Noncommutative Algebra
Winter 2005
Professor K.R. Davidson

CHRIS ALMOST

Contents

1 Rings

1.1 Definition. A *ring* is an ordered 5-tuple $(R, +, \cdot, 0, 1)$ such that

1. $(R, +, 0)$ is an Abelian group.
2. Multiplication is associative and 1 is a multiplicative identity.
3. The left and right distributive laws both hold.

1.2 Example.
1. Some commutative rings are $\mathbb{Z}$, fields $\Bbbk$, $\Bbbk[x]$, $\mathbb{Z}[x]$, $\mathscr{C}(X)$, etc.
2. Let R be a ring. $M_n(R)$, the $n \times n$ matrices over R, is a ring.
3. Let G be a group and $\Bbbk$ be a field. The group algebra,
$$\Bbbk G := \left\{ \sum_{g \in G} a_g g \mid a_g \in \Bbbk \text{ and all by finitely many are zero} \right\}$$
is a ring.
4. Let A be an Abelian group. Then
$$\mathrm{End}(A) := \{\varphi : M \to M \mid \varphi \text{ is a homomorphism}\}$$
is ring under pointwise addition and composition.

1.3 Definition. Let R, S be rings and let $\varphi : R \to S$ be a map. φ is said to be a *homomorphism* if it preserves the ring operations and $\varphi(1_R) = 1_S$. Furthermore:

1. φ is a *monomorphism* if it is 1-1.
2. φ is an *epimorphism* if it is onto.
3. φ is an *endomorphism* if $R = S$.
4. φ is an *isomorphism* if it is invertible and it φ^{-1} is also a homomorphism.
5. φ is an *automorphism* if $R = S$ and φ is an isomorphism.

1.4 Definition. Let R be a ring and $S \subseteq R$. If

1. $0, 1 \in S$
2. $S + S \subseteq S$
3. $S \cdot S \subseteq S$

then S is said to be a *subring* of R. If

1. $S + S \subseteq S$
2. $RS + SR \subseteq S$

then S is said to be an *ideal* of R. We write $S \lhd R$. S is a *left* (resp. *right*) ideal if

1. $S + S \subseteq S$
2. $RS \subseteq S$ (resp. $SR \subseteq S$)

The *centre* of R is the set $Z(R) = \{s \in R \mid rs = sr \ \forall\, r \in R\}$

Remark. $Z(R)$ is a commutative subring of R.

1.5 Proposition (First Isomorphism Theorem for Rings). *If $\varphi : R \to S$ is a homomorphism then $\varphi(R)$ is a subring of S and $\ker\varphi$ is an ideal of R. Furthermore*

$$\varphi(R) \cong R/\ker\varphi$$

1.6 Corollary. *If φ is 1-1 and onto then it is an isomorphism.*

1.7 Example.
1. $\mathcal{T}_n(R) := \{n \times n \text{ upper triangular matrices}\}$ is a subring of $M_n(R)$.
2. If $R_1, \ldots, R_n$ are rings then $R_1 \times \cdots \times R_n = \prod_{i=1}^n R_i$ is a ring under pointwise operations.
3. If R is a ring and $e \in R$ is idempotent, then eRe is a ring with identity e. Generally, eRe is not a homomorphic image of R. If $e \in Z(R)$ then $eRe = Re = eR$ and the map $\varphi : R \to Re$ defined by $\varphi(r) = re$ is a homomorphism.
4. Let G be a group and $\Bbbk$ be a field. Let $H \lhd G$ be finite and define $x = \sum_{h\in H} h$. For any $g \in G$,

$$xg = \sum_{h\in H} hg = \sum_{h\in H} gg^{-1}hg = \sum_{h\in H} gh = gx$$

Hence $x \in Z(\Bbbk G)$. Now

$$x^2 = \sum_{h\in H}\sum_{k\in H} hk = \sum_{m\in H}\sum_{h\in H} h(h^{-1}m) = |H|x$$

so $e := \frac{1}{|H|}\sum_{h\in H} h \in Z(\Bbbk G)$ is idempotent.

2 Modules

This section follows Lambek.

2.1 Introduction

2.1 Definition. Let R be a ring. A *(left) R-module* is an Abelian group $(M, +, 0)$ together with a left action of R on M given by $R \times M \to M : (r, m) \mapsto r \cdot m$ (this is really a representation $\rho : R \to \mathrm{End}(M)$ of R in $\mathrm{End}(M)$), which is to say that

1. $r \cdot (m + n) = r \cdot m + r \cdot n$ for all $r \in R$, $m, n \in M$
2. $r \cdot (s \cdot m) = (rs) \cdot m$ for all $r, s \in R$, $m \in M$
3. $(r + s) \cdot m = r \cdot m + s \cdot m$ for all $r, s \in R$, $m \in M$
4. $1 \cdot m = m$ for all $m \in M$

We sometimes write ${}_RM$ to signify that M is a left R-module. Right R-modules are defined in a similar fashion.

2.2 Example.
1. If M is a left ideal of R then ${}_RM$ is an R-module under ring multiplication. In particular, ${}_RR$ is a module over itself.
2. If $R = \Bbbk$ is a field, then the modules of R are exactly vector spaces over $\Bbbk$.
3. If $R = \mathbb{Z}$, then the modules over R are exactly the Abelian groups. There is only one possible action in this case, $n \cdot m = \underbrace{m + \cdots + m}_{n \text{ times}}$.
4. R^n under the action $r \cdot (r_1, \ldots, r_n) = (rr_1, \ldots, rr_n)$ is called the free R-module of rank n.

2.3 Definition. If M, N are R-modules then $\varphi : M \to N$ is said to be a *module homomorphism* or *R-homomorphism* if

1. φ is a group homomorphism.
2. $\varphi(rm) = r\varphi(m)$ for all $r \in R$ and $m \in M$.

The definitions for mono-, epi-, endo-, iso-, and auto- morphisms are analogous to the case for rings.

Remark. If $\varphi : M \to N$ is a 1-1 and onto R-homomorphism then φ is an isomorphism.

2.2 Submodules

2.4 Definition. A *submodule* $N \subseteq M$ is a subgroup of M such that $R \cdot N \subseteq N$. A *quotient module* M/N (where $N \subseteq M$ is a submodule) is the quotient group with the R-action $r \cdot (m+N) = r \cdot m + N$. This is clearly well-defined.

2.5 Example. Let $R = \Bbbk[x]$, polynomials over a field $\Bbbk$. Let V be a d dimensional vector space over $\Bbbk$. Take $T \in \mathscr{L}(V)$, a linear transformation. Make (V, T) into an R-module by defining $p \cdot v = p(T)v$ for any $p \in R$ and $v \in V$. What are the submodules? They are exactly the T-invariant subspaces of V. Let $W \subseteq V$ be a T-invariant subspace. Then $V = W \oplus X$ for some subpace X, and we can write

$$T = \begin{bmatrix} T|_W & (I-P)T|_X \\ 0 & PT|_X \end{bmatrix}$$

where P is the projection onto X such that $\ker P = W$. (In this case $I - P$ is projection onto W with kernel X). To find the quotient module V/W, notice that $T(x + W) = Tx + W$ and T decomposes as above, hence for any $k \geq 1$,

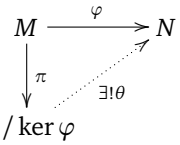
$$T^k = \begin{bmatrix} (T|_W)^k & * \\ 0 & (PT|_X)^k \end{bmatrix}$$

Thus the quotient module is isomorphic to $(X, PT|_X)$ since the R-action becomes $p \cdot (x + W) = p(PT|_X)x + W$.

2.6 Proposition (First Isomorphism Theorem for Modules). *Let R be a ring and $\varphi : M \to N$ be a module homomorphism. Then $\varphi(M)$ is a submodule of N and $\ker\varphi$ is a submodule of M. Furthermore,*

$$\varphi(M) \cong M/\ker\varphi$$

PROOF: That $\varphi(M)$ is a submodule of N and $\ker\varphi$ is a submodule of M are trivial consequences of the fact that φ is a homomorphism. We have the following commutative diagram by the first isomorphism theorem for groups, where $\theta : M/\ker\varphi \to \varphi(M)$ is a group isomorphism.



But θ is actually a module homomorphism since, for any $r \in R$ and $m \in M$,

$$\theta(rm + \ker\varphi) = \varphi(rm) = r\varphi(m) = r\theta(m + \ker\varphi)$$

□

2.7 Definition. The *annihilator* of ${}_RM$ is

$$\operatorname{ann}(M) = \{r \in R \mid rm = 0 \text{ for all } m \in M\}$$

It is the kernel of the representation ρ of R in $\operatorname{End}(M)$, so it is an ideal of R. Call M a *faithful* module if ρ is a faithful representation (that is, if ρ is 1-1, or $\operatorname{ann}(M) = 0$).

2.3 Lattices and Posets

2.8 Definition. A *paritally ordered set* or *poset* is a set S together with a relation $\leq$ such that

1. $a \leq a$ for all $a \in S$
2. $a \leq b$ and $b \leq a$ imply $a = b$ for all $a, b \in S$
3. $a \leq b$ and $b \leq c$ imply $a \leq c$ for all $a, b, c \in S$

Say $a \in S$ is *maximal* if $a \leq b$ implies $b = a$. A *chain* is a subset $C \subseteq S$ such that for each $a, b \in C$ either $a \leq b$ or $b \leq a$. An *upper bound* of a subset $T \subseteq S$ is an element $b \in S$ such that for all $a \in T$, $a \leq b$.

Remark. Notice the difference between a maximal element and an upper bound. Nothing is bigger than a maximal element, while an upper bound is bigger than everything.

2.9 Lemma (Zorn's Lemma). *If $(S, \leq)$ is a non-empty poset and every chain in S has an upper bound then S has a maximal element.*

2.10 Definition. $(L, \wedge, \vee, \leq)$ is a *lattice* if

1. $(L, \leq)$ is a poset.
2. $\wedge$ and $\vee$ binary operations that are commutative and associative.
3. $\wedge$ and $\vee$ satisfy both distributive laws.
4. $a \wedge b$ is the greatest lower bound of a and b, for all $a, b \in L$.
5. $a \vee b$ is the least upper bound of a and b, for all $a, b \in L$.

(It is part of the definition that both of these exist and are unique.) A lattice is *complete* if for any chain there is a least upper bound for that chain in the lattice.

Notation. Let M be a module. The lattice of all submodules of M is denoted by $\mathrm{Sub}(M)$.

$\mathrm{Sub}(M)$ is partially ordered by $\subseteq$. If A and B are submodules of M then $A \cap B$ is a submodule of M and it is the largest submodule of M contained in both of them. In general $A \cup B$ is not a submodule of M. $A + B$ is the smallest submodule of M that contains both A and B. Thus $(\mathrm{Sub}(M), \cap, +, \subseteq)$ is actually a lattice. It is clear that $\mathrm{Sub}(M)$ is a complete lattice since the union of any chain of modules is a module that contains all of them, and it is the smallest such module.

$\mathrm{Sub}(M)$ does not satisfy the distributive law (which states

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

for all $a, b, c \in L$). For example, if A, B, C are distinct linear subspaces of a two dimensional vector space V, then $A \cap (B + C) = A$ and $(A \cap B) + (A \cap C) = 0$. $\mathrm{Sub}(M)$ does, however, satisfy the modular law, which is the restriction of the distributive law taken to hold only when $a \geq b$ (in terms of modules,

$$A \cap (B + C) = B + (A \cap C)$$

for all $A \supseteq B, C \in \mathrm{Sub}(M)$).

2.11 Proposition. *$\mathrm{Sub}(M)$ is modular.*

2.12 Proposition. *Let M be an R-module, $S \subseteq M$, and $N \subseteq M$ a submodule such that $N \cap S = \emptyset$. Then there is a submodule $L \subseteq M$ such that $N \subseteq L$ and $L \cap S = \emptyset$ and L is maximal with respect to these properties.*

PROOF: Exercise. This is a trivial consequence of Zorn's Lemma. □

2.13 Corollary. *If R is a ring and M is a proper left (resp. right) ideal then there is a maximal left (resp. right) ideal that contains M.*

PROOF: Apply the proposition to ${}_R R$, taking $S = \{1_R\}$. □

2.4 Isomorphism Theorems

2.14 Proposition (Third Isomorphism Theorem for Modules). *Let $C \subseteq A$ be modules. The submodules of A/C correspond to submodules $C \subseteq B \subseteq A$ via $B \longleftrightarrow B/C$. Furthermore,*

$$(A/C)/(B/C) \cong A/B$$

PROOF: Let $B' \subseteq A/C$ be a submodule, and let $B = \pi^{-1}(B')$. Then $C = \pi^{-1}(\{0\}) \subseteq B \subseteq A$ and B is a submodule of A. By the First Isomorphism Theorem, $B/C \cong \pi(B) = B'$.

Let π and q be the canonical projections. Consider

$$A \xrightarrow{\pi} A/C \xrightarrow{q} (A/C)/(B/C)$$

$q \circ \pi$ is surjective and $\ker(q \circ \pi) = \pi^{-1}(\ker(q)) = \pi^{-1}(B/C) = B$, so by the First Isomorphism Theorem $(A/C)/(B/C) \cong A/B$. □

2.15 Proposition (Second Isomorphism Theorem for Modules). *If $B, C \subseteq A$ are modules then*

$$(B + C)/B \cong C/(B \cap C)$$

PROOF: Let i be inclusion and π the canonical projection. Consider

$$C \xrightarrow{i} B + C \xrightarrow{\pi} (B + C)/B$$

$\ker(\pi \circ i) = \ker(\pi) \cap C = B \cap C$, and $\pi \circ i$ is surjective since $b + c + B = 0 + c + B$ for any $b \in B$ and $i(c) = 0 + c$. By the First Isomorphism Theorem $(B + C)/B \cong C/(B \cap C)$. □

2.16 Lemma (Zazzenhaus). *Let $B' \subseteq B \subseteq A$ and $C' \subseteq C \subseteq A$ be modules. Then*

$$\frac{B' + (B \cap C)}{B' + (B \cap C')} \cong \frac{C' + (B \cap C)}{C' + (B' \cap C)}$$

PROOF: We will show both are isomorphic to $\frac{B \cap C}{(B' \cap C) + (B \cap C')}$. By symmetry it is enough to show that one of them is isomorphic to this.

$$\begin{aligned}
\frac{B' + (B \cap C)}{B' + (B \cap C')} &\cong \frac{B' + (B \cap C') + (B \cap C)}{B' + (B \cap C')} && B \cap C' \subseteq B \cap C \\
&\cong \frac{B \cap C}{(B' + (B \cap C')) \cap (B \cap C)} && 2^{\text{nd}} \text{ IT} \\
&\cong \frac{B \cap C}{(B' \cap (B \cap C)) + (B \cap C')} && \text{Modular Law} \\
&\cong \frac{B \cap C}{(B' \cap C) + (B \cap C')} && B' \subseteq B
\end{aligned}$$ □

2.17 Definition. Let $B_0 \subseteq B_1 \subseteq \cdots \subseteq B_n$ be a chain of modules. The *factor modules* are B_{i+1}/B_i, $i = 0, 1 \ldots, n-1$. A *refinement* of the chain is a larger chain that contains each of the B_i's.

2.18 Theorem (Schreier). *Suppose that $0 = A_0 \subseteq A_1 \subseteq \cdots \subseteq A_n = M$ and $0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_m = M$ are two chains of modules. Then both chains can be refined so that they have the same length and the same factors (possibly in different order).*

PROOF: Define $A_{i,j} := A_i + (A_{i+1} \cap B_j)$ for $0 \le j \le m$ and $B_{i,j} := B_j + (A_i \cap B_{j+1})$ for $0 \le i \le n$. Then $A_i = A_{i,0}$ for $i = 0, \dots, n$ and $B_j = B_{0,j}$ for $j = 0, \dots, m$. The refined chains are

$$0 = A_{0,0} \subseteq \cdots \subseteq A_{0,i} \subseteq \cdots \subseteq A_{0,m} \subseteq A_{1,0} \subseteq \cdots \subseteq A_{i,j} \subseteq \cdots \subseteq A_{n,0} = M$$

and similarily for the B chain. For $0 \le i \le n$ and $0 \le j \le m$ we have

$$\frac{A_{i,j+1}}{A_{i,j}} \cong \frac{A_i + (A_{i+1} \cap B_{j+1})}{A_i + (A_{i+1} \cap B_j)} \cong \frac{B_j + (A_{i+1} \cap B_{j+1})}{B_j + (A_i \cap B_{j+1})} \cong \frac{B_{i+1,j}}{B_{i,j}}$$

by Zazzenhaus' Lemma. □

2.5 Irreducibility

2.19 Definition. A module M is *irreducible* if it has exactly 2 submodules, namely 0 and $M \neq 0$. A *composition series* for a module M is a chain of submodules $0 = A_0 \subsetneqq A_1 \subsetneqq \cdots \subsetneqq A_n = M$ which cannot be properly refined.

In a composition series, all of the factors A_{i+1}/A_i are irreducible. We get the following corollary to Schreier's Theorem.

2.20 Corollary (Jordan-Hölder). *If M has a composition series, then any two composition series have the same length and the same factors up to permutation.*

2.21 Proposition. *An R-module M is irreducible if and only if M is isomorphic to R/A, where A is a maximal left ideal.*

PROOF: Suppose that $M \cong R/A$ for some left ideal A. The submodules of M correspond to the left ideals $A \subseteq B \subseteq R$. Thus M is irreducible if and only if A is maximal. Conversely, if M is irreducible then $M \neq 0$, so pick $0 \neq a \in M$. Let $\varphi : {}_RR \to M : r \mapsto ra$, a module homomorphism. Then $\varphi(M)$ is a non-zero submodule of M, so $\varphi(M) = M$. Therefore $M \cong R/\ker\varphi$, and $\ker\varphi$ is maximal by the observation in the first part. □

Remark. This proof also shows that if M is an irreducible R-module and $0 \neq a \in M$ then $M \cong Ra$.

2.22 Example.
1. If V is a $\Bbbk$-vector space then V is irreducible if and only if $\dim V = 1$.
2. If $R = \mathbb{Z}$ and G an Abelian group then ${}_RG$ is irreducible if and only if $G \cong C_p$ for some prime p.
3. If $R = M_2(\Bbbk)$ then for $a \in M_2(\Bbbk)$,

$$M_2(\Bbbk)a \cong \begin{cases} M_2(\Bbbk) & \text{if } a \text{ invertible} \\ \Bbbk^2 & \text{if the rank of } a \text{ is } 1 \\ 0 & \text{if } a = 0 \end{cases}$$

2.6 Noetherian and Artinian Modules

2.23 Definition. A module M is *Noetherian* if every non-empty set of submodules has a maximal element. A module M is *Artinian* if every non-empty set of submodules has a minimal element.

2.24 Proposition. *M is Noetherian if and only if Sub(M) satisfies the ascending chain condition (ACC). M is Artinian if and only if Sub(M) satisfies the descending chain condition (DCC).*

The ascending chain condition says that if $\{A_n\}_{n=1}^{\infty}$ is a sequence of submodules with $A_n \subseteq A_{n+1}$ for all $n \ge 1$ then there is N such that $A_n = A_{n+1}$ for all $n \ge N$. The descending chain condition is analogous.

PROOF: Exercise. □

2.25 Example. 1. If V a $\Bbbk$-vector space then V is Noetherian and Artinian if and only if $\dim V < \infty$.

2. In ${}_{\mathbb{Z}}\mathbb{Z}$, any ascending chain of ideals is finite since $n\mathbb{Z} \subseteq m\mathbb{Z}$ if and only if $m|n$, so ${}_{\mathbb{Z}}\mathbb{Z}$ is Noetherian. $\mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \supset \cdots$, is a descending chain of ideals, so ${}_{\mathbb{Z}}\mathbb{Z}$ is not Artinian.

2.26 Definition. A module M is *finitely generated* if $M = \langle b_1, \ldots, b_n \rangle := \sum_{i=1}^{n} Rb_i$.

2.27 Proposition. *A module M is Noetherian if and only if every submodule is finitely generated.*

PROOF: Suppose M is Noetherian and $B \subseteq M$ is a submodule. Let $\mathscr{S}$ be the set of finitely generated submodules of B. Then $\mathscr{S} \subseteq \mathrm{Sub}(M)$, so $\mathscr{S}$ has a maximal element C_0. If $B \neq C_0$ then there is $b \in B \setminus C_0$, and $C_0 \subsetneqq C_0 + Rb \subseteq B$ is finitely generated, contradicting maximality of C_0. Therefore for $B = C_0$ is finitely generated.

