are done as F is already a subset (isomorphic copy) of D. Since D is algebraic over F, we have $p(x) \in F[x]$ such that $p(a) = 0$ where $p(x)$ is monic. In particular, since F is algebraically closed, we have $p(x) = \prod(x - \lambda_i)$.

However, note $F \subseteq Z(D)$, we have

$$p(a) = \prod(a - \lambda_i) = 0$$

where $a - \lambda_i \in D$. Hence, we must have at least one i such that $a - \lambda_i = 0$ and so $a = \lambda_i \in F$. ♡

Remark 4.4.24. Let D be a division F-algebra. If $dim_F(D) < \infty$, then D is algebraic over F.

Theorem 4.4.25. *Let $F = \overline{F}$. If R is a finite dimensional semisimple F-algebra then $R = \bigoplus_{i=1}^{k} M_{n_i}(F)$.*

Proof. Since R is finite dimensional and semisimple, we have $R \cong \bigoplus_{i=1}^{k} M_{n_i}(D_i)$ and $dim_F(D_i) < \infty$. Then, we have D_i is algebraic over F and hence $D_i = F$. ♡

Theorem 4.4.26. *Let $F = \overline{F}$, G be finite group, and $char(F) = 0$ or $char(F) \nmid |G|$. Then, $F[G]$ is semisimple and*

$$F[G] \cong \bigoplus_{i=1}^{k} M_{n_i}(F)$$

Proof. It follows by Maschke Theorem 4.4.7 and Theorem 4.4.25 and other stuff. ♡

4.5 Artin-Wedderburn and Representations

Remark 4.5.1. Let $F = \mathbb{C}$, then

$$\mathbb{C}[G] \cong \bigoplus_{i=1}^{k} M_{n_i}(\mathbb{C})$$

Taking $dim_{\mathbb{C}}$, we have $|G| = n_1^2 + ... + n_k^2$.

Next, we will explore the relationship between the Artin-Wedderburn decomposition and representation theory.

Lemma 4.5.2. *Let R be semisimple, let $R = M_1 \oplus ... \oplus M_k$ where M_i are irreducible. Let M be an irreducible R-module, then $M \cong M_i$ for some i.*

Proof. Let $M = R/I$ for a left maximal ideal I. Consider the natural mapping ϕ_i that maps $M_i \to R \to R/I$. Thus, ϕ_i is isomorphism or $\phi_i = 0$ by irreducibility.

Suppose $\phi_i = 0$ for all i, then define $\phi : R \to R/I$ given by $\phi = \sum \phi_i$. We have $\phi(1) = 0 \Rightarrow 1 \in I$, which is a contradiction. ♡

Lemma 4.5.3. *Let R be semisimple. Suppose $R \cong M_1 \oplus ... \oplus M_m \cong N_1 \oplus ... \oplus N_n$, where M_i, N_i are irreducibles. Then, $n = m$ and $M_i \cong N_i$, up to reordering.*

Proof. Consider $P_i = \bigoplus_{j \neq i} M_j$, then $R/P_i \cong M_i$, which is irreducible. Thus P_i is a maximal submodule by correspondence theorem. Then, we have $\cap_i P_i = \{0\}$.

Note $N_n \not\subseteq P_i$ for some i, and so $N_n \cap P_i = \{0\}$ as N_n is irreducible. Hence, we have $N_n + P_i = N_n \oplus P_i$ and since P_i is maximal, we have $N_n \oplus P_i = R$. Thus, we have $R/P_i \cong N_n \cong M_i$. The rest is done by induction and we are finished. ♡

Remark 4.5.4. Let D be a division ring and let $R = M_n(D)$, then R is semisimple as it is simple and Artinian. Then, we have $R = M_1 \oplus ... \oplus M_n$ where M_i is the ith column submodule of R which is isomorphic to D^n.

Therefore, we have $R \cong D^n \oplus ... \oplus D^n = \bigoplus_{i=1}^n D^n$.

Next, let R be semisimple, then by Artin-Wedderburn, we have

$$R \cong M_{n_1}(D_1) \oplus ... \oplus M_{n_k}(D_k)$$

and so, by the above argument, we see

$$R \cong \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{n_k} D_i^{n_i} = \bigoplus_{i=1}^{k} n_i \cdot D_i^{n_i}$$

Be more particular, we have

$$\mathbb{C}[G] \cong \bigoplus_{i=1}^{k} M_{n_i}(\mathbb{C}) \cong \bigoplus_{i=1}^{k} n_i \cdot \mathbb{C}^{n_i}$$

Now, let M be an irreducible $\mathbb{C}[G]$ module, i.e. a representation. Hence, by the Lemma 4.5.2, we have $M \cong \mathbb{C}^{n_i}$ for some i. The degree of the associated representation is $dim_{\mathbb{C}}(M) = dim_{\mathbb{C}}\mathbb{C}^{n_i} = n_i$. Moreover, M occurs in $\mathbb{C}[G]$ (the regular representation) n_i times.

Moreover, k is equal the number of conjugacy classes of G as we recall from classical representation theory.

Remark 4.5.5. Let C be a conjugacy class, let $Z_C = \sum_{g \in C} g \in \mathbb{C}[G]$. Then, consider $\{Z_C : C \text{ is conjugacy class}\}$, this form a basis for $Z(\mathbb{C}[G])$. Then, use Artin-Wedderburn, we can prove k is equal the number of conjugacy classes.

Example 4.5.6. Consider $\mathbb{C}[S_3]$, then the degree of irreducible representations is $1, 1, 2$. Hence, we have

$$\mathbb{C}[S_3] \cong \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C})$$

Example 4.5.7. Let G be abelian, with $|G| = n$. Then, we have

$$\mathbb{C}[G] \cong \mathbb{C} \oplus ... \oplus \mathbb{C}$$

Moreover, if G, H are abelian, then $\mathbb{C}[G] \cong \mathbb{C}[H]$ if and only if $|G| = |H|$.

Remark 4.5.8. Cut off of midterm 2.

Q1 is relation between group algebra and rep theory. Q2 is modulo theory. Q3 is induced rep.

4.6 Integrality Property of Character

Remark 4.6.1. In this section, all rings are commutative with unital.

Theorem 4.6.2. *Say χ is a character of G, $g \in G$ and $\chi(g) \in \mathbb{Q}$, then $\chi(g) \in \mathbb{Z}$.*

Theorem 4.6.3. *Say ρ is an irreducible representation of G, then deg$(\rho) \mid |G|$.*

Definition 4.6.4. Say $R \subseteq S$ is commutative ring with $1_R = 1_S$, then

1. We say $a \in S$ is ***integral over*** R if there is monic $p \in R[x]$ such that $p(a) = 0$
2. Say S is ***integral over*** R if all $a \in S$ are integral over R.
3. The ***integral closure*** of R in S is $\{a \in S : a \text{ is integral over } R\}$

Example 4.6.5. Let $R = \mathbb{Z}$ and $S = \mathbb{R}$. Then $\sqrt{2}$ and $\frac{1+\sqrt{5}}{2}$ and any $n \in \mathbb{Z}$ are integral over $\mathbb{Z}$. Meanwhile, we have $\frac{\sqrt{2}}{2}$ and $\frac{1}{2}$ are not.

Remark 4.6.6. The idea of integral is a sensible adaptation of "algebraic over" to the context of rings (instead of fields).

So, why not try the following definition: say $a \in S$ is "ring-algebraic" over R if there exists $0 \neq p \in R[x]$ such that $p(a) = 0$. This is a bad definition.

Note we have a nice property of "algebraic": $a \in K$ is algebraic over $L \subseteq K$ if and only if $L[a]$ if a finite dimensional L-vector space i.e. can write higher powers of a as L-linear combinations of lower ones.

This fails for "ring-algebraic". Consider $R = \mathbb{Z}$ and $S = \mathbb{Q}$, and $a = \frac{1}{2}$. We have a satisfies $2x - 1 = 0$ but $\mathbb{Z}[\frac{1}{2}]$ is not a finitely generated $\mathbb{Z}$ module, i.e. cannot write $\frac{1}{2^n}$ as a $\mathbb{Z}$-linear combination of smaller powers.

Theorem 4.6.7. *Say $R \subseteq S$, $a \in S$. The following are equivalent:*

1. *a is integral over R*
2. *$R[a]$ is a finitely generated R-module*
3. *there exists a subring $R \subseteq T \subseteq S$ such that $a \in T$ and T is a finitely generated R-module.*

Proof. $1 \to 2$: Say $p(a) = 0$ for monic $o \in R[x]$. So, there exists $b_0, ..., b_{n-1} \in R$ such that $a^n = b_0 + ... + b_{n-1}a^{n-1} \in R + ... + Ra^{n-1}$. Inductively, we have all $a^k \in R + ... + Ra^{n-1}$ and so $R[a] = R + ... + Ra^{n-1}$ so it is finitely generated R-module.

$2 \to 3$ is trivial as we take $T = R[a]$ then we are done.

We then show $3 \to 1$. Write $T = Rv_1 + ... + Rv_n$ with $v_i \in T$. However, we have T is a subring, so $av_i \in T$. Thus, $av_i = \sum_j a_{ij}v_j$ where $a_{ij} \in R$. Let $b_{ij} = \delta_{ij}a - a_{ij}$ and let $B = (b_{ij})$ be the matrix with coefficients to be b_{ij}'s. Then, we have $Bv = 0$ where $v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$. Thus, by Cramer's rule, we have $det(B)v_i = det(B_i) = 0$ where B_i is the ith column replaced by 0.

So $det(B)T = det(B)(Rv_1 + ... + Rv_n) = 0$ but $1 \in T$, so $det(B) = 0$. So a is a root of $det(xI - A) \in [x]$ where $A = (a_{ij})$ and so a is integral over R. ♡

Proposition 4.6.8. *Say $R \subseteq S$, then the integral closure of R in S is a subring of S.*

Proof. Say $a, b \in S$ be integral over R. By Theorem 4.6.7, we can write $R[a] = Rs_1 + ... + Rs_n$ and $R[b] = Rt_1 + ... + Rt_m$, then $R[a, b]$ is generated by a^kb^l as an R-module. But $a^k \in R[a]$ and $b^l \in R[b]$ so $a^kb^l \in R[a]R[b] = (Rs_1 + ... + Rs_n)(Rt_1 + ... + Rt_m) = \sum_{i,j} Rs_it_j$. So $R[a, b]$ is finitely generated and we have $a + b$ and ab are integral over R. ♡

Definition 4.6.9. Say $K/\mathbb{Q}$ is a field extension, we say $a \in K$ is an ***algebraic integer*** if a is integral over $\mathbb{Z}$.

The integral closure of $\mathbb{Z}$ in K is the ***ring of integer*** of K, denoted by O_k.

Example 4.6.10. $\sqrt{2}$ and $n \in \mathbb{Z}$ are algebraic integers. All roots of unity are as well algebraic intergers by taking $x^n - 1$.

Moreover, if χ is a character of G then $\chi(s)$ is an algebraic interger as $\chi(s)$ is the sum of it's eigenvalues, i.e. sum of roots of unity.

Proposition 4.6.11. *Say $K/\mathbb{Q}$ is a field extension. Say $a \in K$. Then a is algebraic integer if and only if a is algebraic over $\mathbb{Q}$ and the minimal polynomial $p_a(x)$ is in $\mathbb{Z}[x]$.*

Proof. We show $(\Leftarrow)$ first. p_a witnesses that a is integral over $\mathbb{Z}$.

Conversely, pick $p(x) \in \mathbb{Z}[x]$ of minimal degree such that p is monic and $p(a) = 0$.

If p were reducible over $\mathbb{Q}$ then by Gauss's lemma, it is reducible over $\mathbb{Z}$. So one of the factor contradicts minimality. So the minimal polynomial of a over $\mathbb{Q}$ is $p \in \mathbb{Z}[x]$. ♡

Corollary 4.6.11.1. *We have $O_{\mathbb{Q}} = \mathbb{Z}$.*

Proof. If $a \in \mathbb{Q}$ is algebraic integer, then by above proposition, we have $x - a \in \mathbb{Z}[x]$, so $a \in \mathbb{Z}$. ♡

Corollary 4.6.11.2. *If χ is a character of G and $\chi(g) \in \mathbb{Q}$ then $\chi(g) \in \mathbb{Z}$*

Proof. $\chi(g)$ is an algebraic integer so $\chi(G) \in Q_{\mathbb{Q}} = \mathbb{Z}$. ♡

Definition 4.6.12 (Notation)**.** In the following of this section, we will insists the following.

Let G be a fintie group, $\chi_1, ..., \chi_k$ are irreducible characters with $\phi_1, ..., \phi_k$ be their correspond representations. Let $C_1, ..., C_k$ be conjugacy classes.

Proposition 4.6.13. *For $i = 1, 2, ..., k$, define $w_i : \{C_1, ..., C_k\} \to \mathbb{C}$ by*

$$w_i(C_j) = \frac{|C_j|\chi_i(g)}{\chi_i(1)}, g \in C_j$$

Then, $w_i(C_j)$ is an algebraic integer.

Proof. We claim $\sum_{g \in C_j} \phi_i(g) = w_i(C_j) \cdot I$ for a fixed i.

For $h \in G$, we have $\sum_{g \in C_j} \phi_i(g) = \sum_{g \in C_j} \phi_i(hgh^{-1})$, since ϕ_i is homomorphism, we have

$$\sum_{g \in C_j} \phi_i(g) = \sum_{g \in C_j} \phi_i(hgh^{-1}) = \phi_i(h)(\sum_{g \in C_j} \phi_i(g))\phi_i(h)^{-1}$$

Thus, $\sum_{g \in C_j} \phi_i(g) = \alpha I$ for some α as ϕ_i is irreducible and by Schur's lemma. Then, we take traces of both side, we have

$$\sum_{g \in C_j} Tr(\phi_i(g)) = \alpha\chi_i(1) \Rightarrow \sum_{g \in C_j} \chi_i(g) = \alpha\chi_i(1) \Rightarrow |C_j|\chi_i(g) = \alpha\chi_i(1)$$

This proves the claim.

