Representation Theory of Finite Groups

Alex Rutar*
University of Waterloo

Fall 2019†

*arutar@uwaterloo.ca
†Last updated: October 28, 2019

Contents

I. Introduction

Let G be a finite group of order n, and write $G = \{g_1, \dots, g_n\}$. Fix $g \in G$; then $gg_i = gg_j$ if and only if $i = j$. Thus there exists some $\sigma_g \in S_i$ such that $gg_i = g_{\sigma_g(i)}$ for all $i \in \{1, 2, \dots, n\}$. In particular, $\phi : G \to S_n$ by $\phi(g) = \sigma_g$ is an embedding (injective group homomorphism). This observation is usually referred to as Cayley's Theorem.

Now let V be an n–dimensional complex vector space. We then denote $\mathrm{GL}(V)$ as the group of invertible linear operators $T : V \to V$. Now define $\psi : S_n \to \mathrm{GL}_n(V)$ by $\psi(\sigma) = T_\sigma$ where if $\{b_1, \dots, b_n\}$ is a basis for V and $T_\sigma(b_i) = b_{\sigma(i)}$. This is an injective group homomorphism, so $\psi \circ \phi : G \to \mathrm{GL}(V)$ is an embedding of G into $\mathrm{GL}(V)$.

Definition. Let G be a finite group, and V a finite dimensional $\mathbb{C}$–vector space. A **representation** of G is a group homomorphism $\rho : G \to \mathrm{GL}(V)$. We call $\dim(V)$ the **degree** of the representation.

In particular, if V is n–dimensional, then $\mathrm{GL}(V) \cong \mathrm{GL}_n(\mathbb{C})$.

Example.

1. Consider $\rho : G \to \mathrm{GL}(\mathbb{C}) \cong \mathbb{C}^\times$ given by $\rho(g) = 1$ for all $g \in G$. This is called the *trivial representation*.
2. Consider $\rho : S_n \to \mathbb{C}^\times$ given by $\rho(\sigma) = \mathrm{sgn}(\sigma)$, which is called the *sign representation*.
3. The representation fo G afforded by Cayley's theorem is called the *regular representation* of G. The next example is a good way to understand the regular rep of G.
4. Consider G, $X = \{x_1, \dots, x_n\}$, and $V = \mathrm{Free}(X)$. Suppose G acts on X. Then $\rho : G \to \mathrm{GL}(V)$ given by $\rho(g)(x_i) = gx_i$. In particular, if we take $X = G$, then this is the regular representation of G
5. Consider the 4–gon, with vertices labelled a, b, c, d. Take $X = \{a, b, c, d\}$ and the regular representation $\rho : D_4 \to \mathrm{GL}(V)$. This action has a geometric notion.
6. Let C_n be a cyclic group of order n; let us define some $\rho : C_n \to \mathrm{GL}(V)$. Say $\rho(x) = T$ where $t \in \mathrm{GL}(V)$; then this is a representation if and only if $T^n = I$.

Definition. We say that two representations $\rho : G \to \mathrm{GL}(V)$ and $\tau : G \to \mathrm{GL}(W)$ are **isomorphic** if there exists an isomorphism $T : V \to W$ such that for all $g \in G$,

$$T \circ \rho(g) = \tau(g) \circ T$$

Suppose $\rho : G \to \mathrm{GL}(V)$ and $T : V \to W$ is an isomorphism. Then we can define $\tau : G \to \mathrm{GL}(W)$ by $\tau(G) = T \circ \rho(g) \circ T^{-1}$; this $\rho \cong \tau$. In other words, the representation is unique up to isomorphism under change of basis.

Example. Consider $G = \{g_1, \dots, g_n\} = \{h_1, \dots, h_n\}$, and fix $g \in G$. Let $gg_i = g_{\alpha(i)}$ and $gh_i = h_{\beta(i)}$ where $\alpha, \beta \in S_n$. Fix an n–dimensional vector space V with basis $\{b_1, \dots, b_n\}$. Then two regular representations are given by

$$\rho_1 : G \to \mathrm{GL}(V), \rho(g)(b_i) = b_{\alpha(i)}$$
$$\rho_2 : G \to \mathrm{GL}(V), \rho(g)(b_i) = b_{\beta(i)}$$

Let $\gamma \in S_n$ be such that $h_{\gamma(i)} = g_i$, and define $T : V \to V$ by $T(v_i) = b_{\gamma(i)}$. Then

$$gg_i = g_{\alpha(i)} = gh_{\gamma(i)} = h_{\beta\gamma(i)} = g_{\gamma^{-1}\beta\gamma(i)}$$

so that $\alpha = \gamma^{-1}\beta\gamma$. Thus for each b_i,

$$\begin{aligned} T \circ \rho_1(g) \circ T^{-1}(b_i) &= T \circ \rho_1(g)(b_{\gamma^{-1}(i)}) \\ &= T(b_{\alpha\gamma^{-1}(i)})b_{\gamma\alpha\gamma^{-1}(i)} \\ &= b_{\beta(i)} = \rho_2(g)(b_i) \end{aligned}$$

so that $T \circ \rho_1(g) \circ T^{-1} = \rho_2(g)$.

Note: conjugate elements have the same cycle type.

Subrepresentations

What should a subrepresentation of $\rho : G \to \mathrm{GL}(V)$ mean?

We would like a subspace $W \leq V$ such that $\tau : G \to \mathrm{GL}(W)$ is a representation given by $\tau(g)(w) = \rho(g)(w)$ for all $w \in W$. Moreover, to make this well-defined, we need W to b4 $\rho(g)$–invariant for every $g \in G$ ($\rho(g)(W) \subseteq W$).

Suppose $T : V \to V$ is a linear operator, and $W \leq V$ is a T–invariant subspace; i.e. $T(W) \subseteq W$. In particular, the restriction operator $T_W : W \to W$ is well-defined.

Definition. Let $\rho : G \to \mathrm{GL}(V)$ be a representation. A subspqce $W \subseteq V$ is said to be ***G*–stable** if W is $\rho(g)$–invariant for all $g \in G$. A **subrepresentation** of ρ is a representation $\rho_W : G \to \mathrm{GL}(W)$ where for all $g \in G$ and $w \in W$, $\rho_W(g)(w) = \rho(g)(w)$ where W is a G–stable subspace of V.

Example. Suppose $\rho : G \to \mathrm{GL}(V)$ be the regular representation. Take $W = \mathrm{span}\{\sum_{g\in G} v_g\}$, which is clearly G–stable, and $\rho_W : G \to \mathrm{GL}(W)$ is isomorphic to the trivial representation.

Similarly, let $\rho : S_n \to \mathrm{GL}(V)$ be the regular representation, $W = \mathrm{span}\{\sum_{\sigma\in S_n} \mathrm{sgn}(\sigma)v_\sigma\}$; this is isomorphic to the sign representation.