Conversely, let $A_1 \subset A_2 \subset \cdots$ be an ascending chain of submodules. Let $A = \bigcup_{n=1}^{\infty} A_n$, a submodule of M. Then by assumption A is finitely generated, say $A = \langle a_1, \ldots, a_k \rangle$. But then there is some A_N such that $a_1, \ldots, a_k \in A_N$, which implies that $A \subseteq A_N$. Thus $A = A_N = A_{N+1} = \cdots$, so M satisfies the ACC. □

2.28 Proposition. *Let A be a module and $B \subseteq A$ a submodule. A is Artinian (resp. Noetherian) if and only if B and A/B are Artinian (resp. Noetherian).*

PROOF: (Artinian case.) Assume A is Artinian. If S is a set of submodules of B then S is a set of submodules of A, so there is a minimal element. If S is a set of submodules of A/B then there is a bijection between S and a set S' of submodules of A that contain B. S' has a minimal element, and the corresponding element of S will be a minimal element of S.

Assume B and A/B are Artinian. Let $A_0 \supset A_1 \supset \cdots$ be a decreasing chain of submodules of A. Then $A_0 \cap B \supset A_1 \cap B \supset \cdots$ is a decreasing sequence of submodules of B, so there is $n_1 \geq 0$ such that $A_n \cap B = A_{n+1} \cap B$ for all $n \geq n_1$. Similarily, $(A_0 + B)/B \supset (A_1 + B)/B \supset \cdots$ is a decreasing sequence of submodules of A/B, so there is $n_2 \geq 0$ such that $(A_n + B)/B = (A_{n+1} + B)/B$ for all $n \geq n_2$. Hence $A_n + B = A_{n+1} + B$ when $n \geq n_2$. Thus if $n \geq n_1, n_2$ then

$$A_n = A_n \cap (A_n + B) = A_n \cap (A_{n+1} + B) = A_{n+1} + (A_n \cap B) = A_{n+1} + (A_{n+1} \cap B) = A_{n+1}$$

See the assignment for the Noetherian case. □

2.29 Corollary. *A finite product $M_1 \times \cdots \times M_k$ of modules is Artinian (resp. Noetherian) if and only if each M_i is Artinian (resp. Noetherian).*

PROOF: By induction on k, since $(A \times B)/B \cong A$. □

2.30 Corollary. *A module M has a composition series if and only if M is both Artinian and Noetherian.*

PROOF: Suppose that M has a composition series $0 = M_0 \subset \cdots \subset M_k = M$. The factors M_{i+1}/M_i are irreducible and hence both Artinian and Noetherian. Therefore M is Artinian and Noetherian since any chain of submodules of M is of length at most k.

Conversely, let C be a maximal chain of submodules of M. C exists by Zorn's Lemma. If C is finite then it is a composition series for M. If it is infinite either an increasing sequence or decreasing subsequence can be found (fill in the details), contradicting either that M is Artinian or that M is Noetherian. □

3 Radicals

This section follows Herstein.

3.1 Definition. The *Jacobson radical* or *radical* of a ring R is

$$J(R) := \bigcap_{\substack{M \text{ irreducible} \\ \text{left } R\text{-module}}} \operatorname{ann}(M)$$

$J(R)$ is well-defined since each irreducible left R-module is isomorphic to R/A for some maximal left ideal A by Proposition 2.21. $J(R) \lhd R$ because each annihilator is an ideal of R.

3.2 Proposition. *Let A be a maximal left ideal of a ring R. Then $\operatorname{ann}(R/A)$ is the largest ideal contained in A.*

PROOF: Let $M = R/A$, an irreducible R-module by Proposition 2.21. If $r \in \operatorname{ann}(M)$ then $0 = r(1+A) = r + A$, so $r \in A$. Hence $\operatorname{ann}(M)$ is an ideal that is contained in A. Suppose that $I \lhd R$ and $I \subseteq A$. Then

$$IM = IR/A \subseteq I/A \subseteq A/A = \{0\}$$

so $I \subseteq \operatorname{ann}(M)$. □

3.3 Theorem. *The following are equivalent descriptions of $J(R)$:*

1. $\bigcap_{\substack{M \text{ irreducible} \\ \text{left } R\text{-module}}} \operatorname{ann}(M)$
2. $\bigcap_{\substack{A \text{ maximal} \\ \text{left ideal}}} A$
3. $\{a \in R \mid \forall\, r \in R\ \exists u \in R\ (u(1-ra) = 1)\}$
4. *The largest proper ideal J of R such that $1 - a \in R^*$ for all $a \in J$.*

Furthermore, the right analogs of the first three descriptions are also equivalent to these decriptions.

PROOF:

- $i \subseteq ii$. If M is an irreducible left R-module then $M \cong R/A$ for some maximal left ideal A. The proposition above shows $\operatorname{ann}(M) \subseteq A$, so $\bigcap_{M \text{ irred.}} \operatorname{ann}(M) \subseteq \bigcap_{A \text{ max.}} A$.
- $ii \subseteq iii$. Suppose that $a \in \bigcap_{A \text{ max.}} A$ and $r \in R$. If $R(1-ra)$ is a proper left ideal of R then it is contained in some maximal ideal A. But $a \in A$ and $1 - ra \in A$, so $1 \in A$, a contradiction. Therefore $R(1-ra) = R$ and $1 - ra$ is left invertible, so $\bigcap_{A \text{ max.}} A \subseteq \{a \in R \mid \forall\, r \in R\ \exists u \in R\ (u(1-ra) = 1)\}$.
- $iv \subseteq i$. Let $I \lhd R$ be any ideal such that $1-a$ is invertible for every $a \in I$. Let M be an irreducible R-module. If $IM \neq 0$ then $IM = M$, so there is $a \in I$ and $0 \neq m \in M$ such that $am \neq 0$. Then $RaM = M$ so there is $r \in R$ such that $ram = m$. But this implies that $(1-ra)m = 0$, a contradiction because $1 - ra$ is invertible and $m \neq 0$. Therefore $IM = 0$ for every irreducible left R-module M, so $I \subseteq \bigcap_{M \text{ irred.}} \operatorname{ann}(M) = J(R)$.
- $iii \subseteq iv$. Let $S = \{a \in R \mid \forall\, r \in R\ \exists u \in R\ (u(1-ra) = 1)\}$. S is an ideal.

  1. If $a, b \in S$ and $r \in R$ then there is u such that $u(1-ra) = 1$. Then $u(1-ra+rb) = 1+urb$, and there is v such that $v(1-(-urb)) = 1$. Therefore $vu(1-r(a-b)) = 1$, so $a - b \in S$.
  2. Clearly $ra \in S$ for all $a \in S$ and $r \in R$.
  3. Let $a \in S$ and $r, t \in R$. We need to show that $1-tar$ has a left inverse. Let u be such that $u(1-rta) = 1$, so that $u = 1 + urta$. There is v such that $1 = v(1-(-urta) = vu$. u has a left inverse and a right inverse, so u is invertible and $v = 1 - rta$. Consider

$$\begin{aligned}(1+taur)(1-tar) &= 1 + taur - tar - taurtar \\ &= 1 + taur - tar - ta(1-u)r \\ &= 1 + taur - tar - taur + tar = 1\end{aligned}$$

The proof of part (iii) also showed that $1-a$ is invertible on both sides. Therefore since S is an ideal such that $1-a$ is invertible for all $a \in S$, the proof for $iv \subseteq i$ shows that $S \subseteq J(R)$. That proof also shows that $J(R)$ is the largest proper ideal with this property. □

3.4 Example. Let $R = \mathscr{T}_n(\mathbb{C})$ and for $i = 1, \ldots, n$ define $A_i = \{T \in \mathscr{T}_n \mid T_{i,i} = 0\}$. Then for each i, A_i is a maximal ideal of R since $\dim R/A_i = 1$. Suppose that A is a maximal left ideal of $\mathscr{T}_n$ such that $A \not\subset A_i$ for any i. Then for each i there is $T_i \in A$ such that $(T_i)_{i,i} \neq 0$. But then A contains $\sum_{i=1}^{n} \frac{1}{(T_i)_{i,i}} E_{i,i} T_i$, which is equal to $I + N$ for some N with a zero diagonal. Hence $N^n = 0$ and so

$$I = (I - N + N^2 - \cdots + (-1)^{n-1} N^{n-1})(I + N) \in A$$

a contradiction. Therefore $J(\mathscr{T}_n) = \mathscr{T}_n^0$, the set of upper triangular matrices with zero diagonal.

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

Herstein uses *semisimple* to name this property, and this practice is common in functional analysis. Farb and Dennis use *semisimple* for something stronger than this, and they do not even define this property. In these notes I may also use semisimple to name this property, so beware.

In semiprimitive rings the irreducible representations separate points. For $R = \mathscr{T}_n$, if M is an irreducible module then $M = R/A_i \cong \mathbb{C}$ with the action given by $T \cdot 1 = T_{i,i}$. In this case the irreducible modules can only tell us about the diagonal.

3.6 Theorem. *Let R be a ring. Then $R/J(R)$ is semiprimitive.*

PROOF: If M is a maximal left-ideal of $R/J(R)$ and $R \xrightarrow{\pi} R/J(R)$ is the canonical projection then $\pi^{-1}(M)$ is a maximal left ideal of R. Conversely, if N is a maximal left ideal of R then $N \supseteq J(R)$ and $\pi(N)$ is a maximal left ideal of $R/J(R)$. It follows that

$$J(R/J(R)) = \bigcap_{M \text{ max.}} M = \bigcap_{N \text{ max.}} N/J(R) = \left(\bigcap_{N \text{ max.}} N \right)/J(R) = J(R)/J(R) = 0$$

□

3.7 Definition. A left (resp. right, 2-sided) ideal I is *nil* if each $a \in I$ is nilpotent. A left (resp. right, 2-sided) ideal is *nilpotent* if there exists $k \in \mathbb{N}$ such that $I^k = 0$, where I^k is defined to be the left (resp. right, 2-sided) ideal generated by $\{a_1 \cdots a_k \mid a_i \in I\}$.

3.8 Proposition. *If I is a left (resp. right) nil ideal, then $I \subseteq J(R)$.*

PROOF: Let $a \in I$. For any $r \in R$ we would like to show that $1 - ra$ has a left inverse. But $ra \in I$ so there is $k \in \mathbb{N}$ such that $(ra)^k = 0$. Thus $(1-ra)^{-1} = 1 + ra + (ra)^2 + \cdots + (ra)^{k-1}$. Therefore $a \in J(R)$ by Theorem 3.3. □

3.9 Example. There are ideals which are nil but not nilpotent. Let $R = \bigcup_{n \geq 1} \mathscr{T}_n + \mathbb{C}I$, the unitized ring of infinite upper triangular matrices with all but finitely many entries zero. Then $J(R) = \bigcup_{n \geq 1} \mathscr{T}_n^0$. $J(R)$ is nil but not nilpotent since there are elements of $J(R)$ whose powers are not zero for arbitrarily large powers.

3.10 Lemma. *If $e = e^2 \in R$ then $J(eRe) = eJ(R)e$.*

PROOF: Let M be an irreducible left R-module. Notice that $(eRe)eM \subseteq eM$, so eM is an eRe module. If $eM \neq 0$ take any $m \in M$ such that $em \neq 0$. Then $Rem \cong M$ since M is irreducible and so $(eRe)m = eM$. Therefore eM is an irreducible left eRe module. *(This seems fishy.)*

Now $\operatorname{ann}(eM) = \{ere \in eRe \mid ereM = 0\} = \operatorname{ann}(M) \cap eRe$, so

$$J(eRe) = \bigcap_{M \text{ irred.}} \operatorname{ann}(eM) = \bigcap_{M \text{ irred.}} \operatorname{ann}(M) \cap eRe = J(R) \cap eRe = eJ(R)e$$

□

3.11 Theorem. *For any ring R, $J(M_n(R)) = M_n(J(R))$.*

PROOF: Take $e = E_{1,1} \in M_n(R)$, so that $eM_n(R)e \cong R$. By Lemma 3.10, $J(R) = eJ(M_n(R))e$, so the top left entry of $J(M_n(R))$ is in $J(R)$, and all of $J(R)$ occurs as a top left entry of something in $J(M_n(R))$. But it can be shown that all ideals of $M_n(R)$ are of the form $M_n(I)$ for $I \lhd R$, the result is proved. □

3.12 Theorem (Armitsur). *Let A be a $\Bbbk$-algebra such that $\dim_{\Bbbk}(A) < |\Bbbk|$. Then $J(A)$ is nil.*

PROOF: Let $a \in J(A)$, so that for all $\lambda \in \Bbbk$, $1 - \lambda a$ is invertible in A. Then the set $\{(1-\lambda a)^{-1} \mid \lambda \in \Bbbk\}$ has the same cardinality as $\Bbbk > \dim_{\Bbbk}(A)$, so it is linearly dependent. Thus there exist $\lambda_0 = 0, \lambda_1, \ldots, \lambda_n \in \Bbbk$ and $c_0, \ldots, c_n \in \Bbbk$, not all zero, such that

$$0 = \sum_{i=0}^{n} c_i (1-\lambda_i a)^{-1} = \left(\prod_{i=0}^{n} (1-\lambda_i a)^{-1} \right) \sum_{i=0}^{n} c_i \prod_{j \neq i} (1-\lambda_j a)$$

Let $p(x) = \sum_{i=0}^{n} c_i \prod_{j \neq i} (1-\lambda_j x) \in \Bbbk[x]$. Then $p(a) = 0$ since $\prod_{i=0}^{n} (1-\lambda_i a)^{-1}$ is a unit. We would like to know that $p \neq 0$. There are two cases:

1: If $c_0 \neq 0$ then $[x^n]p(x) = c_0 \prod_{j=1}^{n} (-\lambda_j) \neq 0$, so $p \neq 0$.

2: If $c_0 = 0$ then suppose that $c_i \neq 0$ for some $i > 0$. Then $p(\frac{1}{\lambda_i}) = c_i \prod_{i \neq j} (1 - \frac{\lambda_j}{\lambda_i}) \neq 0$. Hence $p \neq 0$.

Since $p(a) = 0$ and $p \neq 0$, we may write $0 = p(a) = a^k(b_k + b_{k+1}a + \cdots + b_{k+l}a^l)$ where $b_k \neq 0$. Since $b_{k+1}a + \cdots + b_{k+l}a^l \in J(A)$ and $\Bbbk$ is a field (hence b_k is a unit), $b_k + b_{k+1}a + \cdots + b_{k+l}a^l$ is invertible in A, so $a^k = 0$. Therefore $J(A)$ is nil. □

This theorem has some powerful corollaries.

3.13 Lemma. *If $\Bbbk$ is a field extension of $\mathbb{C}$ with $\dim_{\mathbb{C}} \Bbbk < |\mathbb{C}|$ then $\Bbbk = \mathbb{C}$.*

PROOF: The argument is the same as to the proof of the last theorem. Let $a \in \Bbbk$, so

$$|\mathbb{C}| \geq |\{(\lambda - a)^{-1} \in \Bbbk \mid \lambda \in \mathbb{C}\}| \geq |\mathbb{C}| - 1 = |\mathbb{C}|$$

Hence this the set is linearly dependent, so there is a non-zero polynomial $p \in \mathbb{C}[x]$ such that $p(a) = 0$. Since $\mathbb{C}$ is algebraically closed, $x \in \mathbb{C}$. □

3.14 Theorem (Hilbert's Nullstellensatz). *Let $p_1, \ldots, p_n, q \in \mathbb{C}[x_1, \ldots, x_k]$ be such that for all $a \in \mathbb{C}^k$, if $p_i(a) = 0$ for all $i = 1, \ldots, n$ then $q(a) = 0$. Then there is $t \geq 1$ such that $q^t \in \langle p_1, \ldots, p_n \rangle$.*

PROOF: Without loss of generality we may assume that p_i is not a constant polynomial for any i. Let $R = \mathbb{C}[x_1, \ldots, x_k]$ and $\pi : R \to A = R/\langle p_1, \ldots, p_n \rangle$ be the canonical projection. Given any maximal ideal M in A, $\pi^{-1}(M)$ is a maximal ideal of R. By the third isomorphism theorem, $A/M \cong R/\pi^{-1}(M)$ is a field extension of $\mathbb{C}$ with dimension at most $\dim_{\mathbb{C}} R = \aleph_0$. Thus $A/M \cong \mathbb{C}$ by Lemma 3.13.

Claim. If J is a maximal ideal of R then there is $a \in \mathbb{C}^k$ such that $J = \{p \in \mathbb{C}[x_1, \ldots, x_k] \mid p(a) = 0\}$.

Consider the projection $R \mapsto R/J \cong \mathbb{C}$. In particular, $x_i \mapsto a_i$ for some $a_i \in \mathbb{C}$ for each $i = 1, \ldots, k$, so $p(x_1, \ldots, x_k) \mapsto p(a_1, \ldots, a_k)$. Since $p \in J$ if and only if p is mapped to zero, it follows that $p \in J$ if and only if $p(a_1, \ldots, a_k) = 0$.

Let $a \in \mathbb{C}^k$ be such that $\pi^{-1}(M) = \{p \in R \mid p(a) = 0\}$. Since $p_1, \ldots, p_n \in \langle p_1, \ldots, p_n \rangle \subseteq \pi^{-1}(M)$, it follows that $q \in \pi^{-1}(M)$. Hence $q + \langle p_1, \ldots, p_n \rangle \in M$, and since this holds for an arbitrary maximal ideal of A, $q + \langle p_1, \ldots, p_n \rangle \in J(A)$. By Armitsur's Theorem, $J(A)$ is nil, so there is $t \geq 1$ such that $0 = (q + \langle p_1, \ldots, p_n \rangle)^t = q^t + \langle p_1, \ldots, p_n \rangle$, or $q^t \in \langle p_1, \ldots, p_n \rangle$. □

3.15 Lemma. *Let G be a group and H a subgroup of G. Then $\mathbb{C}H$ is closed under inverses in $\mathbb{C}G$.*

PROOF: Let $a = \sum_{h\in H} a_h h$ and $b = \sum_{g\in G} b_g g$ be such that $ab = ba = e$. Let $b' = \sum_{g\in H} b_g g$. I must show that $b = b'$. Since $ab = e$, $1 = \sum_{g\in G} a_g b_{g^{-1}} = \sum_{h\in H} a_h b_{h^{-1}}$ and for every non-identity element $k \in G$, $0 = \sum_{g\in G} a_g b_{g^{-1}k} = \sum_{h\in H} a_h b_{h^{-1}k}$. Therefore $ab' = e$. Similarily, $b'a = e$, so $b = b'$ since inverses are unique. □

3.16 Theorem (Rickhart). *If G is any group then $\mathbb{C}G$ is semiprimitive.*

PROOF: Define an involution on $\mathbb{C}G$ by $x^* = (\sum_{g\in G} x_g g)^* = \sum_{g\in G} \overline{x}_g g^{-1}$. (Clearly $(x^*)^* = x$, $(\alpha x)^* = \overline{\alpha} x^*$, $(x+y)^* = x^* + y^*$, and

$$(xy)^* = \left(\sum_{g\in G}\sum_{h\in G} x_g y_h gh\right)^* = \sum_{g\in G}\sum_{h\in G} \overline{x}_g \overline{y}_h h^{-1} g^{-1} = y^* x^*$$

so it is actually an involution on $\mathbb{C}G$.)

Suppose first that G is a countable group. Then $\mathbb{C}G$ is a $\mathbb{C}$-algebra of dimension $|G| \leq \aleph_0 < |\mathbb{C}|$ over $\mathbb{C}$, so $J(\mathbb{C}G)$ is nil by Armitsur's Theorem. Let $x \in J(\mathbb{C}G)$ and suppose that $x \neq 0$. Let $y = x^*x = \sum_{h\in G}(\sum_{g\in G} \overline{x}_g x_{gh})h$. In particular, $y_e = \sum_{g\in G} |x_g|^2 > 0$, so $y \neq 0$. $y^* = (x^*x)^* = x^*x = y$, so $y^2 = y^*y$ and by the same aregument $y^2 \neq 0$. Continuing by induction we see that $y^{2^k} \neq 0$ for any $k \geq 0$. This contradicts the fact that $y \in J(\mathbb{C}G)$. Therefore $J(\mathbb{C}G) = 0$.

Now suppose that G is any group and let $x \in J(\mathbb{C}G)$. Let $H = \langle\{g \in G \mid x_g \neq 0\}\rangle$, a countable subgroup of G. For any $r \in \mathbb{C}H$, $(1-rx)^{-1} \in \mathbb{C}G$. By Lemma 3.15, $(1-rx)^{-1} \in \mathbb{C}H$, so $x \in J(\mathbb{C}H) = 0$. Therefore $J(\mathbb{C}G) = 0$.□

4 Artinian Rings

4.1 Definition. A ring R is *(left) Artinian* if ${}_RR$ is a left Artinian R-module. A ring R is *(left) Noetherian* if ${}_RR$ is a left Noetherian R-module. In less obfuscated terms, R is Artinian if every collection of left ideals has a minimal element, and R is Noetherian if every collection of left ideals has a maximal element. The definitions of *right Artinian* and *right Noetherian* are analogous.

