

Math 753 Algebra III

Christopher Drupieski

Fall 2005

Contents

Introduction	ii
1 Wedderburn–Artin Theory	1
1.1 Basic Terminology and Examples	1
Exercises for §1	6
1.2 Semisimplicity	9
Exercises for §2	12
1.3 Structure of Semisimple Rings	12
Exercises for §3	17
2 Jacobson Radical Theory	20
2.4 The Jacobson Radical	20
Exercises for §4	26
2.5 Jacobson Radical Under Change of Rings	28
Exercises for §5	30
2.6 Group Rings and the J -Semisimplicity Problem	31
Exercises for §6	32
3 Introduction to Representation Theory	35
3.7 Modules over Finite-Dimensional Algebras	35
Exercises for §7	41
3.8 Representations of Groups	43
Exercises for §8	56
7 Local Rings, Semilocal Rings, and Idempotents	58
7.19 Local Rings	58
7.21 The Theory of Idempotents	60

Introduction

This document represents my notes from Mr. Wang's Fall 2005 section of Math 753 Algebra III. The chapter and section numbers of this document have been set up to correspond to the chapter and section numbers of the textbook we used, T.Y. Lam's *A First Course in Noncommutative Rings*. In places where my notes were ambiguous or incomplete, I have relied on Lam's book to complete this document. Included also in this document are my solutions to various exercises from Lam's book.

Chapter 1

Wedderburn–Artin Theory

1.1 Basic Terminology and Examples

We assume that all rings are unital, though not necessarily commutative. We assume that subrings share the same identity element as their parent ring, and that all ring homomorphisms $R \rightarrow S$ necessarily map $1_R \mapsto 1_S$.

Definition. An element $a \in R$ is a left zero divisor if $\exists 0 \neq b \in R$ such that $ab = 0$. An element $a \in R$ is a right zero divisor if $\exists 0 \neq b \in R$ such that $ba = 0$.

Definition. We call a ring reduced if it has no nonzero nilpotent ideals.

Definition. An element $a \in R$ is right-invertible if $\exists b \in R$ such that $ab = 1$. An element $a \in R$ is left-invertible if $\exists b \in R$ such that $ba = 1$.

Definition. Let k be a field, $R = k\langle x_1, \dots, x_n, y_1, \dots, y_n \rangle$ the polynomial ring in noncommuting determinates $x_i, y_i, 1 \leq i \leq n$. Let $F = \{x_i y_j - y_i x_j - \delta_{ij}\}$. We call $R/F = A_n(k)$ the n -th Weyl Algebra.

Definition. Given a ring k and a (semi-) group G (with multiplicative group operation), define the group ring kG as a set to be the set of all k -linear combinations of elements of G , $kG := \bigoplus_{g \in G} k \cdot g$, with multiplication defined by $(\sum_{g \in G} \alpha_g g) (\sum_{h \in G} \beta_h h) = \sum_{g, h} \alpha_g \beta_h (gh)$.

Note that $k = k \cdot 1_G \subseteq kG$, $G = 1_k \cdot G \subseteq kG$, k and G commute in the multiplication of kG , and kG is commutative if and only if k and G are each commutative.

Definition. Given a ring k , define the ring of formal power series in commuting indeterminates $\{x_i : i \in I\}$ by

$$k[[x_i : i \in I]] = \{F = f_0 + f_1 + \dots \mid f_n \text{ homogeneous polynomial in } \{x_i\} \text{ of degree } n\}$$

Define the ring of formal Laurent series in one indeterminate x by

$$k((x)) = \left\{ \sum_{j=-N}^{\infty} a_j x^j : 0 \leq N < \infty \right\}$$

Note that $\mathcal{U}(k[[x_i]]) = \{F : f_0 \in \mathcal{U}(k)\}$, and

$$\mathcal{U}(k((x))) = \{F \in k((x)) : \text{the lowest coefficient of } F \text{ is in } k\}$$

Definition. Given a polynomial ring $k[x]$ and a ring endomorphism $\sigma : k \rightarrow k$, define the (left) skew polynomial ring $k[x; \sigma]$ as a set to be the polynomial ring $k[x]$, with new skew product determined by $x^i \cdot b = \sigma^i(b)x^i$ for all $b \in k$.

Remark.

1. Define right skew polynomial rings and rings of skew formal power series analogously.
2. Given a polynomial ring $k[x]$ and an endomorphism $\sigma \in \text{End}(k)$, the corresponding left and right skew polynomial rings are not necessarily identical (e.g., in one ring x may be a left zero divisor but not a right zero divisor if σ is not injective).
3. If σ is injective and k is a domain, then $k[x; \sigma]$ is a domain and $\mathcal{U}(k[x; \sigma]) = \mathcal{U}(k)$.
4. If $\sigma \in \text{Aut}(k)$, we can define the ring of skew formal Laurent series $k((x; \sigma))$, and $\mathcal{U}(k((x; \sigma))) = \mathcal{U}(k((x)))$.

Definition. Call a map $\delta : k \rightarrow k$ a derivation of k if $\delta(a + b) = \delta(a) + \delta(b)$ and $\delta(ab) = a\delta(b) + \delta(a)b$ for all $a, b \in k$.

Definition. Given a derivation δ of the ring k , define the differential polynomial ring $k[x; \delta]$ as a set to be the polynomial ring $k[x]$, with product $x \cdot a = ax + \delta(a)$ for all $a \in k$.

Remark. Let δ be an inner derivation of the ring k , say $\delta(a) = [c, a] = ca - ac$. Then in $k[x; \delta]$, $(x - c)a = ax + \delta(a) - ca = ax + ca - ac - ca = ax - ac = a(x - c)$, i.e., a and $(x - c)$ commute. Now $\varphi : k[x; \delta] \rightarrow k[t]$ mapping $(x - c) \mapsto t$ and $a \mapsto a$ for $a \in k$ is a ring isomorphism.

Example. Let k_0 be a field, $k = k_0[y]$, and $\delta = \frac{d}{dy}$. Then $ax = xa$ if $a \in k$, and $xy = yx + 1$. We have $k_0[y][x; \delta] \cong k_0\langle x, y \rangle / (xy - yx - 1)$ the Weyl algebra $A_1(k_0)$.

Definition. Let R, S be rings, M an (R, S) -bimodule. We define the triangular ring $A = R \oplus M \oplus S$ as the set of all matrices of the form

$$A = \left(\begin{array}{cc} R & M \\ 0 & S \end{array} \right) = \left\{ \left(\begin{array}{cc} r & m \\ 0 & s \end{array} \right) : r \in R, s \in S, m \in M \right\}$$

with the usual matrix operations.

Lemma. In the triangular ring $A = R \oplus M \oplus S$,

1. R is a left ideal.
2. S is a right ideal.
3. M is an ideal with $M^2 = 0$.

4. $R \oplus M$ and $M \oplus S$ are ideals.

Proposition. Let A be the triangular ring $A = R \oplus M \oplus S$.

1. The left ideals of A are of the form $I_1 \oplus I_2$, where $I_2 \subseteq S$ is a left ideal of S and I_1 is a left R -submodule of $R \oplus M$ such that $MI_2 \subseteq I_1$.
2. The right ideals of A are of the form $J_1 \oplus J_2$ where $J_1 \subseteq R$ is a right ideal and J_2 is a right S -submodule of $M \oplus S$ such that $J_1M \subseteq J_2$.
3. The ideals of A are of the form $K_1 \oplus K_0 \oplus K_2$, where $K_1 \trianglelefteq R$, $K_2 \trianglelefteq S$, and K_0 is an (R, S) sub-bimodule of M such that $K_0 \supseteq K_1M + MK_2$.

Proof.

1. If I_1 and I_2 satisfy the conditions of (1), then $I_1 \oplus I_2$ is a left ideal of A . Conversely, let I be a left ideal of A , $x = rE_{11} + mE_{12} + sE_{22} \in I$. Then $E_{22}x = sE_{22} \in I$ and $E_{11}x = rE_{11} + mE_{12} \in J$, so $I = I_1 \oplus I_2$, $I_2 = I \cap S \subseteq S$ a left ideal of S , $I_1 \subseteq R \oplus M = (R \oplus M) \cap I$ a left R submodule of $R \oplus M$. And $MI_2 = M(I \cap S) \subseteq I \cap M \subseteq I \cap (R \oplus M) = I_1$.
2. If J_1 and J_2 satisfy the conditions of (2), then $J_1 \oplus J_2$ is a right ideal of A . Conversely, let J be a right ideal of A , $x = rE_{11} + mE_{12} + sE_{22} \in J$. Then $xE_{11} = rE_{11} \in J$, $xE_{22} = mE_{12} + sE_{22} \in J$, so $J = J_1 \oplus J_2$, $J_1 \subseteq R$, $J \subseteq M \oplus S$, $J_1 = J \cap R \subseteq R$ a right ideal, $J_2 = (M \oplus S) \cap J$ a right S -submodule of $M \oplus S$. And $J_1M = (J \cap R)M \subseteq J \cap M \subseteq J \cap (M \oplus S) = J_2$.
3. If $K = K_1 \oplus K_0 \oplus K_2$ satisfies the conditions of (3), then K is an ideal of A . Conversely, let K be an ideal of A , $x = rE_{11} + mE_{12} + sE_{22} \in K$. Then $E_{22}x = sE_{22} \in K$, $xE_{11} = rE_{11} \in K$, hence also $mE_{12} \in K$. So $K = K_1 \oplus K_0 \oplus K_2$, where $K_1 = K \cap R \trianglelefteq R$, $K_2 = K \cap S \trianglelefteq S$, and $K_0 = K \cap M$. Since M and K are ideals of A , $K_1M + MK_2 \subseteq K \cap M = K_0$. \square

Theorem. Let $A = R \oplus M \oplus S$ be a triangular ring. Then A is left (resp. right) noetherian iff R, S are left (resp. right) noetherian and ${}_R M$ (resp. M_S) is noetherian.

Proof. We prove the left noetherian case.

(\Rightarrow): By the lemma, $R \cong A/(M \oplus S)$, $S \cong A/(R \oplus M)$, so A noetherian implies that R, S are left noetherian. Let $M_1 \subseteq M_2 \subseteq \dots$ be a chain of R -submodules of M . Then $M_1 \subseteq M_2 \subseteq \dots$ as A -submodules, embedded in the northeast corner, so it must stabilize since A is left noetherian. Hence $\{M_i\}$ stabilizes.

(\Leftarrow): Let $\{I^{(j)}\}$ be an increasing chain of left ideals of A . By the proposition, $I^{(j)} = (I^{(j)} \cap (R \oplus M)) \oplus (I^{(j)} \cap S)$. Let $I_1^{(j)} = I^{(j)} \cap (R \oplus M)$, $I_2^{(j)} = I^{(j)} \cap S$. Then $\{I_2^{(j)}\}$ is an increasing chain of left ideals in S , and $\{I_1^{(j)}\}$ is an increasing chain of left R -submodules of $R \oplus M$, both of which are left noetherian by assumption. Hence these chains must stabilize, and we conclude that A is left noetherian. \square

Definition. A left (or right) R -module M is called artinian if the family of submodules of M satisfies the descending chain condition, that is, if every descending chain of submodules stabilizes.

Example.

1. \mathbb{Z} is noetherian but not artinian.
2. Let R be a noetherian domain, $r \in R$ an element with no left or right inverses. Then $(r) \supseteq (r^2) \supseteq (r^3) \supseteq \cdots$ is an infinite descending chain of R -submodules which does not stabilize. Conclude R is not artinian.

Proposition. Let N be an R -submodule of M . Then M is noetherian (resp. artinian) if and only if N and M/N are noetherian (resp. artinian).

Proof. If M is artinian, then N and M/N are artinian since any descending chain of submodules of N is also a descending chain of submodules of M , and any descending chain of submodules in M/N lifts to a descending chain of submodules in M containing N .

Conversely, suppose N and M/N are artinian, and let $M_1 \supseteq M_2 \supseteq M_3 \supseteq \cdots$ be a descending chain of submodules of M . Since M/N is artinian, the descending chain $(M_1 + N)/N \supseteq (M_2 + N)/N \supseteq \cdots$ of submodules of M/N stabilizes, say at $(M_j + N)/N$. The descending chain $(M_1 \cap N) \supseteq (M_2 \cap N) \supseteq \cdots$ of submodules of N must also stabilize, say at $M_k \cap N$. Let $n = \max j, k$. Given $m \in M_n, m' \in M_{n+1}$ since $(M_n + N)/N = (M_{n+1} + N)/N$, $m - m' \in N \cap M_n$. But $M_n \cap N = M_{n+1} \cap N$, so $m - m' \in M_{n+1} \cap N \Rightarrow m = m' + (m - m) \in M_{n+1}$. Conclude $M_n \subseteq M_{n+1}$, i.e., $M_n = M_{n+1}$, and the chain stabilizes at M_n . \square

Corollary. Finite direct sums of artinian modules are artinian.

Proof. It suffices to consider the direct sum of two artinian modules M, N . By the previous proposition, $M \oplus N$ is artinian if and only if N and $(M \oplus N)/N \cong M$ are artinian, both of which are true by assumption. \square

Definition. A composition series for a module M is a chain of submodules $0 = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_n = M$ such that the quotients M_i/M_{i-1} are simple for all $1 \leq i \leq n$. If M has a composition series, we call $l(M) := n$ the length of M , and we call the simple quotients M_i/M_{i-1} the composition factors of M .

Theorem (Jordan–Hölder). If M has a composition series, then any two composition series for M have the same length, and the composition factors of M are unique (up to isomorphism and ordering).