0.1 Theorem. *Let $\rho : G \to \mathrm{GL}(V)$ be a representation, $W \leq V$ G–stable. Then there exists a G–stable subspace W' such that $V = W \oplus W'$.*

Proof Take any inner product $\langle x, y\rangle$ on V. Then for any $x, y \in V$, define

$$\langle x, y\rangle^* = \sum_{g\in G} \langle \rho(g)(x), \rho(g)(y)\rangle$$

This is also an inner product. Let $x, y \in V$ and let $h \in G$. Then

$$\begin{aligned} \langle \rho(h)(x), \rho(h)(y)\rangle^* &= \sum_{g\in G} \langle \rho(g)\rho(h)(x), \rho(g)\rho(h)(y)\rangle \\ &= \sum_{g\in G} \langle \rho(gh)(x), \rho(gh)(y)\rangle \\ &= \sum_{g\in G} \langle \rho(g)(x), \rho(g)(y)\rangle \end{aligned}$$

Thus every $\rho(h)$ is unitary with respect to $\langle\cdot,\cdot\rangle^*$. Let $W \leq V$ be G–stable, and take $W' = W^\perp$ with respect to $\langle\cdot,\cdot\rangle^*$. Then $V = W \oplus W'$. Let's see that $W^\perp$ is G–stable. Let $x \in W^\perp$, $w \in W$, and $g \in G$, so that

$$\begin{aligned}\langle \rho(g)(x), w\rangle^* &= \langle x, \rho(g)^*(w)^*\rangle = \langle x, \rho(g)^{-1}(w)\rangle^* \\ &= \langle x, \underbrace{\rho(g^{-1})(w)}_{\in W}\rangle^* \\ &= 0\end{aligned}$$

and $\rho(g)(W^\perp) \subseteq W^\perp$ as required. ∎

Definition. Let $\rho : G \to \mathrm{GL}(V)$ be a representation, and $V = W_1 \oplus W_2 \oplus \cdots \oplus W_k$ where each W_i is G–stable. For each i, let $\rho_i = \rho_{w_i}$. For each $v = \sum w_i \in V$, we have $\rho(g)(v) = \sum \rho(g)(w_i) = \rho_i(g)(w_i)$. In this case, we write

$$\rho = \rho_1 \oplus \rho_2 \oplus \cdots \oplus \rho_k$$

and call ρ a direct sum of the ρ_i's.

The previous definition is written as an internal direct sum of V. Externally, given vector spaces $W_1, \dots, W_k$ and representations $\rho_i : G \to \mathrm{GL}(W_i)$, we can define

$$(\rho_1 \oplus \cdots \oplus \rho_k) : G \to \mathrm{GL}(W_1 \oplus \cdots \oplus W_k)$$

by $(\rho_1 \oplus \cdots \oplus \rho_k)(g)(w_1, \dots, w_k) = (\rho_1(g)(w_1), \dots, \rho_k(g)(w_k))$. If $\rho_i : G \to \mathrm{GL}(W_i)$ is a subrepresentation fo $\rho : G \to \mathrm{GL}(V)$, we often say "$W_i$ is a subrepresentation of V".

Definition. Let $\rho : G \to \mathrm{GL}(V)$ be a representation. We say ρ is **irreducible** if $V \neq \{0\}$ and the only G–stable subspaces of V are $\{0\}$ and V.

Clearly,

> ***0.2 Theorem.*** *Every representation $\rho : G \to \mathrm{GL}(V)$ can be written as a direct sum of irreducible sub-representations.*

Example. Let $\rho : S_3 \to \mathrm{GL}(\mathbb{C}^3)$ be the permutation representation with respect to the standard basis $\{e_1, e_2, e_3\}$. Consider $W_1 = \mathrm{span}\{e_1 + e_2 + e_3\}$ and $W_2 = \mathrm{span}\{e_1 - e_2, e_2 - e_3\}$. Is W_2 irreducible?

More generally, if $V = W_1 \oplus \cdots \oplus W_k$ and $\dim W_i = 1$ and $\deg(\rho_i) = 1$,

$$\rho(gh)(\sum w_i) = \sum \rho_i(gh)(w_i) = \sum \rho_i(g)\rho_i(h)(w_i) = \sum \rho_i(h)\rho_i(g)(w_i)$$

so that $\rho(gh) = \rho(hg)$. In the our example, this does not happen, since $\rho(g) \neq I$ when $g \neq 1$ and S_3 is not abelian.

Example. Let $\rho : S_3 \to \mathrm{GL}(V)$ be the regular representation. Let $W_1 = \mathrm{span}\{\sum_{\sigma \in S_3} v_\sigma\}$ and $W_2 = \mathrm{span}\{\sum_{\sigma \in S_3} \mathrm{sgn}(\sigma) v_\sigma\}$, and Now let's focus on W_3. A basis for W_3 is given by

$$\begin{aligned} e_1 &= v_\epsilon - v_{(123)} & e_2 &= v_\epsilon - v_{(123)} \\ e_3 &= v_{(12)} - v_{(13)} & e_4 &= v_{(12)} - v_{(23)} \end{aligned}$$

Recall that $S_3 = \langle (12), (123)\rangle$; suffices to show stability with respect to generators.

$$\begin{aligned} \rho(12) &: e_1 \mapsto e_4, e_2 \mapsto e_3, e_3 \mapsto e_2, e_4 \mapsto e_1 \\ \rho(123) &: e_1 \mapsto e_2 - e_1, e_2 \mapsto -e_1, e_3 \mapsto e_4 - e_3, e_4 \mapsto -e_3 \end{aligned}$$

Let $U_1 = \mathrm{span}\{e_1 - e_4, e_2 + e_3 - e_1\}$

1 Tensor Products

Let $\rho : G \to \mathrm{GL}(V)$ and $\tau : G \to \mathrm{GL}(W)$ be representations. We define the representation $\rho \otimes \tau : G \to \mathrm{GL}(V \otimes W)$

$$(\rho \otimes \tau)(g)(v \otimes w) = \rho(g)(v) \otimes \tau(g)(w)$$

2 Character Theory

We define the character of ρ by $\rho : G \to \mathbb{C}$ as $\chi(G) = \mathrm{Tr}(\rho(g))$.

Remark. If we choose a basis β for V, then define $A(g) = [\rho(g)]_\beta$ and $\chi(G)$ is given by the sum of the diagonal entries of $A(g)$. Furthermore, if $A, B \in M_n(\mathbb{C})$, then $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$.

The remark implies a number of facts:

(i) $\rho \cong \tau$, then $\mathrm{Tr}(\rho(g)) = \mathrm{Tr}(\tau(g))$.

(ii) $\mathrm{Tr}(T)$ is the sum of eigenvalues of T

(iii) $\chi(1) = \dim(V)$.

2.1 Proposition. *For every $g \in G$ the eigenvalues of $\rho(g)$ have modulus 1. In particular, $\chi(g^{-1}) = \overline{\chi(g)}$.*

Proof Set $n = |G|$; then $\rho(g)^n = \rho(g^n) = I$ so that $\lambda^n - 1 = 0$ for any eigenvalue λ, so $|\lambda| = 1$. Furthermore,

$$\overline{\chi(g)} = \overline{\sum \lambda_i} = \sum \overline{\lambda_i} = \sum \lambda_i^{-1} = \chi(g^{-1})$$

proving the second component. ■

2.2 Proposition. *Let $\rho : G \to \mathrm{GL}(V)$ and $\tau : G \to \mathrm{GL}(W)$. Then $\chi_{\rho\oplus\tau} = \chi_\rho + \chi_\tau$ and $\chi_{\rho\otimes\tau} = \chi_\rho \cdot \chi_\tau$.*

Proof Let $\beta_1 = \{v_1, \dots, v_n\}$ be a basis for V and $\beta_2 = \{w_1, \dots, w_m\}$ a basis for W.