4.2 Example.

1. If R is a finite dimensional $\mathbb{k}$-algebra then R is a left and right Artinian and Noetherian, since R has a composition series of length equal to $\dim_{\mathbb{k}}(R)$.
2. Let $R = \left(\begin{smallmatrix}\mathbb{Q} & \mathbb{Q}\\ 0 & \mathbb{Z}\end{smallmatrix}\right)$. $R\left(\begin{smallmatrix}a & b\\ 0 & n\end{smallmatrix}\right) = \left(\begin{smallmatrix}a\mathbb{Q} & b\mathbb{Q}+n\mathbb{Q}\\ 0 & n\mathbb{Z}\end{smallmatrix}\right)$, so the cyclicly generated left ideals of R are $\{0\}$, $\left(\begin{smallmatrix}0 & \mathbb{Q}\\ 0 & n\mathbb{Z}\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}\mathbb{Q} & 0\\ 0 & 0\end{smallmatrix}\right)$, and $\left(\begin{smallmatrix}\mathbb{Q} & \mathbb{Q}\\ 0 & n\mathbb{Z}\end{smallmatrix}\right)$. This is a complete list of submodules of ${}_RR$ since all ideals of R are linear combinations of the ones already listed. Hence R is left Noetherian but not left Artinian for the same reason that ${}_{\mathbb{Z}}\mathbb{Z}$ is Noetherian but not Artinian. On the other hand, $\left(\begin{smallmatrix}a & b\\ 0 & n\end{smallmatrix}\right)R = \left(\begin{smallmatrix}a\mathbb{Q} & a\mathbb{Q}+b\mathbb{Z}\\ 0 & n\mathbb{Z}\end{smallmatrix}\right)$. Hence the cyclic right ideals are $\{0\}$, $\left(\begin{smallmatrix}\mathbb{Q} & \mathbb{Q}\\ 0 & n\mathbb{Z}\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0 & 0\\ 0 & n\mathbb{Z}\end{smallmatrix}\right)$, and $\left(\begin{smallmatrix}0 & b\mathbb{Z}\\ 0 & n\mathbb{Z}\end{smallmatrix}\right)$. The right ideals of R are linear combinations of these, so it follows again that R is not right Artinian. R is not right Noetherian since $\mathbb{Z} \subset \frac{1}{2}\mathbb{Z} \subset \frac{1}{4}\mathbb{Z} \subset \cdots$ is an increasing chain of distinct $\mathbb{QZ}$ modules.
3. Let $R = \left(\begin{smallmatrix}\mathbb{R} & \mathbb{R}\\ 0 & \mathbb{Q}\end{smallmatrix}\right)$. In the same vein as the example above, R is left Artinian and left Notherian, but neither right Noetherian nor right Artinian.

4.3 Theorem. *If A is left Artinian then $J(A)$ is nilpotent.*

PROOF: Let $J = J(A)$. Consider $J \supset J^2 \supset J^3 \supset \cdots$ and note that A is Artinian, so there exists $n \in \mathbb{N}$ such that $J^n = J^{n+1} = \cdots$. Let $B := J^n$, so that $B = BJ = B^2$. If $B \neq 0$ then let $\mathscr{S}$ be the set of left ideals I such that $BI \neq 0$. $\mathscr{S}$ is non-empty since $B, J \in \mathscr{S}$. Since A is Artinian, $\mathscr{S}$ has a minimal element I. There exists $x \in I$ such that $Bx \neq 0$, so $B(Bx) = B^2x = Bx \neq 0$, so $Bx \in S$. $Bx \subseteq I$, so by minimality $Bx = I$. Therefore there is $b \in B$ such that $bx = x$, so $(1-b)x = 0$. But $1 - b \in J$ and hence is invertible, a contradiction. Therefore J is nilpotent. □

4.4 Corollary. *If A is an Artinian ring then $J(A)$ is the unique largest nilpotent ideal, and every left or right nil ideal of A is nilpotent.*

PROOF: $J(A)$ contains all left and right nil ideals of A by Proposition 3.8. □

4.5 Lemma (Schur's Lemma). *If M is an irreducible left R-module then $\mathrm{End}_R(M)$ is a division ring.*

PROOF: Let $\varphi \in \mathrm{End}_R(M)$, $\varphi \neq 0$. $\varphi(M)$ is a non-zero submodule of M, so $\varphi(M) = M$. Similarily, $\ker\varphi$ is a proper submodule of M, so $\ker\varphi = \{0\}$. Therefore φ is an isomorphism, hence $\varphi^{-1} \in \mathrm{End}_R(M)$. □

4.6 Example.

1. Let $\Bbbk$ be a field, $R = M_n(\Bbbk)$, and $V = \Bbbk^n$. R acts on V by matrix multiplication on the left. V is irreducible since R acts transitively on V. Let $T \in \mathrm{End}_R(V) \subseteq \mathrm{End}_\Bbbk(V) = M_n(\Bbbk) = R$. Then $T(rv) = rT(v)$ for all $r \in R$ and $v \in V$, so T commutes with all elements of R. Hence $\mathrm{End}_R(V) = Z(R) = \Bbbk I_n$.
2. Let $R = \mathrm{Alg}_{\mathbb{R}} \left\{ \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \right\} = \left\{ \left[\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right] \mid a, b \in \mathbb{R} \right\}$. Then $V = \mathbb{R}^2$ is an irreducible R-module. Again $\mathrm{End}_R(V) \subseteq \mathrm{End}_{\mathbb{R}}(V) = M_2(\mathbb{R})$, so we are looking for matrices that commute with R.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} \Longrightarrow \begin{bmatrix} b & -a \\ d & -c \end{bmatrix} = \begin{bmatrix} -c & -d \\ a & b \end{bmatrix} \Longrightarrow a = d \text{ and } b = -c$$

   Therefore $\mathrm{End}_R(R) = R$, so R is a division ring.
3. We can have $\mathrm{End}_R(M)$ be a division ring even if M is not irreducible. Let $R = \mathscr{T}_n(\mathbb{C})$ and argue as before to get that $\mathrm{End}_R(R) = \mathbb{C}I_n$.

4.7 Theorem. *Let M be a left ideal of a ring R.*

1. *If $M^2 \neq 0$ and $\mathrm{End}_R(M)$ is a division ring then $M = Re$ for some $e = e^2$ and $\mathrm{End}_R(M) \cong eR^{op}e$.*
2. *If M is a minimal left ideal and $M^2 \neq 0$ then $M = Re$ for some $e = e^2$.*
3. *If R has no non-zero nilpotent ideals (that is, if $J(R) = 0$) and $M = Re$ for some $e = e^2$ then M is minimal if and only if eRe is a division ring (and these happen if and only if eR is a minimal right ideal).*

PROOF:

1. Take $a \in M$ such that $Ma \neq 0$ and define $\rho_a : M \to M$ by $\rho_a(x) = xa$. Then ρ_a is an endomorphism of M, so it has an inverse in $\mathrm{End}_R(M)$. Let $e = \rho_a^{-1}(a) \in M$. $ea = \rho_a(e) = a$, so $ea = e(ea) = e^2a$, or $\rho_a(e - e^2) = 0$. ρ_a is invertible, so $e = e^2$. $M = \rho_a(M) = Ma \supseteq Ra \supseteq Ma$, so $M = Ra$. We can do the same thing for e that we did for a, since $e \in Me$. Therefore $M = Re$. Suppose $\rho \in \mathrm{End}_R(M)$. Let $b = \rho(e)$, so that $b = \rho(e^2) = e\rho(e) = eb = ebe$, showing that $b \in eMe \subseteq eRe$. For any $x \in M$, $\rho(x) = \rho(xe) = x\rho(e) = xb = \rho_b(x)$, so $\rho = \rho_b$. Conversely, for any $b \in eRe$, ρ_b is an endomorphism of M. Finally, $\rho_b \circ \rho_c = \rho_{cb} = \rho_{b*c}$, so $\mathrm{End}_R(M) \cong eR^{\mathrm{op}}e$.
2. Suppose that M is a minimal left ideal. Then M is an irreducible R module, so $\mathrm{End}_R(M)$ is a division ring by Schur's Lemma. Since $M^2 \neq 0$ we are done by part (i).
3. If $M = Re$ is minimal then by (ii) $\mathrm{End}_R(M)$ is a division ring. By (i) $\mathrm{End}_R(M) \cong eR^{\mathrm{op}}e$, so $eR^{\mathrm{op}}e$ is a division ring, and this implies that eRe is also a division ring. Conversely, suppose that eRe is a division ring and $0 \neq N \subseteq M$ is a left R-module. If $eN = 0$ then $N^2 \subseteq MN = (Re)N = 0$, a contradiction since there are no nilpotent ideals. Take $n \in N$ such that $ene = en \neq 0$. $0 \neq ene \in eRe$, so there is $ere \in eRe$ such that $(ere)(ene) = e$. Hence $e \in N$, so $M = Re \subseteq N \subseteq M$ and M is minimal. □

4.8 Corollary. *If R is left Artinian and semiprimitive then every non-zero left ideal J of R contains a non-zero idempotent.*

PROOF: Let $\mathscr{S}$ be the set of non-zero left ideals contained in J. Since R is left Artinian $\mathscr{S}$ has a minimal element I_0. R has no nilpotent ideals since every nilpotent ideal of R is contained in $J(R) = 0$. By Theorem 4.7, $I_0 = Re$ for some $e = e^2$. □

4.9 Theorem. *If R is left Artinian and semiprimitive and M is a left ideal of R then there is $e = e^2 \in M$ such that $M = Re$.*

PROOF: Consider $\mathscr{S} = \{M(1-e) \mid e = e^2 \in M\}$. $\mathscr{S}$ is non-empty since $0 \in M$, and since R is left Artinian there is a minimal element $M(1-e_0)$. Suppose that $M(1-e_0) \neq 0$. $M(1-e_0)$ is a left ideal of R, so by Corollary 4.8 there is a non-zero idempotent $e_1 \in M(1-e_0)$. Then $e_1 = e_1(1-e_0) = e_1 - e_1e_0$, so $e_1e_0 = 0$. Let $f := e_0 + e_1 - e_0e_1$. Then $f^2 = f$, $e_0f = e_0$, and $e_1f = e_1$. Hence

$$Mf \supseteq M(e_0f) = Me_0$$
$$Mf \supseteq M(e_1f) = Me_1$$

It follows that $M(1-f) = M(1-f)(1-e_1) \subsetneqq M(1-e_0) \subseteq M$, a contradiction. Therefore $M(1-e_0)$ is zero, so $Me_0 = M$ and the proof is finished since $Re_0 = Me_0 \oplus M(1-e_0) = M$. □

4.10 Corollary. *If R is left Artinian and semiprimitive and $A \lhd R$ then there is $e = e^2 \in Z(R)$ such that $A = eRe$.*

PROOF: Apply Theorem 4.9 to get $e = e^2 \in A$ such that $A = Re$. Let $B = (1-e)A$, a right ideal of R. $B^2 = ((1-e)Re)((1-e)Re) = 0$, so $B \subseteq J(R) = 0$ Therefore $A = eA = eRe$. Let $a \in A$, so $ea = a = ae$. If $r \in R$ then $re, er \in A$, so $re = e(re) = (er)e = er$. Therefore $e \in Z(R)$. □

4.11 Corollary. *Suppose that R is left Artinian and semiprimitive and $A \lhd R$. Then A has a unit and*

$$R = eRe \oplus (1-e)R(1-e)$$

Furthermore, $(1-e)R(1-e) \lhd R$.

4.12 Definition. A ring R is *simple* if the only 2-sided ideals are $\{0\}$ and R.

4.13 Example. If D is a division ring then $M_n(D)$ is a simple Artinian ring.

4.14 Theorem. *If R is a left Artinian and semiprimitive then R is isomorphic to the product of finitely many simple Artinian rings.*

PROOF: Since R is Artinian, R has minimal 2-sided ideals. Let

$$S = \{A_i = e_iRe_i \mid e_i = e_i^2 \in Z(R),\ A_i \text{ a minimal 2-sided ideal}\}$$

If $A_i \neq A_j$ then $e_ie_j \in A_i \cap A_j = 0$ by minimality. If S is infinite choose a countable subset $\{A_i\}_{i=1}^{\infty}$ and form $M_k := \sum_{i \geq k} A_i$ for each $k \geq 1$. Then $M_1 \supsetneqq M_2 \supsetneqq \cdots$ since $e_jM_k = \sum_{i \geq k} e_jA_i = 0$ for any $j < k$. But this contradicts that R is Artinian, so $\mathscr{S}$ is finite, say $\mathscr{S} = \{A_i\}_{i=1}^n$. Let $e = e_1 + \cdots + e_n$. Then $e = e^2 \in Z(R)$. If $e \neq 1$ then $R(1-e) \neq 0$, so $(1-e)R(1-e)$ is an Artinian ring, which will contain a minimal ideal, contradicting that $\mathscr{S}$ contains all minimal ideals of R. Therefore $R = \oplus_{i=1}^n A_i \cong \prod_{i=1}^n e_iRe_i$, and the e_iRe_i's are simple rings (with identity e_i). □

4.1 Example: Some Simple non-Artinian Rings

4.15 Definition. A *derivation* on a ring R is a map $\delta : R \to R$ such that

1. $\delta(x+y) = \delta(x) + \delta(y)$ for all $x, y \in R$ (δ is additive).
2. $\delta(xy) = \delta(x)y + x\delta(y)$ for all $x, y \in R$ (δ satisfies the product rule).

Let R be a ring with derivation δ. Form $R[x;\delta]$, the set of left polynomials with coefficients in R with the rule that $xr - rx = \delta(r)$ for all $r \in R$. Notice that if δ the zero map then $R[x;\delta] = R[x]$.

4.16 Lemma. *$x^n a = \sum_{k=0}^{n} \binom{n}{k} \delta^k(a) x^{n-k}$, where $\delta^0(a) = a$.*

PROOF: By induction on n. When $n = 1$, $xa = ax + \delta(a)$. Suppose that the result holds for some $n \geq 1$.

$$\begin{aligned}
x^{n+1}a &= x^n(ax + \delta(a)) \\
&= \left(\sum_{k=0}^{n} \binom{n}{k} \delta^k(a) x^{n-k}\right) x + \sum_{k=0}^{n} \binom{n}{k} \delta^k(\delta(a)) x^{n-k} \\
&= \sum_{k=0}^{n} \binom{n}{k} \delta^k(a) x^{(n+1)-k} + \sum_{k=1}^{n+1} \binom{n}{k} \delta^k(a) x^{n-k} \\
&= \sum_{k=0}^{n+1} \left(\binom{n}{k} + \binom{n}{k-1} \right) \delta^k(a) x^{(n+1)-k} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} \delta^k(a) x^{(n+1)-k}
\end{aligned}$$

by Pascal's identity. □

4.17 Definition. A derivation is *inner* if there is $c \in R$ such that $\delta(r) = cr - rc =: \delta_c(r)$.

If $\delta = \delta_c$ is inner then $x - c \in Z(R[x;\delta])$ since

$$(x-c)r - r(x-c) = (xr - rx) - (cr - rc) = \delta(r) - \delta(r) = 0$$

We can write any polynomial as a polynomial in $(x-c)$, so $R[x;\delta] \cong R[t]$. If $R = A[y]$ and $\delta(y^n) = ny^{n-1}$ then δ is not inner. Indeed, y commutes with everything in R even if A is not commutative, so $cy - yc = 0$ for all $c \in R$, but $\delta(y) = 1 \neq 0$.

The Weyl algebra is constructed by taking $R = \mathbb{Q}[y]$ and δ as above. It is $R[x;\delta] \cong \mathbb{Q}\langle x, y\rangle / \langle xy - yx - 1\rangle$.

4.18 Theorem. *Let A be a $\mathbb{Q}$-algebra and δ a derviation on A. Then $R = A[x;\delta]$ is simple if and only if the following hold:*

1. *A is δ-simple (which means that if $J \lhd A$ such that $\delta(J) \subseteq J$ then $J = 0$ or $J = A$).*
2. *δ is not inner.*

PROOF: If δ is inner then $R \cong A[t]$, which is not simple since $\{\langle t^n\rangle \mid n \geq 1\}$ is a collection of distinct ideals. If $0 \neq J \lhd A$ is a proper ideal such that $\delta(J) \subseteq J$ then $J[x;\delta] := \{\sum r_i x^i \mid r_i \in J\}$ is a proper non-zero ideal of R. Indeed, if $r \in J$ then $xr = rx + \delta(r) \in J[a;\delta]$, which shows that $RJ[x;\delta] \subseteq J[x;\delta]$, and if $a \in A$ then $rx^n a = r(\sum_{k=0}^{n} \binom{n}{k} \delta^k(a) x^{n-k}) \in J[x;\delta]$ by Lemma 4.16, which shows that $J[x;\delta]R \subseteq J[x;\delta]$. Therefore the two conditions are necessary.

Conversely, suppose that $0 \neq I \lhd R$. Let n be the smallest degree of a non-zero element of I. Let

$$J = \{0, a \in A \mid a \text{ is a leading coefficient of } p \in I \text{ with } \deg p = n\}$$

J is a left ideal of A since left multiplication of a polynomial does not change its degree. J is a right ideal by Lemma 4.16. Furthermore, $\delta(J) \subseteq J$ since for any $a \in J$ there is $p = ax^n + a_{n-1} + \cdots \in I$, and we have $\delta(a)x^n + \delta(a_{n-1})x^{n-1} + \cdots = xp - px \in I$. Hence J is δ-simple, and so by assumption we have that $J = A$. Therefore $p = x^n + dx^{n-1} + \cdots \in I$. For all $a \in A$ $(\delta_d(a) - n\delta(a)x^{n-1})x^{n-1} + \cdots = ap - pa \in I$, which implies that $ap - pa = 0$. Therefore $\delta(a) = \frac{1}{n}\delta_d(a) = \delta_{\frac{n}{d}}(a)$, so δ must be inner. Since we are assuming that this is not the case, R must be simple. □

4.19 Corollary. *Let A be a $\mathbb{Q}$-algebra and δ a non-inner derivation. If A is simple then $R = A[x;\delta]$ is simple and not Artinian.*

PROOF: Clearly A being simple implies that A is δ-simple. δ is not inner, so R is simple by the above Theorem. $R \supsetneq Rx \supsetneq Rx^2 \supsetneq \cdots$ is a decreasing sequence of ideals, so R is not Artinian. □

5 Primitive Rings and Density

5.1 Definition. A ring R is called *(left) primitive* if there exists a faithful irreducible left R-module. An ideal $A \lhd R$ is a *primitive ideal* if $A = \operatorname{ann}(M)$ for some irreducible R module M (so that R/A is a primitive ring, with faithful irreducible left module M).

Remark. Primitive rings are semiprimitive since if M is a faithful irreducible left R-module then $\operatorname{ann}(M) = 0$ so $J(R) = 0$. We can reformulate the definition of the Jacobson radical as the intersection of all of the primitive ideals.

5.2 Proposition. *If R is simple and left Artinian then R is primitive.*

PROOF: Since R is left Artinian it has minimal left ideals. Let M be one of these ideals, so that M is also an irreducible left R-module. $\operatorname{ann}(M) \lhd R$ and the containment is strict by definition of ideal, so $\operatorname{ann}(M) = 0$ since R is simple. Therefore M is a faithful module. □

If M is an irreducible left R module then there is $0 \neq m \in M$ such that $Rm = M$. So if $n \in M$ then there is $r \in R$ such that $rm = n$. We say that R *acts transitively* on M. For example, if $R = M_n(\mathbb{C})$ acts on $\mathbb{C}^n$, then we can send any non-zero vector to any other with a linear transformation. But we can do much better, in fact we can move any linearly independent set of n vectors to any other linearly independent set of n vectors. By Schur's lemma we know that $D = \operatorname{End}_R(M)$ is a division ring, so ${}_DM$ is a D vector space, with $R \hookrightarrow \operatorname{End}_R(M)$. This will become important later on.

5.3 Definition. Let R be a ring, ${}_RM$ an irreducible R-module, and $D = \operatorname{End}_R(M)$. We say that R *acts densely* on M if for all $n \in \mathbb{N}$, if $v_1, \ldots, v_n \in M$ are D-linearly independent and $w_1, \ldots, w_n \in M$ then there is $r \in R$ such that $rv_i = w_i$ for all $i = 1, \ldots, n$.

5.4 Theorem (Density Theorem). *Let R be a primitive ring, M a faithful irreducible left R-module, and $D = \operatorname{End}_R(M)$. Then R acts densely on M.*

PROOF: First we must prove a small lemma.

Claim. If $V \subseteq M$ finite dimensional D vector space then for any $m \in M \setminus V$ there is $r \in R$ such that $rV = 0$ and $rm \neq 0$.