Next, fix $g \in C_s$ where $1 \le s \le k$. Define

$$a_{ijs} := |\{(g_i, g_j) \in C_i \times C_j : g_i g_j = g\}| \in \mathbb{Z}$$

This definition is independent of choice of g. Indeed, $g_i g_j = g$ and pick $g' = hgh^{-1} \in C_s$. Then, we have $(hg_ih^{-1})(hg_jh^{-1}) = g'$ and so the value of a_{ijs} is independent of g.

We claim, for all i, j, t, we have

$$w_t(C_i)w_t(C_j) = \sum_{s=1}^{k} a_{ijs} w_t(C_s)$$

We prove the claim. Observe that

$$
\begin{aligned}
(w_t(C_i)w_t(C_j))I = (w_t(C_i)I)(w_t(C_j)I) &= (\sum_{g_i\in G_i}\phi_t(g_i)I)(\sum_{g_j\in G_j}\phi_t(g_j)I) \\
&= \sum_{g_i,g_j}\phi_t(g_ig_j) = \sum_{s=1}^{k}\sum_{g\in C_s}a_{ijs}\phi_t(g) \\
&= \sum_{s=1}^{k}a_{ijs}\sum_{g\in C_s}\phi_t(g) = \sum_{s=1}^{k}a_{ijs}w_t(C_s)I
\end{aligned}
$$

This proves our second claim. Thus, the finite generated $\mathbb{Z}$-module generated by $1, w_t(C_1), ..., w_t(C_k)$ is a subring of $\mathbb{C}$. ♡

Theorem 4.6.14. *We have $\chi_i \mid |G|$ for $i = 1, 2, ..., k$, i.e. the degree of an irreducible representation divides $|G|$.*

Proof. We have

$$
\begin{aligned}
\frac{|G|}{\chi_i(1)} &= \frac{|G|}{\chi_i(1)}\langle\chi_i,\chi_i\rangle \\
&= \frac{|G|}{\chi_i(1)}\frac{1}{|G|}\sum_{g\in G}|\chi_i(g)|^2 \\
&= \frac{1}{\chi_i(1)}\sum_{j=1}^{k}|C_j|\cdot|\chi_i(g_j)|^2 \\
&= \sum_{j=1}^{k}\frac{|C_j|\chi_i(g_j)}{\chi_i(1)}\overline{\chi_i(g_j)} \\
&= \sum_{j=1}^{k}w_i(c_j)\overline{\chi_i(g_j)}
\end{aligned}
$$

Note $\overline{\chi_i(g_j)}$ is algebraic integer and $w_i(c_j)$ is algebraic integer, and so $\frac{|G|}{\chi_i(1)} \in O_{\mathbb{Q}} = \mathbb{Z}$. The proof follows. ♡

Remark 4.6.15. Test 2, Friday, Nov 15, $1:30-2:20$, MC 2034.

The topic is from induced representation to module/ring theory.

1. 10 marks, $[4-4-2]$, three short questions, involving relatinoships between representation and CG modules and Artin-Wedderburn.
2. 10 marks, one question, proof. It is a detail we discussed in class, so look for incomplete proofs in class note.
3. 10 marks, induced representation, computational, understand the definition.

Chapter 5

Frobenius Reciprocity and Mackey's Criterion

5.1 Frobenius Reciprocity

Remark 5.1.1. Let M be a $\mathbb{C}[G]$ module, $dim_{\mathbb{C}}(M) < \infty$. Since $\mathbb{C}[G]$ is semisimple, we have M is semisimple and so $M = M_1 \oplus ... \oplus M_k$ where M_i are irreducible. Let N be an irreducible $\mathbb{C}[G]$ module with $dim_{\mathbb{C}} N < \infty$.

Consider $Hom_{\mathbb{C}[G]}(M, N) = \{\phi : M \to N : \phi \text{ is } \mathbb{C}[G]\text{-module homomorphism}\}$, it is a $\mathbb{C}$-vector space. As vector spaces, we have

$$Hom_{\mathbb{C}[G]}(M, N) \cong \bigoplus_{i=1}^{k} Hom_{\mathbb{C}[G]}(M_i, N)$$

By Schur's lemma, we have

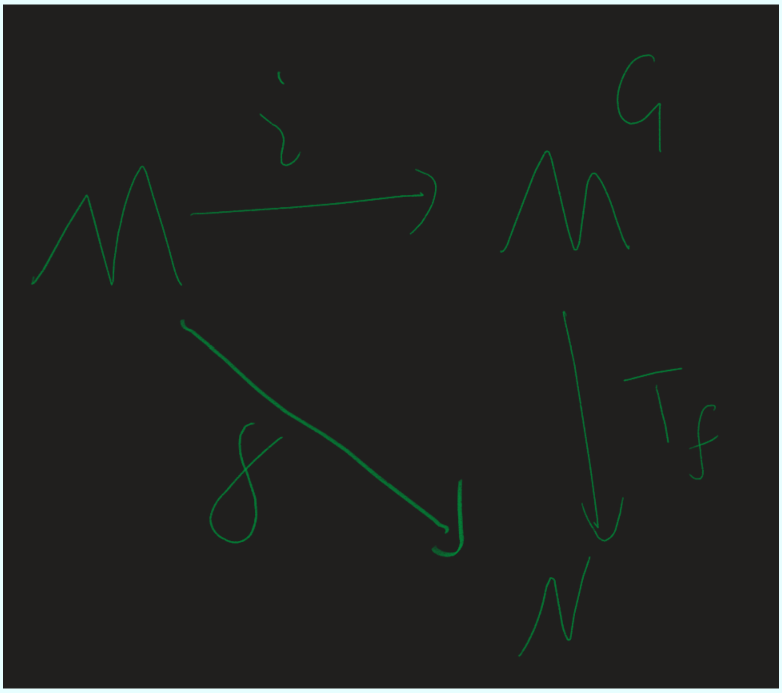
$$dim_{\mathbb{C}}(Hom_{\mathbb{C}[G]}(M_i, N)) = \begin{cases} 0, & \text{if } M_i \ncong N \\ 1, & \text{if } M_i \cong N \end{cases}$$

Therefore, the multiplicity of N in M, i.e. the number of M_i such that $M_i \cong N$, is $dim_{\mathbb{C}}(Hom_{\mathbb{C}[G]}(M, N))$. Say ρ is the corresponding representation of M and τ is of N with χ_ρ and χ_τ being their character. Thus, we have

$$dim_{\mathbb{C}} Hom_{\mathbb{C}[G]}(M, N) = \langle \chi_\rho, \chi_\tau \rangle$$

Remark 5.1.2. [Investigations] Let $H \leq G$, let M be a $\mathbb{C}[H]$ module and N be a $\mathbb{C}[G]$ module. Let $M^G := \mathbb{C}[G] \otimes_{\mathbb{C}[H]} M$, from assignment we see this is the induced representation of M. Let $i : M \to M^G$ given by $i(m) = 1 \otimes m$.

For $f \in Hom_{\mathbb{C}[H]}(M, N)$, there exists a unique $T_f \in Hom_{\mathbb{C}[G]}(M^G, N)$ such that $f = T_f \circ i$. Viz, the following diagram commutes.



Theorem 5.1.3 (Forbenius Reciprocity)**.** *Keep the notation as in Remark 5.1.2. The map*

$$\phi : Hom_{\mathbb{C}[H]}(M, N) \to Hom_{\mathbb{C}[G]}(M^G, N)$$

given by $\phi(f) = T_f$ *is an isomorphism of* $\mathbb{C}$*-vector spaces.*

Proof. Let $f_1, f_2 \in Hom_{\mathbb{C}[H]}(M, N)$. Then,

$$(T_{f_1} + T_{f_2}) \circ i = T_{f_1} \circ i + T_{f_2} \circ i = f_1 + f_2$$

Thus, by uniqueness from Remark 5.1.2, we have $T_{f_1} + T_{f_2} = T_{f_1+f_2}$. Similarly, we have $T_{\alpha f_1} = \alpha T_{f_1}$ and so ϕ is linear.

To see injective, suppose $T_{f_1} = T_{f_2}$, then $T_{f_1} \circ i = T_{f_2} \circ i$ and so $f_1 = f_2$.

To see surjective, take $F \in Hom_{\mathbb{C}[G]}(M^G, N)$. Then, let $f = F \circ i$, we have $f \in Hom_{\mathbb{C}[H]}(M, N)$. Thus, by uniqueness, we have $T_f = F$. ♡

Remark 5.1.4. Let's keep the notation of Remark 5.1.2, and suppose M, N are irreducible in $\mathbb{C}[H]$ and $\mathbb{C}[G]$, respectively. Let ρ be the representation corresponding to M amd τ be of N.

Denote the restriction of τ to H by $Res^H_G(\tau)$, thus we have

$$dim_{\mathbb{C}} Hom_{\mathbb{C}[H]}(M, N) = dim_{\mathbb{C}} Hom_{\mathbb{C}[G]}(M^G, N)$$

by Forbenius reciprocity. This happens if and only if $\langle \chi_\rho, \chi_{Res(\tau)} \rangle_H = \langle \chi_{Ind(\rho)}, \chi_\tau \rangle_G$. For notation, we say the character of $Ind(\rho)$ to be $Ind(\chi_\rho)$ and the character of $Res(\tau)$ to be $Res(\chi_\tau)$, then we have

$$\langle \chi_\rho, Res(\chi_\tau) \rangle_H = \langle Ind(\chi_\rho), \chi_\tau \rangle_G$$

Viz, the number of times ρ appears in $Res(\tau)$ is equal the number of times τ appears in $Ind(\rho)$.

Definition 5.1.5. Let V, W be $\mathbb{C}[G]$ modules, then we define

$$\langle V, W\rangle_G := dim_{\mathbb{C}}(Hom_{\mathbb{C}[G]}(V, W))$$

Moreover, let $H \leq G$, let V be a $\mathbb{C}[G]$ module, then we define

$$Ind_H^G(V) := V^G = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} V$$

Let V be a $\mathbb{C}[G]$ module, then we define $Res_G^H(V)$ to be the module V viewed as $\mathbb{C}[H]$ module, i.e. we restrict the coefficients from $\mathbb{C}[G]$ to $\mathbb{C}[H]$.

Remark 5.1.6. By Frobenius reciprocity, let V be $\mathbb{C}[H]$ module and W be $\mathbb{C}[G]$ module, then we have

$$\langle V, Res_G^H(W)\rangle_H = \langle Ind_H^G(V), W\rangle_G$$

Lemma 5.1.7. *Let G be a finite group, let V, W be $\mathbb{C}[G]$-modules. Then, let χ_ρ be the character of V and χ_τ be the character of W when V and W viewed as its corresponding representations. Then, we have*

$$\langle V, W\rangle_G = \langle \chi_\rho, \chi_\tau\rangle$$

Proof. Suppose $W = W_1 \oplus ... \oplus W_n$ where W_i is irreducible for $1 \leq i \leq n$. Then, recall

$$Hom_{\mathbb{C}[G]}(V, W) = \bigoplus_{i=1}^{n} Hom_{\mathbb{C}[G]}(V, W_i)$$

Taking dimensions, we have

$$\langle V, W\rangle_G = \sum_{i=1}^{n} \langle V, W_i\rangle = \sum_{i=1}^{n} \langle \chi_\rho, \chi_{\tau_i}\rangle = \langle \chi_\rho, \sum \chi_{\tau_i}\rangle = \langle \chi_\rho, \chi_\tau\rangle$$

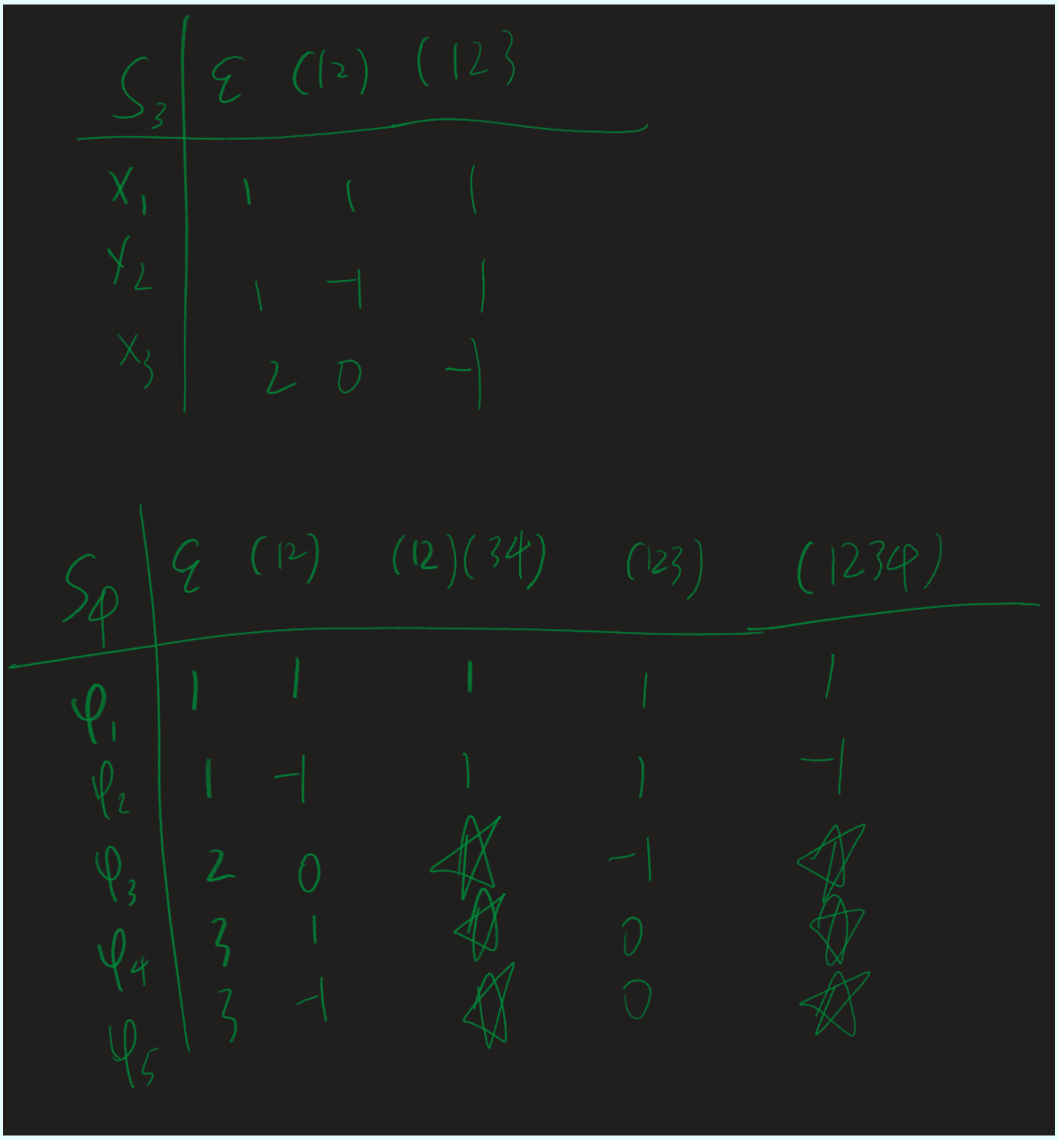
where χ_{τ_i} is the representation of W_i. ♡

Remark 5.1.8. Let $\rho : H \to GL(V)$ and $\tau : G \to GL(W)$, then we have

$$\langle \chi_p, Res(x_\tau)\rangle_H = \langle Ind(\chi_p), \chi_\tau\rangle_G$$

Example 5.1.9. Let $H = S_3 \leq S_4 = G$. Let $\rho : H \to GL(\mathbb{C}^2)$ be the irreducible representation of degree 2. Then, try to decompose $Ind_H^G(\rho)$.