Proof. Let $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ and $0 = N_0 \subset N_1 \subset \cdots \subset N_k = M$ be two composition series for M . We argue by induction on $\min(n, k)$, the case $\min(n, k) = 1$ iff M is simple being clear.

Given a submodule S of M , consider the inclusion $(S \cap M_i)/(S \cap M_{i-1}) \hookrightarrow M_i/M_{i-1}$. Since the composition factors are by assumption simple, the image of this map is either $\{0\}$ or all of M_i/M_{i-1} . Then either $S \cap M_i = S \cap M_{i-1}$ or $(S \cap M_i)/(S \cap M_{i-1}) \cong M_i/M_{i-1}$ is simple. Then $0 = S \cap M_0 \subseteq S \cap M_1 \subseteq \cdots \subseteq S \cap M_n = S \cap M = S$ becomes a composition series for S after deleting redundant terms as necessary.

If $M_{n-1} = N_{k-1}$, we can apply the induction hypothesis with $S = M_{n-1}$. Suppose $M_{n-1} \neq N_{k-1}$. Without loss of generality, assume $N_{k-1} \not\subseteq M_{n-1}$. Then $M = M_{n-1} + N_{k-1}$ since $M_{n-1} \subsetneq M_{n-1} + N_{k-1}$ and M/M_{n-1} is simple. Set $S = M_{n-1} \cap N_{k-1}$. Then $M_{n-1}/S \cong M/N_{k-1}$ is simple and $N_{k-1}/S \cong M/M_{n-1}$ is simple. We now have $S \subset M_{n-1} \subset M_n = M$ and $S \subset N_{k-1} \subset N_k = M$. Moreover, S has a composition series of length $l(S) < \min(n, k)$, so the induction hypothesis applies to S . The result now follows for M by again applying the induction hypothesis. \square

Proposition. An R -module M has a (finite) composition series if and only if M is both noetherian and artinian.

Proof. Let M be an R -module with finite composition series. Argue that M is noetherian and artinian by induction on $l(M)$, the case $l(M) = 1 \iff M$ is simple being clear. By assumption, M has a composition series $0 = M_0 \subset M_1 \subset \dots \subset M_{n-1} \subset M_n = M$. Since $l(M_{n-1}) = n - 1 < n$, M_{n-1} is noetherian and artinian by the induction hypothesis. But M/M_{n-1} is simple, hence noetherian and artinian, which implies by previous results that M must be both noetherian and artinian.

Conversely, let $M \neq 0$ be an R -module that is both noetherian and artinian. Since M is artinian, it contains a minimal nonzero submodule M_1 , which is simple by minimality. If $M_1 = M$, we are done. Otherwise, M/M_1 is artinian, hence contains a minimal nonzero submodule lifting to a submodule $M_1 \subseteq M_2$ of M , and M_2/M_1 is simple by minimality. Since M is noetherian this process must eventually terminate, and the resulting series will be by construction a composition series for M . \square

Remark. If M is a finitely generated left module over a left noetherian (resp. artinian) ring, then M is noetherian (resp. artinian), since R^n is noetherian (resp. artinian) if R is noetherian (resp. artinian), and M is isomorphic to a quotient of R^n for some $n \in \mathbb{N}$.

Theorem. Let $A = R \oplus M \oplus S$ be a triangular ring. Then A is left (resp. right) artinian iff R, S are left (resp. right) artinian and ${}_R M$ (resp. M_S) is artinian.

Corollary. Let S be a commutative noetherian domain, R its fraction field. Assume $S \neq R$. Then the triangular ring $R = R \oplus R \oplus S$ is left noetherian but not right noetherian, and is neither left nor right artinian.

Proof. Follows from the theorem and the fact that S is not artinian (because by assumption it contains a nonzero non-unit) and R_S is not finitely generated (if it were finitely generated, we could find a common denominator $t \in S$ for all fractions in R , in which case $1/t^2 = s/t \Rightarrow 1/t = s \in S \Rightarrow R = S, (\Rightarrow \Leftarrow)$), hence is not noetherian. \square

Corollary. Let $S \subseteq R$ be fields, $\dim_S R = \infty$. Then the triangular ring $A = R \oplus R \oplus S$ is left noetherian and left artinian, but neither right noetherian nor right artinian.

Proof. ${}_A A$ has a composition series, $0 \subset R \subset R \oplus S \subset A$, so by the above proposition A is both left noetherian and left artinian. But R_S is neither noetherian nor artinian, so by the above theorem A is neither right noetherian nor right artinian. \square

Example. Let k be a division ring, σ an endomorphism of k that is injective but not surjective. Then $R = k[x; \sigma]$ is left noetherian but not right noetherian.

Proof. We have $xa = \sigma(a)x$ for all $a \in k$. Let I be a left ideal of R . Choose $f \in I$ monic of minimal degree. Then $I = Rf$. So every left ideal of R is finitely generated, hence R is left noetherian.

Let $b \in k \setminus \sigma(k)$. Claim: $\sum_{i=0}^{\infty} x^i b x R$ is a direct sum of right ideals. Suppose $0 = x^n b x f_n(x) + \cdots + x^{n+m} b x f_{n+m}(x)$ is a nontrivial dependence relation. Since x is not a left zero divisor, we have $b x f_n(x) = -(x b x f_{n+1}(x) + \cdots + x^m b x f_{n+m}(x))$. So $b x f_n(x) = x g(x)$ ($\neq 0$). Comparing highest power terms,

$$\begin{aligned} b x (a_r x^r) &= x (c_r x^r) & (\neq 0) \\ b \sigma(a_r) x^{r+1} &= \sigma(c_r) x^{r+1} & (\neq 0) \\ b &= \sigma(c_r a_r^{-1}) \in \sigma(k) & (\Rightarrow \Leftarrow) \end{aligned}$$

Then $\sum_{i=0}^{\infty} x^i b x R$ is a direct sum of right ideals, hence R is not right noetherian. \square

Exercises for §1

1.1.4. True or false: If ab is a unit, then a, b are units?

1. If $a^n \in R^*$, then $a \in R^*$.
2. If a is left-invertible and not a right zero-divisor, then $a \in R^*$.
3. If R is a domain, then R is Dedekind-finite.

Proof. False. Let k be a field, V a k -vector space with countable basis $\{e_1, e_2, \dots\}$. Let $R = \text{End}_k(V)$. Let $f \in R$ be determined by $f(e_i) = e_{i+1}$, and let $g \in R$ be determined by $g(e_1) = 0$, $g(e_i) = e_{i-1}$. Then $g \notin R^*$ but $g \circ f = \text{id}_V \in R^*$.

1. The proof is routine.
2. Suppose $ba = 1$. Now $ca \neq 0$ for all $0 \neq c \in R$, so $0 = a - a = a(ba) - a = (ab - 1)a \Rightarrow ab = 1$. Conclude $a \in R^*$.
3. Suppose $ab = 1$ for some $a, b \in R$. Then by (b), $ba = 1$. Conclude R is Dedekind-finite. \square

1.1.6. Let a, b be elements in a ring R . If $1 - ba$ is left-invertible (resp. invertible), show that $1 - ab$ is left-invertible (resp. invertible), and construct a left inverse (resp. inverse) for it explicitly.

Proof. Suppose $1 - ba$ is left invertible. Then $R(1 - ab) \supseteq Rb(1 - ab) = R(1 - ba)b = Rb$. In particular, $ab \in R(1 - ab)$, so $(1 - ab) + ab = 1 \in R(1 - ab)$ and $1 - ab$ is left invertible.

If $1 - ba$ is invertible, then $(1 - ab)R \supseteq (1 - ab)aR = a(1 - ba)R = aR$. In particular, $ab \in (1 - ab)R$, so $(1 - ab) + ab = 1 \in (1 - ab)R$ and $1 - ab$ is right invertible, hence invertible.

Suppose $1 - ba$ has left inverse (resp. inverse) $u \in R$. Then $(1 + aub)(1 - ab) = (1 - ab) + au(1 - ba)b = (1 - ab) + ab = 1$ \square

1.1.7. Let B_1, \dots, B_n be left ideals (resp. ideals) in a ring R . Show $R = B_1 \oplus \dots \oplus B_n$ iff there exist idempotents (resp. central idempotents) e_1, \dots, e_n with sum 1_R such that $e_i e_j = 0$ for $i \neq j$ and $B_i = Re_i$ for all i . Suppose the B_i 's are ideals. If $R = B_1 \oplus \dots \oplus B_n$ then each B_i is a ring with identity e_i , and $R \cong B_1 \times \dots \times B_n$. Show that any isomorphism of R with a finite direct product of rings arises in this way.

Proof.

(\Leftarrow) Suppose there exist idempotents $e_1, \dots, e_n \in R$ such that $1 = e_1 + \dots + e_n$, $e_i e_j = 0$ for $i \neq j$, and $B_i = Re_i$ for all $1 \leq i \leq n$. Then for all $r \in R$, $r = re_1 + \dots + re_n \in B_1 + \dots + B_n$, so $R \subseteq B_1 + \dots + B_n$. Suppose $c_1 e_1 + \dots + c_n e_n = 0$ for some $c_1, \dots, c_n \in R$. Then for each $1 \leq i \leq n$, $0 = (c_1 e_1 + \dots + c_n e_n) e_i = c_i e_i$. Conclude $B_i \cap B_j = \{0\}$ for $i \neq j$, hence $R = B_1 \oplus \dots \oplus B_n$.

(\Rightarrow) Suppose $R = B_1 \oplus \dots \oplus B_n$ for left ideals B_1, \dots, B_n . Then there exist $e_1 \in B_1, \dots, e_n \in B_n$ such that $1 = e_1 + \dots + e_n$. Then for each $1 \leq i \leq n$, $0 = e_i - e_i = e_i(e_1 + \dots + e_n) - (e_1 + \dots + e_n)e_i = \left(\sum_{i \neq j} e_i e_j\right) - \left(\sum_{i \neq j} e_j\right) e_i$. Since $e_i e_j \in B_j$ and $\left(\sum_{i \neq j} e_j\right) e_i \in B_i$, conclude by the directness of the sum $R = B_1 \oplus \dots \oplus B_n$ that $e_i e_j = 0$ for all $i \neq j$.

Now $e_i = e_i(e_1 + \dots + e_n) = e_i^2$, i.e., each e_i is idempotent. Let $b_i \in B_i$. Then $b_i = b_i(e_1 + \dots + e_n)$ and $0 = (b_i e_i - b_i) + \left(\sum_{i \neq j} b_i e_j\right)$. Again conclude by the directness of the sum $R = B_1 \oplus \dots \oplus B_n$ that $b_i e_j = 0$ for all $i \neq j$ and $b_i = b_i e_i \in Re_i$. Then $B_i = Re_i$ for all $1 \leq i \leq n$. \square

1.1.9. Show that for any ring R , the center of the matrix ring $M_n(R)$ consists of the diagonal matrices rI_n , $r \in Z(R)$.

1.1.12. A left R -module is said to be *hopfian* if any surjective R -endomorphism of M is an automorphism.

1. Show that any noetherian module M is hopfian.
2. Show that the left regular module ${}_R R$ is hopfian iff R is Dedekind-finite.
3. Deduce that any left noetherian ring R is Dedekind-finite.

Proof.

1. Let $f \in \text{End}_R(M)$ be surjective. Then $f^k : M \rightarrow M$ is also surjective for all $k \in \mathbb{N}$. We have $\ker f \subseteq \ker f^2 \subseteq \dots$. Say the chain stabilizes at $\ker f^m$. Let $g \in \ker f$. Then $\exists h \in M$ such that $g = f^m(h)$. Now $g \in \ker f \subseteq \ker f^m \Rightarrow 0 = f^m(g) = f^{2m}(h) \Rightarrow h \in \ker f^{2m} = \ker f^m \Rightarrow g = f^m(h) = 0$. So $\ker f = \{0\}$. Conclude f is an automorphism.
2. Suppose ${}_R R$ is hopfian. Let $a, b \in R$ and suppose $ab = 1$. Then the map $\varphi : R \rightarrow R$ given by $s \mapsto sb$ is a surjective R -endomorphism, hence an automorphism by (1). Now $\varphi(ba - 1) = (ba - 1)b = b(ab) - b = b - b = 0$. Conclude $ba = 1$, so R is Dedekind-finite. Suppose R is Dedekind-finite. Let $\varphi : R \rightarrow R$ be a surjective R -endomorphism. Let $x \in \ker \varphi$. Since φ is surjective, $\exists y \in R$ such that $\varphi(y) = 1$. Now $1 = \varphi(y) = y\varphi(1) \Rightarrow \varphi(1)y = 1$ since R is Dedekind-finite. Now $x = x(1) = x\varphi(y) = x(y\varphi(1)) = x(\varphi(1)y) = \varphi(x)y = 0$. Then $\ker \varphi = \{0\}$ and φ is injective. Conclude that φ is an automorphism and ${}_R R$ is hopfian.

3. Let R be a noetherian ring. Then R is noetherian as a module over itself $\Rightarrow R$ is hopfian by (1) $\Rightarrow R$ is Dedekind-finite by (2). \square

1.1.13. Let A be an algebra over a field k such that every element of A is algebraic over k .

1. Show that A is Dedekind-finite.
2. Show that a left zero-divisor of A is also a right zero-divisor of A .
3. Show that a non-zero element of A is a unit iff it is not a zero divisor.
4. Let B be a subalgebra of A , and $b \in B$. Show $b \in B^*$ iff $b \in A^*$.