Then a basis for $V \oplus W$ is given by $\beta = \{(v_1, 0), \dots, (v_n, 0), (0, w_1), \dots, (0, w_m)\}$. In particular,

$$[(\rho \oplus \tau)(g)]_\beta = \begin{pmatrix} [\rho(g)]_{\beta_1} & \\ & [\tau(g)]_{\beta_2} \end{pmatrix}$$

and the trace result follows.

A basis for $V \otimes W$ is given by $\gamma = \{v_i \otimes w_j : 1 \le i \le n, 1 \le j \le m\}$ in lexicographic order. Fix $g \in G$, and set $A = [\rho(g)]_{\beta_1}$, $B = [\rho(g)]_{\beta_2}$. Fix $v_i \otimes w_j \in \gamma$. Then

$$\begin{aligned}
(\rho \otimes \tau)(g)(v_i \otimes w_j) &= \rho(g)(v_i) \otimes \tau(g)(w_j) \\
&= (a_{1i} v_1 + \cdots + a_{ni} v_n) \otimes (b_{1j} w_1 + \cdots + b_{mj} v_m) \\
&= \cdots + a_{ii} b_{jj} \cdot (v_i \otimes w_j) + \cdots \\
&= \mathrm{Tr}([\rho \otimes \tau)(g)]_\delta) = \sum_{i,j} a_{ii} b_{jj} = \mathrm{Tr}(A)\mathrm{Tr}() = \chi_\rho(g) \cdot \chi_\tau(g)
\end{aligned}$$ ■

Example. Suppose $\rho : S_n \to \mathrm{GL}(\mathbb{C}^n)$ is the permutation representation with respect to $\{e_1, \ldots, e_n\}$. Then $\chi(\sigma) = |\{e_i : \rho(\sigma)(e_i) = e_i\}| = |\mathrm{Fix}(\sigma)|$, which is the number of indices i fixed by σ. Since S_n acts transitively on $\{1, \ldots, n\}$, there is exactly 1 orbit, so by Burnside's lemma,

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

Example. Let $\rho : G \to \mathrm{GL}(V)$ be the regular representation. Note that if $g \neq 1$, then for all $h \in G$, $gh \neq h$. In particular, this means that $\chi(g) = 0$ if $g \neq 1$, and $\chi(1) = |G|$ (the dimension of V).

Example. Let $\rho : S_3 \to \mathrm{GL}(V)$ be the regular representation. Recall that $V = W_1 \oplus W_2 \oplus U_1 \oplus U_2$ where W_1 is the trivial representation, W_2 is the sign representation, and U_1, U_2 are isomorphic. Let $S_3 = \langle (12), (123) \rangle$; then we have

x_1	1	1
x_2	-1	1
x_3	a	b
x_4	a	b

In particular, $\chi(12) = 1 - 1 + 2a = 0$ and $\chi(123) = 1 + 1 + 2b = 0$, so $b = -1$.

Example. Let $\rho : G \to \mathrm{GL}(V)$ be a representation. In particular, $\rho(ghg^{-1}) = \rho(g)\rho(h)\rho(g)$ so that $\mathrm{Tr}\,\rho(ghg^{-1}) = \mathrm{Tr}\,\rho(h)$ so $\chi(ghg^{-1}) = \chi(h)$; in other words, that characters are constant on conjugacy classes.

2.3 Lemma. (Schur) *Let $\rho : G \to \mathrm{GL}(V)$ and $\tau : G \to \mathrm{GL}(W)$ be irreducible representations, and suppose $T : V \to W$ is linear such that for all $g \in G$, $\tau(g) \circ T = T \circ \rho(g)$. Then either $T = 0$ or T is an isomorphism and $\rho \cong \tau$. Moreover, if $V = W$ and $\rho = \tau$, then T is a scalar multiple of the identity.*

Proof Assume $T \neq 0$.

Let's first see that T is injective, and let $v \in \ker(T)$. Then for any $g \in G$, $T(\rho(g)(v)) = \tau(g)(T(v)) = 0$, so $\rho(g)(v) \in \ker(T)$. Thus $\ker(T)$ is G–stable (with respect to ρ). Since ρ is irreducible and $T \neq 0$, $\ker(T) = \{0\}$.

We also have that T is surjective. Let $v \in \mathrm{Im}(T)$ and say $v = T(X)$ with $x \in V$. Then for $g \in G$, $\tau(g)(v) = \tau(g)(T(x)) = T(\rho(g)(x)) \in \mathrm{Im}(T)$ so $\mathrm{Im}(T)$ is G–stable, and again by irreducibility of τ, $\mathrm{Im}(T) = W$. Thus T is an isomorphism.

Now let $\lambda \in \mathbb{C}$ be an eigenvalue of T and consider $T' = T - \lambda I$. Now, note that for $g \in G$, $\rho(g)T' = T'\rho(g)$, but T' has non-trivial kernel, so in fact $T' = 0$. ■

2.4 Corollary. *Let $\rho : G \to \mathrm{GL}(V)$ and $\tau : G \to \mathrm{GL}(W)$ be irreducible, and $T : V \to W$ linear. Consider*

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

Then

(i) If $T' \neq 0$, then $\rho \cong \tau$ via T'.
(ii) If $V = W$, $\rho = \tau$, then $T' = \mathrm{Tr}(T)/\dim(V) \cdot I$.

Proof Clearly $T' : V \to W$ is linear, and for any $h \in G$,

$$\begin{aligned}\tau(h)T' &= \tau(h)\frac{1}{|H|}\sum_{g\in G}\tau(g^{-1})T\rho(g)\\ &= \frac{1}{|G|}\sum_{g\in G}\tau(hg^{-1})T\rho(g)\\ &= \frac{1}{|G|}\sum_{g\in G}\tau(g^{-1})T(\rho(gh))\\ &= \frac{1}{|G|}\sum_{g\in G}\tau(g^{-1})T\rho(g)\rho(h)\\ &= T'\rho(h)\end{aligned}$$

If $V = W$ and $\rho = T$, then $\mathrm{Tr}(T') = \frac{1}{|G|}\mathrm{Tr}(T)\cdot|G| = \mathrm{Tr}(T) = \alpha\dim(V)$, so $\alpha = \mathrm{Tr}(T)/\dim(V)$.■

Let $\rho : G \to \mathrm{GL}(V)$ and $\tau : G \to \mathrm{GL}(W)$ be irreducible representations, and $T : V \to W$ linear. Let β be a basis for V and γ a basis for W. Then for $g \in G$, let $[\rho(g)]_\beta = (a_{ij}(g))$, $[\tau(g)]_\gamma = (b_{kl}(g))$, $[T]_\beta^\gamma = (X_{ki})$, and $[T']_\beta^\gamma = (x'_{ki})$.