Solution. To compute the number of irreducible representations of S_4 appear in $Ind_H^G(\rho)$, we do not want to work with the big group, so we work with the restriction.



S_3	ε	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

S_4	ε	(12)	$(12)(34)$	(123)	(1234)
φ_1	1	1	1	1	1
φ_2	1	-1	1	1	-1
φ_3	2	0		-1	
φ_4	3	1		0	
φ_5	3	-1		0	

Recall the character table, then we have

$$
\begin{aligned}
\langle Ind(\chi_3), \phi_1 \rangle_G &= \langle \chi_3, Res(\phi_1) \rangle_H \\
&= \langle \chi_3, \chi_1 \rangle_H \\
&= 0
\end{aligned}
$$

and $\langle Ind(\chi_3), \phi_2 \rangle = \langle Ind(\chi_3), \phi_3 \rangle = 0$. In addition, we have

$$\langle Ind(\chi_3), \phi_3 \rangle_G = \langle \chi_3, Res(\phi_3) \rangle_H = 1$$

Then, for ϕ_4 and ϕ_5, we have

$$
\begin{aligned}
\langle Ind(\chi_3), \phi_4 \rangle_G &= \langle \chi_3, \phi_4 \rangle_H \\
&= \langle \chi_3, \chi_3 + \chi_1 \rangle_H \\
&= 1
\end{aligned}
$$

Similarly, we have $\langle Ind(\chi_3), \phi_5 \rangle_G = 1$. Therefore, the induced character of ρ is $\phi_3 + \phi_4 + \phi_5$. ♠

5.2 Mackey's Criterion

Remark 5.2.1. Given $H \leq G$ and a representation $\rho : H \to GL(V)$, when is $ind_H^G(\rho)$ is irreducible?

We may want to look at

$$\langle Ind_H^G(\chi_\rho), Ind_H^G(\chi_\rho)\rangle_G = \langle \chi_\rho, Res_G^H(Ind_H^G(\chi_\rho))\rangle_H$$

Thus, we want to study $Res_G^H(Ind_H^G(\chi_\rho))$.

Remark 5.2.2. Suppose $Ind_H^G(\rho)$ was irreducible. Then ρ must be irreducible.

Indeed, suppose $W \leq V$ is a $\mathbb{C}[H]$ submodule, then $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} W$ is a $\mathbb{C}[G]$ submodule of $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V$. Or, we can see this by $Ind(\rho_1 \oplus \rho_2) = Ind(\rho_1) \oplus Ind(\rho_2)$.

Definition 5.2.3. Let $H \leq G$. For $g \in G$, we define $H_g := gHg^{-1} \cap H \leq H$.

Remark 5.2.4. Let $\rho : H \to GL(V)$ be a representation. We obtained two representations of H_g:

1. $Res_g(\rho) := Res_H^{H_g}(\rho)$
2. $\rho^g : H_g \to GL(V)$ given by $\rho^g(ghg^{-1}) = \rho(h)$

Definition 5.2.5. Let ρ_1, ρ_2 be representations of G, we say ρ_1, ρ_2 are ***disjoint*** if $\langle \chi_{\rho_1}, \chi_{\rho_2}\rangle = 0$.

Theorem 5.2.6 (Mackey's Irreducibility Criterion)**.** *Let $H \leq G$ and $\rho : H \to GL(V)$. Then $Ind_H^G(\rho)$ is irreducible if and only if the following*

a) ρ is irreducible and
b) $\forall g \in G \backslash H := G - H$, ρ^g and $Res_g(\rho)$ are disjoint.

Proof. Consider Theorem 5.2.12 ♡

Corollary 5.2.6.1. *Let $H \trianglelefteq G$ and $\rho : H \to GL(V)$, then $Ind(\rho)$ is irreducible if and only if ρ is irreducible and for all $g \in G - H$, we have ρ^g is disjoint from ρ, i.e. $\rho \not\cong \rho^g$.*

Definition 5.2.7. Let $Q \leq G$ and $A \in G$. The ***double coset*** of Q in G containing A is $QAQ = \{h_1 A h_2 : h_i \in Q\}$

Example 5.2.8. Where is the double coset come from?

Consider $H \times H$ acting on G by $(h_1, h_2) \cdot x = h_1 x h_2$. Then, the double cosets are exactly the orbits of this action.

Thus, we have two double cosets of H in G are equal or disjoint. In addition, the distinct double cosets of H in G partition G.

Example 5.2.9. Let $H = \{\epsilon, (12)\} \leq S_3$. Then

$$H(123)H = \{(13), (23), (123), (132)\}$$

and

$$H\epsilon H = H = \{\epsilon, (12)\}$$

Thus, the counting proeprty of left coset does not apply here as the two double cosets do not share the same size and the number of doulbe cosets is not $|G|/|H|$.

Remark 5.2.10. Let $H \trianglelefteq G$ and let $g_1H, ..., g_mH$ be all its cosets. Consider $Hg_1H, ..., Hg_mH$. Then, we have $g_iH \subseteq Hg_iH$, then let $h_1g_ih_2$ be arbitrary, then $h_1g_ih_2 = g_ih_1'h_2$ for some h_1'. Thus $Hg_iH \subseteq g_iH$ and so $Hg_iH = g_iH$. Therefore, if H is normal, the double cosets are just left cosets.

Proposition 5.2.11. *Let $H \leq G$, and $\rho : H \to GL(V)$. Let S be the double coset representatives. Then,*

$$Res_G^H(Ind_H^G(\rho)) \cong \bigoplus_{s\in S} Ind_{H_s}^H(\rho^s)$$

Proof. We must show that and

$$\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V \cong_{\mathbb{C}[H]} \bigoplus_{s\in S} (\mathbb{C}[H] \otimes_{\mathbb{C}[H_s]} V)$$

i.e. they are isomorphic as $\mathbb{C}[H]$ module.

For each $s \in S$, let $W(s) = span\{x \otimes v : x \in HsH, v \in V\}$ be a $\mathbb{C}$ vector space, note that $W(s)$ is a $\mathbb{C}[H]$ submodule of $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V$ by the definition of double cosets. Therefore, since the double cosets partition G, we have that $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V = \bigoplus_{s\in S} W(s)$ as $\mathbb{C}[H]$ modules.

Claim: for $s \in S$, $W(s) \cong \mathbb{C}[H] \otimes_{\mathbb{C}[H_s]} V$ as $\mathbb{C}[H]$ module.

Consider $f : V \to W(s)$ given by $f(v) = s \otimes v$. Clearly f is additive. Now, note $shs^{-1} \cdot v = hv$ by the definition of ρ^g, and so

$$\begin{aligned} f(shs^{-1} \cdot v) &= f(hv) \\ &= s \otimes hv = sh \otimes v \\ &= (shs^{-1})s \otimes v = shs^{-1}(s \otimes v) \\ &= shs^{-1} \cdot f(v) \end{aligned}$$

Therefore, f is a $\mathbb{C}[H_s]$ module homomorphism.

By the universal property, there exists a $\mathbb{C}[H]$ module homomorphism

$$F : \mathbb{C}[H] \otimes_{\mathbb{C}[H_s]} V \to W(s)$$

such that $F \circ i = f$. This is the desired $\mathbb{C}[H]$ isomorphism.

Hint: Consider $G : W(s) \to \mathbb{C}[H] \otimes_{\mathbb{C}[H_s]} V$ given by $G(s \otimes v) = 1 \otimes v$, then extend to a $\mathbb{C}[H]$ homomorphism, then $G = F^{-1}$. ♡

Theorem 5.2.12. *[Mackey] Proof of Theorem 5.2.6*

Proof. Note

$$\begin{aligned}
\langle Ind_H^G(\chi_\rho), Ind_H^G(\chi_\rho)\rangle &= \langle \chi_\rho, Res_G^H Ind_H^G(\chi_\rho)\rangle \\
&= \langle \chi_\rho, \sum_{s\in S} Ind_{H_s}^H(\chi_{\rho^s})\rangle \\
&= \sum_{s\in S}\langle \chi_\rho, Ind_{H_s}^H(\chi_{\rho^s})\rangle \\
&= \sum_{s\in S}\langle Res_H^{H^s}(\chi_\rho), \chi_{\rho^s}\rangle \\
&= \sum_{s\in S}\langle Res_s(\chi_\rho), \chi_{\rho^s}\rangle \\
&= \sum_{s\in S} d_s, \text{ with } d_s := \langle Res_s(\chi_\rho), \chi_{\rho^s}\rangle \\
&= d_1 + \sum_{s\in S, s\neq 1} d_s \\
&= \langle \chi_\rho, \chi_\rho\rangle + \sum_{s\in S, s\neq 1} d_s
\end{aligned}$$

Thus, $\langle Ind_H^G(\chi_\rho), Ind_H^G(\chi_\rho)\rangle = 1$ if and only if $\langle \chi_\rho, \chi_\rho\rangle = 1$ and $d_s = 0$ for all $s \in S, s \neq 1$. The proof follows as $s \in S, s \neq 1$ imply $s \notin H$. ♡

Example 5.2.13. Consider $G = D_5$, let $H = \langle r\rangle \trianglelefteq G$. Consider $\rho : H \to \mathbb{C}^\times$ by $\rho(r) = \zeta_5$. We want to show $Ind_H^G(\rho)$ is irreducible.

Solution. Note ρ has degree 1, so it is irreducible. That is the first part of the Mackey.

Since $H \trianglelefteq G$ and $deg(\rho) = 1$, we must show $\rho \neq \rho^g$ for all $g \in G - H$. Thus, consider ρ^{sr^i}, we have

$$\begin{aligned}
\rho^{sr^i}(r) &= \rho((sr^i)^{-1}r(sr^i)) \\
&= \rho(r^{-i}srsr^i) = \rho(r^{-i}r^{i-1}) \\
&= \rho(r^{-1}) = \zeta_5^{-1} = \zeta_4 \neq \zeta_5
\end{aligned}$$

Therefore, we have $Ind_H^G(\rho)$ is irreducible by Mackey. ♠

Chapter 6

Addition Materials

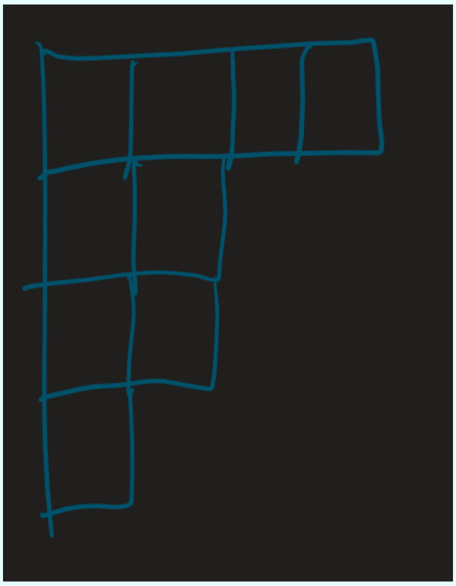
6.1 Representation of Permutation Group

Remark 6.1.1. In this section, we want to find all irreducible $\mathbb{C}[S_n]$ modules. We know the number of irreducible $\mathbb{C}[S_n]$ modules equal number of conjugacy classes equal number of cycle types equal number of partition of n.

Definition 6.1.2. A ***partition*** λ of $n \in \mathbb{N}$ is a sequence $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_k$ such that $\sum \lambda_i = n$. We write $\lambda \vdash n$.