1.1.15. Let $A = \mathbb{C}[x; \sigma]$, where σ denotes complex conjugation.

1. Show $Z(A) = \mathbb{R}[x^2]$.
2. Show $A/(x^2 + 1) \cong \mathbb{H}$.
3. Show $A/(x^4 + 1) \cong M_2(\mathbb{C})$.

1.1.16. Let K be a division ring with center k .

1. Show that the center of the polynomial ring $R = K[x]$ is $k[x]$.
2. For any $a \in K \setminus k$, show that the ideal generated by $x - a$ in $K[x]$ is the unit ideal.
3. Show that any ideal $I \subseteq R$ has the form Rh for some $h \in k[x]$.

1.1.17. Let x, y be elements in a ring R such that $Rx = Ry$. Show that there exists a right R -module isomorphism $f : xR \rightarrow yR$ such that $f(x) = y$.

Proof. Say $y = ax$, $x = by$. Define $f : xR \rightarrow yR$ by $f(xr) = yr$. This map is a well-defined right R -module homomorphism, since if $xr = xs$, then $yr = axr = axs = ys$. Similarly, define $g : yR \rightarrow xR$ by $g(yr) = xr$. This map is a well-defined right R -module homomorphism, since if $yr = ys$, then $xr = byr = bys = xs$. Now $f \circ g = 1_{yR}$ and $g \circ f = 1_{xR}$. Conclude that f is a right R -module isomorphism. \square

1.1.19. Let R be a domain. If R has a minimal left ideal, show that R is a division ring. (In particular, a left artinian domain must be a division ring.)

Proof. Suppose R has a nonzero minimal left ideal I . Let $0 \neq a \in I$. Then $\{0\} \neq (a^2) \subseteq (a) \subseteq I$, in which case $(a^2) = (a) = I$ by the minimality of I . Then $\exists r \in R$ such that $a = ra^2$. Then $0 = a - ra^2 = a(1 - ra)$. But $a \neq 0$ and R is a domain, so $1 - ra = 0$, i.e., $ra = 1$. Then $I = (1) = R$. Now given $0 \neq b \in R$, $\{0\} \neq (b) \subseteq (1) = I \Rightarrow (b) = (1) = I$ by minimality of $I \Rightarrow b \in R^*$. Conclude R is a division ring. \square

1.1.20. Let $E = \text{End}_R(M)$ be the ring of endomorphisms of an R -module M , and let nM denote the direct sum of n copies of M . Show that $\text{End}_R(nM) \cong M_n(E)$.

Proof. Say M is a right R -module, and write the endomorphisms on the left. Let $\epsilon_j : M \rightarrow nM$ be the j -th inclusion, and $\pi_i : nM \rightarrow M$ the i -th projection. For any $F \in \text{End}_R(nM)$, let f_{ij} be the composition $\pi_i F \epsilon_j \in \text{End}_R(M)$. Define $\alpha : \text{End}_R(nM) \rightarrow M_n(E)$ by $\alpha(F) = (f_{ij})$; this map is an isomorphism. \square

1.1.22. For any ring k , let $A = M_n(k)$ and let R (resp. S) denote the ring of $n \times n$ upper (resp. lower) triangular matrices over k .

1. Show $R \cong S$.
2. Suppose k has an anti-automorphism (resp. involution). Show the same is true for A , R and S .
3. Under the assumption of (2), show that R, S, R^{op}, S^{op} are all isomorphic.

1.1.26. For any right ideal in a ring R , the idealizer of A is defined to be $\mathbb{I}_R(A) = \{r \in R : rA \subseteq A\}$.

1. Show $\mathbb{I}_R(A)$ is the largest subring of R that contains A as an ideal.
2. The ring $\mathbb{E}_R(A) = \mathbb{I}_R(A)/A$ is known as the eigenring of the right ideal A . Show $\mathbb{E}_R(A) \cong \text{End}_R(R/A)$ as rings.

1.1.27. Let $R = M_n(k)$ where k is a ring, A the right ideal of R consisting of all matrices whose first r rows are zero. Compute $\mathbb{I}_R(A)$ and $\mathbb{E}_R(A)$.

1.2 Semisimplicity

Definition. An R -module M is semisimple if for every submodule N of M , there exists a submodule N' of M such that $M = N \oplus N'$.

Remark. A simple R -module is not necessarily semisimple.

Lemma. Submodules and quotients of semisimple modules are semisimple.

Proof. Let M be a semisimple R -module, N a submodule. Let W be a submodule of N . By semisimplicity of M , $M = W \oplus W'$ for some submodule W' of M . Then $N = W \oplus (N \cap W')$.

A submodule of M/N lifts to a submodule V containing N . By semisimplicity of M , $M = V \oplus V'$ for some submodule V' of M . Then $M/N = V/N \oplus (V' + N)/N$. \square

Lemma. Any nonzero semisimple R -module M contains a simple submodule.

Proof. Let $0 \neq m \in M$. It suffices to find a simple submodule of Rm . Let \mathcal{F} be the collection of submodules of Rm not containing m . By the usual Zorn's Lemma argument, \mathcal{F} contains a maximal element N , $N \not\subseteq Nm$. Now M semisimple $\Rightarrow Nm$ semisimple $\Rightarrow \exists N' \leq Nm$ such that $Nm = N \oplus N'$. Now N' must be simple: If $0 \neq N'' \leq N'$, then by maximality of N , $N \oplus N'' = Nm = N \oplus N'' \Rightarrow N' = N''$. \square

Theorem. The following are equivalent for a (left) R -module ${}_R M$:

1. M is semisimple.
2. M is a direct sum of simple modules.
3. M is a sum of simple modules.

Proof.

(1) \Rightarrow (2): Let $\mathcal{F} = \{S \leq M : S \text{ is a direct sum of simple modules}\}$. Then $\mathcal{F} \neq \emptyset$ by the previous lemma. By the usual Zorn's Lemma argument, \mathcal{F} contains a maximal element $M' \leq M$. Claim: $M' = M$. If not, $M = M' \oplus M''$ for a nonzero semisimple submodule M'' . Then $\exists S \leq M''$ simple, so $M' \subsetneq M' \oplus S \in \mathcal{F}$, ($\Rightarrow \Leftarrow$).

(2) \Rightarrow (3): Clear.

(3) \Rightarrow (1): Take $N \leq M$. Let $M = \sum_{i \in I} M_i$, M_i simple. Consider

$$\mathcal{F} = \left\{ J \subseteq I : \sum_{i \in J} M_i = \bigoplus_{i \in J} M_i, N \cap \bigoplus_{i \in J} M_i = 0 \right\}$$

Then $\mathcal{F} \neq \emptyset$ if $N \neq M$, so by Zorn's Lemma, \mathcal{F} has a maximal element J . Let $M' = N \oplus \bigoplus_{i \in J} M_i$. Claim: $M = M'$. If $M' \subsetneq M$, then $\exists M_{i_0} \not\subseteq M'$ (because $M = \sum M_i$), $M_{i_0} \cap M' = 0$ because M_{i_0} is simple, $M' + M_{i_0} = N \oplus \bigoplus_{J \cup \{i_0\}} M_i$, so $J \cup \{i_0\} \in \mathcal{F}$, a contradiction to the maximality of J . \square

Theorem. For a ring R , the following are equivalent:

1. All left R -modules are semisimple.
2. All finitely generated left R -modules are semisimple.
3. All cyclic left R -modules are semisimple.
4. ${}_R R$ is semisimple.

A ring with these properties is called a (left) semisimple ring.

Proof. The implications (1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (4) are clear. For the implication (4) \Rightarrow (1), let M be an R -module. Trivially, $M = \sum_{m \in M} Rm$. Now $Rm \cong R/\text{Ann}(m)$ a quotient of the semisimple module ${}_R R$. Then for each $m \in M$, Rm and hence all of M is a sum of simple modules, which implies that M is semisimple by the previous theorem. \square

Remark. Let R be a semisimple ring. Then ${}_R R = \bigoplus_{i \in I} A_i$, $A_i =$ minimal left ideals, and $1_R = \sum_{i \in I} a_i$, almost all $a_i = 0$, $a_i \in A_i$. Then $r = \sum_{i \in I} r a_i$ for all $r \in R$, and $|I| < \infty$.

Corollary. If R is semisimple, then R has a composition series with composition factors $\{A_i : i \in I\}$. In this case R is also left noetherian and left artinian.

Definition.

1. A left R -module P is called projective if for any exact sequence $M \xrightarrow{f} N \rightarrow 0$ of module homomorphisms and module homomorphism $g : P \rightarrow N$, there exists a module homomorphism $h : P \rightarrow M$ such that $f \circ h = g$.

2. A left R -module I is called injective if for any exact sequence $0 \rightarrow M \xrightarrow{f} N$ of module homomorphisms and module homomorphism $g : M \rightarrow I$, there exists a module homomorphism $h : N \rightarrow I$ such that $h \circ f = g$.

Lemma. For a left R -module P , the following are equivalent:

1. P is projective.
2. $P \cong$ a direct summand of a free R -module F .
3. Every exact sequence of R -modules $M \rightarrow P \rightarrow 0$ splits.

Proof.

(a) \Rightarrow (c): Suppose P is projective. Then given $\text{id}_P : P \rightarrow P$, there exists $h : P \rightarrow M$ such that $f \circ h = \text{id}_P$. Then $M \xrightarrow{f} P \rightarrow 0$ splits.

(c) \Rightarrow (b): Let $F = \bigoplus_{p \in P} R \cdot p$, the free R -module with basis the elements of P . Now $F \rightarrow P \rightarrow 0$ is exact, so it splits by (b). Then (c) holds.

(b) \Rightarrow (a): Let $M \xrightarrow{f} N \rightarrow 0$ be exact. Assume F is free and $F = P \oplus Q$. Given $g : P \rightarrow N$, we can extend it to a map $g : F \rightarrow N$ by mapping Q to zero. Say F has generators $\{x_i\}$. Find $m_i \in M$ such that $f(m_i) = g(x_i)$. (possible since f is surjective). Define $H : F \rightarrow M$ by $H(x_i) = m_i$, $h = H|_P$. Then $f \circ h = g$. Conclude P is projective. \square

Theorem. For a ring R , the following are equivalent:

1. R is left semisimple.
2. All left R -modules are projective.
3. All finitely generated left R -modules are projective.
4. All cyclic left R -modules are projective.

Proof.

The implications (2) \Rightarrow (3) \Rightarrow (4) are clear.

For the implication (1) \Rightarrow (2), if R is left semisimple, then every exact sequence of left R -modules $M \rightarrow P \rightarrow 0$ splits (because P is a direct sum of simple R -submodules, each of which must be either contained in or disjoint from the image of the map $M \rightarrow P$), which is equivalent to P being projective.

(4) \Rightarrow (1): Let I be a submodule of ${}_R R$. Now R/I is cyclic, so by (4) the exact sequence $0 \rightarrow I \rightarrow R \rightarrow R/I \rightarrow 0$ splits. Then $R \cong I \oplus R/I$. Conclude R is semisimple. \square

Remark. A left R -module I is injective if and only if any exact sequence of left R -modules $0 \rightarrow I \rightarrow M$ splits.

Exercises for §2

1.2.3. What are the semisimple \mathbb{Z} -modules?

A simple \mathbb{Z} -module is a simple abelian group, and the simple abelian groups are precisely the cyclic groups of prime order. Thus a semisimple \mathbb{Z} -module is a direct sum of cyclic groups of prime order.

1.2.4. Let R be the (commutative) ring of all real-valued continuous functions on $[0, 1]$. Is R a semisimple ring?

No. For $n \geq 1$, let $I_n = \{f \in R : f(x) = 0 \forall x \in [0, 1/n]\}$. Then $I_1 \subset I_2 \subset I_3 \subset \cdots$ is an infinite strictly increasing chain of ideals in R . Conclude that R is not noetherian, hence not semisimple since all semisimple rings are noetherian.

1.2.6. Let R be a right semisimple ring. For $x, y \in R$, show that $Rx = Ry$ if and only if $x = uy$ for some $u \in R^*$.

Proof.

If $x = uy$ for some $u \in R^*$, then clearly $Rx = Ry$.

Suppose $Rx = Ry$. By Exercise 1.1.17, there exists a right R -module homomorphism $f : xR \rightarrow yR$ such that $f(x) = y$. Since R is right semisimple, we can write $R = xR \oplus N = yR \oplus N'$ for some complementary right ideals N, N' of R . Furthermore, since $xR \cong yR$, we must have $N \cong N'$ as right R -submodules of R_R . (Let A_1, \dots, A_r be a complete list of pairwise nonisomorphic right ideals of R . Say $R_R \cong \bigoplus_{i=1}^r n_i A_i$, $xR \cong \bigoplus_{i=1}^r m_i A_i$, $0 \leq m_i \leq n_i$. Then $yR \cong \bigoplus_{i=1}^r m_i A_i$, and $N \cong N' \cong \bigoplus_{i=1}^r (n_i - m_i) A_i$.) We can thus extend f to an automorphism of R_R .

Now $y = f(x) = f(1)x$, and $f(1) \in R^*$ with inverse $f^{-1}(1)$. □

1.2.7. Show that for a semisimple module M over any ring R , the following conditions are equivalent:

1. M is finitely generated.
2. M is noetherian.
3. M is artinian.
4. M is a finite direct sum of simple modules.

1.3 Structure of Semisimple Rings

Theorem.

1. Any ideal I of $M_n(R)$ is of the form $M_n(A)$ for some ideal $A \trianglelefteq R$.
2. If R is simple, then $M_n(R)$ is simple.