By matrix multiplication, $x'_{ki} = \frac{1}{|G|}\sum_g\sum_{j,l} b_{kl}(g^{-1})x_{lj}a_{ji}$. If $\rho \not\cong \tau$, then $T' = 0$, so by viewing the RHS as a polynomial in the x_{ij}, we have

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

But now it $\rho = \tau$, then $T' = \lambda I$ where $\lambda = \mathrm{Tr}(T)/\dim(B)$ so that

$$\frac{1}{|G|}\sum_g\sum_{j,l} a_{kl}(g^{-1})x_{lj}a_{ji}(g) = \lambda\delta_{ki} = \frac{1}{\dim(V)}\sum_{j,l}\delta_{ki}\delta_{jl}x_{lj}$$

Then by equating coefficients of x_{lj}, we have

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

Remark. If G is a finite group, the consider the vector space of all functions $\phi : G \to \mathbb{C}$. For any ϕ, ψ in this vector space, $\langle\phi,\psi\rangle = \frac{1}{|G|}\sum_g \phi(g)\overline{\psi(g)}$ defines an inner product. Then if χ_1, χ_2 are characters of G, then

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

We thus have:

2.5 Theorem. *If χ is a character of an irreducible representation, then $\langle\chi,\chi = 1$, and if χ_1 and χ_2 correspond to non-isomorphic representations, then $\langle\chi_1,\chi_2\rangle = 0$.*

Proof Say $[\rho(g)]_\beta = (a_{ij}(g))$ where ρ is an irreducible representation with character χ. Then

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

To see the second part,

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{|G|}\sum_g \chi_1(g)\chi_2(g^{-1}) = \frac{1}{|G|}\sum_g \sum_{ij} a_{ii}(g)a_{jj}(g^{-1}) = \sum_{i,j} 0 = 0$$ ■

If χ is a character corresponding to an irreducible representation, we say χ is irreducible. If ρ and τ are isomorphic representations, we say χ_ρ and χ_τ are isomorphic (in fact $\chi_\rho = \chi_\tau$).

2.6 Corollary. *Let $\rho : G \to \mathrm{GL}(V)$ be a representation with character χ. Say $V = W_1 \oplus \cdots \oplus W_k$ is an irreducible decomposition of V. If $\tau : G \to \mathrm{GL}(W)$ is an irreducible representations with character ϕ, then the number of W_i isomorphic to W (i.e. $\rho_i \cong \tau$) is $\langle \chi, \phi \rangle$.*

Proof Write $\chi = n_1\chi_1 + \cdots + n_l\chi_l$, where the χ_i are pairwise non-isomorphic. Then $\langle \chi, \chi_i \rangle = n_i$. ■

Let $\tau : G \to \mathrm{GL}(V)$ be irreducible, and let τ have character φ. Then

$$\langle \chi, \varphi \rangle = \sum_{i=1}^k \langle \chi_i, \varphi \rangle$$

Now, $\langle \chi_i, \varphi \rangle = 1$ if and only if $\rho_i \cong \tau$, so that $\langle \chi, \varphi \rangle$ counts the number of times in which τ appears in the irreducible decomposition of ρ.

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

Proof They have the same irreducible decomposition. ■

2.8 Corollary. *If $\rho : G \to \mathrm{GL}(V)$ is a representation and χ is a character, then $\langle \chi, \chi \rangle \in \mathbb{N}$ and $\langle \chi, \chi \rangle = 1$ if and only if χ is ireducible.*

Proof If $\chi_1, \ldots, \chi_k$ are irreducible, write $\chi = n_1\chi_1 + \cdots + n_k\chi_k$ so that $\langle \chi, \chi \rangle = n_1^2 + \cdots + n_k^2 \in \mathbb{N}$. ■

2.9 Proposition. *Every irreducible representation of G occurs as a subgroup fo the regular representation of G, with multiplicity equal to its degree.*

Proof Let χ be an irreducible character of G. Then

$$\langle \chi, \chi_{\text{reg}} \rangle = \frac{1}{|G|} \sum_g \chi(g) \overline{\chi_{\text{reg}}(g)} = \frac{1}{|G|} \chi(1) \overline{\chi_{\text{reg}}(1)} = \frac{1}{|G|} \deg(\chi) \qquad \blacksquare$$

2.10 Corollary. *Let $\chi_1, \dots, \chi_k$ be the distinct irreducible characters of G, with $\deg(\chi_i) = n_i$. Then $\sum n_i^2 = |G|$ for for $g \neq 1$, $\sum_{i=1}^k n_1 \chi_i(g) = 0$*

Proof Recall that $\chi_{\text{reg}} = n_1\chi_1 + \cdots + n_k\chi_k$. Then $\chi_{\text{reg}}(1) = |G| = n_1^2 + \cdots + n_k^2$, and evaluation at $g \neq 1$ gives the desired result. $\blacksquare$

Definition. 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. for all $a, b \in G$, $f(bab^{-1}) = f(a)$.

2.11 Proposition. *Let $\rho : G \to \mathrm{GL}(V)$ be a representation. Then*

$$\rho_f = \sum_g f(g)\rho(g)$$

is a linear operator on V. If ρ is irreducible of degree n, then $\rho_f = \lambda I$, where $\lambda = \frac{|G|}{n}\langle f, \overline{x} \rangle$ where χ is the character of ρ.

Proof Note that

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

so by Schur, $\rho_f = \lambda I$ where $\lambda = \mathrm{Tr}(\rho_f)/n$. However, $\mathrm{Tr}(\rho_f) = \mathrm{Tr}(\sum_g f(g)\rho(g)) = \sum_g f(g)\chi(g) = |G|\langle f, \overline{x} \rangle$. $\blacksquare$

Recall that
- $\langle \chi, \chi \rangle = 1$ if and only if χ is irreducible
- If χ_ρ and χ_τ are irreducible then $\langle \chi_\rho, \chi_\tau \rangle = 0$ if $\rho \ncong \tau$, and 1 otherwise.
- If χ' is an irreducible subrepresentation of χ, then $\langle \chi, \chi' \rangle$ is the multiplicity of χ' in χ.
- $|G| = n_1^2 + \cdots + n_k^2$ where n_i is the multiplicity of χ_i as an irreducible subrepresentation of the regular representation.
- Every irreducible character is a character of some subrepresentation of the regular rep?
- ... every irreducible represetation is a subrepresentation of the regular rep?

and

$$\rho_f = \sum_g f(g)\rho(g) = \lambda I$$

where $\lambda = |G|/\dim(V) \cdot \langle f, \overline{\chi} \rangle$.

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

Proof Let $\beta = \{\chi_1, \ldots, \chi_k\}$ be the irreducible characters of G. We know that β is orthonormal, and hence linearly independent. Let $W = \mathrm{span}(\beta)$. To show $W = V$ where V is the space of class functions, we prove that $W^\perp = \{0\}$. Let $f \in W^\perp$, and suppose $\rho : G \to \mathrm{GL}(V)$ is irreducible. By A2, $\overline{\chi}_1, \ldots, \overline{\chi}_k$ are all irreducible characters of G. Thus $\rho_f = 0$. By considering irreducible decompositions, $\rho_f = 0$ for all representations $\rho : G \to \mathrm{GL}(V)$. In particular, when ρ is the regular representation,

$$0 = \rho_f(v_1) = \sum_g f(g)\rho(g)(v_1) = \sum_g f(g) v_g$$

so by independence of $\{v_g : g \in G\}$, $f(g) = 0$ for all $g \in G$. ∎

2.13 Corollary. *The number of irreducible characters of G is equal to the number of conjugacy classes of G.*

Proof Let $C_1, \ldots, C_k$ be the conjugacy classes. Then a basis for $V_{\text{class}} = \{\phi_1, \ldots, \phi_k\}$ where each ϕ_i is the indicator for C_i. Since bases must have the same size, the result follows. ∎

2.14 Proposition. *Let G be a group, $g \in G$, and O_g the conjugacy class of g. Let $\chi_1, \ldots, \chi_k$ be the irreducible characters of G. Then*

1. $\sum_{i=1}^k |\chi_i(g)|^2 = |G|/|O_g|$
2. *If h is not conjugate to g, then* $\sum_{i=1}^k \chi_i(g)\overline{\chi_i(h)} = 0$.