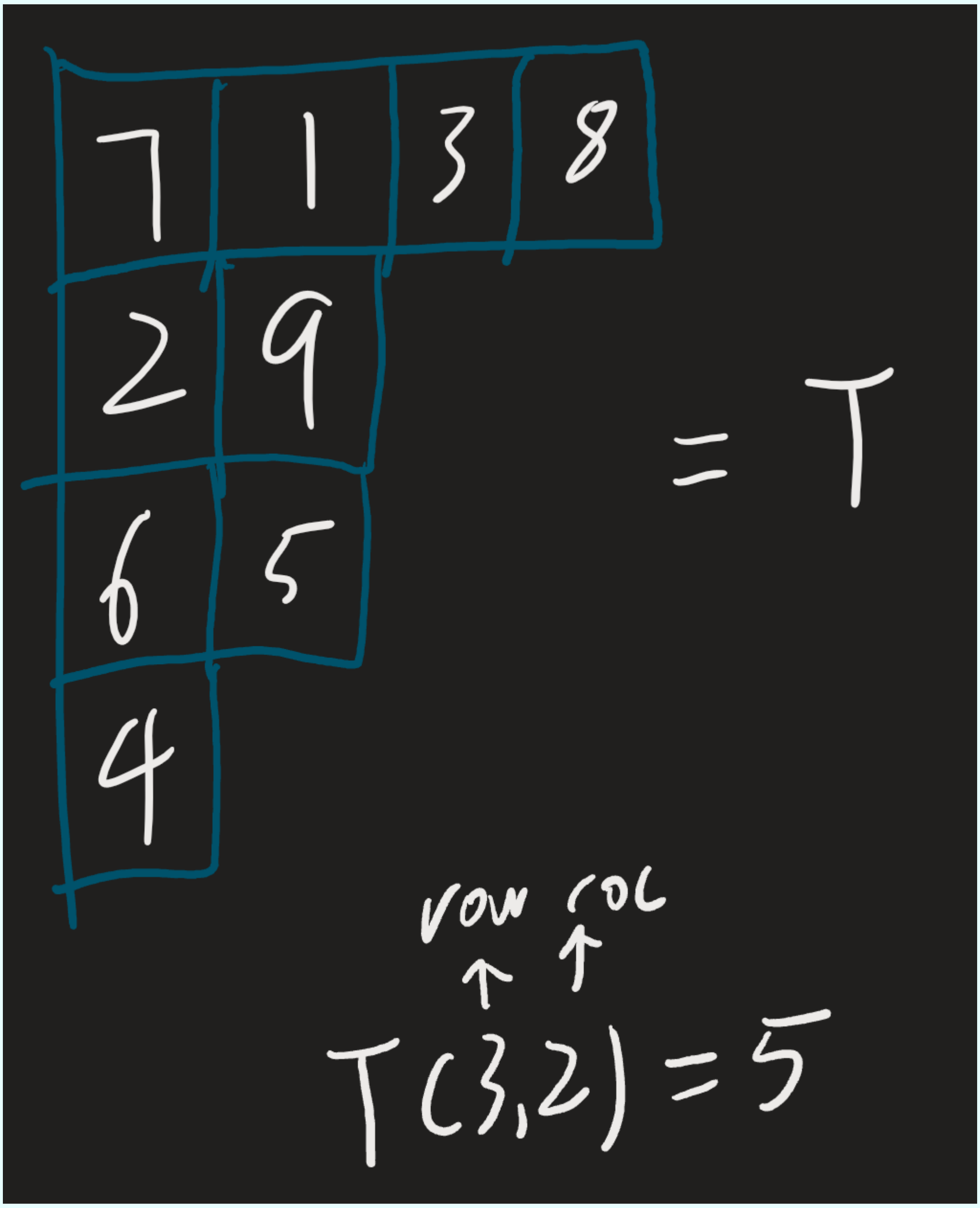
Definition 6.1.3. Let $\lambda = (\lambda_1, ..., \lambda_k) \vdash n$. The ***Young diagram*** of shape λ is a left-justified array of boxes where row i has λ_i boxes.

Example 6.1.4. Let $\lambda = (4, 2, 2, 1) \vdash 9$, then we have



Definition 6.1.5. Let $\lambda \vdash n$, a ***Young tableau*** (plural is tableaux) of shape λ is obtained by taking the corresponding Young diagram and filling in the boxes with $1, 2, 3, ..., n$, bijectively.

Example 6.1.6. For example, we have



Remark 6.1.7.

1. Let T be a λ Tableau with $\lambda \vdash n$. Then S_n acts on T by $(\sigma T)(i,j) = \sigma(T(i,j))$.
2. Let T_1, T_2 be λ tableaux. Then T_1, T_2 are ***row-equivalent*** if their rows contain the same entries and we write $T_1 \sim T_2$. We need to check this is a equivalence relation on the set of λ Tableaux.

Remark 6.1.8. Let $T_1, T_2, ..., T_k$ be all the λ Tableaux with $\lambda \vdash n$ be fixed. Consider $V = span(T_1, ..., T_k)$ to be a $\mathbb{C}[S_n]$ module via the previous action. This is not irreducible.

Indeed, note $W = span(T_1 + ... + T_k)$ is a valid submodule. In addition, consider $[T]$ to be a row equivalence class and let $[T_1], ..., [T_l]$ be the complete list of equivalent classes.

Let $W_2 = span(\sum_{T\in[T_1]} T, ..., \sum_{T\in[T_l]} T)$, this is a submodule.

Definition 6.1.9. Let $\lambda \vdash n$, and T be λ-tableau. The row equivalence classes $[T]$ are called ***λ-tabloids***.

Remark 6.1.10. Let S_n acts on the set of λ-tabloids by $\sigma \cdot [T] = [\sigma \cdot T]$.

Definition 6.1.11. Let $\lambda \vdash n$, say $[T_1], ..., [T_k]$ are all distinct λ-tabloids. We call the $\mathbb{C}[S_n]$-module $M^\lambda = Span_{\mathbb{C}}([T_1], ..., [T_k])$ the ***permutation module*** associated to λ.

Remark 6.1.12. Note $W = Span_{\mathbb{C}}([T_1] + ... + [T_k])$ is a submodule of M^λ.

Example 6.1.13. Let $\lambda = (n)$, consider $M^\lambda = Span_{\mathbb{C}}\{\boxed{1|2|...|n}\}$. This is the trivial representation.

Next, let $\lambda = (1, 1, ..., 1)$. Then $M^\lambda = Span_{\mathbb{C}}\{T_1, ..., T_k\}$ where $T_1, ..., T_k$ are all the λ-Tableau. This is the regular representation.

Let $\lambda = (n-1, 1)$, then the tableaux would look like

$$\begin{array}{|c|c|c|c|}\hline * & * & ... & * \\ \hline i \\ \cline{1-1}\end{array}$$

the row equivalence is determined by the second row (i.e. i) completely. Therefore, let

$$N_i = \begin{array}{|c|c|c|c|}\hline * & * & ... & * \\ \hline i \\ \cline{1-1}\end{array}$$

we have $M^\lambda := span_{\mathbb{C}}(N_1, ..., N_n)$ and $\sigma \cdot N_i = N_{\sigma(i)}$. This is the permutation representation.

Remark 6.1.14. Let $\lambda \vdash n$, M^λ be given and $[T] \in M^\lambda$. Let $[U] \in M^\lambda$. Then there exists $\sigma \in S_n$ such that $\sigma[T] = [\sigma T] = [U]$. Thus, $M^\lambda = \mathbb{C}[S_n][T] = (\mathbb{C}[S_n]T)$ for ***any*** λ tabloids $[T]$.

Definition 6.1.15. The ***row stabilizer*** is

$$R_T = \{\sigma \in S_n : \forall (i,j), (\sigma T)(i,j) \text{ and } T(i,j) \text{ are in the same row}\}$$

Similarly, the ***column stabilizer*** is

$$C_T = \{\sigma \in S_n : \forall (i,j), (\sigma T)(i,j) \text{ and } T(i,j) \text{ are in the same column}\}$$

Remark 6.1.16. Note the row stabilizer and column stabilizer are both subgroup of S_n and $\sigma \in R_T \Leftrightarrow \sigma[T] = [T]$.

Definition 6.1.17. Let $H \subseteq S_n$, then

$$H^- := \sum_{\sigma \in H} sgn(\sigma)\sigma \in \mathbb{C}[S_n]$$

and

$$K_T := C_T^-$$

Definition 6.1.18. Let T be some λ tableau. The ***polytabloid*** associated to T is

$$e_T = K_T[T] \in M^\lambda$$

Example 6.1.19. Let $T = \begin{array}{|c|c|c|}\hline 4 & 1 & 3 \\ \hline 2 & 5 \\ \cline{1-2}\end{array}$. Then, we have

$$C_T = \{\epsilon, (15), (24), (15)(24)\}$$

and

$$K_T = \epsilon + (15)(24) - (15) - (24)$$

and so

$$e_T = [T] + (15)(24)[T] - (15)[T] - (24)[T]$$

Lemma 6.1.20. *Say $\lambda \vdash n$, T is a λ tableau, and $\pi \in S_n$. Then*

1. $R_{\pi \cdot T} = \pi R_T \pi^{-1}$
2. $C_{\pi \cdot T} = \pi C_T \pi^{-1}$
3. $K_{\pi \cdot T} = \pi K_T \pi^{-1}$
4. $e_{\pi T} = \pi e_T$

Proof. For 1. We have

$$\begin{aligned}\sigma \in R_{\pi T} &\Leftrightarrow \sigma[\pi T] = [\pi T] \\ &\Leftrightarrow \sigma\pi[T] = \pi[T] \\ &\Leftrightarrow \pi^{-1}\sigma\pi[T] = [T] \\ &\Leftrightarrow \pi^{-1}\sigma\pi \in R_T \\ &\Leftrightarrow \sigma \in \pi R_T \pi^{-1}\end{aligned}$$

For 2. This is the same, but we need to use $T \sim U$ if and only if T and U are column equivalent.

For 3. We have

$$\begin{aligned}K_{\pi T} = C^-_{\pi T} &= \sum_{\sigma \in C_{\pi T}} sgn(\sigma)\sigma \\ &= \sum_{\sigma \in \pi C_T \pi^{-1}} sgn(\sigma)\sigma \\ &= \sum_{\tau \in C_T} sgn(\pi\tau\pi^{-1})\pi\tau\pi^{-1} \\ &= \pi(\sum_{\tau \in C_T} sgn(\tau)\tau)\pi^{-1} \\ &= \pi K_T \pi^{-1} \text{ All in } \mathbb{C}[S_n]\end{aligned}$$

For 4. We have

$$\begin{aligned}e_{\pi T} &= K_{\pi T}[\pi T] \\ &= \pi K_T \pi^{-1}[\pi T] \\ &= \pi K_T[T] \text{ Module action} \\ &= \pi e_T\end{aligned}$$

$\heartsuit$

Remark 6.1.21. Note $Span_{\mathbb{C}}\{e_T : T \text{ is a } \lambda-\text{tableau}\}$ is a $\mathbb{C}[S_n]$-submodule of M^λ.

Definition 6.1.22. The submodule $S^\lambda = Span_{\mathbb{C}}(e_T : T \text{ is } \lambda-\text{tableau})$ is called the ***Specht module*** associated to λ.

Example 6.1.23. Let $\lambda \vdash n$ and $\lambda = (n)$. We have $T = \boxed{1}\boxed{2}\boxed{3}\boxed{4}\boxed{\ldots}\boxed{n}$ and $M^\lambda = Span_{\mathbb{C}}\{[T]\}$. In addition, $C_T = \{\epsilon\}$, $K_T = 1\epsilon \in \mathbb{C}[S_n]$, $e_T = K_T[T = [T]$ and $S^\lambda = Span_{\mathbb{C}}\{[T]\} = M^\lambda$.

Example 6.1.24. Let $\lambda \vdash n$ with $\lambda = (1, 1, ..., 1)$. Then, say we have

$$T = \begin{array}{|c|} \hline 1 \\ \hline 2 \\ \hline \vdots \\ \hline n \\ \hline \end{array}$$

Consider U be another λ-tableau, then $U = \pi T$, where $\pi \in S_n$. From last time, we have $e_U = e_{\pi T} = sgn(\pi)e_T$. Thus, we have $S^\lambda = Span_{\mathbb{C}}\{e_T\}$ where $\pi e_T = sgn(\pi)e_T$ and so this is the sign representation.

Example 6.1.25. Consider $\lambda = (n-1, 1) \vdash n$. Then, say we have

$$T = \begin{array}{|c|c|c|c|c|c|} \hline i & * & * & * & * & * \\ \hline j \\ \cline{1-1} \end{array}$$

Then, define $[T] := v_j$, we have $C_T = \{\epsilon, (ij)\}$, $K_T = \epsilon - (ij)$, and

$$\begin{aligned} e_T &= (\epsilon - (ij))[T] \\ &= (\epsilon - (ij))v_j = v_j - v_i \end{aligned}$$

Thus, we have $S^\lambda = Span_{\mathbb{C}}\{v_j - v_i : 1 \leq i < j \leq n\}$. This has a basis

$$\{v_1 - v_2, v_1 - v_3, ..., v_1 - v_n\}$$

and so $dim_{\mathbb{C}}(S^\lambda) = n - 1$.

Remark 6.1.26. Consider M^λ as an inner product space via $\langle [T], [U] \rangle = \delta_{[T],[U]}$, which means, $[T] = [U]$ then $\delta_{[T],[U]} = 1$ and otherwise 0.

Lemma 6.1.27. *Let $H \leq S_n$.*

1. *If $\pi \in H$ then $\pi H^- = H^- \pi = sgn(\pi)H^-$*
2. *If $U, V \in M^\lambda$, then*
$$\langle H^- U, V \rangle = \langle U, H^- V \rangle$$
3. *If the transposition $(bc) \in H$, then*
$$H^- = x(\epsilon - (bc))$$
for some $x \in \mathbb{C}[S_n]$.

4. *If $\lambda \vdash n$ and T is λ-tableau. If b, c are in the same row of T and $(bc) \in H$, then $H^-[T] = 0$*

Proof.