Proceed by induction on $\dim_D V$. If V is the zero vector space then $r = 1$ is sufficient. Assume the claim holds for all $W \subseteq M$ with $\dim_D W < n$. Decompose $V = V_0 + Dv$ and let $A = \{r \in R \mid rV_0 = 0\}$, a left ideal of R. We are looking for $a \in A$ such that $av = 0$ and $am \neq 0$. If we can find such an a then we are done. Suppose otherwise. It follows that $av = 0$ implies $am = 0$ for all $a \in A$. By the induction hypothesis $Av \neq 0$, and it is a submodule of M since A is a left ideal of R. Therefore $Av = M = Am$ since M is irreducible. Then let $\varphi : M \to M$ be defined by $\varphi(av) = am$ for all $a \in A$. Then φ is well-defined. For any $r \in R$ $\varphi(rx) = \varphi(rav) = ram = r\varphi(am)$, so φ is a module homomorphism. Therefore $\varphi \in \mathrm{End}_R(M) = D$ and $0 = \varphi(av) - am = a(\varphi(v) - m$ for all $a \in A$. Again by the induction hypothesis, $\varphi(v) - m \in V_0$. But then $m \in \mathrm{span}_D\{V_0, v\} = V$, a contradiction.

Given $v_1, \ldots, v_n$ linearly independent there are $a_i \in R$ such that $a_i v_j = \delta_{i,j} v_j$ for all $i, j = 1, \ldots, n$. Now $Ra_i v_i$ is a non-zero submodule of M, so it is all of M. Hence there is $r_i \in R$ such that $r_i a_i v_i = w_i$, for any $w_i \in M$. Let $r = \sum_{i=1}^n r_i a_i$. Then $rv_i = w_i$ for $i = 1, \ldots, n$. □

5.5 Definition. If D is a division ring and R is a D-algebra then there is a D vector space M such that $R \subseteq \mathrm{End}_D(M)$. We say that R is *transitive* if for all $v \neq 0, w \in M$ there is $r \in R$ such that $rv = w$. R is *doubly transitive* if for all v_1, v_2 and w_1, w_2 linearly independent pairs in M there is $r \in R$ such that $rv_i = w_i$ for $i = 1, 2$.

5.6 Corollary. *If $R \subseteq \mathrm{End}_{\Bbbk}(M)$ is doubly transitive, then $\mathrm{End}_R(M) = \Bbbk$ and R acts densely on M.*

5.7 Corollary. *Let R be a primitive ring, M a faithful irreducible R-module, and $D = \mathrm{End}_R(M)$. Then one of the following holds:*

1. *$R \cong M_n(D)$*
2. *For all $n \geq 1$, there is a subring $S_n \subset R$ and an epimorphism $S_n \to M_n(D)$.*

PROOF: Let $n = \dim_D M$. There are two cases:

1: If $n < \infty$ then ${}_DM$ has a basis $v_1, \ldots, v_n$. We have already seen that $R \hookrightarrow \mathrm{End}_R(M)$ and R commutes with $\mathrm{End}_R(M) = D$, so $R \hookrightarrow \mathrm{End}_D(M)$. For any $w_1, \ldots, w_n \in M$ there is $r \in R$ such that $rv_i = w_i$ since R acts densely on M. Hence $R \subseteq \mathrm{End}_D(M) = M_n(D) \subseteq R$.

2: If $n = \infty$ then choose a linearly indpendent sequence $v_1, v_2, \ldots$ and let $V_k = \mathrm{span}_D\{v_1, \ldots, v_k\}$. Let $S_k = \{r \in R \mid rV_k \subseteq V_k\}$ and $T_k = \{s \in S_k \mid sV_k = 0\}$. Then $T_k \lhd S_k$ and $S_k/T_k \hookrightarrow \mathrm{End}_D(V_k)$. For any $A \in \mathrm{End}(V_k)$, let $w_i = Av_i$ for $i = 1, \ldots, k$. The Density theorem gives $r \in R$ such that $rv_i = w_i$ for $i = 1, \ldots, k$ and $rv_i = 0$ for $i > k$, so $r \in S_k$ and the inclusion map is onto. □

5.8 Theorem (Artin-Wedderburn). *If R is simple and Artinian then there is a division ring D such that $R \cong M_n(D)$. Furthermore, D and n are uniquely determined.*

PROOF: $R^2 = R$, so $J(R) \neq R$, therefore $J(R) = 0$. R is simple, so it is primitive. Let M be a faithful irreducible R-module. By Corollary 5.7, either the theorem is proved or M is infinite dimensional over $D = \mathrm{End}_R(M)$. If the latter, pick $v_1, v_2, \ldots$ linearly independent and let $L_k = \{r \in R \mid rv_i = 0 \text{ for } i = 1, \ldots, k\}$. Then $L_k \subsetneqq L_{k+1}$ because by the Density theorem there is $r \in R$ such that $rv_i = 0$ for $i = 1, \ldots, k$ and $rv_{k+1} = v_{k+1}$. Then L_i is a descending chain of ideals, contradicting that R is Artinian.

Therefore $R \cong M_n(D)$, where $D = \mathrm{End}_R(R)$ and $n^2 = \dim_D(R)$. For uniqueness, you will just have to wait. □

5.9 Theorem (Artin-Wedderburn Structure Theorem). *Let R be Artinian and semiprimitive. Then R is isomorphic to a finite direct sum of matrix rings over division rings, $M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$, and this decomposition is unique.*

PROOF: We showed earlier that R is the direct sum of finitely many simple Artinian rings. Applying the Artin-Wedderburn theorem for simple rings, we get the result.

To prove uniqueness, suppose that $R = R_1 \oplus \cdots \oplus R_n$, where $R_i = Re_i$ for some minimal idempotent $e_i = e_i^2 \in Z(R)$. If $f = f^2 \in Z(R)$ is minimal, then $f = f1 = f(e_1 + \ldots e_n) = fe_1 + \cdots + fe_n$ and $(fe_i)^2 = f^2 e_i^2 = fe_i$. Since f is minimal, there is i_0 such that $f = fe_{i_0} \leq e_{i_0}$ and $fe_j = 0$ for all $j \neq i_0$. Since e_{i_0} is minimal, $f = e_{i_0}$. It follows that the minimal central idempotents from the matrix decomposition correspond the e_i's, so this decomposition is the same. □

5.10 Corollary. *If $\Bbbk$ is an algebraically closed field and R is a finite dimensional semiprimitive $\Bbbk$-algebra then $R \cong M_{n_1}(\Bbbk) \oplus \cdots \oplus M_{n_\ell}(\Bbbk)$*

5.11 Example. Let G be a finite group and let $R = \mathbb{C}G$. Then R is semiprimitive by Rickhart's theorem, and R is Artinian because $\dim_{\mathbb{C}}(R) = |G| < \infty$.

1. If G is Abelian, then R is commutative. $M_n(\mathbb{C})$ is commutative if and only if $n = 1$, so $R \cong \mathbb{C}^{|G|}$. Thus there are $|G|$ idempotents $e_1, \ldots, e_{|G|}$ with $R = \bigoplus_{i=1}^{n} \mathbb{C}e_i$. For each i we get a group homomorphism $\chi_i : G \to \mathbb{T} : g \mapsto ge_i$. $\widehat{G} = \mathrm{Hom}(G, \mathbb{T})$ is called the dual group.
2. Let $G = \mathfrak{S}_3 = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = 1, \tau\sigma\tau = \sigma^2 \rangle$. Now $\dim_{\mathbb{C}}(\mathbb{C}\mathfrak{S}_3) = 6$ and we know $\mathbb{C}\mathfrak{S}_3$ is a direct sum of matrix rings, so we must be able to write 6 as a sum of squares. Since $6 = 1+1+1+1+1+1$ and $6 = 1+1+4$ are the only ways of writing 6 as a sum of squares, either $\mathbb{C}\mathfrak{S}_3 \cong \mathbb{C}^6$ or $\mathbb{C}\mathfrak{S}_3 \cong \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C})$. The later must be correct since $\mathbb{C}\mathfrak{S}_3$ is not commutative. The normal subgroups are $0, \langle\sigma\rangle$, and $\mathfrak{S}_3$, so the only possible maps from $\mathfrak{S}_3$ into $\mathbb{T}$ are the trivial map and the sgn map. These correspond to the one dimensional factors.

5.12 Theorem (Maschke). *Let G be a finite group and $\Bbbk$ a field of characteristic p. Then $\Bbbk G$ is semiprimitive if and only if p does not divide $|G|$.*

PROOF: $\dim_{\Bbbk}(\Bbbk G) = |G| < \infty$, so $\Bbbk G$ is Artinian. It follows by Theorem 4.3 that $J(\Bbbk G)$ is nilpotent. Assume that $x \in J(\Bbbk G)$ is non-zero, so that $x_h \neq 0$ for some $h \in G$. Then $h^{-1}x = x_h e + \sum_{g \neq h} x_g (h^{-1}g) \in J(\Bbbk G)$. But $\Bbbk G \hookrightarrow \mathrm{End}_{\Bbbk}(\Bbbk G) \cong M_{|G|}(\Bbbk)$ via the left regular representation. Now $\{\lambda_g \mid g \in G\}$ is a basis for this representation, and $\mathrm{Tr}(\lambda_g) = \delta_{g,e}|G|$. Therefore $\mathrm{Tr}(\lambda_{h^{-1}x}) = x_h|G| \neq 0$ since $p \nmid |G|$. But nilpotent elements always have trace zero, so this is a contradiction.

Conversely, suppose that $p \mid |G|$. Let $a = \sum_{g \in G} g \in Z(\Bbbk G)$. Then $a^2 = |G|a = 0$ in $\Bbbk$. Observe that Ra is nilpotent since $(Ra)^2 = RaRa = R^2a^2 = 0$, so $Ra \subseteq J(\Bbbk G)$ since Ra is a nilpotent 2-sided ideal. □

5.13 Theorem (Wedderburn). *If A is a finite dimensional algebra over an algebraically closed field $\Bbbk$, and A has a basis of nilpotent elements, then A is nilpotent.*

Remark.
1. This algebra need not have an identity. If A does not have an identity then the *unitization* of A is $A_1 = \Bbbk \oplus A$. A_1 has a unit and $A \lhd A_1$.
2. We don't actually need $\Bbbk$ to be algebraically closed for this theorem to hold, but without this the proof requires some ideas that we haven't covered yet.

PROOF: A is Artinian, so $J(A)$ is nilpotent. If $J(A) = A$ then we are done. Otherwise $A/J(A)$ is a non-trivial semiprimitive Artinian ring. The homomorphic image of a nilpotent element is nilpotent and the image of a spanning set is a spanning set, so the quotient also has a basis of nilpotent elements. By the Artin-Wedderburn Theorem, $A/J(A) \cong M_{n_1}(\Bbbk) \oplus \cdots \oplus M_{n_k}(\Bbbk)$. We may take further quotients onto $M_{n_1}(\Bbbk)$, which will have a basis of nilpotents. But nilpotents always have trace 0, contradicting that there are elements of $M_{n_1}(\Bbbk)$ with trace other than zero. □

5.14 Proposition. *Let G be a finite p-group and $\Bbbk$ an algebraically closed field of characteristic p. Then $J(\Bbbk G) = \{\sum_{g\in G} x_g g \mid \sum_{g\in G} x_g = 0\}$.*

PROOF: Let I be the right hand side of the above equation. I is an ideal. Indeed, for any $x \in I$ and $y \in \Bbbk G$, $xy = \sum_{g\in G}\sum_{h\in G}(x_g y_h)gh$ and $\sum_{g\in G}\sum_{h\in G}(x_g y_h) = \sum_{h\in G} y_h \sum_{g\in G} x_g = 0$. Thus $xy \in I$, and similarily $yx \in I$. As I is defined by a linear condition, $I + I \subseteq I$. Observe that $I = \operatorname{span}\{g - e \mid g \in G \setminus \{e\}\}$ since $x \in I$ implies $x = \sum_{g\neq e} x_g(g-e) + \sum_{g\neq e} x_g e + x_e e$, and the two right summands add to zero since $x \in I$. $(g-e)^{p^k} = g^{p^k} - e$ for any k since we are working in characteristic p, so taking k such that $|G| = p^k$ we see that $(g-e)^{p^k} = 0$, so $g - e$ is nilpotent. Therefore I is spanned by nilpotents, so by Theorem 5.13, I is nilpotent. Therefore $I \subseteq J(\Bbbk G)$. But I has codimension one, that is, $\Bbbk G = \Bbbk \oplus I$, so since $J(\Bbbk G)$ is a proper ideal we must have $J(\Bbbk G) = I$. □

6 Semisimple Modules

6.1 Definition. An R-module M is called *semisimple* if every submodule $N \subseteq M$ is a direct summand. That this, there is another $N' \subseteq M$ such that $M = N \oplus N'$

6.2 Proposition. *If M is semisimple then every submodule and every quotient module is semisimple.*

6.3 Lemma. *If M is a non-zero semisimple left R-module then M has an irreducible submodule.*

PROOF: Take $0 \neq m \in M$. Let $\mathscr{S}$ be the set of all submodules that are contained within Rm but do not contain m. $\mathscr{S}$ is not empty since it contains the zero module. By Zorn's Lemma $\mathscr{S}$ has a maximal element N_0. $Rm = N_0 \oplus N'$, and N' is irreducible. (If not then there is $0 \neq N'' \subsetneq N'$, and $N_0 \oplus N'' \supsetneq N_0$. By maximality $Rm \subseteq N_0 \oplus N'' \subseteq Rm$, so $N'' = N'$, a contradiction.) □

6.4 Theorem. *Let M be a left R-module. The following are equivalent:*

1. *M is semisimple.*
2. *M is the direct sum of some irreducible submodules.*
3. *M is the sum of all of its irreducible submodules.*

PROOF: Suppose M is semisimple. Let M_1 be the sum of all irreducible submodules of M. If $M_1 \neq M$ then $M = M_1 \oplus M_1'$, and M_1' is semisimple so it contains an irreducible submodule which should have been added to M_1. Therefore $(i) \Rightarrow (iii)$ and (ii).

On the other hand, suppose that M is the sum of all of its irreducible submodules. Let $N \subseteq M$ be an irreducible proper submodule. We will find $N' \subseteq M$ that is a direct sum of irreducible modules such that $M = N \oplus N'$. Let

$$\mathscr{S} = \left\{ S \text{ is a collection of irreducible submodules} \mid \sum_{L\in S} L \text{ is direct, and } \sum_{L\in S} L \cap N = 0 \right\}$$

Order $\mathscr{S}$ by inclusion and apply Zorn's Lemma. If $\mathscr{C}$ is a chain in $\mathscr{S}$ then let $S_0 = \bigcup \mathscr{C}$. Then S_0 is clearly an upper bound for $\mathscr{C}$. Furthermore $S_0 \in \mathscr{S}$ since each of these properties is algebraic (that is, finite), so if S_0 were to fail to be in $\mathscr{S}$ it would have to have failed at some finite stage. Let S be a maximal element of $\mathscr{S}$ and $N' = \sum_{L\in S} L$. Let $M_1 = N \oplus N'$. If $M_1 \neq M$ then we can find an irreducible submodule L such that $L \not\subset M_1$. Then $L \cap M_1 = 0$ since L is irreducible. Therefore $M_1 + L = M_1 \oplus L = N \oplus (N' \oplus L)$, a contradiction because $N' \oplus L$ is a direct sum of irreducibles and $N \cap (N' \oplus L) = 0$, but $N' \oplus L \supsetneq N'$, which contradicts maximality. Therefore M is semisimple. □

6.5 Definition. A ring R is *(left) semisimple* if ${}_R R$ is a semisimple R-module. In less obfuscated terms, R is semisimple if for every left ideal I of R there is a left ideal J of R such that $R = I \oplus J$.

6.6 Corollary. *If R is a left semisimple ring then every left R-module is semisimple.*

PROOF: If M is a left R-module then $M = \sum_{m\in M} Rm$, so given Theorem 6.4 it suffices to prove the result for cyclic modules. But $Rm \cong R/N$, where $N = \{r \in R \mid rm = 0\}$. So R semisimple implies that Rm is semisimple, which implies that $Rm = \sum_{\substack{L \text{ irred} \\ L\subseteq Rm}} L$, so Rm is semisimple. Therefore $M = \sum_{m\in M} Rm$ is semisimple. □

6.7 Lemma. *Let D be a division ring and $R = M_n(D)$. Then every irreducible R-module is isomorphic to ${}_RD^n$, the n dimensional vector space over D with R acting by matrix multiplication on the left. Therefore $M_n(D)$ has a unique class of irreducible modules.*

PROOF: Let M be an irreducible R module. If $0 \neq m \in M$ then $M = Rm \cong R/N$, where N is the left ideal $\{r \in R \mid rm = 0\}$. R is Artinian and semiprimitive, so there is $e = e^2 \in R$ such that $N = Re$. Then $M \cong R/N = R/Re \cong R(1-e)$. Let $f = 1 - e$, so $f = f^2$ and Rf is irreducible and therefore a minimal left ideal. R acts transitively on $RE_{1,1} \cong {}_RD^n$, so RE_{11} is an irreducible R module. $\operatorname{ann}(RE_{11}) = 0$ since R is simple, so $fRE_{1,1} \neq 0$. Pick $r \in R$ such that $frE_{1,1} \neq 0$. Define $\varphi : Rf \to RE_{1,1} : x \mapsto xr_0f_1$. Clearly φ is an R-module map. $\ker\varphi \subsetneq Rf$, so $\ker\varphi = 0$. Similarily, φ is onto, so φ is an isomorphism. □

6.8 Corollary. *If $R = M_n(D)$ then D and n are unique.*

This corollary finishs the proof of the Artin-Wedderburn Theorem.

Remark. If $R = M_n(D)$, then ${}_RR = \sum_{i=1}^n RE_{i,i}$. We get a composition series $\{\sum_{i=1}^j RE_{i,i}\}_{j=1}^n$, where the factors are $RE_{j,j}$, which are irreducible. The Jordan-Hölder Theorem implies that every composition series has the same factors.

6.9 Corollary. *If $R \cong M_{n_1}(D_1)\oplus\cdots\oplus M_{n_k}(D_k)$, where the D_i's are division rings then R has k isomorphism classes of irreducible modules, namely $D_i^{n_i}$ as a module over e_iR, where e_i is the minimal central idempotent projecting onto the i^{th} summand.*

6.10 Theorem. *Let R be a ring. The following are equivalent:*

1. *R is left semisimple.*
2. *${}_RR$ is a finite direct sum of irreducible left R-modules.*
3. *R is left Artinian and semiprimitive.*

The right analogues are also all equivalent. We call such rings semisimple.

PROOF: Exercise. Use the Artin-Wedderburn Theorem and the corollaries and remark above. □

6.11 Theorem (Hopkins-Levitzki). *If R is a ring then R is Artinian if and only if*

1. *R is Noetherian*
2. *$J(R)$ is nilpotent*
3. *$R/J(R)$ is semisimple*

PROOF: If R is Artinian then we have already shown that $J(R)$ is nilpotent and that $R/J(R)$ is Artinian and semiprimitive. It follows that $R/J(R)$ is semisimple.

Assume that R satisfies (ii) and (iii) and that R is either Artinian or Noetherian. We will show that R has a composition series, and so by the Jordan-Hölder Theorem R is both Artinian and Noetherian. Write $J = J(R)$. Then $R \supset J \supset J^2 \supset \cdots \supset J^n = 0$ for some n, by (ii). It suffices to find a composition series for each J^k/J^{k+1}, $k = 0, \ldots, n-1$. But J^k/J^{k+1} is a module over R/J because for $x \in J^k$, $(r+J)(x+J^{k+1}) = rx + J^{k+1}$. Therefore J^k/J^{k+1} is semisimple and hence a direct sum of irreducibles. Since R is either Artinian or Noetherian, this sum must be finite. Therefore each J^k/J^{k+1} has a composition series, so R has a composition series. □

6.12 Example. Let $A = \{\frac{m}{n} \in \mathbb{Q} \mid n \text{ is odd}\}$, a commutative ring. If $0 \neq I \lhd A$, let k be the smallest integer such that $2^k \in I$. Then $2^k A \subseteq I$, and if $a \in I \setminus 2^k A$ then $a = \frac{m}{n}$ where $m = 2^l m_0$ with m_0 odd and $l < k$. But then $2^l = \frac{n}{m_0} a \in I$, a contradiction. Therefore $I = 2^k A$ and A is Noetherian. $A \supsetneq 2A \supsetneq 4A \supsetneq \cdots$ is a decreasing chain of ideals, so A is not Artinian. If $a \in 2A$ then $a = \frac{2m}{n}$, so $1 - a = \frac{n-2m}{n} \in A^*$, since $n - 2m$ is odd. Therefore $J(A) = 2A$. $J(A)^k = 2^k A$, which is not nilpotent, but $A/2A \cong \mathbb{Z}_2$ is a field, so it is semisimple.