Proof Define $\phi : G \to \mathbb{C}$ where $\phi(x)$ is the indicator function for O_g. Write $\phi = \sum_{i=1}^k \lambda_i \chi_i$ where

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

Therefore,

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

Then the result follows by evaluating ϕ at g and h. ∎

Example. Let's compute the character table of S_3. There are 2 degree 1 representations, and 3 irreducible characters since there are three conjugacy classes (cycle types). In particular, $|S_3| = 6 = 1^2 + 1^2 + n_3^2$, so $n_3 = 2$.

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

Note that the columns must be orthogonal, so by the previous proposition, we have $a = 0$ and $b = -1$.

Let $\chi_1, \ldots, \chi_k$ be the irreducible characters of G. Then $\sum_{g|\chi_i}^2 = |G|$ and $\sum_{i=1}^k |\chi_i(g)|^2 = |G|/|O_g|$.

Let G be abelian. By A1, G has $|G|$ representations of degree 1, and $[G : [G,G] = |G|$. Since G as $|G|$ conjugacy classes, these are all of the irreducible representations of G. Suppose G is a group whose irreducible representations are all degree one. Since $n_1^2 + \cdots + n_k^2 = |G|$, then $k = |G|$.

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

Proof Let $\rho : G \to \mathrm{GL}(V)$ be an irreducible representation of G. Consider the restriction $\tilde{\rho} : H \to \mathrm{GL}(V)$. Let $W \leq V$ be an irreducible subrepresentation of $\tilde{G}$. Since H is abelian, $\dim W = 1$. Suppose $W = \mathrm{span}\{x\}$, and let $W' = \{\rho(g)(x) : g \in G\}$ so that V' is G–stable, and in fact $V' = V$ since ρ is irreducible.

Take $g \in G$ and $h \in H$, so $\rho(gh) = \rho(g)\rho(h)(x) = \rho(g)(\alpha x) = \alpha\rho(g)(x)$ Say $g_1, \ldots, g_m$ are coset representatives of H in G. Then $V = V' = \mathrm{span}\{\rho(g_i)(x) : 1 \leq i \leq m\}$, then $\dim(V) \leq m = [G : H]$. ■

Example. Consider D_4. Then the number of degree 1 representations is $[D_4 : \langle r^2 \rangle] = 4$. Since there are 5 conjugacy classes, we know that there are 5 irreducible representations, so that $n_5^2 = 8$. Let's make the character table:

D_4	1	r	r^2	s	rs
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

But then by column orthogonality, we have $a = 0$, $b = -2$, $c = 0$, $d = 0$.

Example. Consider S_4. Then $[S_4 : A_4] = 2$ so there are two degree 1 representations (the trivial and the sign), and the conjugacy classes are given by 1, (12), (12)(34), (123), (1234), so there are 5 irreducible representations. Since $24^2 = 1^2 + 1^2 + n_3^2 + n_4^2 + n_5^2$, we have $22 = n_3^2 + n_4^2 + n_5^2$, which forces $n_3 = 2$ and $n_4 = n_5 = 3$. Now we have

D_4	1	(12)	(12)(34)	(123)	(1234)
χ_1	1	1	1	1	1
χ_2	1	−1	1	1	−1
χ_3	2	1	1	−1	−1
χ_4	3	−1	1	−1	1
χ_5	3	a	b	c	d

Note that $K = \{1, (12)(34), (13)(24), (14)(23)\} \trianglelefteq S_4$ and $H = \{1, (12), (13), (123), (132), (23)\}$, so $S_4 = KH$. Let ρ be an irreducible representation of H of degree 2:

S_3	1	(12)	(123)
α_1	1	1	1
α_2	1	−1	1
α_3	2	0	−1

Then $\rho : S_4 \to \mathrm{GL}(V)$ by $\rho(kh) := \rho(h)$ is an irreducible representation of S_4 since $K \trianglelefteq S_4$.

3 Induced Representations

Given a subgroup $H \leq G$ and a representation $\rho : H \to \mathrm{GL}(V)$, construct a representation of G. Let $H \leq G$ and $\rho : H \to \mathrm{GL}(V)$ a representation. Say the cosets of H in G are $g_1H, \dots, g_mH$. For each i, let $g_iV = \{g_iv : v \in V\}$ be an isomorphic copy of G, and let $W = \bigoplus_{i=1}^m g_iV$ so that every $w \in W$ can be uniquely written as $w = g_1v_1 + \cdots + g_mv_m$, where $m = [G : H]$. Fix $g \in G$; then there exists $\pi \in S_m$ such that for every i, $gg_i = g_{\pi(i)}h_i$, $h_i \in H$. We then define $\mathrm{Ind}_H^G(\rho) : G \to \mathrm{GL}(W)$ by

$$\mathrm{Ind}_H^G(\rho)(g)(\sum g_iw_i0 = \sum g_{\pi(i)}\rho(h_i)v_i$$

Example. Let $\{1\} \leq G$ and suppose $\rho : \{1\} \to \mathrm{GL}(\mathbb{C})$ is the trivial representation. Then $G = \{g_1, \dots, g_n\}$. Then for $g \in G$, $gg_i1 \in G$ and

$$\mathrm{Ind}(\rho)(s)\left(\sum_{i=1}^n g_i\alpha_i\right) = \sum gg_i\rho(1)(\alpha_i) = \sum gg_i\alpha_i$$

so that $\mathrm{Ind}(\rho)$ is isomorphic to the regular representation.

Example. Consider $\langle r\rangle \leq D_n$, and let $\rho : \langle r\rangle \to \mathrm{GL}(\mathbb{C})$ be given by $\rho(r)(1) = \zeta_n$. Let the coset representatives be given by ϵ and s.

(i) Let $r \in D_n$¡ so $r\epsilon = \epsilon r$ and $rs = sr^{n-1}$. Fix $W = \epsilon\mathbb{C} \oplus s\mathbb{C}$. Then $\mathrm{Ind}(\rho) : D_n \to \mathrm{GL}(W)$ is given by $\mathrm{Ind}(\rho)(r)(\epsilon\alpha_1 + s\alpha_2) = \epsilon\zeta_n\alpha + 1 + s\zeta_n^{n-1}\alpha_2$.

(ii) Let $s \in D_n$. Then $s\epsilon = s\epsilon$ and $ss = \epsilon\epsilon$. Then $\mathrm{Ind}(\rho)(s)(\epsilon\alpha_1 + s\alpha_2) = s\rho(\epsilon)(\alpha_1) + \epsilon\rho(\epsilon)(\alpha_2) = s\alpha_1 + \epsilon\alpha_2$.

Take the basis $\beta = \{\epsilon, s\}$ for W, so we have

$$[\mathrm{Ind}(\rho)(r)]_\beta = \begin{pmatrix} \zeta_n & 0 \\ 0 & \zeta_n^{n-1} \end{pmatrix} \quad [\mathrm{Ind}(\rho)(s)]_\beta = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

4 Non-Commutative Module Theory

Let R be a ring with unity and $(M, +)$ an abelian group. We can equip $\mathrm{End}(M)$ with a ring structure given by $(f + g)(x) = f(x) + g(x)$ and $fg(x) = f(g(x))$.

Definition. A (left) R–module is an abelian group $(M, +)$ equipped with a unitary ring homomorphism $\alpha : A \to \mathrm{End}(M)$.