Proof. Part (a) obviously implies part (b).

Given an ideal $A \trianglelefteq R$, it is clear that $M_n(A)$ is an ideal of $M_n(R)$. Conversely, let $I \trianglelefteq M_n(R)$, and let $A = \{(a_{ij}) : (a_{ij}) \in I\}$. It is easy to check that $A \trianglelefteq R$. Claim: $I = M_n(A)$. First note that if $(r_{ab}) \in M_n(R)$, then $E_{ij}(r_{ab})E_{kl} = r_{jk}E_{il}$. Now, given $(r_{ab}) \in I$, we have $E_{1j}(r_{ab})E_{k1} = r_{jk}E_{11} \in I$, so $r_{jk} \in A$ and $I \subseteq M_n(A)$.

Let $(r_{ij}) \in M_n(A)$. Given $1 \leq a, b \leq n$, there exists $M = (m_{kl}) \in I$ with $r_{ab} = m_{11}$. Then for such an M , we get $E_{a1}ME_{1b} = r_{ab}E_{ab} \in I$. Then $(r_{ab}) = \sum r_{ab}E_{ab} \in I$, i.e., $M_n(A) \subseteq I$. Conclude $M_n(A) = I$. \square

Theorem. Let D be a division ring, $R = M_n(D)$. Then

1. R is simple and left semisimple.
2. R has a unique (up to iso.) left simple module V . R acts faithfully on V with ${}_R R \cong nV$.
3. $\text{End}({}_R V) \cong D$ as rings.

Proof.

1. Simplicity follows from the previous theorem. Semisimplicity follows from (2).
2. Let $V = D^n$, the n -dimensional right D -vector space. Note that R acts faithfully on V by left multiplication, $R \cong \text{End}(V_D)$, and V is a simple left R -module. Now ${}_R R = A_1 \oplus \cdots \oplus A_n$, where A_i denotes the set of matrices with a nonzero i -th column and zeros elsewhere. Have that $A_i \cong V$ as R -modules, hence ${}_R R \cong nV$ a direct sum of simple submodules, and R is left semisimple. From the above decomposition of ${}_R R$ we have that all composition factors of R are isomorphic to the simple R -module V . Any simple left submodule of R is a composition factor of R , so isomorphic to V .
3. Claim: The homomorphism $\Delta : D \rightarrow \text{End}({}_R V)$, $\Delta(d) =$ right multiplication by d on V , is an isomorphism. This map is injective since D acts faithfully on $V = D^n$. Let $f \in \text{End}({}_R V)$. Then $(1, 0, \dots, 0)^t f = (d, *, \dots, *)^t$ for some $d \in D$. Then

$$\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} f = \left(\begin{bmatrix} a_1 & 0 & \cdots & 0 \\ a_2 & 0 & \cdots & 0 \\ \vdots & & & \vdots \\ a_n & 0 & \cdots & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \right) f = \begin{bmatrix} a_1 & 0 & \cdots & 0 \\ a_2 & 0 & \cdots & 0 \\ \vdots & & & \vdots \\ a_n & 0 & \cdots & 0 \end{bmatrix} \begin{bmatrix} d \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} a_1 d \\ a_2 d \\ \vdots \\ a_n d \end{bmatrix}$$

So f acts as (right) scalar multiplication by d . Conclude that Δ is an isomorphism. \square

Lemma. Given left semisimple rings R_i ($1 \leq i \leq r$), $R = \prod_{i=1}^r R_i$ is a left semisimple ring.

Proof. Viewing each R_i as an ideal in R , a minimal left ideal of R_i is also a minimal left ideal of R . Since each R_i is a direct sum of minimal left ideals, we can write R as a direct sum of minimal left ideals. Then R is semisimple. \square

Lemma (Schur's Lemma). Given a ring R and a simple left R -module V , $\text{End}({}_R V)$ is a division ring.

Proof. Let $0 \neq f \in \text{End}({}_R V)$. Now $f(V) \neq \{0\}$ is a nonzero R -submodule of V , and $\ker f \neq V$ is a proper R -submodule of V . By the simplicity of V , we then have $f(V) = V$ and $\ker f = \{0\}$, i.e., f is invertible. \square

Theorem (Wedderburn–Artin). Let R be a left semisimple ring. Then $R \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$ where the D_i are division rings, $n_i \in \mathbb{N}$, $r \in \mathbb{N}$ is determined uniquely by R , and $\{(n_i, D_i) : 1 \leq i \leq r\}$ is unique up to permutation. In particular, R has exactly r pairwise nonisomorphic left simple R -modules.

Proof. A ring R of the above form is left semisimple by previous results. Conversely, let R be a left semisimple ring. Write ${}_R R \cong n_1 V_1 \oplus \cdots \oplus n_r V_r$ for pairwise nonisomorphic left simple R -modules V_i (minimal left ideals). Then $\{V_1, \dots, V_r\}$ is a complete set of left simple R -modules by the Jordan–Hölder theorem.

By Schur’s Lemma $D_i = \text{End}({}_R V_i)$ is a division ring, and $\text{End}(n_i V_i) \cong M_{n_i}(D_i)$ by Exercise 1.1.20. We have $\text{Hom}(V_i, V_j) = \{0\}$ for $i \neq j$ since V_i, V_j are simple and $V_i \not\cong V_j$ for $i \neq j$. Then $R \cong \text{End}({}_R R) \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$.

Applying the Jordan–Hölder theorem to the decomposition ${}_R R \cong n_1 V_1 \oplus \cdots \oplus n_r V_r$, r and $\{(n_i, V_i) : 1 \leq i \leq r\}$ is uniquely determined up to ordering, and $D_i = \text{End}(V_i)$ is determined by V_i , so the uniqueness claim follows. \square

Corollary. A ring R is left semisimple if and only if it is right semisimple.

Proof. This follows since a finite direct product of matrix rings over skew fields is simultaneously left semisimple and right semisimple. \square

Remark. Let k be a field, R a finite dimensional k -algebra. Then R satisfies the ascending and descending chain conditions on ideals because an ideal is a k -vector subspace of bounded dimension.

If R is simple, then $R \cong M_n(D)$. If V denotes the unique left simple module of R , then $D \cong \text{End}({}_R V)$ is a k -algebra.

If $R \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$, D_i division k -algebras, and if additionally $\bar{k} = k$ (i.e., k is algebraically closed), then $D_i \cong k$ for all $1 \leq i \leq r$. (D_i is a finite-dimensional k -algebra, hence all elements of D_i are algebraic over $k = \bar{k} \Rightarrow D_i \cong k$.)

Lemma. Let R be a ring, A a minimal left ideal of R , \mathcal{B}_A the sum of all left ideals of R isomorphic to A (“isotypical component of R ”).

1. \mathcal{B}_A is an ideal in R .
2. If A, A' are nonisomorphic minimal left ideals of R , then $\mathcal{B}_A \mathcal{B}_{A'} = \{0\}$.

Proof.

1. Let $I \cong A$ be a left ideal of R , $I \subseteq \mathcal{B}_A$. Then $\forall r \in R$, the map $I \rightarrow Ir, i \rightarrow ir$ is an R -module homomorphism. By the simplicity of I , $Ir = \{0\}$ or $Ir \cong I \cong A$. Either way, $I \cdot r \subseteq \mathcal{B}_A$.

2. It suffices to show $AA' = \{0\}$. If $AA' \neq \{0\}$, then $\exists r' \in A'$ such that $Ar' \neq \{0\}$. Consider the homomorphisms $f : A \twoheadrightarrow Ar'$, $g : Ar' \hookrightarrow A'$. By the simplicity of A, A' and since $Ar' \neq \{0\}$, f, g are isomorphisms. Then $A \cong A'$, ($\Rightarrow \Leftarrow$). Conclude $AA' = \{0\}$. \square

Assume R is left semisimple. Write ${}_R R = A_1 \oplus \cdots \oplus A_r \oplus \cdots$ where $\{A_1, \dots, A_r\}$ is a complete set of pairwise nonisomorphic minimal left ideals, and let $B_i = \mathcal{B}_{A_i} \trianglelefteq R$. Then $R = B_1 \oplus \cdots \oplus B_r$.

Proposition. Let R be a left semisimple ring with notation as above. Then each B_i is a simple left artinian ring.

Proof. That each B_i is a ring and $R \cong B_1 \times \cdots \times B_r$ follows from Exercise 1.1.7. Each B_i is a quotient of the left artinian ring R , hence is also left artinian.

Let $\{0\} \neq I \trianglelefteq B_i$. Then $I \trianglelefteq R$, so I contains some minimal left ideal A , isomorphic to some A_k . Since $I \subseteq B_i$ $k = i$. A is a direct summand of R because R is semisimple. Then by Exercise 1.1.7, $A = Re$ for some idempotent $e \in A$. Let $A' \cong A_i$ be a minimal left ideal of R , and let $\varphi : A \rightarrow A'$ be an R -module isomorphism. Then $A' = \varphi(A) = \varphi(Ae) = A\varphi(e) \subseteq I$ because I is an ideal, and consequently $B_i \subseteq I$. Conclude $B_i = I$. \square

Theorem. Let R be a simple ring. Then the following are equivalent:

1. R is left artinian.
2. R is left semisimple.
3. R has a minimal left ideal.
4. $R \cong M_n(D)$ for some $n \in \mathbb{N}$ and some division ring D .

Proof.

(2) and (4) are equivalent by the Wedderburn–Artin Theorem.

(1) \Rightarrow (3) is immediate.

(3) \Rightarrow (2): Let A be a minimal left ideal of R , and consider $\mathcal{B}_A \neq \{0\}$. Then $\mathcal{B}_A = R$ by the simplicity of R , and ${}_R R = \mathcal{B}_A \cong A \oplus \cdots \oplus A$, A simple left R -module. Then R is left semisimple.

(2) \Rightarrow (1): A left semisimple ring has a composition series, and we already proved that a left module has a composition series if and only if it is left artinian. \square

Theorem (Double Centralizer Property). Let R be a simple ring, $\{0\} \neq A$ a left ideal of R , $D = \text{End}({}_R A)$ acting on A from the right. Then the natural map $L : R \rightarrow \text{End}(A_D)$, $r \mapsto L_r$ left multiplication, is an isomorphism.

Proof. Let $E = \text{End}(A_D)$. $L : R \rightarrow E$ is injective because R is simple.

Claim 1: For all $h \in E$, $r \in A$, $h \cdot L(r) = L(h(r)) \in E$. Indeed, given $a \in A$, $h \cdot L(r)(a) = h(ra) = h(r)a$ (since $R_a \in D$) $= L(h(r))a$, i.e., $h \cdot L(r) = L(h(r))$.

Claim 2: $L(R)$ is a left ideal of E . AR is an ideal in R , so $AR = R$ by the simplicity of R . Then $L(R) = L(AR) = L(A)L(R)$. Now $E \cdot L(R) = E \cdot L(A)L(R) \subseteq L(A)L(R)$ (by Claim 1) $= L(R)$. So $L(R)$ is a left ideal of E .

The result now follows, because $1 \in L(R) \Rightarrow L(R) = E$. \square

Example (Nonartinian Simple Ring). Given a chain of simple rings $R_1 \subseteq R_2 \subseteq R_3 \subseteq \dots$ sharing the same identity, their union $R = \bigcup_{i=1}^{\infty} R_i$ is also simple.

Let D be a division ring, $R_i = M_{2^i}(D)$. Then $R_i \subseteq R_{i+1}$ via the embedding

$$M \mapsto \begin{bmatrix} M & \\ & M \end{bmatrix}$$

Define $e_i \in R_i$ as the E_{11} matrix unit (in $R_i = M_{2^i}(D)$, so under the embeddings $R_i \hookrightarrow R_j$, $j > i$, e_i will be a sum of diagonal matrix units). Then $e_i e_{i+1} = e_{i+1}$, but $e_i \notin R e_{i+1}$. (If $z \in R_j$, then considering the images of e_i, e_{i+1} in R_j , $z e_{i+1}$ will have smaller column rank than e_i .)

Then $R e_0 \supsetneq R e_1 \supsetneq \dots$ is an infinite strictly descending chain of left ideals in R , and R is not artinian.

Define $f_i \in R_i$ by $f_i = I_i - e_i$ (I_i the identity matrix in R_i). Then $f_i f_{i+1} = f_i$, $f_{i+1} \notin R f_i$, and $R f_0 \subsetneq R f_1 \subsetneq R f_2 \subsetneq \dots$ is an infinite strictly increasing chain in R , so R is not noetherian.

Definition. Let k be a ring and let $\delta \in \text{Der}(k)$. An ideal $A \trianglelefteq K$ is called a δ -ideal if $\delta(A) \subseteq A$. Call k δ -simple if it has no proper δ -ideals.

Theorem. Let k be a \mathbb{Q} -algebra with derivation δ . Then the differential polynomial ring $R = k[x; \delta]$ is simple if and only if k is δ -simple and δ is not an inner derivation (i.e., is not a commutator).

Proof.

(\Rightarrow) If k has a proper δ -ideal A , let $I = \{\sum a_i x^i : a_i \in A\} \subsetneq R$. It is clear that $I = AR$, while $x(\sum a_i x^i) = \sum a_i x^{i+1} + \sum \delta(a_i) x^i \in I$, so I a proper ideal of R and R is not simple. If δ is an inner derivation, $R = k[x; \delta] \cong k[t]$ is not simple, because $(t) \triangleleft R$ is a proper ideal.