6.13 Theorem (Levitzki). *Let R be a Noetherian ring. Then R contains a largest nilpotent ideal, and it contains every left or right nil ideal. (So nil ideals in a nilpotent ring are nilpotent.)*

PROOF: Let $\mathscr{S} = \{\text{nilpotent ideals of } R\}$. Since R is Noetherian $\mathscr{S}$ has a maximal element N_0. If N_1 is another nilpotent ideal, say $N_1^{k_1} = 0$ and $N_0^{k_0} = 0$. Form $N_1 + N_0$, a nilpotent ideal of R. Indeed, $(N_1 + N_0)^{k_1} \subseteq N_1^{k_1} + N_0 = N_0$ since N_0 is an ideal. $N_0 \subseteq N_1 + N_0$ and N_0 is maximal, so this containment is an equality, implying that $N_1 \subseteq N_0$.

Let A be a left or right nil ideal of R. Factor out by N_0 to get $\overline{A}$, a left or right nil ideal of $\overline{R}$. We would like to show that $\overline{A} = 0$, so that $A \subseteq N_0$. Suppose not, and let $0 \neq a \in \overline{A}$.

Claim. aR is a right nil ideal

If A is a right ideal then $aR \subseteq \overline{A}$ is nil. If A is a left ideal then for any $r \in R$, $ra \in \overline{A}$ and so nilpotent of order k. But then $(ar)^{k+1} = a(ra)^k r = 0$, so aR is nil.

For each $b \in aR$, let $L(b) = \{r \in R \mid rb = 0\}$, a left ideal of R. Let $\mathscr{L} = \{L(b) \mid 0 \neq b \in aR\}$. Since R is left Noetherian $\mathscr{L}$ has a maximal element $L(b_0)$. For all $r \in R$, $L(br) \supseteq L(b)$, for any $b \in aR$. But for b_0, either $L(b_0 r) = L(b_0)$ or $b_0 r = 0$. For any $r \in R$, $b_0 r \in aR$, so there is k such that $(b_0 r)^k = 0 \neq (b_0 r)^{k-1}$ or $b_0 r = 0$. In the first case, $b_0 r \in L(b_0 r)^{k-1} = L(b_0)$, so $b_0 r b_0 = 0$ (clearly this holds in the other case as well). Therefore $b_0 R b_0 = 0$, but $0 \neq R b_0 R \lhd R$ is a nilpotent ideal of R. This is a contradiciton because we factored out the nilpotent ideals long ago! □

7 Tensor Products

7.1 Definition. Let $\Bbbk$ be a commutative ring (as it will be for the rest of this section. The important cases are for $\Bbbk$ field or $\mathbb{Z}$.) Let V, W be $\Bbbk$-modules and let $X = \bigoplus_{(v,w) \in V \times W} \Bbbk v \odot w$, the free module over $\Bbbk$ with generators $\{v \odot w \mid v \in V, w \in W\}$. Let X_0 be the submodule generated by

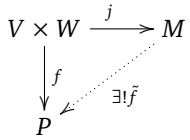
$$\{\alpha(v \odot w) - (\alpha v) \odot w, \alpha(v \odot w) - v \odot (\alpha w), v_1 \odot w + v_2 \odot w - (v_1 + v_2) \odot w, \\ v \odot w_1 + v \odot w_2 - v \odot (w_1 + w_2) \mid \alpha \in \Bbbk, v_i \in V, w_i \in W\} \quad (1)$$

Define the *tensor product* of V and W (over $\Bbbk$) as $V \otimes_{\Bbbk} W := X/X_0$ and write $v \otimes w = [v \odot w]$.

7.2 Definition. A $\Bbbk$-*bilinear* map of $\Bbbk$-modules $f : V \times W \to P$ is a map that is linear in each coordinate.

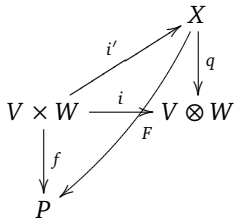
7.3 Example. By construction of $V \otimes W$, the map $i : V \times W \to V \otimes W : (v, w) \mapsto v \otimes w$ is bilinear.

7.4 Proposition (Universal Property of Tensor Products). *If V and W are $\Bbbk$-modules then there is a unique pair (M, j) consisting of a $\Bbbk$-module M and a map $j : V \times W \to M$ bilinear such that whenever (P, f) is a pair consisting of a $\Bbbk$-module P and a bilinear map $f : V \times W \to P$*



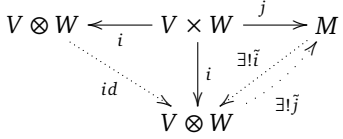
And this unique object is $(V \otimes W, i)$.

PROOF: For existence, we have the diagram



Define $F : X \to P$ by $F(v \odot w) = f(v,w)$ and extend by linearity. It is easy to check that $\ker F \supseteq X_0$ by definition of X_0. Therefore there is a unique map $\tilde{f} : V \otimes W \to P$ such that $F = \tilde{f} \circ q$. Then $f(i(v,w)) = \tilde{f}(v \otimes w) = \tilde{f}(q(v \odot w)) = F(v \odot w) = f(v,w)$, so $\tilde{f} \circ i = f$ since $\{v \otimes w \mid v \in V, w \in W\}$ generates $V \otimes W$.

For uniqueness, suppose that (M, j) is another such pair (we have already seen that the pair $(V \otimes W, i)$ works). Chase this diagram for the result.



□

7.5 Proposition. *Let $\Bbbk$ be a field and V and W be $\Bbbk$-vector spaces. Let $\{v_i\}_{i\in I} \subseteq V$ and $\{w_j\}_{j\in J} \subseteq W$, respectively. Then*

1. *If $V = span\{v_i\}$ and $W = span\{w_j\}$ then $V \otimes W = span\{v_i \otimes w_j\}$.*
2. *If $\{v_i\}$ and $\{w_j\}$ are linearly independent then $\{v_i \otimes w_j\}$ is linearly independent.*
3. *If $\{v_i\}$ and $\{w_j\}$ are are bases then $\{v_i \otimes w_j\}$ is a basis.*

PROOF: Exercise. □

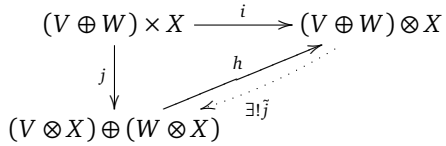
7.6 Example. Let $n, m \in \mathbb{N}$ such that $\gcd(n,m) = 1$. Then $\mathbb{Z}/n\mathbb{Z} \otimes \mathbb{Z}/m\mathbb{Z} = 0$. Indeed, the Euclidean algorithm says that there are $a, b \in \mathbb{Z}$ such that $an + bm = 1$. For any $v \in \mathbb{Z}/n\mathbb{Z}$ and $w \in \mathbb{Z}/m\mathbb{Z}$ we have

$$v \otimes w = (1v) \otimes w = (an + bm)v \otimes w = a(nv) \otimes w + (bv) \otimes (mw) = 0$$

7.7 Proposition. *If $\Bbbk$ is a commutative ring and V, W, X are $\Bbbk$-modules then*

1. $\Bbbk \otimes V \cong V$
2. $V \otimes W \cong W \otimes V$
3. $(V \otimes W) \otimes X \cong V \otimes (W \otimes X)$
4. $(V \oplus W) \otimes X \cong (V \otimes X) \oplus (W \otimes X)$

PROOF: Exercise. (iv) will be done as an example. Consider the following commutative diagram:

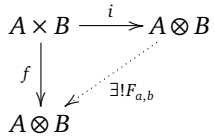


where $j((v,w),x) = (v \otimes x, w \otimes x)$ and $h(v \otimes x, w \otimes x) = (v,w) \otimes x$. Then $h \circ \tilde{j} \circ i = id_{(V\oplus W)\otimes X} \circ i$, so by uniqueness $h \circ \tilde{j} = id_{(V\oplus W)\otimes X}$. j is surjective so $\tilde{j}$ is as well, whence $\tilde{j}$ is right invertible and bijective. □

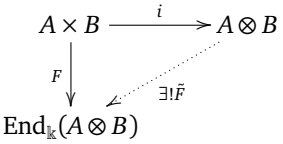
7.8 Proposition. *If $\Bbbk$ is a field and A and B are $\Bbbk$-algebras then $A \otimes B$ is also a $\Bbbk$-algebra, with*

$$(a_1 \otimes b_2)(a_2 \otimes b_2) = (a_1 a_2) \otimes (b_1 b_2)$$

PROOF: $A \otimes B$ is a $\Bbbk$-modules, so we only need to find a multiplication. For $a \in A$, $b \in B$, consider the following commutative diagram attempting to define right multiplication by $a \otimes b$:



where $f(a_1, b_1) = (a_1 a) \otimes (b_1 b)$, which is clearly bilinear. Next consider the following diagram which defines multiplcation in general:



where $F(a, b) = F_{a,b}$. Hence multiplication is defined by

$$(a_1 \otimes b_2)(a_2 \otimes b_2) = (F(a_2, b_2))(a_1, b_1) = (a_1 a_2) \otimes (b_1 b_2)$$

By the properties of the endomorphism ring, we are done. (Check this.) □

Notice that A and B embed in $A \otimes B$ in such a way that they commute. In fact, $A \otimes B$ is called the universal algebra containing A and B as commutative subrings.

7.9 Example.
1. $\Bbbk[x] \otimes \Bbbk[y] \cong \Bbbk[x, y]$ via the homomorphism $x \otimes y \mapsto xy$.
2. $A \otimes M_n(\Bbbk) \cong M_n(A)$ by considering the standard basis of $M_n(\Bbbk)$ and multiplication on it.
3. $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} = \text{span}\{1, 1 \otimes i, i \otimes 1, i \otimes i\}$, a 4-dimensional commutative $\mathbb{R}$-algebra. Notice that $e = \frac{1 \otimes 1 + i \otimes i}{2}$ is idempotent. Let $j = e(i \otimes 1)$, so that $j^2 = -e$. Then it is easy to see that $e\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} = \text{span}\{e, j\} \cong \mathbb{C}$. Similarily, $(e-1)\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C}$, so $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \oplus \mathbb{C}$.
4. If $\Bbbk$ is a field and K is a field extension and A is a $\Bbbk$-algebra, let $A_K = K \otimes_{\Bbbk} A$ a K-algebra. If $\{a_i\}_{i \in I}$ is a basis of A then $\{1 \otimes a_i\}_{i \in I}$ is a basis A_K that acts the same in terms of multiplication. (Indeed, if $a_i a_j = \sum c_i a_i$ then $(1 \otimes a_i)(1 \otimes a_j) = 1 \otimes \sum c_i a_i = \sum c_i (1 \otimes a_i)$.)

7.10 Theorem (Generalized Wedderburn). *If A is a finite dimensional $\Bbbk$-algebra, where $\Bbbk$ is a field, and if A has a basis of nilpotents then A is nilpotent.*

PROOF: Let K be the algebraic closure of $\Bbbk$. Then A_K has a basis of nilpotents (the embedded basis of A), so it is nilpotent by Wedderburn's Theorem. Since A embeds into A_K, A is nilpotent. □

7.11 Definition. A $\Bbbk$-algebra A is *central* if $Z(A) = \Bbbk$.

7.12 Example.
1. $M_n(\Bbbk)$ is central and simple.
2. The quaterion ring $\mathbb{H}$ is central (over $\mathbb{R}$) and simple. Indeed, $\mathbb{H} = \text{span}\{1, i, j, k\}$ with $ij = k = -ji$ and $i^2 = j^2 = k^2 = -1$. If $x = a + bi + cj + dk \in Z(\mathbb{H})$ then in particular, $ix - xi = 0$, so $2ck - 2dj = 0$, and hence $c = d = 0$. Similarily $0 = jx - xj$ so $b = 0$ and $x \in \mathbb{R}$.

7.13 Lemma. *Let A and B be $\Bbbk$-algebras with B central and simple. If $0 \neq J \lhd A \otimes B$ then $J \cap A \neq 0$.*

PROOF: Amoung the non-zero elements of J, pick an element $z = \sum_{i=1}^{\ell} a_i \otimes b_i \in J$ such that ℓ is minimal. Then $\{a_1, \ldots, a_\ell\}$ is linearly independent since ℓ is minimal. B is simple, so $Bb_1B = B$. Hence there are $x_j, y_j \in B$ such that $1 = \sum_{j=1}^{k} x_j b_1 y_j$. Then $z' := \sum_{j=1}^{k} (1 \otimes x_j) z (1 \otimes y_j) \in J$.

$$z' = \sum_{i=1}^{\ell} \sum_{j=1}^{k} (1 \otimes x_j)(a_i \otimes b_i)(1 \otimes y_j) = \sum_{i=1}^{\ell} a_i \otimes \sum_{j=1}^{k} x_j b_i y_j =: \sum_{i=1}^{\ell} a_i \otimes b_i'$$

Now $b_1' = 1$ so $z' \neq 0$ since the a_i's are linearly independent. For all $b \in B$, J contains

$$(1 \otimes b)z' - z'(1 \otimes b) = \sum_{i=1}^{\ell} (1 \otimes b)(a_i \otimes b_i') - (a_i \otimes b_i')(1 \otimes b) = \sum_{i=1}^{\ell} a_i \otimes (bb_i' - b_i'b) = \sum_{i=2}^{\ell} a_i \otimes (bb_i' - b_i'b)$$

If, for some $b \in B$ and some i, $bb_i' - b_i'b \neq 0$ then J contains a non-zero element which is representable as a sum of less than ℓ terms. This is a contradiction. Therefore $b_i' \in Z(B) = \Bbbk$ for each i, so

$$0 \neq z' = \sum_{i=1}^{\ell} a_i \otimes b_i' = \left(\sum_{i=1}^{\ell} a_i b_i' \right) \otimes 1 \in A$$

□

7.14 Theorem. *Let A and B be $\Bbbk$-algebras with B central and simple. Then*

1. *every ideal of $A \otimes B$ has the form $I \otimes B$, where $I \lhd A$.*
2. *$Z(A \otimes B) = Z(A) \otimes \Bbbk = Z(A)$.*

PROOF: Let $J \lhd A \otimes_{\Bbbk} B$ and let $I = J \cap A$, so that $I \otimes B \subseteq J$. Consider the canonical projection

$$q : A \otimes B \to (A/I) \otimes B : a \otimes b \mapsto \dot{a} \otimes b$$

Choose a basis $\{x_i\}_{i \in \mathcal{I}}$ for I and extend it to a basis $\{x_i\}_{i \in \mathcal{I}} \cup \{y_j\}_{j \in \mathcal{J}}$ for A. If $z \in A \otimes B$ then there are $b_i, c_j \in B$ such that $z = \sum x_i \otimes b_i + \sum y_j \otimes c_j$ and $q(z) = \sum \dot{y}_j \otimes c_j$. But $\{\dot{y}_j\}$ forms a basis of A/I, so $q(z) = 0$ if and only if $c_j = 0$ for all $j \in \mathcal{J}$. Therefore $\ker(q) = I \otimes B$. $q(J) \lhd (A/I) \otimes B$, so apply Lemma 7.13 and find $q(J) \cap A/I = q(J \cap A) = q(I) = 0$, so $q(J) = 0$ and $J = I \otimes B$.

Suppose that $x = \sum_{i=1}^{\ell} a_i \otimes b_i \in Z(A \otimes B)$, where we may assume that the a_i's are linearly independent. By the same argument as in Lemma 7.13, $b_i \in Z(B) = k$ for each i. It follows that $x \in Z(A) \otimes 1 = Z(A)$. □

7.15 Corollary. *If A, B are both central and simple $\Bbbk$-algebras then $A \otimes_{\Bbbk} B$ is a central simple $\Bbbk$-algebra.*

7.16 Proposition. *Let D be a central division ring over $\Bbbk$ such that $\dim_{\Bbbk} D < \infty$. Then $\dim_{\Bbbk} D$ is a square integer.*

PROOF: Let K be the algbraic closure of $\Bbbk$. Form $D_K = K \otimes_{\Bbbk} D$. Then $\dim_K D_K = \dim_{\Bbbk} D$. D is a simple finite dimension algebra over K. By the Artin-Wedderburn Theorem, $D_K \cong M_n(K)$. □

7.17 Corollary. *If A is a finite dimensional central simple $\Bbbk$-algebra then $\dim_{\Bbbk} A$ is a square integer.*

PROOF: The Artin-Wedderburn Theorem implies that $A \cong M_k(D)$ for some finite dimensional division ring D over $\Bbbk$. Then $Z(A) = Z(D) = \Bbbk$ so $\dim_{\Bbbk} D = n^2$ and hence $\dim_{\Bbbk} A = (kn)^2$. □

7.18 Example. Try out these results with $D = \mathbb{H}$.

7.19 Theorem. *If A is a finite dimensional central simple algebra over $\Bbbk$ of dimension n^2 and A^{op} is its opposite algebra then $A \otimes_{\Bbbk} A^{op} \cong M_{n^2}(\Bbbk)$.*

PROOF: $\mathrm{End}_{\Bbbk}(A) \cong M_{n^2}(\Bbbk)$. Embed A in $\mathrm{End}(A)$ by left multiplication and embed A^{op} in $\mathrm{End}(A)$ by right multiplication. Left and right multiplication commute, so by Assignment 3, question 5, there is a unique homomorphism φ from $A \otimes_{\Bbbk} A^{\mathrm{op}}$ into $\mathrm{End}(A)$ such that $\varphi(a \otimes b) = L_a R_b$. Since A and A^{op} are central and simple, so is $A \otimes_{\Bbbk} A^{\mathrm{op}}$, and so φ is 1-1.

$$\dim_{\Bbbk} A \otimes_{\Bbbk} A^{\mathrm{op}} = (n^2)(n^2) = n^4 = \dim_{\Bbbk} \mathrm{End}(A)$$

Therefore φ is onto as well, so φ is an isomorphism. □

7.20 Definition. Put an equivalence relation $\sim$ on the finite dimensional central simple $\Bbbk$-algebras by defining $A \sim B$ if there exists $m, n \in \mathbb{N}$ such that $A \otimes M_m(\Bbbk) \cong B \otimes M_n(\Bbbk)$. Put a multiplication on the equivalence classes by $[A][B] = [A \otimes B]$. Let $\mathcal{B}(\Bbbk)$ denote the set of equivalence classes with this multiplication. This is called the Brauer group.

7.21 Theorem. *Multiplication on $\mathcal{B}(\Bbbk)$ is well defined and $\mathcal{B}(\Bbbk)$ is an Abelian group with this multiplication.*

PROOF: If $A_1 \sim A_2$ and $B_2 \sim B_2$ then $A_1 \otimes M_{m_1}(\Bbbk) \cong A_2 \otimes M_{m_2}(\Bbbk)$ and $B_1 \otimes M_{n_1}(\Bbbk) \cong B_2 \otimes M_{n_2}(\Bbbk)$. Hence

$$(A_1 \otimes B_1) \otimes M_{m_1 n_1} \cong A_1 \otimes B_1 \otimes M_{m_1} \otimes M_{n_1} \cong (A_1 \otimes M_{m_1}) \otimes (B_1 \otimes M_{n_1}) \cong (A_2 \otimes B_2) \otimes M_{m_2 n_2}$$

so the multiplication is well defined. It is commutative and associative because the tensor product is commutative and associative. The identity element is $[\Bbbk]$ because $A \otimes \Bbbk \cong A$. By the last theorem, the inverse of $[A]$ is $[A^{\mathrm{op}}]$. Therefore $\mathcal{B}(\Bbbk)$ is a group. □

Note that every element of $\mathcal{B}(\Bbbk)$ has the form $[D]$ for some finite dimensional division ring D over $\Bbbk$ since $A \cong M_n(D)$ implies that $[A] = [D]$.

7.22 Example. If $\Bbbk$ is algebraically closed and A is a finite dimensional central simple $\Bbbk$-algebra, then by the Artin-Wedderburn Theorem $A \cong M_n(D)$ for some division ring D over $\Bbbk$, with $\dim_{\Bbbk} D < \infty$. Therefore $[A] = [M_n(\Bbbk)] = [\Bbbk]$, so $\mathcal{B}(\Bbbk) = 0$.

7.23 Lemma. *Let D be a finite dimensional division ring over a field $\Bbbk$ and $\Bbbk \subseteq K \subseteq D$ be a subfield. Then $C(K) = K$ if and only if K is a maximal subfield of D. ($C(K)$ is the centralizer, all of the elements of D that commute with everything in K.)*

7.24 Theorem. *Let D be a finite dimensional division ring over $\Bbbk$ of dimension n^2. Let K be a maximal subfield of D. Then $D_K := D \otimes_{\Bbbk} K \cong M_n(K)$ and $\dim_{\Bbbk} K = n = \sqrt{\dim_{\Bbbk} D}$.*

PROOF: D_K is simple since it is the tensor product of simple algebras. $\dim_K D_K = \dim_{\Bbbk} D = n^2$, so

$$D_K \cong D \otimes_{\Bbbk} K^{\mathrm{op}} \subseteq D \otimes D^{\mathrm{op}} \cong \mathrm{End}_{\Bbbk}(D) \cong M_{n^2}(\Bbbk)$$

Find $\mathrm{End}_{D_K}(D)$. D is an irreducible D module, so it is an irreducible D_K module. Take $T \in \mathrm{End}_{\Bbbk}(D)$ such that T commutes with D_K. Let $t = T1 \in D$. Then T is right multiplication by t. $D \hookrightarrow \mathrm{End}_{\Bbbk}(D)$ by left multiplication. $K \hookrightarrow \mathrm{End}_{\Bbbk}(D)$ by right multiplication. Conclude that $\mathrm{End}_{D_K}(D) = K = Z(D_K)$. D_K simple Artinian implies that $D_K \cong M_m(K)$ for some m.