This map α defines a multiplication between elements of r and m given by $rm = \alpha(r)(m)$.

Example. (i) If F is a field, a F–module is a F–vector space.
(ii) M is a $\mathbb{Z}$–module if and only if M is an abelian group.
(iii) R is an R–module (left multiplication)
(iv) If I is a left ideal of R, then I is a left R–module.
(v) $R = M_n(F)$, and $V = F^n$. Then V is an R–module.
(vi) Let R be a ring and I a left ideal of R. Then $R/I = \{a + I : a \in R\}$, so R/I is an R–module with $r(a + I) = ra + I$.

Let M be an R–module. We say a subgroup $(N,+)$ of $(M,+)$ is an R–submodule of M if N is $\alpha(r)$–invariant for each $r \in R$.

Definition. Let G be a finite group and F a field. We define the group algebra $F[G] = \{\alpha_1 g_1 + \cdots + \alpha_n g_n : \alpha_i \in F\}$ equipped with G–pointwise addition and multiplication $ag_i \cdot bg_j = (ab)g_i g_j$, extended by distributivity.

Example. Let M be a $\mathbb{C}[G]$–module. Then M is also a $\mathbb{C}$–vector space, and $\rho : G \to \mathrm{GL}(M)$ given by $\rho(g)(m) = gm$ is a representation.

Example. If $\rho : G \to \mathrm{GL}(V)$ be a representation, the ρ induces a $\mathbb{C}[G]$–multiplication on V, making V a $\mathbb{C}[G]$–module. Moreover, if $N \leq M$ is a submodule, then it is $\rho(cg)$–invariant for any $cg \in \mathbb{C}[G]$ if and only if N as a subspace of M is G–stable.

To be precise, we have $cg \cdot v = \rho(g)(cv)$. In fact, there is an isomorphic of categories from representations of G and $\mathbb{C}[G]$-modules.

Definition. Let N, M be R–modules. We say $\psi : N \to M$ is a (module) homomorphism if ϕ commutes with the structures on N and M.

If $\phi : N \to M$ is a homomorphism where N, M are $\mathbb{C}[G]$–modules, with multiplication maps ρ and τ. Then $\phi \circ \rho = \tau \circ \phi$, in other words that it is an intertwining map. Note that $\rho : G \to \mathrm{GL}(V)$ is faithful if only if the unique zero map on v is 0.

Definition. Let M be an R–module. The **annhilator** $\mathrm{Ann}(M) = \{r \in R : rm = 0\}$. Then M is **faithful** if $\mathrm{Ann}(M) = (0)$.

4.1 Proposition. *Let M be an R–module. Then $\mathrm{Ann}(M)$ is a (2-sided) ideal of R. Moreover, M is a faithful $R/\mathrm{Ann}(M)$–module.*

Definition. An R–module M is **irreducible** if $M \neq (0)$ and the only submdules of M are (0) and M.

Recall that a division ring is a unital ring such that every non-zero element is invertible.

4.2 Theorem. (Schur) *Let M be an irreducible R–module. Then $\mathrm{End}_R(M)$ is a division ring.*

4.3 Theorem. *Let M, N be R–modules and let $\psi : M \to N$ be a module homomorphism. Then $M/\ker\psi \cong \psi(M) \leq N$.*

4.4 Proposition. *Let M is an irreducible R–module, then $M \cong R/I$, where I is a maximal left ideal. Conversely, if I is a maximal let ideal, then R/I is irreducible.*

Proof Let M be an irreducible R–module and fix $0 \neq m \in M$, and define $\phi : R \to M$ by $\phi(r) = rm$, so ϕ is a homomorphism and $R/\ker\phi \cong \phi(R) = M$ by irreducibility. But then I is maximal since $R/I \cong M$ is simple. ∎

Definition. Let R be a ring. Then the **Jacobson radical** of R is $J(R) = \bigcap_{\text{irred left } M} \mathrm{Ann}(M)$.

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

4.5 Theorem. *If R is a ring, then the following are equivalent:*

(i) $a \in J(R)$.
(ii) *Ra is left quasiregular*
(iii) $a \in \bigcap_{I \leq R \text{ maximal}} I$.

Proof ($i \Rightarrow ii$) Let $a \in J(R)$ and for contradiction assume for some $x \in R$ $R(1+xa) \neq R$. Thus there exists a maximal let ideal I such that $R(1+xa) \subseteq I$, so that R/I is an irreducible R–module. Thus $a(R/I) = (0)$, so that $a(\overline{1}) = \overline{a} = \overline{0}$, so $xa \in I$ and $1 \in I$, a contradiction.

($ii \Rightarrow iii$) Assume Ra is left quasiregular. Assume there exists some maximal left ideal I with $a \notin I$. Since R/I is irreducible, $I + Ra/I \leq R/I$ is a non-zero ideal. By irreducibility, $I + Ra/I = R/I$, so there exists $x \in R$ so that $\overline{xa} = \overline{-1}$, so $1 + xa \in I$ is left-invertible, so $I = R$, a contradiction.

($iii \Rightarrow i$) Let $A = \bigcap_{I \text{ left max}} I$. Suppose there exists an irreducible module M so that $AM \neq (0)$. Then there exists $0 \neq m \in M$ such that $Am \neq (0)$. Note that am is a left R–submodule of M, so there exists $a \in A$ so that $am = -m$. Thus $(1+a)m = 0$, so if $(1+a)$ is in a maximal left ideal, then $1 + a - a$ is as well. Thus $(1+a)$ is left-invertible, so $m = 0$, a contradiction. ■

Remark.

$$J(R) = \bigcap_{M \text{ irreducible}} \mathrm{Ann}(M) = \bigcap_{\text{left max}} I = \sum_{\text{left quasi-reg}} Ra$$

Let $a \in J(R)$, $x \in R$, and suppose $R(1+ax) \neq R$, so $R(1+ax) \subseteq I$ where I is left maximal. Thus R/I is irreducible, so $a(x+I) = \overline{0}$, so $ax \in I$, so $1 \in I$.

If $a \in J(R)$, then $1+a$ is invertible so get $b \in R$ so that $b(1+a)-a$. Then since $a+b+ba = 0$, so $b \in J(R)$. By the same argumetn, get $c \in J(R)$ with $c(1+b) = -b$. But then subtracting, manipulating, we get $cb = ba$ so that $a+b = b+c$ and in fact $a = c$. Thus $(1+a)b = b+ab = b+cb = -a$. Thus $(1+a)b = -a$, so $(1+a)R = R$. Thus $J(R) = \{x : xr \text{ is right quasiregular}\}$.

Definition. A ring is **semiprimitive** if $J(R) = (0)$.

Recall that

$$J(R) = \bigcap_{\text{left max}} I = \bigcap_{\text{irred left}} \mathrm{Ann}(M) = \bigcap_{\text{left quasi-ref}} \{Ra : \forall x, R(1+xa) = R\}$$

Example.

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

Definition. Let R be a ring. We say $a \in R$ is **nilpotent** if there exists $n = n(a) \in \mathbb{N}$ such that $a^n = 0$. An ideal (left,right,both) is **nil** if every element is nilpotent. An ideal I (left,right,both) is **nilpotent** if there exists some $n \in \mathbb{N}$ such that $I^n = (0)$.