(\Leftarrow) It is equivalent to show that if k is δ -simple but R is not simple, then δ is an inner derivation. Suppose k is δ -simple but R has a proper nonzero ideal $\{0\} \neq I \triangleleft R$. Let $n = \min\{\deg(f) : 0 \neq f \in I\}$, and let $A = \{a_n \in k : a_n x^n + \text{lower terms} \in I\} \cup \{0\}$. If $a_n x^n + \dots \in I$, then $x(a_n x^n + \dots) - (a_n x^n + \dots)x = \delta(a_n) x^n + \dots \in I \Rightarrow \delta(a_n) \in A$, so A is a nonzero δ -ideal of $k \Rightarrow A = k$ by the δ -simplicity of k . Then there exists $g \in I$ of degree n of the form $g = x^n + dx^{n-1} + \dots$ for some $d \in k$.

Claim: For $b \in k$, $x^n b = bx^n + n\delta(b)x^{n-1} + \dots$, and if $g = x^n + dx^{n-1} + \dots$ as above, $bg - gb = (bd - db - n\delta(b))x^{n-1}$.

We have $(bd - db - n\delta(b))x^{n-1} + \dots = bg - gb \in I$. By the minimality of n , $bg - gb = 0$. So $bd - db - n\delta(b) = 0$. If $n = 0$, then $g = 1$ and $I = R$, in contradiction to the choice of I . Then since $\mathbb{Q} \subseteq k$ we can write $\delta(b) = n^{-1}(bd - db)$, i.e., $\delta = [-d/n, \cdot]$ is an inner derivation. \square

Corollary. Let k be a simple \mathbb{Q} -algebra. Then $R = k[x; \delta]$ is a nonartinian simple ring for any non-inner derivation δ .

Proof. R is simple by the previous theorem, and is nonartinian since $Rx \supsetneq Rx^2 \supsetneq Rx^3 \supsetneq \dots$ is an infinite strictly descending chain in R . \square

Corollary. Let k_0 be a simple \mathbb{Q} -algebra, $n \geq 1$. Then the Weyl Algebra $A_n(k_0)$ is nonartinian simple.

Proof. Since $A_n(k_0) = A_1(A_{n-1}(k_0))$, it suffices to prove the case $n = 1$. Recall $A_1(k_0) \cong k_0[y][x; \delta]$, $\delta = \frac{d}{dy}$. $R = A_1(k_0)$ is nonartinian because $Rx \supsetneq Rx^2 \supsetneq \cdots$ is an infinite strictly decreasing chain of ideals in R . δ is not an inner derivation of $k_0[y]$ because $\delta(y) = 1$ and an inner derivation would map central elements to zero.

Let $\{0\} \neq A \trianglelefteq k_0[y]$ be a δ -ideal, and let $f = ay^n + \cdots \in A$ be a nonzero polynomial of minimal degree. Then $\delta(f) = nay^{n-1} + \cdots \in A$. Have $a \neq 0$ by choice of f , but $\delta(f) = 0$ by minimality of n . Conclude $n = 0$ and $f = a \in A \cap k_0$. Now $\{0\} \neq A \cap k_0 \trianglelefteq k_0$. By the simplicity of k_0 , $A \cap k_0 = k_0$, so $1 \in A$ and $A = k_0[y]$. Conclude that $k_0[y]$ is δ -simple. \square

Exercises for §3

1.3.1. Show that if R is semisimple, so is $M_n(R)$.

Proof. Let $J \trianglelefteq M_n(R)$. Then $J = M_n(I)$ for some uniquely determined ideal $I \trianglelefteq R$. Say $R = I \oplus I'$ for another ideal $I' \trianglelefteq R$. Then $M_n(I') \trianglelefteq M_n(R)$, and $M_n(R) = M_n(I) \oplus M_n(I')$. Conclude $M_n(R)$ is semisimple. \square

1.3.3. Let R be a semisimple ring.

1. Show that any ideal $I \trianglelefteq R$ is a sum of simple components of R .
2. Show that any quotient ring of R is semisimple.
3. Show that a simple artinian ring S is isomorphic to a simple component of R if and only if there exists a surjective ring homomorphism from R onto S .

Proof.

1. Have $R = B_1 \oplus \cdots \oplus B_r$ for some simple ideals B_1, \dots, B_r . Moreover, there exist central idempotents $e_1, \dots, e_r \in R$ such that $e_1 + \cdots + e_r = 1$, $e_i e_j = 0$ for $i \neq j$, and $B_i = R e_i$. Let $I \triangleleft R$. Given $a = a_1 e_1 + \cdots + a_r e_r \in I$, have $a e_i = a_i e_i \in I$. So $I = \bigoplus_{i=1}^r B_i \cap I$. Now B_i simple implies $B_i \cap I = \{0\}$ or B_i . Conclude I is a direct sum of some subcollection of the simple components B_1, \dots, B_r of R .
2. Let $I \trianglelefteq R$ and consider R/I . By (1), $R/I \cong \bigoplus \{B_i : B_i \cap I = \{0\}\}$, a direct sum of simple (left) ideals. Then R/I is semisimple.
3. Suppose $S \cong B_j$. Let $I = \bigoplus_{i \neq j} B_i$. Then $R \twoheadrightarrow R/I \cong B_j \cong S$ is a surjective ring homomorphism. Conversely, suppose there exists a surjective ring homomorphism $f : R \twoheadrightarrow S$ for some simple artinian ring S . Then $S \cong R/I$ for some $I \trianglelefteq R$. Now $S \cong$ a direct sum of some subcollection of the B_1, \dots, B_r . But S simple implies that only one of the B_i appears in the direct sum.

\square

1.3.4. Show that the center of a simple ring is a field, and the center of a semisimple ring is a finite direct product of fields.

Proof. Let R be a simple ring, $0 \neq r \in Z(r)$. Then $\{0\} \neq (r) \trianglelefteq R \Rightarrow (r) = R \Rightarrow r \in R^*$. So $Z(R)$ is a commutative subring of R in which every nonzero element is invertible, i.e., $Z(R)$ is a field. Now if R is semisimple, $R \cong B_1 \times \cdots \times B_r$ for some simple subrings B_1, \dots, B_r . Then $Z(R) \cong Z(B_1) \times \cdots \times Z(B_r)$, a direct product of fields. \square

1.3.5. Let M be a finitely generated left R -module, $E = \text{End}({}_R M)$. Show that if R is semisimple (resp. simple artinian), then so is E .

Proof.

Suppose M is semisimple. Let $\{M_i : 1 \leq i \leq m\}$ be a complete list of pairwise nonisomorphic simple left R -submodules of M (the list is finite because M is finitely-generated as an R -module and is a direct sum of simple submodules). Let B_i denote the direct sum of all submodules of M isomorphic to M_i , so $M = \bigoplus_{i=1}^m B_i$.

Now $\text{Hom}(B_i, B_j) = \{0\}$ for $i \neq j$, for if $0 \neq f \in \text{Hom}(B_i, B_j)$ and $i \neq j$, then $f|_N \neq 0$ for some simple submodule $N \cong B_i$. By the simplicity of N we have $\ker f|_N = \{0\}$, so $M_i \cong N \cong f(N) \subseteq B_j$, i.e., B_j contains a simple submodule isomorphic to B_i , $i \neq j$, a contradiction to the definition of the B_i .

Conclude $E = \text{End}({}_R M) = \text{End}(\bigoplus_{i=1}^m B_i) \cong \prod_{i=1}^m \text{End}(B_i)$. Write $B_i \cong n_i M_i$ for some $n_i \in \mathbb{N}$. Then $\text{End}(B_i) \cong \text{End}(n_i M_i) \cong M_{n_i}(\text{End}_R(M_i))$. But $D_i = \text{End}_R(M_i)$ is a division ring by Schur's Lemma. Conclude $E \cong \prod_{i=1}^m M_{n_i}(D_i)$ is semisimple.

Suppose R is simple artinian. Then R is semisimple, so R has a unique (up to isomorphism) left simple module V . Any simple submodule of M must be isomorphic to V . Conclude that $m = 1$ and $M = B_1 \cong n_1 M_1 \cong n_1 V$. Then $E \cong M_{n_1}(D_1)$ is simple artinian. \square

1.3.7. Let R be a simple ring which is finite-dimensional over its center k (k is a field by Exercise 1.3.4). Let M be a finitely-generated left R -module and let $E = \text{End}({}_R M)$. Show $(\dim_k M)^2 = (\dim_k R)(\dim_k E)$.

Proof. Since R is finite-dimensional over its center k , it is simple artinian, hence semisimple. Let V denote the unique (up to isomorphism) simple left R -module, and let $D = \text{End}_R(V)$ (a finite-dimensional k -division algebra by Schur's Lemma). Then $R \cong M_n(D)$ for some $n \in \mathbb{N}$, and $V \cong D^n$. So $\dim_k R = n^2 \dim_k D$.

Let M be a finitely-generated left R -module. Then ${}_R M$ is semisimple, and since R has a unique (up to isomorphism) simple left R -module, $M \cong mV$ for some $m \in \mathbb{N}$. Then $\dim_k M = m \dim_k V = mn \dim_k D$.

Now $E = \text{End}({}_R M) \cong \text{End}(mV) \cong M_m(\text{End}(V)) = M_m(D)$. Then $\dim_k E = m^2 \dim_k D$. Conclude $(\dim_k M)^2 = m^2 n^2 (\dim_k D)^2 = (n^2 \dim_k D)(m^2 \dim_k D) = (\dim_k R)(\dim_k E)$. \square

1.3.11. Let R be an n^2 -dimensional algebra over a field k . Show $R \cong M_n(k)$ (as k -algebras) if and only if R is simple and has an element whose minimal polynomial over k has the form $(x - a_1) \cdots (x - a_n)$ for some $a_1, \dots, a_n \in k$.

Proof.

(\Rightarrow): Suppose $R \cong M_n(k)$ as k -algebras. Then R is simple because k , hence $M_n(k)$ is simple. Let $A \in M_n(k)$ be the matrix with 1s on the first superdiagonal and zeros elsewhere. Then the isomorphic image of A in R has minimal polynomial over k equal to $x^n = (x - 0)^n$.

(\Leftarrow): Suppose R is simple and $\exists r \in R$ such that r has minimal polynomial over k equal to $\prod_{i=1}^n (x - a_i)$, $a_i \in k$. Since R has the structure of a finite-dimensional k -vector space, R is simple artinian. Then $R \cong M_m(D)$ for some division k -algebra D and for some $m \in \mathbb{N}$.

Let $e_j = \prod_{i=1}^j (r - a_i)$. Then $Re_1 \neq R$ because e_1 is a left zero divisor, hence not invertible in R . By Exercise 1.2.6, $Re_j = Re_{j-1}$ if and only if $e_{j-1} = ue_j$ for some $u \in R^*$. But if this were the case, we'd have $0 = u \cdot 0 = u \prod_{i=1}^n (r - a_i) = \prod_{i \neq j} (r - a_i)$, a contradiction to the minimality of $\prod_{i=1}^n (r - a_i)$.

Then $\{0\} = Re_n \subset Re_{n-1} \subset \cdots \subset Re_1 \subset R$ is a strictly increasing chain of left ideals in R . This chain can be refined to a composition series for $R \Rightarrow R$ must have at least n simple left modules $\Rightarrow m \geq n$. But $n^2 = \dim_k R = m^2 \dim_k D$ and $m \geq n \Rightarrow m = n$ and $\dim_k D = 1$, i.e., $D = k$. Then $R \cong M_n(k)$. \square

1.3.12. For a subset S in a ring R , define $\text{Ann}_l(S) = \{a \in R : aS = 0\}$, and $\text{Ann}_r(S) = \{a \in R : Sa = 0\}$. Let R be a semisimple ring, I a left ideal in R , J a right ideal in R . Show $\text{Ann}_l(\text{Ann}_r(I)) = I$ and $\text{Ann}_r(\text{Ann}_l(J)) = J$.

Proof. Write $R = I \oplus I'$ for some complimentary left ideal I' of R . Now $I = Re$ for some idempotent $e \in I$. Let $f = 1 - e$. Certainly $fR \subseteq \text{Ann}_r(I)$. If $a \in \text{Ann}_r(I)$, then $a = a - ea = (1 - e)a = fa$, so $a \in fR$. Conclude $fR = \text{Ann}_r(I)$. Now $I = Re \subseteq \text{Ann}_l(\text{Ann}_r(I))$. If $a \in \text{Ann}_l(\text{Ann}_r(I))$, then $a = a - af = a(1 - f) = ae$, so $a \in Re = I$. Conclude $\text{Ann}_l(\text{Ann}_r(I)) = I$. The proof of $\text{Ann}_r(\text{Ann}_l(J)) = J$ is argued similarly. \square

1.3.19. True or false: If I is a minimal left ideal in a ring R , then $M_n(I)$ is a minimal left ideal in $M_n(R)$.

Proof. False. Let $I \subset R$ be a minimal left ideal. Then $M_n(I)$ is certainly a left ideal of $M_n(R)$. Let $A_i \subset M_n(I)$ denote the set of matrices with entries equal to zero outside of the i -th column. Then for $1 \leq i \leq n$, A_i is a nonzero left ideal in $M_n(R)$, and $M_n(I) = \bigoplus_{i=1}^n A_i$, so $M_n(I)$ is not a minimal left ideal in $M_n(R)$. \square

1.3.24. A subset S of a ring R is said to be *nil* (resp. *nilpotent*) if every $s \in S$ is nilpotent (resp. if $S^m = 0$ for some m , where S^m denotes the set of all products $s_1 \cdots s_m$ with $s_i \in S$).