1. Homework
2. Note $\delta_{[T],[U]} = \delta_{[\pi T],[\pi U]}$ and so
$$\langle [T], [U] \rangle = \langle \pi[T], \pi[U] \rangle$$
Therefore, we have
$$\begin{aligned}\langle H^- U, V \rangle &= \sum_{\pi \in H} \langle sgn(\pi)\pi U, V \rangle \\ &= \sum_{\pi \in H} \langle \pi U, sgn(\pi) V \rangle \\ &= \sum_{\pi \in H} \langle U, sgn(\pi)\pi^{-1} V \rangle \\ &= \sum_{\pi \in H} \langle U, sgn(\pi^{-1})\pi^{-1} V \rangle = \langle U, H^{-1} V \rangle\end{aligned}$$
3. Say $(bc) \in H$, then $K = \{\epsilon, (bc)\} \leq H$. Let r_σ be coset representatives of K in H. Then, we have
$$\left(\sum_\sigma sgn(r_\sigma) r_\sigma \right) (\epsilon - (bc)) = H^-$$
4. Note $H^- = x(\epsilon - (bc))$. Then $H^-[T] = x(\epsilon - (bc))[T] = x([T] - [(bc)T]) = 0$.

♡

6.2 Final

Definition 6.2.1. Saturday, Dec 7. $4:00 - 6:30$, MC 2034. 6 questions, 10 marks each.

1. Q1 is T/F, ten questions, 1 marks each. This last chapter will be in Q1.
2. Q2-Q5 are ***directly from Assignment***.
3. Q6 is not from assignment. On Forbenius/Mackey.

6.3 Back To Permutation

Definition 6.3.1. Let $\lambda = (\lambda_1, ..., \lambda_k) \vdash n$ and $\mu = (\mu_1, ..., \mu_m) \vdash n$. We say λ ***dominates*** μ and written $\mu \trianglelefteq \lambda$, if for all $i \geq 1$, we have
$$\lambda_1 + ... + \lambda_i \geq \mu_1 + ... + \mu_i$$
where $\lambda_i = 0$ for $i > k$ and $\mu_i = 0$ for $i > m$.

Example 6.3.2. We have $(2,2,2,2,2) \trianglelefteq (4,4,1,1)$.

Lemma 6.3.3. *Let T be λ tableau, S be μ tableau, where $\lambda, \mu \vdash n$. If the elements of an arbitrary row of S are all in different columns of T then $\mu \trianglelefteq \lambda$.*

Proof. For every i, we can sort the entries of S so that they occur in the first i rows of T. Then, $\lambda_1 + ... + \lambda_i$ is equal the number of entries of T in first i rows. This is greater than or equal to the number of entries of S in first i rows, which is equal $\mu_1 + ... + \mu_i$. ♡

Corollary 6.3.3.1. *Let $\lambda, \mu \vdash n$, T a λ tableau, S a μ tableau. Suppose $K_T[S] \neq 0$, then $\lambda \trianglelefteq \mu$ and if $\lambda = \mu$, then $K_T[S] = \pm e_T$.*

Proof. Suppose $K_T[S] \neq 0$. Suppose b, c are entries in the same row of S. For contradiction, suppose b, c are in the same column of T, i.e. $(bc) \in C_T$. By 3 in a lemma (in the first section), we have $K_T = C_T^- = x(\epsilon - (bc))$ for some $x \in \mathbb{C}[S_n]$. However, then $K_T[S] = x(\epsilon[S] - (bc)[S]) = x([S] - [S]) = 0$. This is the desired contradiction and we obtained the first assertion.

Now, suppose $\lambda = \mu$. By the argument of the previous lemma (the sorting argument), I can turn $[T]$ into $[S]$ via π, where $\pi \in C_T$, i.e. $[S] = \pi[T]$. Therefore,

$$\begin{aligned} K_T[S] &= K_T[\pi T] = K_T \pi [T] \\ &= sgn(\pi) \cdot K_T[T] = e_T \end{aligned}$$

♡

Corollary 6.3.3.2. *Let $\mu \in M^\lambda$, T a λ tableau. Then $K_T \mu = f e_t$ where $f \in \mathbb{C}$.*

Proof. Note $\mu = \sum c_i [S_i]$ where S_i are λ tableaux. Then $K_T \mu = \sum c_i K_T[S_i] = f \cdot e_T$ where $f \in \mathbb{C}$. ♡

Theorem 6.3.4. *Let U be a submodule M^λ. Then $S^\lambda \subseteq U$ or $U \subseteq (S^\lambda)^\perp$. In particular, S^λ is irreducible.*

Proof. Let U be a submodule of M^λ and let $u \in U$, say T is a λ tableau. Then $K_T u = f e_T, f \in \mathbb{C}$.

First, suppose $\exists u \in U$, such that $K_T u = f e_T$ where $f \neq 0$. So, $e_T = f^{-1} K_T u \in U$. If S is a λ tableau then $S = \pi T$ for $\pi \in S_n$, Moreover, $e_S = e_{\pi T} = \pi e_T \in U$. Therefore, $S^\lambda \subseteq U$.

Second, suppose we always has $K_T u = 0$. Let $u \in U$, T a λ tableau be arbitrary. Then $\langle u, e_T \rangle = \langle u, K_T[T] \rangle = \langle 0, [T] \rangle = 0$. So $U \subseteq (S^\lambda)^\perp$.

Now, take V to be a proper submodule of S^λ. Then $V \subseteq (S^\lambda)^\perp$ and so $V \subseteq S^\lambda \cap (S^\lambda)^\perp$ and so $V = 0$. Therefore S^λ is irreducible. ♡

Lemma 6.3.5. *Let $\lambda, \mu \vdash n$ and suppose we can find $0 \neq \theta \in Hom_{\mathbb{C}[S_n]}(S^\lambda, M^\mu)$. Then $\mu \trianglelefteq \lambda$. If $\lambda = \mu$ then θ is a scalar multiple of the identity.*

Proof. We will find a λ tableau T and μ tableau S such that $K_T[S] \neq 0$. Observe that $M^\lambda = S^\lambda \oplus (S^\lambda)^\perp$ as $\mathbb{C}$ vector spaces.

Moreover, for $x \in (S^\lambda)^\perp$, T a λ tableau and $\pi \in S_n$. Then, we have

$$\langle \pi x, e_T \rangle = \langle \pi^{-1}\pi x, \pi^{-1} e_T \rangle = \langle x, e_{\pi^{-1}T} \rangle = 0$$

Therefore, $(S^\lambda)^\perp$ is a submodule of M^λ and so $M^\lambda = S^\lambda \oplus (S^\lambda)^\perp$ as a $\mathbb{C}[S_n]$ module.

We can extend θ to $\theta \in Hom_{\mathbb{C}[S_n]}(M^\lambda, M^\mu)$ by setting $\theta((S^\lambda)^\perp) = 0$. Since $\theta \neq 0$, there exists a λ-tableau T such that $\theta(e_T) \neq 0$. Say $\theta([T]) = \sum c_i[S_i]$ where each S_i has shape μ. Now, as we extended θ above, we have

$$0 \neq \theta(e_T) = \theta(K_T[T]) = K_T\theta([T]) = \sum c_i K_T[S_i]$$

So, there exists i such that $K_T[S_i] \neq 0$ and so $\mu \trianglelefteq \lambda$.

Suppose $\lambda = \mu$. Then

$$\theta(e_T) = K_T\theta([T]) = \sum c_i K_T[S_i] = \sum c_i f_i e_T$$

where $f_i \in \mathbb{C}$. Hence,

$$\theta(e_T) = (\sum c_i f_i)e_T := \alpha e_T$$

For $\pi \in S_n$, we have

$$\theta(e_{\pi T}) = \theta(\pi e_T) = \pi\theta(e_T) = \pi(\alpha e_T) = \alpha e_{\pi T}$$

Therefore, θ is indeed a scalar multiple as desired. ♡

Theorem 6.3.6. *The Specht modules are all irreducible $\mathbb{C}[S_n]$ module up to isomorphism.*

Proof. It suffices to show $S^\lambda \neq S^\mu$ for $\mu \neq \lambda$. Suppose $S^\lambda \cong S^\mu$. An isomorphism between S^λ and S^μ gives nonzero $\theta_1 \in Hom(S^\lambda, M^\mu)$ and $\theta_2 \in Hom(S^\mu, M^\lambda)$. So $\lambda \trianglelefteq \mu$ and $\mu \trianglelefteq \lambda$ and so $\lambda = \mu$. ♡

Definition 6.3.7. A Young tableau is ***standard*** if its entries increase along rows (i.e. left to right) and down columns.

Example 6.3.8. One example is

1	3	6
2	4	8
5	7	

Theorem 6.3.9. *A basis for S^λ over $\mathbb{C}$ is*

$$\{e_T : T \text{ is standard, shape } \lambda\}$$

Definition 6.3.10. Let T be a Young diagram, the ***hook length*** of the (i,j) entry of T is h_{ij}, which equal the number of blocks to the right plus the number of the block below plus 1.

Example 6.3.11. How many standard λ tableaux are there?

Theorem 6.3.12 (Hook-Length Formula)**.** *The number of standard λ-tableaux with $\lambda \vdash n$ is*

$$n! \prod_{i,j} \frac{1}{h_{ij}} = \frac{n!}{\prod_{i,j} h_{ij}}$$

Remark 6.3.13. We have

$$dim_{\mathbb{C}}(S^\lambda) = \frac{n!}{\prod h_{ij}}$$

Example 6.3.14. Consider $\lambda = (3,5) \vdash 5$. Then, $dim(S^\lambda) = \frac{5!}{4 \cdot 3 \cdot 2} = 5$.

Example 6.3.15. Find the largest degree of an irreducible representation of S_6.

Solution. Consider $\lambda = (3,2,1)$, and we have the max is 16. ♠

Chapter 7

Appendix I, Classical Commutative Algebra

7.1 Intro

Remark 7.1.1. In this chapter, all rings are unital and ***commutative***. We begin with recall of definition.

Definition 7.1.2. A ***ring homomorphism*** is a mapping from ring R to Q such that $f(x+y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$, and $f(1) = 1$.

Definition 7.1.3. An ***ideal*** I of ring R is a subset of R such that is closed under addition and $RI \subseteq I$, i.e. $\forall x \in R, y \in I, xy \in I$.

Example 7.1.4. $\{0\}$ is an ideal in R and we will write $0 := \{0\}$ by abuse of notation. Also, for $x \in R$, we have $\langle x \rangle := Rx = \{yx : y \in R\}$ is an ideal.

Proposition 7.1.5 (Correspondence theorem)**.** *Let I be an ideal of R. There is a bijection between ideals J of R which contains I and the ideals of A/I.*

Proof. We use a proof by triviality.

Trivial! ♡

Remark 7.1.6. Let I be an ideal of R, then we may write $x \equiv y \pmod{I}$ to mean $x - y \in I$.

Definition 7.1.7. A ***zero-divisor*** x of ring R is an element such that there exists $0 \neq y \in R$ such that $xy = 0$. A ring R without non-zero zero divisor is called ***integral domain*** and is denoted to be

$$\int_{-\infty}^{\infty} \zeta(\text{omain})d(\text{omain})$$

by analysts(kidding!).

Definition 7.1.8. An element $x \in R$ is called ***nilpotent*** if $x^n = 0$ for some $n > 0$. A ***unit*** in A is an element x such that $xy = 1$ for some $y \in A$. We write this y to be y^{-1}. We write the collection of units of R to be $R^\times$.

Definition 7.1.9. A field is a (commutative) ring R where $1 \neq 0$ and $R^\times = R\backslash\{0\}$. Note every fields are integral domain but not the converse.

Proposition 7.1.10. *Let R be a non-trivial ($R \neq \{0\}$) ring, then the following are equivalent:*

1. *R is a field*
2. *The only ideals in R are 0 and R*
3. *Every homomorphism of R into a non-trivial ring B is injective.*

Proof. $1 \to 2$: Let $I \neq 0$ be an ideal of R. Then I contains a non-zero element x. Note x must be a unit and so $I = R$.

$2 \to 3$: Let $\phi : R \to N$ be a homomorphism. Then $Ker(\phi)$ is an ideal. Note $Ker(\phi) = R$ imply R is trivial, so $Ker(\phi) \neq R$, hence $Ker(\phi) = 0$.

$3 \to 1$: Let x be an element of R which is not a unit. Then $\langle x \rangle \neq R$ and hence $B = R/\langle x \rangle$ is not the zero ring. Let $\phi : R \to B$ be the natural homomorphism of R to B, i.e. $\phi(x) := x + \langle x \rangle = \overline{x}$, then the kernel of ϕ is $\langle x \rangle$. Since ϕ is injective, we have $\langle x \rangle = 0$ and so $x = 0$. ♡

Definition 7.1.11. An ideal I of R is ***prime*** if $xy \in I$ imply $x \in I$ or $y \in I$. An ideal I of R is ***maximal*** if $I \neq R$ and $I \subset J$ where J is an ideal then $J = R$. Or, we say I is maximal if $I \neq R$ and there does not exist ideal J such that $I \subset J \subset R$.

Remark 7.1.12. I is prime if and only if A/I is an integral domain. I is maximal if and only if A/I is a field. Thus every maximal ideal is prime but not the converse.

If $f : R \to N$ is a homomorphism and I is a prime ideal in N then $f^{-1}(N)$ is a prime ideal in R. Indeed, note $R/f^{-1}(I) \cong N/I$ and so it has no zero divisor other than 0. This does not hold for maximal ideal, i.e. $f^{-1}(I)$ may not be maximal even if I is maximal in N. Consider $R = \mathbb{Z}$ and $N = \mathbb{Q}$ with $I = 0$.

Proposition 7.1.13. *Every ring R has at least one maximal ideal.*

Proof. We use proof by triviality (and Zorn's lemma).

Trivial!! ♡

Corollary 7.1.13.1. *If I is an proper ideal of R then I is contained in a maximal ideal of A.*

Proof. Use the above proposition to A/I. There exists a maximal ideal $\overline{M}$ in R/I and by correspondence theorem, there exists ideal M in R such that $I \subseteq M$ and $M/I = \overline{M}$. Then, we need to show M is indeed maximal in R. We do that by triviality. Alternatively, we can use proof by exercise, i.e. ***this part is left as an exercise***. ♡

Corollary 7.1.13.2. *Every non-unit of R is contained in a maximal ideal.*

7.2 The Basic

Definition 7.2.1. A ring R is called ***local ring*** if R has only one maximal ideal. The field $K = R/M$ is called ***residue field*** of R, where M is the only maximal ideal.