(This is not complete.) □

7.25 Theorem (Noether-Skolem). *Let R be a finite dimensional central simple $\Bbbk$-algebra, A be a simple $\Bbbk$-algebra, and $\varphi_1, \varphi_2 : A \to R$ be algebra homomorphisms. Then there is $r \in R^*$ such that $\varphi_1(a) = r\varphi_2(a)r^{-1}$ for all $a \in A$.*

PROOF: $R \cong M_n(D)$ for some division ring D, and $Z(R) = Z(D) = \Bbbk$. A is simple, so φ_1, φ_2 are 1-1. Therefore $\dim_\Bbbk A \leq \dim_\Bbbk R < \infty$. $A \otimes_\Bbbk D$ is also simple, so extend φ_i to a D-linear map $\widehat{\varphi}_i : A \otimes D \to R$. Let V be an n dimensional D-module, so that $R \cong \mathrm{End}_D(V)$. Make V into an $A \otimes D$ module in two ways, via $a \cdot v = \varphi_i(a)v$ for $i = 1, 2$. $A \otimes D$ is simple and Artinian, so it is semisimple. Therefore is has a unique irreducible module W, and $V_i = (V, \varphi_i)$ decomposes as a sum of copies of W.

$$\#\text{ of copies} =: p_i = \frac{\dim_D V_i}{\dim_D W} = \frac{n}{\dim_D W}$$

Therefore $p_1 = p_2$, and note for reference that $\dim_D W \mid \dim_D V_i$. Therefore $V_i \cong V_2$ as $A \otimes D$ modules, so there is $T : V_1 \to V_2$ D-linear. Hence $T(\widehat{\varphi}_1(a)v) = \widehat{\varphi}_2(a)T(v)$ for all $a \in A \otimes D$, $v \in V$. $T \in \mathrm{End}_D(V) = R$ and T is an isomorphism, so it is invertible. □

7.26 Corollary. *Take $R = M_n(\Bbbk)$ and $A = M_m(\Bbbk)$. Then there exists a homomophism $\varphi : A \to R$ if and only if $m \mid n$. If ψ is another such homomorphism then there is $T \in M_n(\Bbbk)$ such that $T\varphi T^{-1} = \psi$.*

PROOF: Take $V = \Bbbk^n$ and $W = \Bbbk^m$ in the proof above. □

7.27 Corollary. *If R is a finite dimensional central simple $\Bbbk$-algebra then every $\Bbbk$-linear automorphism of R is inner.*

PROOF: The identity map is an automorphism, and any automorphism is similar to the identity map. □

7.28 Corollary. *If R is a finite dimensional central simple $\Bbbk$-algebra then every $\Bbbk$-linear derivation of R is inner.*

PROOF: Let δ be any derivation on R. Note that $M_2(R)$ is also a finite dimensional central simple $\Bbbk$-algebra. Let $\varphi_1 : R \to M_2(R) : a \mapsto \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ and $\varphi_2 : R \to M_2(R) : a \mapsto \left(\begin{smallmatrix} a & \delta(a) \\ 0 & a \end{smallmatrix}\right)$. Then

$$\varphi_2(a)\varphi_2(b) = \begin{pmatrix} ab & a\delta(b) + \delta(a)b \\ 0 & ab \end{pmatrix} = \begin{pmatrix} ab & \delta(ab) \\ 0 & ab \end{pmatrix} = \varphi_2(ab)$$

By the Noether-Skolem Theorem, there is $T \in M_2(R)^*$ such that $T\varphi_1(a)T^{-1} = \varphi_2(a)$ for all $a \in R$. Suppose that $T = \left(\begin{smallmatrix} w & x \\ y & z \end{smallmatrix}\right)$ and take it from there. □

7.29 Lemma. *If G is finite group and $H \subsetneq G$ then $\bigcup_{g \in G} gHg^{-1} \neq G$.*

PROOF: Let $N(H)$ be the normalizer of H, a subgroup of G. The number of conjugates of H in G is $[G : N(H)] \leq [G : H]$

$$\left| \bigcup_{g \in G} g(H \setminus \{e\})g^{-1} \right| \leq [G : N(H)](|H| - 1) \leq [G : H](|H| - 1) = |G| - \frac{|G|}{|H|} \neq |G \setminus \{e\}|$$

unless $H = G$. □

7.30 Theorem (Wedderburn's Little Theorem). *Every finite division ring is a field.*

PROOF: Let D be a finite division ring. $\Bbbk = Z(D)$ is a finite field, say of characteristic $p > 1$. Suppose $\dim_\Bbbk D = n^2$. Let K be a maximal subfield of D, so that $\dim_\Bbbk K = n$ and $\dim_K D = n$. If $d \in D \setminus \Bbbk$ then $\Bbbk(d)$ is a subfield of D, so it is contained in some maximal subfield L. Since $\dim_\Bbbk L = n$ as well, $|K| = |\Bbbk|^n = |L|$, so $K \cong L$. By the Noether-Skolem Theorem there is $d \in D$ such that $dKd^{-1} = L$. In particular, $\bigcup_{d \in D} dK^*d^{-1} = D^*$, a contradiction to Lemma 7.29 □

7.31 Corollary. *If $\Bbbk$ is a finite field then $\mathcal{B}(\Bbbk) = 0$.*

7.32 Theorem (Frobenius). *Let D be a finite dimensional division ring which is an algebra over $\mathbb{R}$. Then $D \in \{\mathbb{R}, \mathbb{C}, \mathbb{H}\}$.*

PROOF: If D is a field that is algebraic over $\mathbb{R}$, then $D = \mathbb{R}$ or $D = \mathbb{C}$ because $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$ and any algebraic extension of $\mathbb{C}$ is just $\mathbb{C}$. Suppose that D is noncommuting. Choose a maximal subfield $\mathbb{R} \subseteq K \subseteq D$, so $K = \mathbb{R}$ or $K = \mathbb{C}$. If $n = \dim_{\mathbb{R}} K \in \{1, 2\}$ then $\dim_{\mathbb{R}} D = n^2 \in \{2, 4\}$. D is noncommutative, so $\dim_{\mathbb{R}} D = 4$ and $K = \mathbb{C}$. $Z(D)$ is a field containing $\mathbb{R}$. If $Z(D) \neq \mathbb{R}$ then pick $d \in D \setminus Z(D)$. $Z(D)(d)$ is a $Z(D)$ vector space of dimension at least 2, hence of real dimension at least 4. It follows that the dimension is 2 and $D = Z(D)(d)$, a commutative ring. Therefore $\mathbb{R} = Z(D)$.

Conjugation gives a real linear algebra automorphism of $K = \mathbb{C}$. Since D is central simple and K is simple, the Noether-Skolem Theorem implies that there is $d \in D$ such that $\overline{z} = dzd^{-1}$. In particular, $di = -id$ and so $d^2 i = id^2$, so d^2 commutes with $\{\mathbb{R}, i, d\}$, which implies $d^2 \in K$, since K is equal to its centralizer. i does not commute with d, so $d^2 \in \mathbb{R}$. If $d^2 \geq 0$ then d is a root of $x^2 - d^2 = 0$ in $\mathbb{R}(d)$, which would implies that $d \in \mathbb{R}$. Hence $d^2 < 0$. Let $j = \frac{d}{\sqrt{-d^2}}$ and $k = ij$. Then $D = \operatorname{span}_{\mathbb{R}}\{1, i, j, k\}$ and it can been seen that $D = \mathbb{H}$. □

7.33 Corollary. $\mathcal{B}(\mathbb{R}) \cong C_2$

8 Representations of Finite Groups

Though we will only consider complex representations, most of the results in this section hold for any algebraically closed field $\Bbbk$ such that the characteristic of $\Bbbk$ does not divide the order of the group.

8.1 Definition. A *representation* of a finite group G is a pair (V, φ), where V is a finite dimensional complex vector space and $\varphi : G \to \operatorname{End}_{\mathbb{C}}(V)$ is a group homomorphism with $\varphi(e) = I_V$.

There is a unique way to extend (V, φ) to a homomorphism $\varphi : \mathbb{C}G \to \operatorname{End}_{\mathbb{C}}(V)$, namely linearly. The linear extension is obviously linear, and it is multiplicative because it is multiplicative on the elements of the group. Therefore V is a $\mathbb{C}G$-module. Conversely, given a $\mathbb{C}G$-module we can obtain a group representation by restricting the scalar multiplication to only the elements of the group.

We already know a lot about $\mathbb{C}G$ and its modules. By Maschke's Theorem (or Rickhart's Theorem), $\mathbb{C}G$ is semiprimitive. If G is finite then $\mathbb{C}G$ is Artinian and hence semisimple. By the Artin-Wedderburn Theorem, since $\mathbb{C}$ is algebraically closed, $\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_k}(\mathbb{C})$, for some positive integers $n_1, \ldots, n_k$. It follows that V is a semisimple module, so it decomposes as a direct sum $V \cong V_1^{t_1} \oplus \cdots \oplus V_k^{t_k}$ of irreducible submodules (V_i, ψ_i), where $V_i \cong \mathbb{C}^{n_i}$ with $M_{n_i}(\mathbb{C})$ acting on V_i by matrix multiplication.

One may begin to think that all of the ring theory we have done so far this term has been developed precisely for this purpose, and in some respects, one would be correct.

8.2 Definition. If (V, φ) is a representation of G and $W \subseteq V$ is a $\mathbb{C}G$ submodule then $(W, \varphi|_W)$ is a *subrepresentation* of (V, φ).

8.3 Example. The *left regular representation* $(\mathbb{C}G, \lambda)$ is defined by $\lambda(g)h = gh$ and extending linearly. We can write $V \cong V_1^{n_1} \oplus \cdots \oplus V_k^{n_k}$ since $M_n(\mathbb{C}) \cong (\mathbb{C}^n)^n$. If (V, ψ) is a representation (usually irreducible) then we will write $n\psi$ to mean $\underbrace{\psi \oplus \cdots \oplus \psi}_{n}$ acting on $V^n = \underbrace{V \oplus \cdots \oplus V}_{n}$. In this notation, $\lambda = \sum_{i=1}^{k} n_i \psi_i$ and

$$\dim_{\mathbb{C}} \mathbb{C}G = |G| = \sum_{i=1}^{k} n_i \dim V_i = \sum_{i=1}^{k} n_i^2$$

Schur's Lemma becomes the statement that if (V,ψ) is an irreducible $\mathbb{C}G$ module then $\mathrm{End}_{\mathbb{C}}(V) \cong \mathbb{C}$. As a quick corollary, we get that if V and W are irreducible $\mathbb{C}G$ modules then

$$\mathrm{Hom}_{\mathbb{C}G}(V,W) = \begin{cases} 0 & \text{if } V \ncong W \\ \mathbb{C}\varphi & \text{if } \varphi : V \to W \text{ is an isomorphism} \end{cases}$$

8.4 Proposition. *If (V,φ) is a representation of G then there is a G-invariant inner product on V. Hence $\varphi(g)$ is unitary for all $g \in G$.*

PROOF: Pick a basis $\{v_i\}_{i=1}^n$ for V and define

$$\left[\sum_{i=1}^n \alpha_i v_i, \sum_{i=1}^n \beta_i v_i\right] = \sum_{i=1}^n \alpha_i \overline{\beta}_i$$

Define an inner product $(\cdot,\cdot) : V^2 \to \mathbb{C}$ by

$$(v,w) = \frac{1}{|G|}\sum_{g\in G}[g\cdot v, g\cdot w]$$

Then for any $g \in G$ and $v,w \in V$,

$$(gv,gw) = \frac{1}{|G|}\sum_{h\in G}[hgv,hgw] = \frac{1}{|G|}\sum_{g\in G}[v,w] = (v,w)$$

It follows that $\varphi(g)$ is unitary since it is invertible and $\|gv\|^2 = (gv,gv) = (v,v) = \|v\|^2$. □

8.1 Tensor Products

8.5 Definition. Let (V_1,φ_1) and (V_2,φ_2) be two representations of G. The *tensor product representation* $(V_1 \otimes V_2, \varphi_1 \otimes \varphi_2)$ is defined by letting $\varphi_1 \otimes \varphi_2 : G \to \mathrm{End}_{\mathbb{C}}(V_1 \otimes V_2) : g \mapsto \varphi_1(g) \otimes \varphi_2(g)$. This extends uniquely to $\mathbb{C}G$ and the module is just $V_1 \otimes V_2$ as a $\mathbb{C}G$-module.

Generally, if φ_1 and φ_2 are irreducible then $\varphi_1 \otimes \varphi_2$ need not be irreducible.

8.6 Example. Let (V,φ) be a representation of G and define $\theta : V \otimes V \to V \otimes V : v_1 \otimes v_2 \mapsto v_2 \otimes v_1$. Then $\theta^2 = id_V$, so θ has eigenvalues ± 1. Let $\{e_1,\ldots,e_n\}$ be a basis for V and define

$$\mathrm{Sym}^2(V) = \{x \in V \otimes V \mid \theta(x) = x\} = \mathrm{span}\{e_i \otimes e_i, e_1 \otimes e_j + e_j \otimes e_i\}$$

and

$$V \wedge V = \mathrm{Alt}^2(V) = \{x \in V \otimes V \mid \theta(x) = -x\} = \mathrm{span}\{e_i \otimes e_j - e_j \otimes e_i\}$$

The spanning sets given have dimension $\frac{n(n+1)}{2}$ and $\frac{n(n-1)}{2}$, respectively. Since $\dim_{\mathbb{C}}(V \otimes V) = n^2$, the spanning sets given are bases and $V \otimes V = \mathrm{Sym}^2(V) \oplus \mathrm{Alt}^2(V)$.

8.7 Theorem. *Let G be a finite group. The one dimensional representations of G are exactly $(\mathbb{C},\varphi)$, where $\varphi \in \mathrm{Hom}(G,\mathbb{T}) \cong G/G'$. ($G'$ is the commutator subgroup of G, $G' = \langle ghg^{-1}h^{-1} \mid g,h \in G\rangle$.) Moreover, if $\psi \in \mathrm{Hom}(G,\mathbb{T})$, the corresponding one dimensional central idempotent in $\mathbb{C}G$ is*

$$e_\psi = \frac{1}{|G|}\sum_{g\in G}\overline{\psi(g)}g$$

PROOF: If $\varphi : G \to \mathbb{C}$ is a representation, then for $g \in G$, $(\varphi(g))^{|G|} = \varphi(g^{|G|}) = \varphi(e) = 1$. Therefore $\varphi \in \mathrm{Hom}(G, \mathbb{T})$. Conversely, if $\varphi \in \mathrm{Hom}(G, \mathbb{T})$ then φ is a one dimensional representation. Since $\mathbb{T}$ is Abelian, $\ker \varphi \supseteq G'$, so $\mathrm{Hom}(G, \mathbb{T}) \cong \mathrm{Hom}(G/G', \mathbb{T})$. If C is a cyclic subgroup of $\mathbb{T}$ then $\mathrm{Hom}(C, \mathbb{T}) \cong \mathrm{Hom}(C) \cong C$. G/G' is a finite Abelian group, so $G/G' \cong C_{n_1} \times \cdots \times C_{n_k}$.

$$\mathrm{Hom}(G/G', \mathbb{T}) \cong \mathrm{Hom}(C_{n_1}, \mathbb{T}) \times \cdots \times \mathrm{Hom}(C_{n_k}, \mathbb{T}) \cong C_{n_1} \times \cdots \times C_{n_k} \cong G/G'$$

Finally, if $\psi \in \mathrm{Hom}(G, \mathbb{T})$ then

$$\begin{aligned} e_\psi^2 &= \frac{1}{|G|^2} \sum_{g,h \in G} \overline{\psi(g)\psi(h)} gh \\ &= \frac{1}{|G|^2} \sum_{g,h \in G} \overline{\psi(gh)} gh \\ &= \frac{1}{|G|} \sum_{g \in G} \overline{\psi(g)} \\ &= e_\psi \end{aligned}$$

so e_ψ is an idempotent. Furthermore, for any $g \in G$,

$$g e_\psi = \frac{1}{|G|} \sum_{h \in G} \overline{\varphi(h)} gh = \frac{1}{|G|} \psi(g) \sum_{h \in G} \overline{\varphi(gh)} gh = \psi(g) e_\psi$$

□

8.8 Corollary. *If G is a finite Abelian group then $\mathbb{C}G \cong \mathbb{C}^{|G|}$ and all of the representations are given by $\widehat{G} = \mathrm{Hom}(G, \mathbb{T})$.*

8.9 Corollary. *If $\varphi, \psi \in \mathrm{Hom}(G, \mathbb{T})$ then $\varphi \otimes \psi = \varphi\psi$.*

8.10 Corollary. *If φ is a one dimensional representation and ψ is an irreducible representation then $\varphi \otimes \psi$ is irreducible.*

PROOF: First consider the trivial representation $\varphi_1(g) = 1$ for all $g \in G$. Then

$$(\varphi_1 \otimes \psi)(g)(1 \otimes v) = \varphi_1(g) \otimes \psi(g)(v) = 1 \otimes \psi(g)(v)$$

so $V_\psi \cong V_{\varphi_1} \otimes V_\psi$. Now suppose that $V_\varphi \otimes V_\psi = W_1 \oplus W_2$ is a decomposition. Then

$$V_\psi \cong V_{\varphi_1} \otimes V_\psi \cong V_{\varphi^{-1}} \otimes V_\varphi \otimes V_\psi = (V_{\varphi^{-1}} \otimes W_1) \oplus (V_{\varphi^{-1}} \otimes W_2)$$

which is a contradiction. □

8.11 Theorem. *The number of inequivalent irreducible representations of G is equal to the number of conjugacy classes of G.*

PROOF: We know that the distinct irreducible representations of G are in one to one correspondence with the summands of $\mathbb{C}G$, so the number is just $\dim_{\mathbb{C}} Z(\mathbb{C}G)$. For $g \in G$, let $C(g) = \{hgh^{-1} \mid h \in G\}$, the conjugacy class of g. Define $c_g = \sum_{h \in C(g)} h$, so that we get a distinct element for each conjugacy class. For $k \in G$,

$$k c_g = \sum_{h \in C(g)} kh = \left(\sum_{h \in C(g)} khk^{-1} \right) k = \left(\sum_{h \in C(g)} h \right) k = c_g k$$

Conjugacy classes are disjoint, so $\{c_g \mid g \in G\}$ is linearly independent. Take $z = \sum_{g \in G} z_g g \in Z(\mathbb{C}G)$. Then for all $k \in G$, $kzk^{-1} = z$, so $\sum_{g \in G} z_g (kgk^{-1}) = \sum_{g \in G} z_{k^{-1}gk} g$, so $z_{k^{-1}gk} = z_g$ for all $g, k \in G$. Therefore the coefficients z_g are constant on conjugacy classes, so $z = \sum_{\text{conj. classes}} z_g c_g \in \mathrm{span}\{c_g\}$. Therefore $\dim_{\mathbb{C}} Z(\mathbb{C}G)$ is equal to the number of conjugacy classes of G. □

8.2 Permutation Groups

Recall that we can write a permutation as a product of disjoint cycles. Two permutations are conjugate if and only if they have the same cycle structure. It follows that the conjugacy classes of $\mathfrak{S}_n$ are determined by partitions (in the C&O sense of the word) of n. There are 5 partitions of $n = 4$, so $\mathfrak{S}_4$ has 5 irreducible representations. There are

- 6 4-cycles.
- 8 permutations with cycle structure (3,1)
- 3 permutations with cycle structure (2,2)
- 6 2-cycles
- 1 identity permutation

$\mathfrak{S}_4' \lhd \mathfrak{S}_4$ is a proper subgroup that contains all 3-cycles, 2-cycles, and the identity, so $\mathfrak{S}_4' = A_4$. Of course, for $n \geq 5$, A_n is the only proper normal subgroup of $\mathfrak{S}_n$. We have $\mathfrak{S}_n/A_n \cong C_2$, so $\mathrm{Hom}(\mathfrak{S}_n, \mathbb{T}) \cong \widehat{C}_2 \cong C_2$. Specifically, these are the trivial map and the sgn map. The sgn map corresponds to what is known as the alternating representation U'. $\mathfrak{S}_n$ acts on $\mathbb{C}^n$ by permuting the basis vectors. Let $v_0 = \sum_{i=1}^n e_i$. Then $gv_0 = v_0$ for all $g \in \mathfrak{S}_n$. It follows that $\mathbb{C}v_0$ is a subrepresentation isomorphic to the trivial representation U. Write $\mathbb{C}^n \cong U \oplus V$. V is called the standard representation of $\mathfrak{S}_n$. For $n = 4$,

$$V = \left\{ \sum_{i=1}^4 a_1 e_i \mid \sum_{i=1}^4 a_i = 0 \right\}$$

V is irreducible and 3 dimensional. (Check this.) Now consider $V' = U' \otimes V$, a 3 dimensional irreducible representation that is not isomorphic to V. (Check this too.) There is a fifth representation, call it W. Since $24 = 1^2 + 1^2 + 3^2 + 3^2 + (\dim_{\mathbb{C}} W)^2$, $\dim_{\mathbb{C}} W = 2$. $\mathfrak{S}_4$ contains V as a normal subgroup, and $\mathfrak{S}_3/V \cong \mathfrak{S}_3$. It follows that W is the standard representation of $\mathfrak{S}_3$.