1. Let $R = M_n(D)$ where D is a division ring. Let $S \subseteq R$ be a nonempty nil set which is closed under multiplication. Show that $S^n = 0$.
2. Let R be any semisimple ring. Show that any nonempty nil set $S \subseteq R$ closed under multiplication is nilpotent.

Chapter 2

Jacobson Radical Theory

2.4 The Jacobson Radical

Definition. The Jacobson radical of a ring R is defined as the intersection of all maximal left ideals of R , and is denoted by $\text{rad } R$ or $J(R)$.

$$\text{rad } R = J(R) = \bigcap \{M \subset R : M \text{ maximal left ideal of } R\}$$

Remark. The Jacobson radical is invariant under automorphisms of R : If M is maximal left ideal of R and $f \in \text{Aut}(R)$, then $f(M)$ is a maximal left ideal of R .

Example. Have $\text{rad } \mathbb{Z} = \{0\}$. If D is a division ring, then $\text{rad } D = \{0\}$.

Lemma. For $y \in R$, the following are equivalent.

1. $y \in \text{rad } R$
2. $1 - xy$ is left invertible $\forall x \in R$
3. $yM = 0$ for any simple left R -module M ($y \in \text{Ann}(M)$)
4. $1 - xyz \in R^* \forall x, z \in R$

Proof.

(1) \Rightarrow (2): Let $y \in \text{rad } R$, $x \in R$. Then $xy \in \text{rad } R$, since if y is an element of every maximal left ideal of R , then so is xy . Now if xy is an element of every maximal left ideal of R , then $1 - xy$ is not an element of any maximal left ideal of R (else the left ideal would contain the identity), which implies that $1 - xy$ is not an element of any proper left ideal of R (because every proper left ideal is contained in some maximal left ideal). Then $R(1 - xy) = R$ and $1 - xy$ must be left invertible.

(2) \Rightarrow (3): Suppose $1 - xy$ is left invertible for all $x \in R$ but that $yM \neq \{0\}$ for some simple left R -module M . Then $\exists m \in M$ such that $ym \neq 0$. By the simplicity of M , $M = Rm$. Then $\exists x \in R$ such that $x(ym) = m$, i.e., $(1 - xy)m = 0$. By the left invertibility of $1 - xy$, this implies $m = 0$, a contradiction to the initial choice of m . Conclude $yM = \{0\}$ for all simple left R -modules M .

(3) \Rightarrow (1): Suppose $yM = \{0\}$ for all simple left R -modules M . Given a maximal left ideal $I \subset R$, R/I is a simple left R -module. Then $y(R/I) = 0 \Rightarrow y \in I$. Then $y \in \text{rad } R$.

(4) \Rightarrow (2): Put $z = 1$.

(2) \Rightarrow (4): If $1 - (zx)y$ is left invertible, then $\exists v \in R$ such that $v(1 - zxy) = 1$. Then $v = 1 + (vzx)y$ is left invertible by (2) $\Rightarrow v \in R^*$ since it is both left and right invertible. As the right inverse of v , $1 - zxy$ must then also be the left inverse of v , so $1 - zxy \in R^*$. Then by Exercise 1.1.6, $1 - (xy)z \in R^*$. \square

Corollary. Let R be a ring. Then:

1. $\text{rad } R = \bigcap \{\text{Ann}(M) : {}_R M \text{ simple left } R\text{-module}\}$. In particular, $\text{rad } R$ is an ideal.
2. $\text{rad } R$ is the largest left/right/two-sided ideal A of R such that $1 + A \subseteq R^*$. Moreover, the left and right radicals of R coincide.

Proof.

1. This is condition (3) of the above lemma.
2. Let A be a left ideal of R such that $1 + A \subseteq R^*$, and let $y \in A$. Then $-xy \in A$ for all $x \in R$ and $1 - xy \in R^*$. Then $y \in \text{rad } R$ by condition (2) of the above lemma. Conclude $A \subseteq \text{rad } R$, and $\text{rad } R$ is the largest left (hence two-sided, as well) ideal A satisfying $1 + A \subseteq R^*$. That the left and right radicals of R coincide follows from this symmetric characterization of $\text{rad } R$. \square

Example. Let R be a semisimple ring. By the Wedderburn–Artin Theorem, we have $R \cong \prod_{i=1}^r M_{n_i}(D_i)$ with simple modules $\{V_i\}$, ${}_R R = \bigoplus_{i=1}^r n_i V_i$. Have $\text{Ann}(V_i) = \prod_{j \neq i} M_{n_j}(D_j)$. Conclude $\text{rad } R = \{0\}$.

Proposition. For any ideal I of R such that $I \subseteq \text{rad } R$, $\text{rad}(R/I) = (\text{rad } R)/I$. In particular, $\text{rad}(R/\text{rad } R) = \{0\}$.

Proposition. Simple R -modules are in bijective correspondence with simple $R/\text{rad } R$ -modules.

Proof. This follows by property (3) of the above lemma. \square

Definition. A ring R is called Jacobson semisimple if $\text{rad } R = 0$.

Example. \mathbb{Z} is Jacobson semisimple but not semisimple. All semisimple rings are necessarily Jacobson semisimple by the previous example. A simple ring is Jacobson semisimple.

Example. Let $p \in \mathbb{Z}$ be prime. The localization of \mathbb{Z} at (p) is $\mathbb{Z}_{(p)} = \{\frac{m}{n} \in \mathbb{Q} : (n, p) = 1\}$. Given $\frac{m}{n}, \frac{m'}{n'} \in \mathbb{Z}_{(p)}$, $1 - (\frac{m}{n})p(\frac{m'}{n'})$ is invertible in $\mathbb{Z}_{(p)}$ with inverse $\frac{nn'}{nn' - pmm'}$ (since $p \nmid n$ and $p \nmid n'$, $p \nmid nn' - pmm'$), so $p\mathbb{Z}_{(p)} \subseteq \text{rad } \mathbb{Z}_{(p)}$.

Conversely, let $\frac{m}{n} \in \mathbb{Z}_{(p)}$ and suppose $p \nmid m$. Then $\exists a, b \in \mathbb{Z}$ such that $am + bp = 1$. Then $1 - (an)(\frac{m}{n}) = bp$ has no inverse in $\mathbb{Z}_{(p)}$. Then $\frac{m}{n} \notin \text{rad } \mathbb{Z}_{(p)}$. Conclude $\text{rad } \mathbb{Z}_{(p)} = p\mathbb{Z}_{(p)}$.

Definition. A subset S of a ring R is nil (resp. nilpotent) if every $s \in S$ is nilpotent (resp. $S^m = 0$ for some $m \in \mathbb{N}$).

Proposition. Any nilpotent left ideal A of any ring R is contained in $\text{rad } R$.

Proof. Given a simple left R -module ${}_R M$, AM is an R -submodule of M . If $AM \neq \{0\}$, $AM = M$. In this case, $A^k M = M \forall k \geq 1$. But $A^k = 0$ for $k \gg 0$, implying that $M = \{0\}$, a contradiction to the choice of M . Conclude $AM = \{0\}$, so $A \subseteq \bigcap \{\text{Ann}(M) : {}_R M \text{ simple}\} = \text{rad } R$. \square

Proposition. Any nil left ideal A of R is contained in $\text{rad } R$.

Proof. Let A be a nil left ideal of R , and let $y \in A$. Then $xy \in A$ for all $x \in R$ and xy is nilpotent. Now $1 - xy \in R^*$ with inverse $\sum_{i=0}^{\infty} (xy)^i$ (well-defined by nilpotency of xy). Then $y \in \text{rad } R$. Conclude $A \subseteq \text{rad } R$. \square

Theorem. Let R be a left artinian ring. Then $\text{rad } R$ is the largest nilpotent left (right or two-sided) ideal N of R .

Proof. By the above proposition, any nilpotent left ideal of R is contained in $\text{rad } R$, so it suffices to show that $\text{rad } R$ is nilpotent. Let $J = \text{rad } R$. Then $J \supseteq J^2 \supseteq J^3 \supseteq \dots$. Since R is artinian, the chain stabilizes, say at $I = J^k$. Suppose $I \neq \{0\}$. Let $\mathcal{F} = \{\text{left ideals } A \subseteq R : IA \neq \{0\}\}$. Then $\mathcal{F} \neq \emptyset$ (in particular, $J \in \mathcal{F}$), so there exists a minimal element $A_0 \in \mathcal{F}$. Now $\exists a \in A_0$ such that $Ia \neq 0$. Since $I^2 = I$, we have $I^2 a = Ia \neq \{0\}$. Then $Ia \in \mathcal{F}$, $Ia \subseteq A_0 \Rightarrow Ia = A_0$ by minimality of A_0 . Now $\exists i \in I$ such that $ia = a$. Then $(1 - i)a = 0$. But $i \in J \Rightarrow 1 - i \in R^* \rightarrow a = 0$, a contradiction to the choice of a . Conclude $I = 0$, i.e., $J = \text{rad } R$ is nilpotent. \square

Corollary. Let A be a left (right or two-sided) ideal of a left artinian ring. Then A is nil if and only if A is nilpotent.

Proof. Any nilpotent ideal is automatically a nil. Conversely, if A is a left nil ideal of the left artinian ring R , then A is contained in $\text{rad } R$ by the above proposition. But $\text{rad } R$ is nilpotent by the above theorem, so $A \subseteq \text{rad } R$ is nilpotent as well. \square

Example. Recall that in a commutative ring R , the nilradical $\text{Nil } R$ consists of all nilpotent elements in R and is the largest nil ideal in R . Let $R = \mathbb{Z}/p^n \mathbb{Z}$, $n \geq 1$. Then $\text{Nil } \mathbb{Z}/p^n \mathbb{Z} = p(\mathbb{Z}/p^n \mathbb{Z})$.

Theorem. For any ring R , the following are equivalent:

1. R is semisimple.
2. R is Jacobson semisimple and left artinian.
3. R is Jacobson semisimple and has the DCC on principal left ideals.

Proof.

1. (1) \Rightarrow (2): As previously noted, a semisimple ring is Jacobson semisimple. By Exercise 1.3.3, any ideal $I \trianglelefteq R$ is a sum of simple components of R , of which there are only finitely many, say r . Then any descending chain of ideals of R must stabilize after at most r steps. Conclude R is artinian.

2. (2) \Rightarrow (3): Trivial.

3. (3) \Rightarrow (1): Since R has the DCC on principal left ideals, every left ideal of R contains a minimal left ideal. Let $B \neq \{0\} = \text{rad } R$ be a minimal left ideal of R . Then there exists a maximal left ideal M of R such that $B \not\subseteq M$ (else $B \subseteq \text{rad } R$, the intersection of all maximal left ideals). Now ${}_R R = B \oplus M$ because $B + M = R$ and $B \cap M = \{0\}$ by the minimality of B and the fact that $B \not\subseteq M$. In particular, B is a direct summand of R .

Fix a minimal left ideal B_1 of R . Then $R = B_1 \oplus A_1$ for some left ideal A_1 of R , and by Exercise 1.1.7, $A_1 = Re_1$ for some idempotent $e_1 \in A_1$. Choose a minimal left ideal B_2 of R in A_1 . Then $A_1 = B_2 \oplus A_2$ for some left ideal A_2 of A_1 , and $A_2 = Re_2$ for some idempotent $e_2 \in A_2$. Repeat this process to obtain a descending chain of principal left ideals $A_1 \supseteq A_2 \supseteq \cdots$. This chain must stabilize, since by assumption R has the DCC on principal left ideals. Say the chain stabilizes at A_k . Then $R = B_1 \oplus \cdots \oplus B_k$ is a direct sum of minimal left ideals. Conclude R is semisimple. \square

Example. Let k be a field, and let R be a finitely generated commutative k -algebra. Then $R \cong k[x_1, \dots, x_n]/I$ for some ideal $I \trianglelefteq k[x_1, \dots, x_n]$. Define the radical of I by

$$\sqrt{I} = \{f \in k[x_1, \dots, x_n] : f^r \in I \text{ for some } r \in \mathbb{N}\}$$

By Hilbert's Nullstellensatz, $\sqrt{I} = \bigcap \{M : M \triangleleft k[x_1, \dots, x_n] \text{ maximal}, I \subseteq M\}$. It follows that $\text{rad } R = \text{Nil } R$, $\text{Nil } R \cong \sqrt{I}/I$, and R is Jacobson semisimple if and only if R is reduced (i.e., it has no nonzero nilpotent elements).

Example. Let k be a division ring, $R \subset M_n(k)$ the set of upper triangular matrices. Then the set $J \subset R$ of strictly upper triangular matrices is an ideal of R . Have $J^{n+1} = 0$ so $J \subseteq \text{rad } R$. And $R/J \cong D_n(k)$ the set of diagonal matrices. But $D_n(k) \cong \bigoplus_1^n k$ is semisimple. Then $\text{rad}(R/J) = 0 \Rightarrow (\text{rad } R)/J = 0 \Rightarrow J = \text{rad } R$. Now by the fact that the simple R modules are the simple $R/\text{rad } R$ modules, conclude that R has n nonisomorphic simple modules $M_i \cong k$. The upper triangular matrix (a_{kl}) acts on M_i as scalar multiplication by $e_{ii}^*(a_{kl}) = a_{ii}$.

Definition. A ring R is semiprimary if $\text{rad } R$ is nilpotent and $\overline{R} = R/\text{rad } R$ is semisimple.