Proposition 7.2.2. *Let R be a ring and $M \neq R$ be an ideal of R such that $\forall x \in R \backslash M$ is a unit in R, then R is local ring and M is its maximal ideal.*

Proof. Every proper ideal consists of non-units, hence is contained in M. Hence M is the only maximal ideal of R. ♡

Proposition 7.2.3. *Let R be a ring and M be a maximal ideal of R such that every element of $1 + M := \{1 + x : x \in M\}$ is a unit in R, then R is local.*

Proof. Let $x \in R\backslash M$, since M is maximal, the ideal generated by x and M, i.e. $\langle x\rangle + M := \{z + y : z \in \langle x\rangle, y \in M\}$, is R as $M \subset \langle x\rangle + M$. Hence there exists $y \in R$ and $t \in M$ such that $xy + t = 1$ and so $xy = 1 - t \in 1 + M$ and hence a unit. Then, by the above proposition we are done. ♡

Definition 7.2.4. A ring with finite number of maximal ideals is called ***semi-local***.

Definition 7.2.5. A principal ideal domain (PID) is an integral domain in which every ideal is principal, i.e. every ideal is generated by one element.

Remark 7.2.6. Note in a PID, every prime ideal is maximal. Indeed, if $\langle x\rangle \neq 0$ is a prime ideal and $\langle y\rangle \supset \langle x\rangle$. Then $x \in \langle y\rangle$ and suppose $x = yz$ so that $yz \in \langle x\rangle$. Since $y \notin \langle x\rangle$, we have $z \in \langle x\rangle$ and so $z = tx$ so $x = yz = ytz$ and so $yt = 1$ and so $\langle y\rangle = R$.

Proposition 7.2.7. *The set N of all nilpotent elements in R is an ideal, and R/N has no nilpotent elements other than 0.*

Proof. If $x \in N$ then $ax \in N$ for all $a \in R$. Let $x, y \in N$ and suppose $x^m = 0$ and $y^n = 0$. Then by binomial theorem (which holds in commutative ring), we have

$$(x + y)^{m+n-1} = \sum_{r+s=m+n-1} a_\lambda x^r y^s$$

where a_λ are integer coefficients. In particular, we cannot have both $r < m$ and $s < n$ so every single term vanishes. Thus $x + y \in N$ and so N is an ideal.

Let $\overline{x} \in R/N$ then $\overline{x}^n = \overline{x^n}$ and so

$$\overline{x}^n = 0 \Rightarrow x^n \in N \Rightarrow \exists k \in \mathbb{N}(x^n)^k = 0 \Rightarrow x \in N \Rightarrow \overline{x} = 0$$

♡

Definition 7.2.8. The above ideal N is called ***nilradical*** of R. We may also write $Nil(R)$.

Proposition 7.2.9. *The nilradical of R is the intersection of all the prime ideals of R.*

Proof. Let N' denote the intersection of all prime ideals of R. If $r \in R$ is nilpotent and P is a prime ideal then $r^n = 0 \in P$ and so $r \in P$ as P is prime. Then $r \in N'$ and so $N \subseteq N'$.

Conversely, suppose $f \in R$ is not nilpotent. Let Σ be the set of ideals I such that $n > 0 \Rightarrow f^n \notin I$. Then Σ is not empty as $0 \in \Sigma$. Consider the poset $(\Sigma, \subseteq)$ and thus Σ has a maximal element by an application of Zorn's lemma. Let P be a maximal element of Σ. Let $x, y \notin P$, then the ideal $P + \langle x \rangle$ and $P + \langle y \rangle$ strictly contain P and therefore do not belong to Σ.

Thus $f^m \in P + \langle x \rangle, f^n \in P + \langle y \rangle$ for some n, m. It follows $f^{m+n} \in P + \langle xy \rangle$ and so the ideal $P + \langle xy \rangle$ is not in Σ and therefore $xy \notin P$. Hence we have a prime ideal P such that $f \notin P$ and so $f \notin N'$. The proof follows as we have, for every non-nilpotent element f, there exists a prime ideal that does not contain f, so non-nilpotent elements are not in N' and so $N' \subseteq N$. ♡

Definition 7.2.10. The ***Jacobson radical*** $J(R)$ of R is defined to be the intersection of all the maximal ideals of R.

Proposition 7.2.11. *We have $x \in J(R)$ if and only if $\forall y \in R, 1 - xy \in R^\times$*

Proof. Suppose $x \in J(R)$. Suppose for a contradiction that $1 - xy$ is not a unit, then $1 - xy$ is in some maximal ideal M, but $x \in J(R) \subseteq M$ and hence $xy \in M$ and so $1 \in M$, a contradiction.

Conversely, we use contrapositive. Suppose $x \notin J(R)$. Thus$x \notin M$ for some maximal ideal M. Then $M + \langle x \rangle = R$. So that we have $u + xy = 1$ for some $u \in M$ and $y \in R$. Thus $1 - xy \in M$ and is therefore not a unit. ♡

Definition 7.2.12. Let A, B be ideals of R then $A + B := \{a + b : a \in A, b \in B\}$. More generally, we have $\sum_{i \in I} A_i$ defined similarly where I is an index set. In particular, the elements of $\sum_{i \in I} A_i$ is of the form of $\sum x_i$ where $x_i \in A_i$ for all $i \in I$ with finite many non-zero terms in the sum.

Definition 7.2.13. The ***product*** of two ideals A, B in R is the ideal AB generated by all products xy where $x \in A, y \in B$. It is the set of all finite sums $\sum x_i y_i$ where each $x_i \in A$ and $y_i \in B$. Similarly, we define the product of any fintie family of ideals. In particular, we define A^n for $n \in \mathbb{N}$ and $A^0 = R$.

Example 7.2.14. If $R = \mathbb{Z}$ and $A = \langle m \rangle$, $B = \langle n \rangle$ then $A+B$ is the ideal generated by $gcd(m, n)$ and $A \cap B$ is the ideal generated by $lcm(a, b)$. In addition, $AB = \langle mn \rangle$. Thus, in this example, $AB = A \cap B$ if and only if $gcd(m, n) = 1$.

Remark 7.2.15. Let A, B, C be ideals, then $A(B + C) = AB + AC$. We also have, if $A \supseteq B$ or $A \supseteq C$ then $A \cap (B + C) = A \cap B + A \cap C$.

Definition 7.2.16. Two ideals A, B of R is said to be ***comaximal/coprime*** if $A + B = R$.

Remark 7.2.17. Note A, B are comaximal then $A \cap B = A + B$. Indeed, note $(A+B)(A\cap B) = A(A\cap B)+B(A\cap B) \subseteq AB$ and if $A+B = R$ then $(A+B)(A\cap B) = A \cap B$. Hence $A \cap B \subseteq AB$ and we note $AB \subseteq A \cap B$ trivially. The proof follows.

Definition 7.2.18. Let $A_1, ..., A_n$ be rings, their ***direct product*** $A = \prod_{i=1}^n A_i$ is the set of all sequences $x = (x_1, ..., x_n)$ where $x_i \in A_i$ and component-wise addition and multiplication.

Remark 7.2.19. We have the projection mapping $\rho_i : A \to A_i$ defined by $\rho_i(x) = x_i$.

Proposition 7.2.20. *Let A be a ring and $I_1, ..., I_n$ be ideals of A. Define $\phi : A \to \prod_{i=1}^n (A/I_i)$ by $\phi(x) = (x + I_1, ..., x + I_n)$. Then, we have*

1. *I_i, I_j are comaximal for $i \neq j$ then $\prod I_i = \cap I_i$*
2. *ϕ is surjective if and only if I_i, I_j are comaximal for $i \neq j$*
3. *ϕ is injective if and only if $\cap I_i = 0$*

Proof. To show 1, we use induction on n. When $n = 2$ we are done. Suppose it holds for $n - 1$. Let $B = \prod_{i=1}^{n-1} I_i I_i = \cap_{i=1}^{n-1} I_i$. Since $I_i + I_n = A$ for $1 \leq i \leq n - 1$, we have $x_i + y_i = 1$ for $x_i \in I_i$ and $y_i \in I_n$. Therefore,

$$\prod_{i=1}^{n-1} x_i = \prod_{i=1}^{n-1} (1 - y_i) \equiv 1 \pmod{I_n}$$

Hence $I_n + B = R$ and so

$$\prod_{i=1}^{n} I_i = BI_n = B \cap I_n = \bigcap_{i=1}^{n} I_i$$

Then, we show 2. Suppose ϕ is surjective. We do proof by example to show I_1, I_2 are coprime (and clearly this extend to arbitrary $i \neq j$). Since ϕ is surjective, there exists $x \in A$ such that $\phi(x) = (1, 0, ..., 0)$. Thus $x \equiv 1 \pmod{I_1}$ and $x \equiv 0 \pmod{I_2}$, hence

$$1 = (1 - x) + x \in I_1 + I_2$$

Conversely, we do proof by example as well. It is enough to show that there exists an element $x \in A$ such that $\phi(x) = (1, 0, ..., 0)$. Since $I_1 + I_i = R$ for $i > 1$, we have $u_i + v_i = 1$ for $u_i \in I_1$ and $v_i \in I_i$. Take $x = \prod_{t=2}^n v_t$, then $x = \prod(1 - u_t) \equiv 1 \pmod{I_1}$ and $x \equiv 0 \pmod{I_i}$ for $i > 1$. Thus $\phi(x) = (1, 0, ..., 0)$ as desired.

To show 3, we note $\cap I_i$ is the kernel of ϕ and the proof follows. ♡

Remark 7.2.21. We note the union of two ideals may not be an ideal.

Proposition 7.2.22.

1. *Let $P_1, ..., P_n$ be prime ideals and let A be an ideal contained in $\bigcup_{i=1}^n P_i$. Then $A \subseteq P_i$ for some i.*
2. *Let $A_1, ..., A_n$ be ideals and let P be a prime ideal containing $\bigcap A_i$. Then $P \supseteq A_i$ for some i and if $P = \bigcap A_i$ then $P = A_i$ for some i.*

Proof. To show 1, we use induction (by contrapositive) on n in the following statement:

$$(\forall 1 \leq i \leq n, A \nsubseteq P_i) \Rightarrow A \nsubseteq \bigcup_{i=1}^n P_i$$

This holds for $n = 1$. Suppose it holds for $n-1$, then for each $1 \leq i \leq n$ there exists $x_i \in A$ such that $x_i \notin P_j$ whenever $j \neq i$. Indeed, if there exists i_0 such that all elements of A we have $x \in P_j$ whenever $j = i_0$ then we obtained a contradiction. If for some i we have $x_i \notin P_i$ then we are done. If not, then $x_i \in P_i$ for all i. Consider

$$y = \sum_{i=1}^n \left(\prod_{j \in [n] \setminus \{i\}} x_j \right)$$

where $[n] = \{1, 2, ..., n\}$. We have $y \in A$ and $y \notin P_i$ for $1 \leq i \leq n$, hence $A \nsubseteq \bigcup_{i=1}^n P_i$. Indeed, for each P_i, note

$$y \equiv \prod_{j \in [n] \setminus \{i\}} x_j \not\equiv 0 \pmod{P_i} \Rightarrow y \notin P_i$$

Now we show 2 via contrapositive. Suppose $P \nsupseteq A_i$ for all i. Then there exist $x_i \in A_i$ such that $x_i \notin P$ for all $1 \leq i \leq n$. Therefore, $\prod x_i \in \prod A_i \subseteq \cap A_i$ but $\prod x_i \notin P$ since P is prime. Hence $P \nsupseteq A_i$. In particular, if $P = \cap A_i$ then $P \subseteq A_i$ and hence $P = A_i$ for some i. ♡

7.3 Ideal Quotient and Radical

Definition 7.3.1. Let A, B be two ideals in a ring R, then the ***ideal quotient*** of A and B is

$$(A : B) = \{x \in R : xB \subseteq A\}$$

Moreover, the ***annihilator*** of A is $(0 : A)$ and is denoted by $Ann(A)$.

Remark 7.3.2. The ideal quotient of A and B is an ideal.

In addition, the set of all zero-divisors in R is

$$D = \bigcup_{x \neq 0} Ann(\langle x \rangle)$$

Note if B is a principal ideal $\langle x \rangle$, then we write $(A : x)$ instead of $(A : \langle x \rangle)$

Example 7.3.3. If $R = \mathbb{Z}$, $A = \langle m \rangle$ and $B = \langle n \rangle$, where $m = \prod_{i=1}^{n} p_i^{k_i}$ and $n = \prod_{i=1}^{n} p_i^{l_i}$. Then, we have $(A : B) = \langle q \rangle$ where $q = \prod_{i=1}^{n} p_i^{h_i}$ where

$$h_i = \max(k_i - l_i, 0) = k_i - \min(k_i, v_i)$$

Hence we have $q = \frac{m}{gcd(m,n)}$

Example 7.3.4. The reader should try to show the following:

1. $A \subseteq (A : B)$
2. $(A : B)B \subseteq A$
3. $((A : B) : C) = (A : BC) = ((A : C) : B)$
4. $(\cap_i A_i : B) = \cap_i (A_i : B)$
5. $(A : \sum_i B_i) = \cap_i (A : B_i)$

Solution. I will provide some sketch solutions:

1. Clear
2. Let $x \in (A : B)$ then $xB \subseteq A$, thus $(xB)B \subseteq A$. Since x was arbitrary, we are done.
3. Suppose $y \in ((A : B) : C)$ then $yC \subseteq (A : B)$. Hence, we have $(yC)B \subseteq A$. Hence $((A : B) : C) \subseteq (A : BC)$. Suppose $y \in (A : BC)$, then $yBC \subseteq A$ and so $yCB \subseteq A$, hence $(yC)B \subseteq A$ and so $yC \subseteq (A : B)$. Thence we have $((A : B) : C) = (A : BC)$. The next equality should be similar.
4. Let $x \in (\cap A_i : B)$, then $xB \subseteq \cap A_i$. In particular, then we have $xB \subseteq A_i$ for each A_i, hence $x \in \cap(A_i : B)$. The converse should be easy to show.
5. Note $x(\sum B_i) \subseteq A \Rightarrow xB_i \subseteq A$ and thus $x \in (A : B_i)$ for all i and hence $(A : \sum B_i) \subseteq \cap(A : B_i)$. The converse should be clear.