8.3 Characters

8.12 Definition. If $\psi : G \to V$ is a representation of a finite group G, the *character* of ψ is the function

$$\chi_V : G \to \mathbb{C} : g \mapsto \mathrm{Tr}(\psi(g))$$

The character is an invariant of the representation and is independent of the basis chosen.

8.13 Proposition. *1. If $V_1 \cong V_2$ then $\chi_{V_1} = \chi_{V_2}$*

2. $\chi_V(e) = \dim V$
3. $\chi_V(g^{-1}) = \overline{\chi_V(g)}$
4. $\chi_V(hgh^{-1}) = \chi_V(g)$ *(χ_V is a class function)*
5. $\chi_{V_1 \oplus V_2} = \chi_{V_1} + \chi_{V_2}$
6. $\chi_{V_1 \otimes V_2} = \chi_{V_1}\chi_{V_2}$

PROOF: 1. Trace is a class function and is invarient under change of bases.

2. $\varphi(e) = I$.
3. If $\lambda_1, \ldots, \lambda_n$ are the eigenvalues of $\varphi(g)$ with multiplicity then $\chi_V(g) = \sum_{i=1}^n \lambda_i$. $\varphi(g)^{|G|} = I$, so each λ_i is a root of unity. The eigenvalues of $\varphi(g^{-1}) = \varphi(g)^{-1}$ are exactly the inverses, $\frac{1}{\lambda_i} = \overline{\lambda_i}$, so $\chi_V(g^{-1}) = \sum_{i=1}^k \overline{\lambda_i} = \overline{\chi_V(g)}$.

4. $\chi_V(hgh^{-1}) = \mathrm{Tr}(\varphi(hgh^{-1})) = \mathrm{Tr}(\varphi(h)\varphi(g)\varphi(h)^{-1}) = \mathrm{Tr}(\varphi(g)) = \chi_V(g)$.
5. $\varphi_1(g) \oplus \varphi_2(g) = \begin{bmatrix} \varphi_1(g) & 0 \\ 0 & \varphi_2(g) \end{bmatrix}$.
6. $\mathrm{Tr}(\varphi_1(g) \otimes \varphi_2(g)) = \mathrm{Tr}(\varphi_1(g))\,\mathrm{Tr}(\varphi_2(g))$ (look up "Kronecker product"). □

8.14 Lemma (Orthogonality). *Let (V_1, φ_1) and (V_2, φ_2) be non-isomorphic irreducible representations of a finite group G. Fix bases $\{e_1, \ldots, e_m\}$ for V_1 and $\{f_1, \ldots, f_n\}$ for V_2. If $\psi_1(g) = [a_{i,j}(g)]_{m\times m}$ and $\psi_2(g) = [b_{i,j}(g)]_{n\times n}$ then for all i, j, k, l we have*

1. $\frac{1}{|G|}\sum_{g\in G} a_{i,j}(g)b_{k,l}(g^{-1}) = 0$
2. $\frac{1}{|G|}\sum_{g\in G} a_{i,j}(g)a_{k,l}(g^{-1}) = \begin{cases} \frac{1}{m} & \text{if } j = k \text{ and } i = l \\ 0 & \text{otherwise} \end{cases}$

PROOF: For the moment, drop the restriction that V_1 and V_2 are non-isomorphic. Let $A \in \mathrm{Hom}_{\mathbb{C}}(V_2, V_1)$, and let $\overline{A} = \frac{1}{|G|}\sum_{g\in G} \varphi_1(g)A\varphi_2(g^{-1})$. For $h \in G$,

$$\varphi_1(h)\overline{A} = \frac{1}{|G|}\sum_{g\in G} \varphi_1(hg)A\varphi_2(g^{-1}h^{-1})\varphi_2(h) = \overline{A}\varphi_2(h)$$

Therefore $\overline{A} \in \mathrm{Hom}_{\mathbb{C}G}(V_2, V_1) \cong \begin{cases} 0 & \text{if } V_2 \ncong V_1 \\ \mathbb{C} & \text{if } V_2 \cong V_1 \end{cases}$

1. Let $V_1 \ncong V_2$ and $A = E_{j,k}$, so that $\overline{A} = 0$ Then

$$0 = \overline{A}_{i,l} = \frac{1}{|G|}\sum_{g\in G} a_{i,j}(g)b_{k,l}(g^{-1})$$

2. Let $V_1 = V_2$ and $A = E_{j,k}$, so that $\overline{A} = \lambda I$ for some $\lambda \in \mathbb{C}$.

$$\mathrm{Tr}\overline{A} = \frac{1}{|G|}\sum_{g\in G} \mathrm{Tr}(\varphi_1(g)A\varphi_1(g^{-1})) = \frac{1}{|G|}\sum_{g\in G} \mathrm{Tr}A = \mathrm{Tr}A = \delta_{j,k}$$

Therefore $\lambda = \frac{1}{m}\delta_{j,k}$, and so

$$\frac{1}{|G|}\sum_{g\in G} a_{i,j}(g)a_{k,l}(g^{-1}) = \overline{A}_{i,l} = \begin{cases} 0 & \text{if } j \neq k \text{ or } i \neq l \\ \frac{1}{m} & \text{if } j = k \text{ and } i = l \end{cases}$$

□

8.15 Theorem (Orthogonality Relation for Characters). *Let V_1 and V_2 be irreducible $\mathbb{C}G$-modules. If $(\cdot,\cdot)$ is the standard inner product on $\mathbb{C}^G$ then*

$$\langle \chi_{V_1}, \chi_{V_2} \rangle = \begin{cases} 0 & \text{if } V_1 \ncong V_2 \\ 1 & \text{if } V_1 \cong V_2 \end{cases}$$

PROOF:

$$\begin{aligned}\langle \chi_{V_1}, \chi_{V_2} \rangle &= \frac{1}{|G|} \sum_{g \in G} \chi_{V_1}(g) \overline{\chi_{V_2}(g)} \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_{V_1}(g) \chi_{V_2}(g^{-1}) \\ &= \frac{1}{|G|} \sum_{g \in G} \left(\sum_{i=1}^{m} a_{i,i}(g) \right) \left(\sum_{k=1}^{n} b_{k,k}(g^{-1}) \right) \\ &= \sum_{i=1}^{m} \sum_{k=1}^{n} \frac{1}{|G|} \sum_{g \in G} a_{i,i}(g) b_{k,k}(g^{-1})\end{aligned}$$

By the previous lemma, if $V_1 \ncong V_2$ then $\langle \chi_{V_1}, \chi_{V_2} \rangle = 0$, and if $V_1 \cong V_2$ then $\langle \chi_{V_1}, \chi_{V_2} \rangle = \sum_{i=1}^{m} \frac{1}{m} = 1$. □

8.16 Corollary. *If G is a finite group and $V_1, \ldots, V_k$ are all of the distinct irreducible representations of G then $\chi_{V_1}, \ldots, \chi_{V_k}$ forms an orthonormal basis for the space of class functions on G.*

PROOF: χ_{V_i} is a class function for each i, and by the previous theorem the characters form an orthonormal (and hence linearly independent) set. Moreover, k is number of conugacy classes of G, which is the dimension of the space of class functions. □

8.17 Corollary. *If W is a finite dimensional representation of G with $W \cong V_1^{a_1} \oplus \cdots \oplus V_k^{a_k}$, then $a_i = \langle \chi_W, \chi_{V_i} \rangle$ for all i. Thus W is determined up to isomorphism by its character.*

PROOF: $\chi_W = \sum_{i=1}^{k} a_i \chi_{V_i}$. □

8.18 Corollary. *W is an irreducible representation of G if and only if $\|\chi_W\| = 1$.*

PROOF: If $W \cong V_1^{a_1} \oplus \cdots \oplus V_k^{a_k}$ then $\|\chi_W\|^2 = \sum_{i=1}^{k} a_i^2$, so the result follows. □

8.4 Character Tables

For a group G, the character table of G is a table containing information describing all of the irreducible characters. Namely, the columns are conjugacy classes of G and the rows are irreducible representations. Each cell contains the value of the character function for a given row evaluated on the conjugacy class of the given column.

8.19 Example. $\mathfrak{S}_4$ has 5 irreducible representations; the trivial representation U, the alternating representation U', the standard representation V (such that $U \oplus V$ is the action of $\mathfrak{S}_4$ on $\mathbb{C}^4$), $V' = U' \otimes V$, and a leftover 2 dimensional representation W.

	(1,1,1,1)	(2,1,1)	(2,2)	(3,1)	(4)
U	1	1	1	1	1
U'	1	−1	1	1	−1
V	3	1	−1	0	−1
V'	3	−1	−1	0	1
W	2	0	2	−1	0

Table 1: Character Table for $\mathfrak{S}_4$

8.20 Proposition. *The columns of the character table are orthogonal. Specifically,*

$$\sum_{i=1}^{k} \chi_{V_i}(g)\overline{\chi_{V_i}(h)} = \begin{cases} \frac{|G|}{|C_g|} & \text{if } h \in C_g \\ 0 & \text{otherwise} \end{cases}$$

PROOF: Consider the $k \times k$ matrix with columns indexed by conjugacy classes of G and rows indexed by irreducible representations of G, where the (V, C_g)-entry is $\sqrt{\frac{|G|}{|C_g|}}\chi_V(g)$. The inner product of rows V and W is $\frac{1}{|G|}\sum_{C_g} |C_g|\chi_V(g)\overline{\chi_W(g)} = \delta_{V,W}$, by Theorem 8.15. Since the rows are orthonormal, the matrix must be unitary, so the columns are orthonormal as well. Therefore

$$\sum_{i=1}^{k} \sqrt{\frac{|C_g|}{|G|}}\sqrt{\frac{|C_h|}{|G|}}\chi_{V_i}(g)\overline{\chi_{V_i}(h)} = \begin{cases} 1 & \text{if } h \in C_g \\ 0 & \text{if } h \notin C_g \end{cases}$$

and the result follows. □

8.21 Theorem. *Let G be a finite group and (V, φ) an irreducible representation of dimension n. The central idempotent $e \in \mathbb{C}G$ mapping to the summand $M_n(\mathbb{C})$ associated with V is given by $e = \frac{n}{|G|}\sum_{g\in G} \overline{\chi_V(g)}g$.*

PROOF: Let $V_1, \ldots, V_k$ be all of the irreducible representations of G, with $n_s = \dim V_s$ and φ_s the action of G on V_s, for each s. Let $\varphi_s(g) = [a_{i,j}^{(s)}(g)]_{n_s \times n_s}$ for all s and define $A_s = \frac{n_s}{|G|}\sum_{g\in G} \overline{\chi_{V_s}(g)}g$. We would like to show that $A_s = e_s$, where $e_s\mathbb{C}G = M_{n_s}(\mathbb{C})$. Well,

$$\begin{aligned}
\varphi_t(A_s)_{i,j} &= \frac{n_s}{|G|}\sum_{g\in G} \overline{\chi_{V_s}(g)}a_{i,j}^{(t)}(g) \\
&= \frac{n_s}{|G|}\sum_{g\in G}\left(\sum_{k=1}^{n_s} a_{k,k}^{(s)}(g^{-1})\right)a_{i,j}^{(t)}(g) \\
&= n_s\sum_{k=1}^{n_s}\frac{1}{|G|}\sum_{g\in G} a_{k,k}^{(s)}(g^{-1})a_{i,j}^{(t)}(g) \\
&= \begin{cases} 0 & \text{if } s \neq t \text{ or } i \neq j \\ 1 & \text{if } s = t \text{ and } i = j \end{cases} \qquad \text{by the orthogonality lemma}
\end{aligned}$$

Thus $\varphi_t(A_s) = \begin{cases} 0 & \text{if } s \neq t \\ I_{V_s} & \text{if } s = t \end{cases}$. Hence A_s picks out $M_{n_s}(\mathbb{C})$ when acting on $\mathbb{C}G = M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_s}(\mathbb{C})$. Therefore $A_s = e_s$. □

8.22 Corollary. *If (W, φ) is a representation of G, say $W \cong V_1^{a_1} \oplus \cdots \oplus V_k^{a_k}$, then the projection onto $V_i^{a_i}$ is $\varphi(e_i) = \frac{n_i}{|G|}\sum_{g\in G} \overline{\chi_{V_i}(g)}\varphi(g)$.*

8.23 Proposition. *If $W \cong V_1^{a_1} \oplus \cdots \oplus V_k^{a_k}$ and $X \cong V_1^{b_1} \oplus \cdots \oplus V_k^{b_k}$ are representations of G then*

$$\operatorname{Hom}_{\mathbb{C}G}(W, X) = \bigoplus_{s=1}^{k} \operatorname{Hom}(V_s^{a_s}, V_s^{b_s}) \cong \bigoplus_{s=1}^{k} M_{a_s,b_s}(\mathbb{C})$$

In particular, $\langle \chi_W, \chi_X \rangle = \dim_{\mathbb{C}} \operatorname{Hom}_{\mathbb{C}G}(W, X) = \sum_{s=1}^{k} a_s b_s$.

8.5 Induced Representations

8.24 Definition. Let H be a subgroup of G.

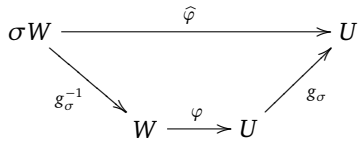
1. Let (V,φ) be a representation of G. Then the *restriction* of (V,φ) to H is $\mathrm{Res}^G_H(V) = (V, \varphi|_H)$, a representation of H.
2. If (V,φ) and (W,ϕ) are representations of G and H, respectively, then W *induces* V if
   (a) $W = \mathrm{Res}^G_H(V)$
   (b) $V = \oplus_{\sigma\in G/H}\sigma W$

8.25 Theorem. *Given $H < G$ and W a representation of H, there is a unique representation V of G induced by W. This is denoted $Ind^G_H(W)$ and is called the representation induced by W.*

8.26 Proposition. *Let H be a subgroup of G, W a representation of H and U a representation of G. Given $\varphi \in \mathrm{Hom}_H(W, Res(U))$, there is a unique extension $\widehat{\varphi} \in \mathrm{Hom}_G(Ind(W), U)$ (so that $\widehat{\varphi}|_W|_H = \varphi$). That is,*

$$\mathrm{Hom}_H(W, Res(U)) \cong \mathrm{Hom}_G(Ind(W), U)$$

PROOF: Let $V = \mathrm{Ind}(W) = \bigoplus_{\sigma\in G/H}\sigma W$. Any G-module extension must satisfy



So $\widehat{\varphi}(g_\sigma w) = g_\sigma\varphi(w)$. This is a well definition since if $g_1w_1 = g_2w_2$ then $w_1 = g_1^{-1}g_2w_2$, and since these are in the same coset we get $g_1^{-1}g_2 = h \in H$. Therefore

$$\widehat{\varphi}(g_1w_1) = g_1\varphi(w_1) = g_1\varphi(hw_2) = g_1h\varphi(w_2) = g_2\varphi(w_2) = \widehat{\varphi}(g_2w_2)$$

Therefore the extension is unique and well-defined. □

8.27 Corollary (Frobenius Reciprocity). *Let H be a subgroup of G, W a representation of H, and U a representation of G. Then $\langle\chi_W, \chi_{Res(U)}\rangle_H = \langle\chi_{Ind(W)}, \chi_U\rangle_G$.*

PROOF: By Proposition 8.23

$$\langle\chi_W, \chi_{\mathrm{Res}(U)}\rangle_H = \dim\mathrm{Hom}_H(W, \mathrm{Res}(U)) = \dim\mathrm{Hom}_G(\mathrm{Ind}(W), U) = \langle\chi_{\mathrm{Ind}(W)}, \chi_U\rangle_G$$ □

8.28 Proposition. *Let H be a subgroup of G, W a representation of H. Define χ_W on G by*

$$\chi_W(g) = \begin{cases} \chi_W(g) & \text{if } g \in H \\ 0 & \text{if } g \notin H \end{cases}$$

Then $\chi_{Ind^G_H(W)}(g) = \frac{1}{|H|}\sum_{k\in G}\chi_W(k^{-1}gk)$. For $g \in G$, let $C(g)$ be the conjugacy class of g in G. Then $C(g)\cap H = D_1 \amalg \cdots \amalg D_r$, where the D_r are disjoint conjugacy classes of H. Hence

$$\chi_{Ind^G_H(W)}(g) = \frac{|G|}{|H|}\sum_{i=1}^{r}\frac{|D_i|}{|C(g)|}\chi_W(D_i)$$

8.29 Example. Let $G = C_7 \rtimes_\theta C_3$. Then $G = \{(n,i) \mid n \in C_7, i \in C_3\}$, where $(n,i)(m,j) = (n + \theta^i(j), i+j)$. Then

$$C((0,0)) = \{(0,0)\}$$
$$C((1,0)) = \{(1,0),(2,0),(4,0)\}$$
$$C((-1,0)) = \{(-1,0),(-2,0),(-4,0)\}$$
$$C((0,1)) = \{(n,1) \mid n \in C_7\}$$
$$C((0,2)) = \{(n,2) \mid n \in C_7\}$$

	$(0,0)$	$(1,0)$	$(-1,0)$	$(0,1)$	$(0,2)$
U	1	1	1	1	1
U'	1	1	1	ω	ω^2
U''	1	1	1	ω^2	ω
W_1	3	a	$\overline{a}$	0	0
W_2	3	$\overline{a}$	a	0	0

$\rho_1 : C_7 \to V_1 = \mathbb{C} : k \mapsto \zeta_7^k$
$W_1 = \mathrm{Ind}_{C_7}^G(V_1)$

8.6 The Representation Ring and Artin's Theorem

8.30 Definition. The *representation ring* of G is $R(G)$ is the $\mathbb{Z}$-span of the characters of G.

The set of characters is closed under addition and multiplication because $\chi_V + \chi_W = \chi_{V\oplus W}$ and $\chi_V \chi_W = \chi_{V\otimes W}$. If $\chi_1, \ldots, \chi_k$ are the irreducible characters of G, then every character has the form $\chi = n_1\chi_1 + \cdots + n_k\chi_k$, for $n_i \in \mathbb{N}$. So if $\chi = \sum_{i=1}^k n_i\chi_i$ for $n_i \in \mathbb{Z}$ then $\chi = \sum_{n_i \geq 0} n_i\chi_i - \sum_{n_i<0} |n_i|\chi_i$. Therefore $R(G) = \{\varphi - \psi \mid \varphi, \psi \text{ are characters}\} = \chi_1\mathbb{Z} + \cdots + \chi_k\mathbb{Z}$, a free Abelian group. Furthermore $R(G)$ is a commutative ring.

Now $R(G)$ is a subring of the algebra of class functions on G. (Indeed, the algebra of class functions is just the $\mathbb{C}$-span of the characters.) Suppose that $H < G$. Then $\mathrm{Res}_H^G : R(G) \to R(H)$ (defined by restriction) is a homomorphism of rings. $\mathrm{Ind}_H^G : R(H) \to R(G)$ is additive but not multiplicative. $\mathrm{Ind}_H^G(R(H)) \lhd R(G)$ since, for $\varphi \in R(H)$ and $\psi \in R(G)$, $\mathrm{Ind}(\varphi)\psi = \mathrm{Ind}(\varphi \mathrm{Res}(\psi))$ by Assignment 5.

8.31 Definition. If G is any finite group, let $T(G) = \sum_{\substack{H \leq G \\ \text{cyclic}}} \mathrm{Ind}_H^G(R(H))$, the group of *virtual characters*

which are integer combinations of $\mathrm{Ind}_H^G(\rho)$ for $\rho \in \widehat{H}$, the one dimensional representations of cyclic subgroups. For H cyclic, $R(H)$ is the $\mathbb{Z}$ span of the one dimensional representations of H, given by $\widehat{H}$. Therefore the elements of $T(G)$ are linear combinations of $\mathrm{Ind}_H^G(\rho)$, for $\rho \in \widehat{H}$. $T(G) \lhd R(G)$ because it is a sum of ideals.