Any left artinian ring R is semiprimary since the Jacobson radical of a left artinian ring is always nilpotent, and because $\overline{R} = R/\text{rad } R$ inherits the descending chain condition on ideals.

Theorem (Hopkin–Levitzki). Let R be a semiprimary ring and M a left R -module. Then the following are equivalent:

1. M is artinian.
2. M is noetherian.
3. M has a composition series.

In particular, (A) a ring is left artinian if and only if it is left noetherian and semiprimary, and (B) any finitely generated left module over a left artinian ring has a composition series.

Proof.

(3) \Rightarrow (1),(2): This implication was already established in §1.1.

(1),(2) \Rightarrow (3): Assume that M is artinian (resp. noetherian). Write $J = \text{rad } R$, $\bar{R} = R/J$. R is semiprimary by assumption, so \bar{R} is semisimple and $J^n = \{0\}$ for some n . Then $M \supset JM \supset J^2M \supset \cdots \supset J^nM = \{0\}$ is a descending chain of submodules, and $J^iM/J^{i+1}M$ is artinian (resp. noetherian) as an \bar{R} -module. By the semisimplicity of \bar{R} , $J^iM/J^{i+1}M$ is a direct sum of simple modules over \bar{R} (equivalently, over R since $J = \text{rad } R$ acts trivially). Moreover, because M is artinian (resp. noetherian), this must be a finite direct sum. It therefore follows that ${}_R M$ has a composition series.

(A) now follows from the established equivalencies and the above observation that all artinian rings are semiprimary. A finitely generated left module over a left artinian ring is in particular noetherian, hence has a composition series by the established equivalencies. \square

Example. Let k be a division ring, σ a non-invertible endomorphism of k . We established above that the skew polynomial ring $R = k[x; \sigma]$ is left noetherian but not artinian ($Rx \supset Rx^2 \supset Rx^3 \supset \cdots$ is an infinite descending chain). Then R is not semiprimary.

Example. Let R be a commutative \mathbb{Q} -algebra. Let $R = \mathbb{Q}[x_1, \dots]/(x_i x_j, \forall i, j)$. R is semiprimary but not noetherian. Observe that $\text{rad } R = (x_1, x_2, \dots)$ is nilpotent and $R/\text{rad } R = \mathbb{Q}$ is semisimple, but $(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \cdots$ is an infinite increasing chain of ideals.

Proposition. Let $e \in R$ be an idempotent, $J = \text{rad } R$. Then $\text{rad}(eRe) = J \cap eRe = eJe$. (Note that eRe is a ring with identity e .)

Proof.

Let $r \in \text{rad}(eRe)$, $y \in R$. Then $e - (eye)r \in (eRe)^*$ and $\exists b \in eRe$ such that $e = b(e - eyer) = be(1 - yer) = b(1 - yr)$ since $b, r \in eRe \Rightarrow be = b$ and $er = r$. Then $(1 + yrb)(1 - yr) = (1 - yr) + yrb(1 - yr) = (1 - yr) + yre = 1 - yr + yr = 1$. Conclude $r \in J$, so $\text{rad}(eRe) \subseteq J \cap eRe$.

Let $r \in J \cap eRe$. Then $r = ere \in eJe$, so $J \cap eRe \subseteq eJe$.

Let $r \in eJe$, $y \in eRe$. Then $r \in eJe \subseteq J$, so $\exists x \in R$ such that $x(1 - yr) = 1$. Then $exe(e - yr) = ex(e - yr) = ex(1 - yr)e = e1e = e$. So $r \in \text{rad}(eRe)$, so $eJe \subseteq \text{rad}(eRe)$. Conclude $\text{rad}(eRe) = J \cap eRe = eJe$. \square

Corollary. Let R be a ring. Then $\text{rad } M_n(R) = M_n(\text{rad } R)$.

Proof. Any ideal of $M_n(R)$ has the form $M_n(A)$ for some ideal $A \trianglelefteq R$. Suppose $\text{rad } M_n(R) = M_n(A)$ for $A \trianglelefteq R$. Let $e = E_{11} \in M_n(R)$. Then $eM_n(R)e = RE_{11} \cong R$. Now by the proposition, $A = eM_n(A)e = e(\text{rad } M_n(R))e = \text{rad}(eM_n(R)e) = \text{rad } R$. \square

Proposition. Let R be a ring, and suppose $S := \mathcal{U}(R) \cup \{0\}$ is a division ring. Then R is J -semisimple.

Proof. Have $S \cap \text{rad } R = \{0\}$ because $\text{rad } R$ contains no units of R . Let $y \in \text{rad } R$. Then $1 + y \in \mathcal{U}(R) \subset S$. Then $y = (1 + y) - 1 \in S \cap \text{rad } R = \{0\}$. So $\text{rad } R = \{0\}$ and R is J -semisimple. \square

Example. Let k be a division ring. The following rings are J -semisimple by the above proposition.

1. $R = k\langle x_i, i \in I \rangle, \mathcal{U}(R) = k.$
2. $R = k[x_i, i \in I], \mathcal{U}(R) = k.$
3. $R = k[x; \sigma]$ (σ an endomorphism or derivation of k), $\mathcal{U}(R) = k.$

Proposition. Let k be a field, and let R be a k -algebra. Let $x \in \text{rad } R$. Then x is algebraic over k if and only if x is nilpotent.

Proof. Nilpotent elements are automatically algebraic. Let $x \in \text{rad } R$ and suppose $x^n + a_1x^{n+1} + \dots + a_mx^{n+m} = 0$ for some $a_i \in k$. Then $0 = x^n(1 + a_1x + \dots + a_mx^m)$. But $a_1x + \dots + a_mx^m \in \text{rad } R$, so $(1 + a_1x + \dots + a_mx^m) \in R^*$. Conclude $x^n = 0$, i.e., x is nilpotent. \square

Corollary. Let R be an algebraic k -algebra. Then $\text{rad } R$ is the largest nil ideal of R .

Proof. By the above proposition, $\text{rad } R$ is nil, and any nil ideal is contained in $\text{rad } R$. \square

Lemma (Nakayama's Lemma). Let R be a ring, and let $J \subseteq R$ be a left ideal. Then the following are equivalent:

1. $J \subseteq \text{rad } R.$
2. For all finitely generated left R -modules M , $JM = M \Rightarrow M = \{0\}.$
3. For all left R -modules M , if ${}_R N \subseteq {}_R M$ is such that M/N is finitely generated, then $N + JM = M \Rightarrow M = N.$

Proof.

(1) \Rightarrow (2): Suppose $J \subseteq \text{rad } R$, $JM = M$, but $M \neq \{0\}$. Take a minimal set of generators $\{m_1, \dots, m_k\}$ for M . Since $JM = M$, we can find $r_1, \dots, r_k \in J$. Such that $m_1 = r_1m_1 + \dots + r_k m_k$. Then $(1 - r_1)m_1 = r_2m_2 + \dots + r_k m_k$. But $1 - r_1 \in R^*$, so $m_1 \in Rm_2 + \dots + Rm_k$, a contradiction to the minimality of this collection of generators. Conclude $M = \{0\}$.

(2) \Rightarrow (3): Suppose $JM = M \Rightarrow M = \{0\}$ for all finitely generated left R -modules M . Suppose ${}_R N \subseteq {}_R M$ is a submodule such that M/N is finitely generated and $N + JM = M$. Then $J(M/N) = M/N$, which implies by (2) that $M/N = \{0\}$, i.e., that $M = N$.

(3) \Rightarrow (2): Set $N = \{0\}$.

(2) \Rightarrow (1): Suppose $JM = M \Rightarrow M = \{0\}$ for all finitely generated left R -modules M . Let M be a simple R -module. In particular, M is cyclic, generated by any $0 \neq m \in M$. Now JM is an R -submodule of M , so by simplicity either $JM = M$ or $JM = \{0\}$. If $JM = M$, then $M = 0$ by (2), a contradiction to the choice of M . Conclude $JM = \{0\}$, and $J \subseteq \text{rad } R$. \square

Remark. Let R_1, \dots, R_k be rings. Then $\text{rad}(R_1 \times \dots \times R_k) = \text{rad } R_1 \times \dots \times \text{rad } R_k.$

Exercises for §4

2.4.9. Let R be a J -semisimple domain and let a be a nonzero central element of R . Show that the intersection of all maximal left ideals not containing a is zero.

Proof. Let N (resp. N') denote the intersection of all maximal left ideals of R not containing a (resp. containing a). If $a \in R^*$, then $N = \text{rad } R = \{0\}$. Suppose $a \notin R^*$. Then there exists a maximal left ideal M of R with $a \in M$. Suppose $N \neq \{0\}$. Then $\exists 0 \neq b \in N$. Now $ba = ab \in N \cap M$. Note that $\text{rad } R = N \cap N'$. Now $ba \in N'$, so $ab = ba \in \text{rad } R$, a contradiction because $\text{rad } R = \{0\}$ and $ab \neq 0$ (R is a domain). Conclude $N = \{0\}$. \square

2.4.10. Show that if $f : R \rightarrow S$ is a surjective ring homomorphism, then $f(\text{rad } R) \subseteq \text{rad } S$. Give an example to show $f(\text{rad } R)$ may be smaller than $\text{rad } S$.

Proof. Let $r \in \text{rad } R$, $y = f(r)$. Let $x \in S$, and say $x = f(t)$ for $t \in R$. Then $1_S - xy = f(1_R - tr)$. Since $r \in \text{rad } R$, $1_R - tr$ is left invertible in R . Then $\exists v \in R$ such that $v(1_R - tr) = 1_R$. Say $w = f(v)$. Then $w(1_S - xy) = f(v(1_R - tr)) = f(1_R) = 1_S$, i.e., $1_S - xy$ is left invertible in S . Since $x \in S$ was arbitrary, conclude $f(r) = y \in \text{rad } S$, hence $f(\text{rad } R) \subseteq \text{rad } S$.

Let p be a prime, $n > 1$, and $f : \mathbb{Z} \rightarrow \mathbb{Z}/p^n\mathbb{Z}$ the usual reduction mod p^n homomorphism. Now $\text{rad } \mathbb{Z} = \{0\}$, but $\text{rad } \mathbb{Z}/p^n\mathbb{Z}$ equals the largest nilpotent ideal N in $\mathbb{Z}/p^n\mathbb{Z}$. This obviously contains $p(\mathbb{Z}/p^n\mathbb{Z}) \neq \{0\}$. \square

2.4.11. If an ideal $I \trianglelefteq R$ is such that R/I is J -semisimple, show that $\text{rad } R \subseteq I$. (Therefore, $\text{rad } R$ is the smallest ideal $I \trianglelefteq R$ such that R/I is J -semisimple.)

Proof. If $\text{rad}(R/I) = \{0\}$, then

$$\begin{aligned} \{0\} &= \bigcap \{ \overline{M} \subset R/I : \overline{M} \text{ maximal left ideal} \} \\ &\Leftrightarrow \bigcap \{ M \subset R : M \text{ maximal left ideal, } I \subseteq M \} \subseteq I \end{aligned}$$

Now $\text{rad } R \subseteq \bigcap \{ M \subset R : M \text{ maximal left ideal, } I \subseteq M \} \subseteq I$. \square

2.4.12. Show that, for any direct product of rings, $\prod R_i$, that $\text{rad}(\prod R_i) = \prod \text{rad } R_i$.

2.4.16. A left R -module is said to be *cohopfian* if any injective R -endomorphism of M is an automorphism.

1. Show that any artinian module M is cohopfian.
2. Show that the left regular module ${}_R R$ is cohopfian if and only if every non right zero-divisor in R is a unit. In this case, show that ${}_R R$ is also hopfian.

Proof.

1. Let ${}_R M$ be an artinian module, and let $f : M \rightarrow M$ be an injective R -endomorphism. Then $M \supseteq \text{im } f \supseteq \text{im } f^2 \supseteq \cdots$ is a descending chain of submodules. Say the chain stabilizes at $\text{im } f^k$. Suppose $k > 1$. Let $m \in \text{im } f^{k-1} \setminus \text{im } f^k \neq \emptyset$. Then $f(m) \in \text{im } f^k = \text{im } f^{k+1}$, so $\exists m' \in \text{im } f^k$ such that $f(m) = f(m')$. Now $0 = f(m) - f(m') = f(m - m')$ but $m - m' \neq 0$ because $m \notin \text{im } f^k$, a contradiction to the injectivity of f . Conclude $f(M) = M$ and f is an automorphism.

2. Suppose ${}_R R$ is cohopfian. Let $a \in R$ be a non-right zero-divisor in R . Define $f : R \rightarrow R$ by $f(b) = ba$. Then f is an injective R -endomorphism of ${}_R R \Rightarrow f$ is an automorphism. Then $\exists c \in R$ such that $f(c) = 1$, i.e., $ca = 1$. Now $0 = a - a = a(ca) - a = (ac - 1)a \Rightarrow ac = 1$. Conclude $a \in R^*$.

Suppose every non-right zero-divisor of R is a unit, and let $f : R \rightarrow R$ be an injective R -endomorphism of ${}_R R$. Then $f = R_{f(1)}$ and f is injective $\Rightarrow f(1)$ is a non-right zero-divisor $\Rightarrow f(1) \in R^*$. Then f is an automorphism with inverse $R_{f(1)^{-1}} : R \rightarrow R$.