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

Proof It suffices to show that for every nil element a that $(1+a)$ is invertible. Indeed, since $a^n = 0$ for some n, $(1 - a + a^2 - \cdots + (-1)^{n-1}a^{n-1})(1+a) = 1$. ■

4.7 Proposition. $J\left(R/J(R)\right) = (0)$*, in other words,* $R/J(R)$ *is semiprimitive.*

Proof

$$J\left(R/J(R)\right) = \bigcap_{\substack{I \subseteq R \text{ max} \\ J(R) \subseteq I}} I/J(R) = \bigcap_{\substack{I \subseteq R \\ \text{left max}}} I/J(R) = J(R)/J(R) = (0)$$ ■

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

Example. (i) $\mathbb{Z}$ is not Artinian.

(ii) If R Artinian, then $M_n(R)$ is Artinian. If I is an ideal of $M_n(R)$, then $I = M_n(I')$ where I' is an ideal of R.

(iii) Division rings are artinian

(iv) Suppose R is an F−algebra, where F is a field (isomorphic copy of F contained in the center of R). If $\dim_F R < \infty$, then R is Artinian

(v) If F is a field and G is a finite group, then $F[G]$ is Artinian since $\dim F[G] = |G| < \infty$

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

Proof Consider $J(R) \supseteq J(R)^2 \supseteq \cdots$. Thus there exists N such that $J(R)^k = J(R)^n$ for all $k \geq N$. Let $I = J(R)^N$; let's see that $I = (0)$. Suppose $I \neq (0)$. Let A be a minimal left ideal fo R such that $IA \neq (0)$. Let $a \in A$ so that $Ia \neq (0)$, so Ia is a left ideal and $I(Ia) = I^2 a = Ia$. Thus by minimality, $A = Ia$ so there is some $x \in I$ such that $a = xa$. Thus $(1-x)a = 0$ so $a = 0$, a contradiction. ■

4.9 Theorem. (Maschke) *Let G be a finite group. If F is a field such that* $\mathrm{char}(F) = 0$ *or* $\mathrm{char}(F) = p$ *does not divide $|G|$, then $F[G]$ is semiprimitive and Artinian (and hence semisimple, by the assignment).*

Proof Since $\dim_F F[G] < \infty$, $F[G]$ is Artinian. For contradiction, suppose I is a nonzer nil ideal of R. Take $0 \neq x \in I$, so $x = \sum a_g g$ where $a_h \neq 0$ for some $h \in G$. By multiplying by h^{-1}, we may assume $a_1 \neq 0$. For each $a \in F[G]$, define $T_a : F[G] \to F[G]$ by $T_a(v) = av$, so T_a is a F−linear operator. Note that $T_x = \sum a_g T_g$ so that $\mathrm{Tr}(T_x) = \sum a_g \mathrm{Tr}(T_g)$, so x is not nilpotent, a contradiction. ■

Artin-Wedderburn Theory

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

Note that primitive rings are semiprimitive.

Example. If D is a division ring, then $M_n(D)$ is primitive. In particular, D^n is faithful and irreducible

Let R be primitive and commutative. Then if M is faithful and irreducible, $M \cong R/I$ where I is a maximal ideal so R is a field.

Definition. A ring R is **simple** if $R \neq (0)$ and R has no proper non-zero two-sided ideals.

For example, $M_n(D)$ is simple. If $J \leq M_n(D)$ is an ideal, then $J = M_n(I)$ for some ideal I of D.

Remark. If R is irreducible, then R is simple. However, the converse does not hold since $M_2(\mathbb{R})$ is simple but $I = \{\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} : a, b \in \mathbb{R}\}$ is a left ideal.

4.10 Proposition. *Every simple ring is primitive.*

Proof Let R be simple and I be a maximal left ideal of R so that $M := R/I$is irreducible. Since $\mathrm{Ann}(M)$ is an ideal of R and $\mathrm{Ann}(M) \neq R$, $\mathrm{Ann}(M) = (0)$. ■

For the remainder of this section, R is primitive, M is faithful and irreducible, and $D = \mathrm{End}_R(M)$ is a division ring. We give M the structure of a D–module by $\phi \cdot m = \phi(m)$.

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

Remark. Suppose $\dim_D M < \infty$ and R acts densely on M If $\{v_1, \dots, v_n\}$ is a D–basis, then for all $w_1, \dots, w_n$, there exists $r \in R$ so that $rv_i = w_i$. Thus $R \cong \{T : M \to M : D - \text{linear}\} \cong M_n(D)$.

4.11 Lemma. *If for every finite dimensional D–subspace V of M and every $m \in M \setminus V$ there exists $r \in R$ such that $rV = (0)$ but $rm \neq 0$, then R acts densely on M.*

PROOF Let $v_1, \dots, v_n$ be D–linearly independent in M and suppose $w_1, \dots, w_n$ are in M. For each i, let $V_i = \mathrm{span}\{v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n\}$. By assumption, since $v_i \notin V_i$, there exists $t_i \in R$ so that $t_i V_i = (0)$ but $t_i v_i \neq 0$. Observe that $Rt_i v_i = M$ since M is irreducible, so get $r_i \in R$ such that $r_i t_i V_i = (0))$ and $r_i t_i v_i = w_i$. Let $t = r_1 t_1 + \cdots + r_n t_n$, so $tv_i = w_i$. ■

4.12 Theorem. (Jacobson Density) *Let R be primitive and M a faithful irreducible R–module. Then R acts densely on M.*

PROOF Let V be a finite dimensional D–subspace of M, and let $m \in M \setminus V$. We proceed by induction on $\dim V$. If $\dim V = 0$, $V = (0)$, and take $r = 1$. Proceeding inductively, suppose $\dim V > 0$ and $0 \neq w \in V$ with $V = V_0 \oplus \mathrm{span}\{w\}$, where $\dim V_0 = \dim V - 1$. Let $A(V_0) = \{x \in R : xV_0 = (0)\}$. By induction, for every $y \in V_0$, there exists $r \in A(V_0$ such that $ry \neq 0$. Note that $A(V_0)$ is a left ideal: since $w \notin V_0$, $A(v_0)w \neq (0)$ so $A(v_0)w = M$ by irreducibility. Consider $\tau : M \to M$ given by $\tau(aw) = am$, where $a \in A(v_0)$. This is well-defined for if $aw = a'w$, then $(a - a')w = 0$ so $(a - a')V = 0$ (since $V = V_0 \oplus \mathrm{span}_D\{w\}$). For contradiction, assume that if $r \in R$ and $rV = (0)$, then $rm = 0$. Thus $(a - a')m = 0$ so $am = a'm$ and $\tau(a2) = \tau(a'w)$ and τ is well-defined. Notice that $\tau \in \mathrm{End}_R(M) = D$. For all $a \in A(v_0)$, $am = \tau(aw) = a\tau(w)$ so $a(m - \tau(w)) = 0$. Thus by the inductive hypothesis, $M - \tau(w) \in V_0$, so $m \in v_0 \oplus \mathrm{span}_D(w) = V$. ■

4.13 Proposition. *If R is primitive and (left) Artinian, then $R \cong M_n(D)$ where $D \cong \mathrm{End}_R(M)$.*

PROOF We first show that $\dim_D(M) < \infty$. Suppose $\{v_1, v_2, \dots\}$ is infinite and D–linearly independent. For each m, let $I_m = \{r \in R : rv_i = 0 \text{ for } i = 1, \dots, m\}$, so that $I_1 \supseteq I_2 \supseteq \cdots$. By the JDT, R acts densely on M. In particular, for every $m > 1$, there exists $r \in R$ so that $rv_1 = \cdots = rv_{m-1} = 0$ but $rv_m = v_m \neq 0$, so $r \in I_{m-1} \setminus I_m$. Thus $I_1 \supsetneq I_2 \supsetneq \cdots$, contradicting Artinianity.