8.32 Theorem (Artin). *$R(G)/T(G)$ is finite. In particular, $|G|R(G) \subseteq T(G)$.*

PROOF: If H is a cyclic group, define $\theta_H : H \to \mathbb{Z}$ by $\theta_H(h) = |H|$ if h generates H and $\theta_H(h) = 0$ otherwise. Then θ_H is a class function on H. Therefore $\mathrm{Ind}_H^G(\theta_H)$ is defined.

$$\mathrm{Ind}_H^G(\theta_H) = \frac{1}{|H|} \sum_{k \in G} \theta_H(k^{-1}gk)$$

Claim. If G is a finite group then $\sum_{\substack{H \leq G \\ \text{cyclic}}} \mathrm{Ind}_H^G(\theta_H) = |G|$.

Each $k^{-1}gk$ generates a unique cyclic subgroup.

Claim. $\theta_H \in R(H)$

By induction on $|H|$. If $|H| = 1$ then $\theta_H = \chi_1 \in R(H)$. Assume the result for all cyclic subgroups of order less than $|H|$. By the first claim, $\sum_{K \leq H} \mathrm{Ind}_K^H(\theta_K) = |H| \in R(H)$, so by induction we must have $\theta_H = \mathrm{Ind}_H^H(\theta_H) \in R(H)$.

By the claims, $|G| \in T(G)$. But $T(G) \lhd R(G)$, so $\varphi \in R(G)$ implies that $|G|\varphi \in T(G)$. □

8.33 Corollary. *Every character of G is a rational combination of characters induced from cyclic subgroups. That is, $\mathbb{Q} \otimes T(G) = \mathbb{Q} \otimes R(G)$.*

8.7 Algebraic Integers

8.34 Definition. If $\Bbbk$ is a commutative ring, then we say that $x \in \Bbbk$ is *integral* if there is a monic polynomial $p(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \Bbbk[X]$ such that $p(x) = 0$. $\alpha \in \mathbb{C}$ is an *algebraic integer* if α is integral.

8.35 Example.
1. Every root of unity is an algebraic integer.
2. If $\alpha \in \mathbb{Q}$ is an algebraic integer then $\alpha \in \mathbb{Z}$.

8.36 Proposition. *Let $\Bbbk$ be a commutative ring and $x \in \Bbbk$. The following are equivalent:*

1. *x is integral.*
2. *$\mathbb{Z}[x]$ is a finitely generated $\mathbb{Z}$-module.*
3. *$\mathbb{Z}[x]$ is contained in a finitely generated $\mathbb{Z}$-submodule of $\Bbbk$.*

PROOF: (iii) implies (ii) because $\mathbb{Z}$ is Noetherian, so $\mathbb{Z}^k$ is a finitely generated (hence Noetherian) $\mathbb{Z}$-module. Any finitely generated $\mathbb{Z}$-module is a quotient of $\mathbb{Z}^k$, so it is Noetherian. Submodules of Noetherian modules are Noetherian.

The rest are trivial. □

8.37 Corollary. *The set of algebraic integers of $\Bbbk$ is a subring of $\Bbbk$.*

PROOF: If x and y are algebraic integers, then $\mathbb{Z}[x]$ and $\mathbb{Z}[y]$ are finitely generated. Therefore $\mathbb{Z}[x] \otimes_{\Bbbk} \mathbb{Z}[y]$ is finitely generated. $\mathbb{Z}[x, y]$ is finitely generated since it is a homomorphic image of $\mathbb{Z}[x] \otimes_{\Bbbk} \mathbb{Z}[y]$. But $xy, x \pm y \in \mathbb{Z}[x, y]$, so the set of integral elements is closed under $+$, $-$, $\times$ and it contains 1, so it is a subring. □

8.38 Proposition. *Let (V, φ) be a representation of G. If $g \in G$ then $\chi_V(g)$ is an algebraic integer.*

PROOF: $\chi_V(g)$ is the sum of the eigenvalues of $\varphi(g)$, each of which is a root of unity, hence an algebraic integer. □

8.39 Proposition. *If $z \in Z(\mathbb{C}G)$ and $z = \sum_{g \in G} a_g g$, where each a_g is an algebraic integer, then z is integral in $Z(\mathbb{C}G)$.*

PROOF: Recall that $Z(\mathbb{C}G)$ is the span of elements of the from $c_g = \sum_{h \in C_g} h$, where C_g is the conjugacy class of g. In particular, $a_g = a_h$ if $h \in C_g$. Write $z = \sum_{C_g} a_g c_g$. Look at $\mathbb{Z}[\{c_g\}]$ and notice that $\{c_g\}$ forms a ring basis for this ring (that is, the product of two c_g's is a $\mathbb{Z}$-sum of c_g's). Therefore $\mathbb{Z}[\{c_g\}]$ is finitely generated, so each c_g is integral in $Z(\mathbb{C}G)$. Therefore Z is a sum of integral elements, so it is integral. □

8.40 Corollary. *Let $z \in \mathbb{C}G$ be integral. Let V_s be an irreducible representation of G, with character χ_s and dimension n_s. Then $\frac{1}{n_s}\chi_s(z)$ is an algebraic integer.*

PROOF: We claim that $\frac{1}{n_s}\chi_s|_{Z(\mathbb{C}G)}$ (χ_g may be extended linearly to all of $\mathbb{C}G$), is a homomorphism. Recall that $Z(\mathbb{C}G)$ has a basis consisting of the minimal central idempotents $e_t = \frac{n_t}{|G|}\sum_{g\in G}\overline{\chi_t(g)}g$. But

$$\frac{1}{n_s}\chi_s(e_t) = \frac{n_t}{n_s}\left(\frac{1}{|G|}\sum_{g\in G}\overline{\chi_t(g)}\chi_s(g)\right) = \begin{cases}1 & \text{if } t = s\\ 0 & \text{otherwise}\end{cases}$$

so $\frac{1}{n_s}\chi_s|_{Z(\mathbb{C}G)}$ is projection onto the s^{th} coordinate. Homomorphisms map integral elements to integral elements, so $\frac{1}{n_s}\chi_s(z)$ is integral. □

8.41 Corollary. *If V_s is an irreducible representation of G of dimension n_s then $n_s \mid |G|$.*

PROOF: $\frac{|G|}{n_s}e_s = \sum_{g\in G}\overline{\chi_s(g)}g$ is integral. Therefore $\frac{|G|}{n_s}$ is an algebraic integer in the rationals, so it is an integer and $n_s \mid |G|$. □

8.8 Applications to Solvable Groups

8.42 Lemma. *Let G be a finite group and (V,φ) a representation of G. Then $N = \{g \in G \mid |\chi_V(g)| = \chi_V(e)\}$ is a normal subgroup of G and $N = \{g \in G \mid \varphi(g) \text{ is scalar}\}$.*

8.43 Lemma. *Let (V_s,ψ_s) be an irreducible representation of G of degree n_s. For any $g \in G$, let h_g be the size of the conjugacy class of g. If $\gcd(n_s,h_s) = 1$ then $\chi_{V_s}(g) = 0$ or $\psi_s(g)$ is scalar.*

8.44 Theorem. *Let G be a finite group and $g \in G$. Suppose that $h_g := |C_g| = p^a$, where p is a prime and $a \geq 1$. Then G is not simple.*

PROOF: Let (V_s,ψ_s) for $1 \leq s \leq k$ be the irreducible representations of G, with characters χ_s. By orthogonality of the columns of the characters table, $\sum_{s=1}^{k} n_s\chi_s(g) = 0$. Take (V_1,ψ_1) to be the trivial representation, so $1 + \sum_{s=2}^{k} n_s\chi_s(g) = 0$. Fix $s \geq 2$. Consider $N = \{h \in G \mid \chi_s(h) \text{ is scalar}\}$. Then $N \lhd G$ and if $0 \neq N \subsetneq G$ then G is not simple. If $N = G$ then ψ_s is one dimensional, but $\psi_s \neq \psi_1$. Let $N_0 = \{h \in G \mid \psi_s(h) = 1\} \lhd G$. $G/N_0 \cong \psi_s(G) \subseteq \mathbb{T}$. N_0 is not trivial because G is not Abelian if C_g has more than one element. Therefore G is not simple. Finally, if $N = 0$ then ψ_s is not scalar for any $s \geq 2$. Apply Lemma 8.43 to see that either $\gcd(p^a,n_s) = 1$ and $\chi_s(g) = 0$ or $\gcd(p^a,n_s) \neq 1$ and $p \mid n_s$. But $0 = 1 + \sum_{s=2}^{k} n_s\chi_s(g) \equiv 1 \pmod{p}$, a contradiction. □

8.45 Theorem (Burnside's p,q-Theorem). *If G is a finite group with $|G| = p^aq^b$, where p and q are primes and $a,b \in \mathbb{N}_0$, then G is solvable.*

PROOF: It suffices to find a proper normal subgroup $N \lhd G$. If we have shown this then we can prove the theorem by induction on $|G|$. Assume true for all smaller groups than G. Then if $N \lhd G$, both N and G/N are pq-groups of strictly smaller size.

Assume without loss of generality that $a \geq 1$. Let H be a p-Sylow subgroup of G. Then $Z(H) \neq \{e\}$, so let $e \neq h \in H$. Then $H \subseteq C_G(h)$, so $|C_h| = \frac{|G|}{|C_G(h)|} = q^c$ for some c, since $|H| = p^a$. By Theorem 8.44, G is not simple. □

9 More about the Symmtric Group

There is a natural pairing between the conjugacy class of $\mathfrak{S}_n$ and the irreducible representations — something that is not known for any other group.

9.1 Definition. A *Young tableau* is the diagram of a partition λ of n elements filled in with $\{1,\dots,n\}$ in any order.

Given a tableau D, define two subgroups of $\mathfrak{S}_n$:

$$P_D = \{g \in \mathfrak{S}_n \mid g \text{ preserves the rows of } D\}$$
$$Q_D = \{g \in \mathfrak{S}_n \mid g \text{ preserves the columns of } D\}$$

Set $a_D = \sum_{p\in P_D} p$ and $b_D = \sum_{q\in Q_D} \operatorname{sgn}(q)q$, and $c_D = a_D b_D$. Let $V_D = (\mathbb{C}\mathfrak{S}_n)c_D$.

9.2 Theorem. *There exists an integer $n_D > 0$ such that $c_D^2 = n_D c_D$. V_D is a minimal left ideal of $\mathbb{C}\mathfrak{S}_n$, and thus determines an irreducible representation. Furthermore, $V_D \cong V_{D'}$ if and only if $\lambda = \lambda'$ where D is a tableau on λ and D' is a tableau on λ'.*

9.3 Example.

1. If λ is of cycle type (n) then $V_\lambda \cong U$, the trivial representation.
2. If λ is the identity permutation then $V_\lambda = U'$, the alternating representation.

9.4 Lemma. *If λ is a partition of n and D, D' are tableaux on λ then $V_{D'} \cong V_D$.*

PROOF: There exists a permutation $g \in \mathfrak{S}_n$ such that $gD = D'$. Let $h \in P_D$. Then ghg^{-1} preserves the rows of D'. Indeed, suppose that $(ghg^{-1})(i') = j'$. Let $i = g^{-1}(i')$ and $j = g^{-1}(j')$. Then $h(i) = j$ so they are in the same row of D. But $i' = g(i)$ and $j' = g(j)$, so they are in the same row of D'. Similarily, $gP_Dg^{-1} = P_{D'}$ and $gQ_Dg^{-1} = Q_{D'}$. Therefore

$$V_{D'} = (\mathbb{C}\mathfrak{S}_n)c_{D'} = (\mathbb{C}\mathfrak{S}_n)gc_Dg^{-1} = V_Dg^{-1}$$

$R_{g^{-1}} : V_D \to V_{D'}$ is a $\mathbb{C}\mathfrak{S}_n$-module map with inverse $R_g : V_{D'} \to V_D$. Therefore they are isomorphic. □

9.5 Example.

1. If λ is of cycle type $(n-1,1)$ then V_λ is the standard representation. Indeed, $P_D = \mathfrak{S}_{n-1}$ and $Q_D = \{e, (1\ n) = s\}$. Then $a_D = \sum_{p\in P_D} p$ and $b_D = e - s$. Hence $c_D = \sum_{g(n)=n} g - \sum_{h(1)=n} h$. $V_D = \mathbb{C}\mathfrak{S}_n c_D$. For any $k \in \mathfrak{S}_n$,

$$kc_D = \sum_{g(n)=n} kg - \sum_{h(1)=n} kh = \sum_{g(n)=j} g - \sum_{h(1)=j} h =: v_j$$

   Therefore $V_D = \operatorname{span}\{v_1,\dots,v_n\}$. But $\sum_{i=1}^n v_i = \sum_{g\in\mathfrak{S}_n} g - \sum_{h\in\mathfrak{S}_n} h = 0$. We claim that this is the only relation. If $\sum_{j=1}^n a_j v_j = 0$ then look at the coefficient of $(j\ n)$, for $j \geq 2$. $0 = a_j - a_1$, so $a_1 = a_2 = \cdots = a_n$. Therefore the dimension of V_D is $n-1$. $\mathfrak{S}_n$ acts on $\mathbb{C}^n =: W$ by permutation of basis, and $W = U \oplus V$, where $U = \mathbb{C}\sum_{i=1}^n e_i$ is the trivial representation and V is the standard representation. Map V_D to V via

$$J : \sum_{i=1}^n a_j v_j \longmapsto \sum_{i=1}^n a_j e_j - \frac{1}{n}\left(\sum_{j=1}^n a_j\right)\sum_{j=1}^n e_j$$

   Then J is well-defined and J is a module isomorphism.
2. $V_\lambda \otimes U' \cong V_{\lambda'}$, where λ' is the conjugate partition to λ (obtained by flipping the diagram for λ along the diagonal).

9.6 Lemma. *Let D be a Young tableau. For any $g \in \mathfrak{S}_n$, $g \in P_DQ_D$ if and only if no two symbols α and β occur in the same row in of D but the same column of gD.*

PROOF: Suppose that $g \in P_D Q_D$, say $g = pq$. Take two symbols α and β in some row of D. Then α and β belong to the same row of pD. $pqD = (pqp^{-1})pD$, so $q' := pqp^{-1} \in Q_{pD}$ by Lemma 9.4. Since α and β are in different columns of pD, they remain in different columns in $pqD = gD$.

Conversely, consider the first column of gD. Each entry comes from a different row of D. So there is an element $p_1 \in P_D$ which interchanges each element α in this column with the first element of the row of D in which α lies. Look in turn at each other column. Find $p_2 \in P_D$ such that $p_2 p_1 gD$ has the elements of the second column of D in the second column (leaving the first column fixed). Eventually we arrive at $p_k \cdots p_1 gD = D'$, where the columns of D' are the columns of D permuted. That is, there is $q \in Q_D$ such that $D' = qD$. Hence $gD = pqD$ where $p = (p_k \cdots p_1)^{-1}$. □

9.7 Definition. The *lexicographical order on partitions* is defined according to $\lambda > \mu$ if and only if $\lambda_i = \mu_i$ for $i < i_0$ and $\lambda_{i_0} > \mu_{i_0}$. This is just as you would expect.

9.8 Lemma. *Let $\lambda > \mu$ be partitions of n, D a tableau on λ and E a tableau on μ. Then $a_D(\mathbb{C}\mathfrak{S}_n)b_E = 0$. In particular, $c_D c_E = 0$.*

PROOF: It is enough to consider $a_D g b_E = a_D(g b_E g^{-1})g = a_D b_{E'} g$, where $E' = gE$, where $g \in \mathfrak{S}_n$. Hence it is enough to show that $a_D b_{E'} = 0$. By the pigeonhole principle, there must be two symbols α and β so that α and β lie in the same row of D but in the same column of E'. Therefore $t = (\alpha\ \beta) \in P_D \cap Q_{E'}$. But

$$a_D b_{E'} = (a_D t)(t b_{E'}) = \left(\sum_{p \in P_D} pt\right)\left(\sum_{q \in Q_{E'}} tq\operatorname{sgn}(q)\right) = a_D(-b_{E'}) = -a_D b_{E'}$$

Therefore $a_D b_{E'} = 0$. □

9.9 Corollary. *If $\lambda < \mu$ then $b_D(\mathbb{C}\mathfrak{S}_n)a_E = 0$, so in particular, $c_D c_E = 0$.*

9.10 Lemma. *Let λ be a partition of n and D a tableau on λ.*

1. *$p a_D = a_D p = a_D$ for all $p \in P_D$*
2. *$\operatorname{sgn}(q) q b_D = b_D \operatorname{sgn}(q) q = b_D$ for all $q \in Q_D$*
3. *If $x \in \mathbb{C}\mathfrak{S}_n$ and $x = px(\operatorname{sgn}(q)q)$ for all $p \in P_D$ and $q \in Q_D$ then $x \in \mathbb{C}c_D$.*

PROOF: Write $x = \sum_{g \in \mathfrak{S}_n} x_g g$. Then for all $p \in P_D$ and $q \in Q_D$, $x = px(\operatorname{sgn}(q)q)$, so $x_h = \operatorname{sgn}(q) x_{phq}$ for all $p \in P_D$ and $q \in Q_D$. Taking $h = e$ we see that $\operatorname{sgn}(q)x_e = x_{pq}$. Therefore

$$x = x_e \sum_{\substack{p \in P_D \\ q \in Q_D}} \operatorname{sgn}(q) pq + \sum_{g \notin P_D Q_D} x_g g = x_e c_D$$

since if $g \notin P_D Q_D$ then by Lemma 9.6 there are α, β that lie in the same row of D but in the same column of gD. Let $t = (\alpha\ \beta)$ and notice that $t \in P_D \cap Q_{gD} = P_D \cap gQ_D g^{-1}$, so $g^{-1}tg \in Q_D$. Hence $x_g = \operatorname{sgn}(g^{-1}tg)x_{tg(g^{-1}tg)} = -x_g$, so $x_g = 0$. Therefore $x \in \mathbb{C}c_D$. □

9.11 Corollary. *$c_D^2 = n_D c_D$, where $n_D \in \mathbb{Z}$.*

PROOF: $pc^2 \operatorname{sgn}(q)q = (pa)ba(b\operatorname{sgn}(q)q) = abab = c^2$, so $c^2 = \gamma c$ for some $\gamma \in \mathbb{C}$. But c has coeffients in $\{\pm 1, 0\}$, and c^2 has integers coeffiencts, so $\gamma = c_e \in \mathbb{Z}$. □

9.12 Theorem.

1. *V_λ is an irreducible representation of $\mathfrak{S}_n$.*

2. $V_\lambda \cong V_\mu$ *if and only if* $\lambda = \mu$.
3. $n_\lambda = \frac{n!}{\dim V_\lambda}$.

PROOF: 1. $V_\lambda \cong V_D = (\mathbb{C}\mathfrak{S}_n)c_D$ is a $\mathbb{C}\mathfrak{S}_n$-module. $\mathbb{C}\mathfrak{S}_n$ is semisimple, so there is an idempotent $e \in \mathbb{C}$ such that $V_D = (\mathbb{C}\mathfrak{S}_n)e$. $c_D V_D = c_D(\mathbb{C}\mathfrak{S}_n)c_D \subseteq \mathbb{C}c_D$ by Lemma 9.8.

Suppose that $W \subseteq V_D$ is a submodule. Either $c_D \in W$, which implies that $W = (\mathbb{C}\mathfrak{S}_n)W \supseteq (\mathbb{C}\mathfrak{S}_n)c_D = V$, or $c_D \notin W$, in which case $c_D W \subseteq W \cap c_D V = W \cap \mathbb{C}c_D = \{0\}$. If $W \neq 0$ then $W = (\mathbb{C}\mathfrak{S}_n)f$, with $f^2 = f$. Then $W^2 \subseteq VW = (\mathbb{C}\mathfrak{S}_n)c_D W = 0$, a contradiction since $f \in W^2$. Therefore V is irreducible.

2. Davidson lost me here. Ask Aaron.
3. See above. □

Suppose that $\lambda = (\lambda_1, \ldots, \lambda_k)$ is a partition of n. Let $P_j(x) = \sum_{i=1}^k x_i^j$, $\delta(x) = \prod_{1 \leq i < j \leq k} x_i - x_j$, and $\ell_i = \lambda_i + k - i$ for $i = 1, \ldots, k$.

9.13 Theorem (Frobenius). *If C_i is a conjugacy class for the partition $i = (i_1, \ldots, i_p)$ then*

$$\chi_\lambda(C_i) = [x_1^{\ell_1} \cdots x_l^{\ell_k}]\Delta(x) \prod_{j=1}^{p} P_j(x)^{i_j}$$

References

- "Noncommutative Algebra" by Farb and Dennis
- "Rings & Modules" by Lambek
- "Noncommutative Rings" by Herstein
- "A First Course on Noncommutative Rings" by Lam