♠

Definition 7.3.5. Let A be an ideal of R, then the ***radical*** of A is

$$rad(A) = r(A) := \{x \in R : \exists n \in \mathbb{N}, x^n \in A\}$$

Remark 7.3.6. Consider the natural homomorphism $\phi : R \to R/A$, then $r(A) = \phi^{-1}(\overline{N})$ where $\overline{N}$ is the nilradical of R/A. Thus $r(A)$ is an ideal as $\overline{N}$ is.

Example 7.3.7. The readers should try to show the following:

1. $A \subseteq r(A)$
2. $r(r(A)) = r(A)$
3. $r(AB) = r(A \cap B) = r(A) \cap r(B)$
4. $r(A) = R \iff A = R$
5. $r(A + B) = r(r(A) + r(B))$
6. If P is prime, then $r(P^n) = P$ for all $n \in \mathbb{N}$

Solution. I will provide some sketch solutions

1. Let $x \in A$, then $x^1 \in A$ and so $x \in r(A)$.
2. Suppose $x \in r(r(A))$ then $x^n \in r(A)$, thus $(x^n)^m \in A$. Suppose $x \in r(A)$ then $x^1 \in r(A)$ so $x \in r(r(A))$.

3. Suppose $x \in r(AB)$ then $x^n \in AB \subseteq A \cap B$. Suppose $x \in r(A \cap B)$ then $x^n \in A \cap B$ and so $x^n \in A$ and $x^n \in B$. In particular, then $x^n \cdot x^n = x^{2n} \in AB$ and so $x \in r(AB)$. The next equality we will use proof by exercise.
4. Suppose $r(A) = R$, then $1 \in r(A)$, hence there exists $n \in \mathbb{N}$ such that $1^n \in A$, since A is an ideal, $A = R$. Suppose $A = R$, clearly $r(A) \subseteq R$ and $R \subseteq r(A)$.
5. Let $x \in r(A+B)$, then $x^n \in A+B$, thus $x^n = a+b$ where $a \in A, b \in B$. Note $a \in r(A)$ and $b \in r(B)$ so $x \in r(r(A)+r(B))$. Let $x \in r(r(A)+r(B))$, then $x^m \in r(A)+r(B)$. Say $x^m = a+b$ where $a^q \in A$ and $b^p \in B$. Then $(x^m)^{q+p-1} \in A+B$ as A, B are ideals and the proof follows.
6. Note $r(P^n) = r(P) \cap r(P^{n-1})$. Thus $x \in r(P^n)$ then $x \in r(P)$. Thus $x^n \in P$ and so $x \in P$ as P is prime. Suppose $x \in P$, then $x^n \in P^n$ and so $x \in r(P^n)$.

♠

Proposition 7.3.8. *The radical of an ideal A of R is the intersection of the prime ideals that contains A.*

Proof. Trivial. Indeed, note the nilradical $\overline{N}$ of R/A is the intersection of all prime ideals of R/A and $r(A) = \phi^{-1}(\overline{N})$ where ϕ is the natural homomorphism. By correspondence theorem, we know those prime ideals are (bijectively) prime ideals in R that contains A and the proof follows. ♡

Remark 7.3.9. More generally, we define the radical $r(E)$ of any ***subset*** E of R in the same way, i.e. $r(E) = \{x \in R : \exists n \in \mathbb{N}, x^n \in E\}$. This $r(E)$ is not an ideal in general. In particular, we have $r(\bigcup_{\alpha \in A} E_\alpha) = \bigcup_{\alpha \in A} r(E_\alpha)$ for any family of subsets E_α of R.

Proposition 7.3.10. *$D =$ the set of zero divisors of $R = \bigcup_{x \in R, x \neq 0} r(Ann(\langle x \rangle))$*

Proof. We note $D = r(D)$. Indeed, $D \subseteq r(D)$ and suppose $x \in r(D)$ then $x^n \in D$. Thus $x^n y = x^{n-1}(xy) = 0$ for some $0 \neq y \in R$. If $xy = 0$ then we are done. If not then $xy \neq 0$ and so $x^{n-1} \in D$. Inductively we are done as n must be finite (we use the same argument on x^{n-1} and so on).

Next, note $r(D) = r(\bigcup_{x \in R, x \neq 0} Ann(\langle x \rangle)) = \bigcup_{x \in R, x \neq 0} r(Ann(\langle x \rangle))$. ♡

Example 7.3.11. Let $R = \mathbb{Z}$, $A = \langle m \rangle$. Let $1 \leq i \leq r$ and p_i be distinct prime divisors of m. Then $r(A) = \langle \prod p_i \rangle = \cap \langle p_i \rangle$

Proposition 7.3.12. *Let A, B be ideals in a ring R such that $r(A), r(B)$ are comaximal. Then A, B are comaximal.*

Proof. Note $r(A+B) = r(r(A)+r(B)) = r(R) = R$, hence $A+B = R$ by above example and the proof follows. ♡

7.4 Extension and Contraction

Definition 7.4.1. Let $f : A \to B$ be a ring homomorphism and I be an ideal of A. Then, we define the ***extension*** I^e of I to be the ideal $Bf(I)$.

On the other hand, let J be an ideal of B, we define the ***contraction*** J^c to be the ideal $f^{-1}(J)$.

Remark 7.4.2. Explicitly, I^e is the set of all fintie sums $\sum y_i f(x_i)$ where $x_i \in I$ and $y_i \in B$.

Note if J is prime ideal in B then J^c is prime. If I is prime in A, it is not always true that I^e is prime.

Remark 7.4.3. Let $f : A \to B$ be ring homomorphism. Then, we can factor f as follows:

$$A \xrightarrow{s} f(A) \xrightarrow{i} B$$

where s is a surjective and i is injective.

By first isomorphism theorem, we have $A/Ker(f) \cong f(A)$ via $\psi : A/Ker(f) \to f(A)$ and note $S : A \to A/Ker(f)$ given by $S(a) = a + Ker(f)$ is surjective. Thus define $s = \psi \circ S$, this is clearly surjective. Next, note the mapping $I : A/Ker(f) \to B$ given by $I(a + Ker(f)) = f(a)$ is injective. Thus, consider $i = I \circ \psi$, it is clearly injective.

Note under s, prime ideals correspond to prime ideals, but this may not be the case for i and the general situation is very complicated. Consider the following example.

Example 7.4.4. Consider $f : \mathbb{Z} \to \mathbb{Z}[i]$ given by $f(x) = x$ where $i^2 = -1$. A prime ideal $\langle p \rangle$ of $\mathbb{Z}$ may or may not be prime when extended to $\mathbb{Z}[i]$. In fact, note $\mathbb{Z}[i]$ is a PID as it has an Euclidean algorithm, and the situation when we consider extensions is as follows:

1. The square of a prime ideal in $\mathbb{Z}[i]$, for example, $\langle 2 \rangle^e = \langle (1+i)(1+i) \rangle$.
2. If $p \equiv 1 \pmod 4$ then $\langle p \rangle^e$ is the product of two distinct prime ideals, for example, $\langle 5 \rangle^e = \langle 2+i \rangle \langle 2-i \rangle$.
3. If $p \equiv 3 \pmod 4$ then $\langle p \rangle^e$ is prime in $\mathbb{Z}[i]$.

Note point 2 is not a trivial result, it is effectively equivalent to Fermat's theorem on sums of two squares.

In particular, we note the behavior of prime ideals under extensions is one of the central problem of algebraic number theory.

Proposition 7.4.5. *Let $f : A \to B$ be a ring homomorphism and I be an ideal of A, J be an ideal of B. Then, we have*

1. $I \subseteq (I^e)^c$ *and* $J \supseteq (J^c)^e$
2. $J^c = (((J)^c)^e)^c := J^{cec}$ *and* $I^e = I^{ece}$
3. *If C is the set of contracted ideals in A and if E is the set of extended ideals in B, then $C = \{I : I^{ec} = I\}$ and $E = \{J : J^{ce} = J\}$, and $I \mapsto I^e$ is a bijective map of C onto E, whose inverse is the mapping $J \mapsto J^c$.*

Proof.
1. Let $x \in I$. Note $I^e = Bf(I)$ and $I^{ec} = f^{-1}(Bf(I))$. In particular, note $f(x) \in f(I)$ and so $1_B f(x) \in Bf(I)$. Thus $f(x) \in Bf(I)$ and so $x \in f^{-1}(Bf(I))$. Hence $I \subseteq I^{ec}$. Similarly we can show $J \supseteq J^{ce}$
2. We show the first half and conduct proof by exercise on the second half. Note $J^c \supseteq J^{cec}$ as $J \supseteq J^{ce}$. Next, let $x \in J^{cec}$, we have $f(x) \in J^{ce}$. Note $J^{ce} = (f^{-1}(J))^e = BJ$ and so $f(x) \in BJ$, thus $f(x) = \sum x_i y_i$ where $x_i \in B, y_i \in J$. Thus $f(x) \in J$ and so $x \in J^c$.
3. If $I \in C$, then $I = J^c = J^{cec} = I^{ec}$. Conversely, if $I = I^{ec}$ then I is the contraction of I^e. The case is similar for E.

♡

Example 7.4.6. One should try to proof the following:

1. $(I_1 + I_2)^e = I_1^e + I_2^e$ and $(J_1 + J_2)^c \supseteq J_1^c + J_2^c$
2. $(I_1 \cap I_2)^e \subseteq I_1^e \cap I_2^e$ and $(J_1 \cap J_2)^c \supseteq J_1^c \cap J_2^c$
3. $(I_1 I_2)^e = I_1^e I_2^e$ and $(J_1 J_2)^c \supseteq J_1^c J_2^c$
4. $(I_1 : I_2)^e \subseteq (I_1^e : I_2^e)$ and $(J_1 : J_2)^c \subseteq (J_1^c : J_2^c)$
5. $(r(I))^e \subseteq r(I^e)$ and $r(J)^c = r(J^c)$

Solution. I will conduct a proof by impatience.

I'm not doing this!!! ♠

Definition 7.4.7. Let R be a ring and let $R[x]$ be the ring of polynomials with coefficients in R. Then, $f(x) = a_0 + a_1 x + ... + a_n x^n \in A[x]$ and we say f is primitive if $\langle a_0, a_1, ..., a_n \rangle = R$.

Remark 7.4.8. Let $f, g \in R[x]$, then fg is primitive if and only if f and g are primitive. Also, in $R[x]$, the Jacobson radical is equal the nilradical. The reader should try to proof the above remarks.

Definition 7.4.9. Let $R[[x]]$ be the set of formal power series $f = \sum_{i=0}^{\infty} a_i x^i$ with coefficients in R.

Remark 7.4.10. The contraction of a maximal ideal M of $R[[x]]$ is a maximal ideal of R and M is generated by M^c and x. In addition, every prime ideal of R is the contraction of a prime ideal of $R[[x]]$.

7.5 Miscellaneous I

Example 7.5.1. Let R be a ring and N be its nilradical. Then, the following are equivalent:

1. R has exactly one prime ideal
2. Every element of R is either a unit or nilpotent
3. R/N is a field

Definition 7.5.2. A ring is ***Boolean*** if $x^2 = x$ for all $x \in R$.

Example 7.5.3. The characteristics of Boolean ring R is 2. In addition, every prime ideal P in R is maximal and $R/P \cong \mathbb{Z}_2$. Also, every finitely generated ideal in R is principal.

Example 7.5.4 (Prime Spectrum)**.** Let R be a ring and let X be the set of all prime ideals of R. For each subset E of R, let $V(E)$ denote the set of all prime ideals of R which contains E. Then, one should try to show the following

1. If I is the ideal generated by E, then $V(E) = V(I) = B(r(I))$.
2. $V(0) = X, V(R) = \emptyset$
3. If $(E_i)_{i\in I}$ is any family of subsets of R, then

$$V(\bigcup_{i\in I} E_i) = \bigcap_{i\in I} V(E_i)$$

4. $V(I \cap J) = V(IJ) = V(I) \cup V(J)$ for any ideal I, J of R

The above results show that the set $V(E)$ satisfy the axioms for closed sets in a topological space. The resulting topology is called the ***Zariski topology***. The topological space X is called the ***prime spectrum*** of R and is written as $Spec(R)$.

Example 7.5.5. For each $f \in R$, let X_f denote the complement of $V(f)$ in $X = Spec(R)$. The set X_f is open. Show that they form a basis of open sets for the Zariski topology and that

1. $X_f \cap X_g = X_{fg}$
2. $X_f = \emptyset \iff f \in Nil(R)$
3. $X_f = X \iff f \in R^\times$
4. $X_f = X_g \iff r(\langle f\rangle) = r(\langle g\rangle)$
5. Every open cover of X has a finite subcover. In algebraic geometry we call this ***quasi-compact*** and reserve the term "compact" for spaces that are both Hausdroff and quasi-compact.
6. Every X_f is quasi-compact.
7. An open subset of X is quasi-compact if and only if it is a finite union of sets X_f.

The sets X_f is called ***basic open sets*** of X.

Remark 7.5.6. It is sometimes convenient to denote a prime ideal of R by a letter x or y when considering them as points in $X = Spec(R)$. Try to show the following:

1. $\{x\}$ is closed in $Spec(R)$ if and only if x is maximal in R.
2. $\overline{\{x\}} = V(x)$.
3. $y \in \overline{\{x\}}$ if and only if $x \subseteq y$ in R.

Definition 7.5.7. A topological space X is ***irreducible*** if $X \neq \emptyset$ and every pair of non-empty open sets in X intersect. Equivalently, this is saying every non-empty open set is dense in X.