Consider the map $\phi : R \to \mathrm{End}_D(M) \cong M_n(D)$ by $\phi(r) = (v_i \mapsto rv_i)$. Then by the homework, this is a ring isomorphism. ■

In particular, on A4, we prove that every semiprimitive Artinian ring is a finite direct sum of primitive Artinian rings. We thus have

4.14 Theorem. (Artin-Wedderburn) *Every semiprimitive Artinian (i.e. semisimple) ring is isomorphic to a finite direct sum of matrix rings over division rings, i.e. $R \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$*

Note that the D_i and the n_i are unique up to reordering.

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

Let R be primitive F–algebra where F is a field. Let M be a faithful, irreducible R–module, and $D = \mathrm{End}_R(M)$. For $\alpha \in F$, consider $\phi_\alpha : M \to \mathcal{M}$ given by $\phi_\alpha(m) = \alpha m$ since $F \subseteq Z(R)$, $\phi_\alpha \in D$.

Now define $\psi : F \to D$ by $\psi(\alpha) = \phi_\alpha$, which is an injective homomorphism. Furthermore, for each $\psi \in D$, $\psi(\phi_\alpha(m)) = \phi(\alpha m) = \phi_\alpha(\phi(m))$ so $\phi(\phi_\alpha(m)) = \phi(\alpha m) = \alpha\phi(m) = \phi_\alpha(\phi(m))$ so $\phi \circ \phi_\alpha = \phi_\alpha \circ \phi$, so D is an F–algebra.

4.16 Lemma. *Suppose $F = \overline{F}$. If D is a division F–algebra which is algebraic over F, then $D = F$.*

Proof Let $a \in D$, and let $p(x) \in F[x]$ with $p(a) = 0$. Then $p(x) = \prod_i (x - \lambda_i)$ with $\lambda_i \in F$. However, $p(a) = \prod_i (a - \lambda_i)$ since $F \subseteq Z(D)$. Since D is a division ring, $(a - \lambda_i) = 0$ so that $a = \lambda_i \in F$. ∎

Remark. Suppose D is a division F–algebra. If $\dim_F(D) < \infty$, then D is algebraic over F.

4.17 Theorem. *Let $F = \overline{F}$. If R is a finite dimensional semisimple F–algebra, then $R \cong M_{n_1}(F) \oplus \cdots \oplus M_{n_k}(F)$.*

Proof Write $R \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$, so that $\dim_F(D_i) < \infty$. Thus since each D_i is an F–algebra with finite dimension, each $D_i = F$. ∎

We thus have

4.18 Theorem. *If $F = \overline{F}$, G a finite group, and $\mathrm{char}\, F = 0$ or $\mathrm{char}\, F \nmid |G|$, then $F[G]$ is semisimple and thus $F[G] \cong M_{n_1}(F) \oplus \cdots \oplus M_{n_k}(F)$.*

Remark. Suppose $F = \mathbb{C}$. Then $\mathbb{C}[G] \cong M_{n_1}(\mathbb{C}) \oplus M_{n_k}(\mathbb{C})$. Taking $\dim_{\mathbb{C}}$: $|G| = n_1^2 + \cdots + n_k^2$.

5 Facts about Non-Commutative Modules

General structures on modules:

Definition. A **(left) *R*–module** is an abelian group $(M, +)$ equipped with a unitary ring homomorphism $\alpha : A \to \mathrm{End}(M)$. If N, M be R–modules, then a group homomorphism $\psi : N \to M$ is a **(module) homomorphism** if $\phi(rm) = r\phi(m)$ for any $r \in R$. The kernel and image of ψ are submodules of N and M respectively. The **annhilator** $\mathrm{Ann}(M) = \{r \in R : rm = 0\}$. Then M is **faithful** if $\mathrm{Ann}(M) = (0)$.

Annhilators:

Definition. Let R be a ring. We say $a \in R$ is **nilpotent** if there exists $n = n(a) \in \mathbb{N}$ such that $a^n = 0$. An ideal (left,right,both) is **nil** if every element is nilpotent. An ideal I (left,right,both) is **nilpotent** if there exists some $n \in \mathbb{N}$ such that $I^n = (0)$.

Key example:

Definition. Let G be a finite group and F a field. We define the **group algebra** $F[G] = \{\alpha_1 g_1 + \cdots + \alpha_n g_n : \alpha_i \in F\}$ equipped with G–pointwise addition and multiplication $ag_i \cdot bg_j = (ab)g_i g_j$, extended by distributivity.

Example. Let M be a $\mathbb{C}[G]$–module. Then M is also a $\mathbb{C}$–vector space, and $\rho : G \to \mathrm{GL}(M)$ given by $\rho(g)(m) = gm$ is a representation. If $\rho : G \to \mathrm{GL}(V)$ be a representation, the ρ induces a $\mathbb{C}[G]$–multiplication on V, making V a $\mathbb{C}[G]$–module. Moreover, if $N \leq M$ is a submodule, then it is $\rho(cg)$–invariant for any $cg \in \mathbb{C}[G]$ if and only if N as a subspace of M is G–stable. To be precise, we have $cg \cdot v = \rho(g)(cv)$. In fact, there is an isomorphic of categories from representations of G and $\mathbb{C}[G]$-modules.

Basic results on modules:

> **5.1 Proposition.** *Let M be an R–module. Then $\mathrm{Ann}(M)$ is a (2-sided) ideal of R. Moreover, M is a faithful $R/\mathrm{Ann}(M)$ –module.*

> **5.2 Theorem. (First Isomorphism)** *Let M, N be R–modules and let $\psi : M \to N$ be a module homomorphism. Then $M/\ker\psi \cong \psi(M) \leq N$.*

Types of modules:

Definition. Let M be an R–module.

- M is **irreducible** if $M \neq (0)$ and the only submodules of M are (0) and M.

Types of ideals:

Definition. Let R be a ring.

- A left ideal I of R is called **left quasiregular** if for all $a \in I$, $R(1+a) = R$.
- The **Jacobson radical** of R is $J(R) = \bigcap_{\text{irred left } M} \mathrm{Ann}(M)$.

Types of rings:

Definition. Let R be a ring.

- R **semiprimitive** if $J(R) = (0)$.
- R is **(left) Artinian** if whenever $I_1 \supseteq I_2 \supseteq \cdots$ is a descending chain of left ideals, then there exists $N \in \mathbb{N}$ such that $I_k = I_N$ for all $k \geq N$.

Relationships:

> **5.3 Proposition.** *The following hold:*
> - *Every nil left ideal of R is contained in $J(R)$.*
> - *$R/J(R)$ is semiprimitive.*
> - *If R is Artinian, then $J(R)$ is nilpotent.*
> - *M is an irreducible R–module if and only if then $M \cong R/I$ as R–modules, where I is a maximal left ideal of R.*

> **5.4 Theorem. (Schur)** *Let M be an irreducible R–module. Then $\mathrm{End}_R(M)$ is a division ring.*

> **5.5 Theorem.** *If R is a ring, then the following are equivalent:*
> *(i)* $a \in J(R)$.
> *(ii)* *Ra is left quasiregular*
> *(iii)* $a \in \bigcap_{I \leq R \text{ maximal}} I$.