Example 7.5.8. Show that $Spec(R)$ is irreducible if and only if $Nil(R)$ is prime ideal in R.

Chapter 8

Appendix II, Module Theory for Commutative Algebra

Remark 8.0.1. In this chapter, all rings are commutative and unital unless we say so. Assume we already learned definition of modules and quotient modules and everything covered in the notes above.

8.1 Intro

Definition 8.1.1. Let R be a ring and M, M', N, N' be R modules. Then, let $u \in Hom_R(M, M'), v \in Hom_R(N, N')$, we obtain two induced (module) homomorphisms

$$\overline{u} : Hom(M, N) \to Hom(M', N), \quad \text{with } \overline{u}(f) = f \circ u$$

$$\overline{v} : Hom(M, N) \to Hom(M, N'), \quad \text{with } \overline{v}(f) = v \circ f$$

Remark 8.1.2. For any R module M, there is a natural isomorphism

$$Hom(R, M) \cong M$$

as every $f \in Hom(R, M)$ is uniquely determined by $f(1)$.

Definition 8.1.3. Let $f \in Hom_R(M, N)$, then the ***cokernel*** of f is

$$Coker(f) = N/Im(f)$$

Definition 8.1.4. Let M be a R module. Let $\{M_i\}_{i\in I}$ be a family of submodules of M. Then, the ***sum*** $\sum_{i\in I} M_i$ is the set of all finite sums $\sum x_i$ where $x_i \in M_i$.

Remark 8.1.5. The sum $\sum M_i$ is the smallest submodule of M that contains all M_i. In addition, the intersection of family of submodule is again a submodule.

Proposition 8.1.6. *Let $L \supseteq M \supseteq N$ be R modules, then*

$$(L/N)/(M/N) \cong L/M$$

Moreover, let M_1, M_2 be submodules of M, then

$$(M_1 + M_2)/M_1 \cong M_2(M_1 \cap M_2)$$

Proof. Let $\theta : L/N \to L/M$ be $\theta(x + N) = x + M$. Then $Ker(\theta) = M/N$ and the proof follows by first isomorphism theorem.

The second assertion follows from consider $M_2 \to M_1 + M_2 \to (M_1 + M_2)/M_1$ where $M_2 \to M_1 + M_2$ is given by $m \mapsto m$ and $M_1 + M_2 \to (M_1 + M_2)/M_1$ is given by $m \mapsto m + M_1$ is a chain of surjective mapping with kernel $M_1 \cap M_2$. ♡

Definition 8.1.7. Let I be an ideal of R and M be a R module. Then, we define the product $IM := \sum_{i=1}^{n} a_i x_i$ with $a_i \in I$, $x_i \in M$ and $n \in \mathbb{N}$.

Definition 8.1.8. Let N, P be submodules of M. We define $(N : P)$ be the set of all $r \in R$ such that $rP \subseteq N$.

In particular, we define the ***annihilator of M*** to be

$$Ann(M) := (0 : M)$$

Remark 8.1.9. If $I \subseteq Ann(M)$ is an ideal of R, then M is also a R/I module with $(r + I) \cdot m = rm$ where $r \in R, m \in M$.

Definition 8.1.10. A R module is ***faithful*** if $Ann(M) = 0$.

Remark 8.1.11. Let M be R module. Then M is always faithful $R/Ann(M)$ module.

Definition 8.1.12. If $x \in M$, then $Rx := (x)$ is the set of all multiples rx where $r \in R$. This is a submodule of M. If $M = \sum_{i \in I} Ax_i$, then we say $\{x_i\}$ is a ***set of generators of M***.

If I is finite, we say M is ***finitely generated***.

8.2 Finitely Generated Modules

Definition 8.2.1. Let N, M be R modules, their ***direct sum*** $M \oplus N$ is a R module with set of all pairs (x, y) with $x \in M, y \in N$ with component-wise operations.

Similarly, let M_i be family of R modules, then $\bigoplus_{i \in I} M_i$ is the set of all finite sums of x_i's where $x_i \in M_i$.

In addition, we define the ***direct product*** of $\{M_i\}_{i \in I}$ to be $\prod_{i \in I} M_i$, to be the set of all sums of x_i.

Remark 8.2.2. If I is finite, direct product and direct sum is the same. When I is infinite, the product admits infinite sums while sum omits infinite sums and only allow finite many terms to be added.

Definition 8.2.3. A ***free R module*** is a R module which is isomorphic to a R module of the form $\bigoplus_{i\in I} M_i$ where each $M_i \cong R$. We denote this to be $R^{(I)}$.

A ***finitely generated free R module*** is a module isomorphic to $A^n := \bigoplus_{i=1}^n R$ with the convention R^0 is the zero module.

Proposition 8.2.4. *Let M be R module. Then M is finitely generated if and only if M is isomorphic to a quotient of R^n for some $n \in \mathbb{N}$.*

Proof. Suppose $x_1, ..., x_n$ generates M. Consider $\phi : R^n \to M$ given by $(a_1, ..., a_n) \mapsto a_1x_1+...+a_nx_n$. Then ϕ is a surjective R module homomorphism and so the assertion follows by first isomorphism theorem.

Conversely, since M is isomorphic to a quotient of R^n, we have an surjective R homomorphism $\phi : R^n \to M$. Consider a basis $\{e_i := (0, ..., 1, ..., 0) : 1 \le i \le n\}$ of R^n, we have $\{\phi(e_i) : 1 \le i \le n\}$ generates M. ♡

Proposition 8.2.5. *Let M be finitely generated R module. Let $I \trianglelefteq R$ be an ideal. Let ϕ be an R module endomorphism of M such that $\phi(M) \subseteq IM$, then where exists $a_1, ..., a_n \in I$ such that*

$$\phi^n + a_1\phi^{n-1} + ... + a_n = 0$$

Proof. Let $x_1, ..., x_n$ generates M. Then each $\phi(x_i) \in IM$ and so we have $\phi(x_i) = \sum_{j=1}^n a_{ij}x_j$ for $1 \le i \le n, a_{ij} \in I$. In particular, then we have

$$\sum_{j=1}^n (\delta_{ij}\phi - a_{ij})x_j = 0$$

where δ_{ij} is the Kronecker delta. Consider the matrix

$$M = \begin{bmatrix} \delta_{11}\phi - a_{11} & \delta_{12}\phi - a_{12} & ... & \delta_{1n}\phi - a_{1n} \\ \delta_{21}\phi - a_{21} & \delta_{22}\phi - a_{22} & ... & \delta_{2n}\phi - a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \delta_{n1}\phi - a_{n1} & \delta_{n2}\phi - a_{n2} & ... & \delta_{nn}\phi - a_{nn} \end{bmatrix}$$

Then, we have

$$M \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

Thus, by Cramer's rule, we have $det(M)x_i = det(M_i)$ where M_i is M with i th column replaced with 0. Therefore, we have $det(M) = 0$, which imply $det(M)$ is the expression we are looking for after we expand this out. ♡

Corollary 8.2.5.1. *Let M be finitely generated R module and I be an ideal of R such that $IM = M$. Then there exists $x \in R$ such that $x - 1 \in I$ and $xM = 0$. Note when $a - b \in I$ we also say $a \equiv b \pmod I$.*

Proof. Consider $\phi = Id$ in Proposition 8.2.5, then $1 \cdot Id + a_1 \cdot Id^2 + ... + a_n = 0$ is the zero endomorphism. Then, we let $x = 1 + a_1 + ... + a_n$ and the proof follows. Indeed, $xm = (1 + a_1 + ... + a_n)m = (1 \cdot Id + a_1 \cdot Id^2 + ... + a_n)m = 0$ for all $m \in M$. ♡

Theorem 8.2.6. *[Nakayama's Lemma] Let M be finitely generated R module. Let $I \subseteq J(R)$. Then $IM = M$ imply $M = 0$.*

Proof. Note we have $xM = 0$ for some $x \in R$ and

$$x \equiv 1 \pmod{I} \Rightarrow x \equiv 1 \pmod{J(R)}$$

Therefore, recall $x - 1 \in J(R)$ imply $x - 1$ is quasi-regular and so $(1 + (1 - x))R = R$ and so x is a unit. Thus, we have $M = x^{-1}xM = x0 = 0$ as desired. ♡

Corollary 8.2.6.1. *Let M be a finitely generated R module, N a submodule of M, and $I \subseteq J(R)$ is an ideal. Then $M = IM + N$ imply $M = N$.*

Proof. Consider the R module M/N. We have $M/N = (IM + N)/N = IM/N = I(M/N)$ and so we can apply Nakayama's lemma 8.2.6 and conclude $M/N = 0$, thus $M = N$. ♡

8.3 Exact Sequences

Definition 8.3.1. A sequence of R modules and R homomorphisms

$$... \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow ...$$

is said to be ***exact at*** M_i if $Im(f_i) = Ker(f_{i+1})$. The sequence is exact if it is exact at each M_i.

Example 8.3.2. We have

1. $0 \to M' \xrightarrow{f} M$ is exact if and only if f is injective
2. $M \xrightarrow{g} M' \to 0$ is exact if and only if g is surjective
3. $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is exact if and only if f is injective, g is surjective, and g induces an isomorphism between $Coker(f) = M/f(M')$ and M''. This is called a ***short exact sequence***

Remark 8.3.3. Any long exact sequence can be split up into short exact sequences. Indeed, consider

$$A_0 \xrightarrow{f_1} A_2 \xrightarrow{f_2} A_3 \xrightarrow{f_3} A_4 \longrightarrow ... \xrightarrow{f_n} A_n$$

Then, let $K_i = Im(f_i) = Ker(f_{i+1})$, the above long exact sequence is the equivalent to the following sequences of short exact sequence:

$$A_0 \longrightarrow K_1 \longrightarrow 0$$

$$0 \longrightarrow K_1 \longrightarrow A_1 \longrightarrow K_2 \longrightarrow 0$$

$$\vdots$$

$$0 \longrightarrow K_{n-1} \longrightarrow A_{n-1} \longrightarrow K_n \longrightarrow 0$$

$$0 \longrightarrow K_n \longrightarrow A_n$$

Proposition 8.3.4. *Let $M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$ be a sequences of R modules and homomorphisms. Then the above sequence is exact if and only if, for all R modules N, the sequence*

$$0 \longrightarrow Hom(M'', N) \xrightarrow{\overline{v}} Hom(M, N) \xrightarrow{\overline{u}} Hom(M', N)$$

is exact.

Similarly, $0 \to N' \xrightarrow{u} N \xrightarrow{v} N'' \to 0$ is exact if and only if

$$0 \longrightarrow Hom(M, N') \xrightarrow{\overline{u}} Hom(M, N) \xrightarrow{\overline{v}} Hom(M, N'')$$

is exact.

Proof. Exercises.

We show one part. Suppose for all R modules N,

$$0 \longrightarrow Hom(M'', N) \xrightarrow{\overline{v}} Hom(M, N) \xrightarrow{\overline{u}} Hom(M', N)$$

is exact. Then, since $\overline{v}$ is injective for all N it follows that v is surjective. Then, $\overline{u} \circ \overline{v} = 0$, that is $v \circ u \circ f = 0$ for all $f : M'' \to N$. Taking N to be M'' and f to be the identity mapping, it follows that $v \circ u = 0$, hence $Im(u) \subseteq Ker(v)$. Next, take $N = M/Im(u)$ and let $\phi : M \to N$ to be the projection. Then $\phi \in Ker(\overline{u})$ and hence there exists $\psi : M'' \to N$ such that $\phi = \psi \circ v$. Thus $Im(u) = Ker(\phi) \supseteq Ker(v)$. ♡

Proposition 8.3.5. *Let*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{u} & M & \xrightarrow{v} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ 0 & \longrightarrow & N' & \xrightarrow{u'} & N & \xrightarrow{v'} & N'' & \longrightarrow & 0 \end{array}$$

be a commutative diagram of R modules and homomorphisms, with the row exact. Then, there exists an exact sequence

$$0 \to Ker(f') \xrightarrow{\overline{u}} Ker(f) \xrightarrow{\overline{v}} Ker(f'') \xrightarrow{d} Coker(f') \xrightarrow{\overline{u}'} Coker(f) \xrightarrow{\overline{v}'} Coker(f'') \to 0$$

in which $\overline{u}$, $\overline{v}$ are restrictions of u, v and $\overline{u}', \overline{v}'$ are induced by u', v'.

*In addition, d, the **boundary homomorphism**, is defined as follows: if $x'' \in Ker(f'')$ then we have $x'' = v(x)$ for some $x \in M$ and $v'(f(x)) = f''(v(x)) = 0$, hence $f(x) \in Ker(v') = Lm(u')$, so that $f(x) = u'(y')$ for some $y' \in N'$. Then $d(x'')$ is defined to be the image of y' in $Coker(f')$.*

Proof. I have no idea what this is...... for the first time. ♡

Definition 8.3.6. Let C be a class of R modules and let $\lambda : C \to G$ where G is an abelian group G. The function λ is ***additive*** if, for each short exact sequence

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

in which all terms belong to C, we have $\lambda(M') - \lambda(M) + \lambda(M'') = 0$.

Example 8.3.7. Let R be a field and let C be the class of all finite-dimensional R vector spaces. Then, $V \mapsto dim(V)$ is an additive function on C.

Proposition 8.3.8. *Let $0 \to M_0 \to ... \to M_n \to 0$ be an exact sequence of R modules in which all modules M_i and the kernel of all homomorphisms belong to C. Then for any additive function λ on C we have*

$$\sum_{i=0}^{n} (-1)^i \lambda(M_i) = 0$$

Proof. Split up the sequence into short exact sequences

$$0 \to N_i \to M_i \to N_{i+1} \to 0$$

with $N_0 = N_{n+1} = 0$. Then we have $\lambda(M_i) = \lambda(N_i) + \lambda(N_{i+1})$ and the sum cancels out. ♡

Remark 8.3.9. Its finally over.

8.4 Tensor Product of Modules