Suppose the above equivalent conditions hold. By Exercise 1.1.12, R is hopfian $\Leftrightarrow R$ is Dedekind-finite. Let $a, b \in R$, and suppose $ab = 1$. Then $ca \neq 0$ for all $0 \neq c \in R$. Then $a \in R^*$, so $\exists d \in R$ such that $da = 1$. Now $d = d(ab) = (da)b = b$, so $ba = 1$. Then R is Dedekind-finite, hence hopfian. \square

2.4.18. The *socle* $\text{soc}(M)$ of a left module M over a ring R is defined to be the sum of all simple submodules of M . Show that $\text{soc}(M) \subseteq \{m \in M : (\text{rad } R)m = 0\}$, with equality if $R/\text{rad } R$ is an artinian ring.

Proof. The inclusion $\text{soc}(M) \subseteq \{m \in M : (\text{rad } R)m = 0\}$ is clear from one of the equivalent characterizations of $\text{rad } R$. Suppose $\bar{R} = R/\text{rad } R$ is artinian. Then \bar{R} is semisimple. Let $N = \{m \in M : (\text{rad } R)m = 0\}$. Note that N is an R -submodule of M because $\text{rad } R$ is an ideal in R . Then N is a \bar{R} -module as well. Now $N = \bigoplus_i N_i$ for some collection of simple left \bar{R} -modules N_i . Each N_i is then also a simple left R -module. Then $N \subseteq \text{soc}(M)$. Conclude in this case that $\text{soc}(M) = N$. \square

2.4.21. For any ring R , let $GL_n(R)$ denote the group of units in $M_n(R)$. Show that for any ideal $I \subseteq \text{rad } R$, the natural map $GL_n(R) \rightarrow GL_n(R/I)$ is surjective.

Proof.

Note that $\text{rad } M_n(R) = M_n(\text{rad } R)$, so if $I \subseteq \text{rad } R$ is an ideal, then $M_n(I)$ is an ideal contained in $\text{rad } M_n(R)$. Also note that $M_n(R/I) \cong M_n(R)/M_n(I)$. It thus suffices to prove the case $n = 1$ by considering the new ring $R' = M_n(R)$ and the new ideal $I' = M_n(I) \subseteq \text{rad } R'$.

Let $x + I \in (R/I)^*$. Then $\exists y + I \in (R/I)^*$ such that $xy + I = yx + I = 1 + I$. Say $xy = 1 + i$, $i \in I \subseteq \text{rad } R$. Then $xy \in R^*$, because $1 + \text{rad } R \subseteq R^*$. In particular, $x \in R$ is right invertible, $xyz_1 = 1$ for some $z_1 \in R$. By a similar consideration of $yx = 1 + j$ for some $j \in I \subseteq \text{rad } R$, we get that x is left invertible in R , and $z_2yx = 1$ for some $z_2 \in R$. Now x is both left and right invertible $\Rightarrow x \in R^*$. Conclude $x + I \in (R/I)^*$ is the image under the natural projection map of $x \in R^*$. \square

2.4.22. Using the definition of $\text{rad } R$ as the intersection of all maximal left ideals in R , show $\text{rad } R$ is an ideal in R .

Proof. Let $y \in \text{rad } R$, $r \in R$, and let M be a maximal left ideal of R . If $yr \notin M$, then $R = M + Ryr$ by the maximality of M , in which case $\exists m \in M, s \in R$ such that $1 = m + syr$. Then $m = 1 - syr \in R^*$ because $y \in \text{rad } R$, a contradiction to the choice of m . Conclude $yr \in M$. Since M was arbitrary, conclude $yr \in \text{rad } R$, and $\text{rad } R$ is closed under right multiplication by elements of R . Thus $\text{rad } R$ is an ideal. \square

2.5 Jacobson Radical Under Change of Rings

Lemma. Let R be a commutative ring. Then $\text{Nil } R = \bigcap \{P : P \trianglelefteq R \text{ is prime}\}$.

Proof.

\subseteq : If $x \in \text{Nil } R$, then $x^n = 0$ for some n . Then if $P \trianglelefteq R$ is a prime ideal, $x^n \in P \Rightarrow x \in P$.

\supseteq : Suppose $x \notin \text{Nil } R$. Let $S = \{1, x, x^2, \dots\}$ (so $0 \notin S$, and S is multiplicatively closed). Let $\mathcal{F} = \{I \trianglelefteq R : I \cap S = \emptyset\}$. Then $\mathcal{F} \neq \emptyset$ ($(0) \in \mathcal{F}$), so by Zorn's Lemma there exists a maximal element $P \in \mathcal{F}$. Suppose P is not prime. Then there exist $a \notin P, b \notin P$ such that $ab \in P$. By the maximality of P , there exist $s, t \in S$ such that $s \in P + (a)$ and $t \in P + (b)$. Then $st \in (P + (a))(P + (b)) \subseteq P$, i.e., $st \in S \cap P = \emptyset$, a contradiction. Conclude P is prime. Then $x \notin \bigcap \{P : P \trianglelefteq R \text{ is prime}\}$. \square

Theorem. Let R be a commutative ring, $T = \{t_i, i \in I\}$ a set of commuting independent variables. Then $\text{rad } R[T] = \text{Nil } R[T] = (\text{Nil } R)[T]$.

Proof.

Given a commutative ring S with ideal $I \subseteq \text{Nil } S$, we have $I = \text{Nil } S$ if and only if S/I is reduced, i.e., it has no nonzero nilpotent elements. Now $R[T]/(\text{Nil } R)[T] \cong (R/\text{Nil } R)[T]$. Since $(R/\text{Nil } R)[T]$ is reduced, we conclude $\text{Nil } R[T] = (\text{Nil } R)[T]$.

Have $\text{Nil } R[T] \subseteq \text{rad } R[T]$ by the above lemma because every maximal ideal of $R[T]$ is in particular a prime ideal. For the other containment, it suffices to consider the case $T = \{t\}$. Let $f(t) = r_0 + r_1t + \dots + r_nt^n \in \text{rad } R[t]$. Then $1 + tf(t) \in \mathcal{U}(R[t])$, hence $1 + tf(t) \in \mathcal{U}((R/P)[t])$ for all prime ideals $P \triangleleft R$. Recall $P \triangleleft R$ is prime if and only if R/P is a domain, and in this case $\mathcal{U}(R/P) = \mathcal{U}((R/P)[t])$. Now $1 + tf(t) = 1 + r_0t + \dots + r_nt^{n+1} \in \mathcal{U}((R/P)[t]) \Rightarrow r_i \in P, \forall 1 \leq i \leq n$. Since this holds for all prime ideal $P \triangleleft R$, we must have $r_i \in \text{Nil } R, \forall 1 \leq i \leq n$ by the above lemma. Conclude $f(t) \in (\text{Nil } R)[T] = \text{Nil } R[T]$. \square

Lemma. Let $R \subseteq S$ be rings. Assume that either

1. ${}_R R$ is a direct summand of ${}_R S$ as a left R -module, or
2. There is a group G of automorphisms of the ring S such that R is the subring of fixed points, $R = S^G = \{s \in S : g(s) = s \forall g \in G\}$.

Then $R \cap \text{rad } S \subseteq \text{rad } R$.

Proof. Let $a \in R \cap \text{rad } S$. Then for all $x \in R \subseteq S$, $1 - xa \in \mathcal{U}(S)$.

Suppose ${}_R R$ is a direct summand of ${}_R S$ as a left R -module. Write ${}_R S = {}_R R \oplus {}_R T$ for some complimentary left R -module T . Then $\exists s = r + t$ such that $1 = (1 - xa)s = (1 - xa)r + (1 - xa)t$. Note that $(1 - xa)r \in R$ and $(1 - xa)t \in T$, and $1 \in R$. Conclude $1 = (1 - xa)r$. Then $r = (1 - xa)^{-1} \in R$ and $a \in \text{rad } R$.

Suppose there exists a group of automorphisms G of S such that R is the subring of fixed points. Let $s \in S$ be the unique inverse of $1 - xa \in R \cap \mathcal{U}(S)$. Now $1 \in S^G$ and $1 - xa \in S^G$, so from the equation $(1 - xa)s = 1$ and by the uniqueness of $(1 - xa)^{-1}$, we conclude $s \in S^G = R$, so $a \in \text{rad } R$. \square

Theorem. For any k -algebra R and any field extension $K|k$, we have $R \cap \text{rad } R^K \subseteq \text{rad } R$. If $\dim_k R < \infty$ or if $K|k$ is algebraic, then $R \cap \text{rad } R^K = \text{rad } R$. (In particular, in this case $(\text{rad } R)^K \subseteq \text{rad } R^K$.) If $[K : k] = n$, then $(\text{rad } R^K)^n \subseteq (\text{rad } R)^K$.

Proof. Let $\{e_i : i \in I\}$ be a k -basis for K with $e_{i_0} = 1$. Then $R^K = R \oplus (\oplus_{i \neq i_0} R e_i)$, i.e., R is a direct summand of R^K as a left R -module. Then $R \cap \text{rad } R^K \subseteq \text{rad } R$ by the previous lemma.

Suppose $\dim_k R < \infty$ (so $\dim_K R^K < \infty$ as well). Now R is artinian $\Rightarrow \text{rad } R$ is nilpotent $\Rightarrow (\text{rad } R)^K$ is nilpotent. Then $(\text{rad } R)^K \subseteq \text{rad } R^K$, and we have $\text{rad } R \subseteq (\text{rad } R)^K \subseteq \text{rad } R^K$, i.e., $\text{rad } R \subseteq R \cap \text{rad } R^K$. Conclude in this case that $\text{rad } R = R \cap \text{rad } R^K$.

Suppose $[K : k] = n < \infty$. Then the above direct sum decomposition of R^K is finite, and each $1 \otimes e_i$ centralizes R . Let M be a simple left R^K -module. Then ${}_R M$ is a finitely generated left R -module, $M = R^K \cdot a = \sum_{i=1}^n R(1 \otimes e_i) \cdot a$ for some $a \in M$. Let $J = \text{rad } R$. Then JM is a simple left R^K -module, since for each $1 \otimes e_i$, $(1 \otimes e_i)JM = J(1 \otimes e_i)M \subseteq JM$. Since $M \neq \{0\}$, we have by Nakayama's Lemma $JM \subsetneq M$. But M is a simple R^K -module by assumption, so we must have $JM = \{0\}$. Conclude $\text{rad } R \subseteq R \cap \text{rad } R^K$.

Now apply a direct limit argument to prove the case where $K|k$ is an arbitrary algebraic extension.

Suppose $[K : k] = n$, and let $z \in (\text{rad } R^K)^n$. Write $z = \sum_{i=1}^n r_i \otimes e_i$. Let ${}_R V$ be a simple R -module. Then $V^K = \oplus_{i=1}^n V \otimes e_i$, and V^K as an R -module has a composition series of length $n = [K : k]$. Then as an R^K -module, any composition series of V^K has length $\leq n$. Now $zV^K = 0$, for any element of $\text{rad } R^K$ reduced the composition length by one, hence an element of $(\text{rad } R^K)^n$ must reduce the length to zero. Then for all $v \in V$, we have $0 = z(v \otimes 1) = \sum_{i=1}^n r_i v \otimes e_i$. Conclude $r_i V = \{0\}$, and $z \in (\text{rad } R)^K$. Then $(\text{rad } R^K)^n \subseteq (\text{rad } R)^K$. \square

Proposition. Let $K|k$ be a non-algebraic field extension. For any k -algebra R , $R \cap \text{rad } R^K$ is a nil ideal in R .

Proof. Let $a \in R \cap \text{rad } R^K$, and let $t \in K$ be transcendental over k . We may assume that $K = k(t)$, since by the previous theorem we have $R \cap \text{rad } R^K \subseteq R \cap \text{rad } R^{k(t)} \Rightarrow a \in R \cap \text{rad } R^{k(t)}$.

Now $1 - at \in \mathcal{U}(R^K)$, so $(1 - at) \cdot f(t)/g(t) = 1$ for some $f(t) = b_0 + b_1 t + \cdots + b_m t^m \in R[t]$ and $g(t) = c_0 + c_1 t + \cdots + c_{m+1} t^{m+1} \in k[t]$. Comparing coefficients, $c_0 = b_0$, $c_i = b_i - ab_{i-1}$ ($1 \leq i \leq m+1$), with the convention $b_{m+1} = 0$. Solving for the b_s s in terms of the c_j s, we have $b_i = a^i c_0 + a^{i-1} c_1 + \cdots + c_i$. In particular, $0 = b_{m+1} = a^{m+1} c_0 + \cdots + ac_m + c_{m+1}$, and a is algebraic over k . Then by a previous result ($x \in \text{rad } S$ is algebraic iff it is nilpotent), a is nilpotent. Conclude $R \cap \text{rad } R^K$ is a nil ideal in R . \square

Remark. If $\text{rad } R$ is not nil, then $R \cap \text{rad } R^K \subsetneq \text{rad } R$.

Lemma. Let R be a k -algebra. If $K|k$ is a separable algebraic field extension, then R is Jacobson semisimple if and only if R^K is Jacobson semisimple.

Proof. By the above theorem, $\text{rad } R = R \cap \text{rad } R^K$, so if R^K is Jacobson semisimple, $\text{rad } R = R \cap \{0\} = \{0\}$ and R is Jacobson semisimple. Conversely, suppose R is Jacobson semisimple.

Let $z \in \text{rad } R^K$, and write $z = \sum_{i=1}^n r_i \otimes a_i$ for some $r_i \in R, a_i \in K$. Let $L = k(a_1, \dots, a_n)$. Then L is a finite field extension of k , and $z \in R^L \cap \text{rad}(R^L)^K \subseteq \text{rad } R^L$ by the above theorem. We may therefore assume that $[K : k] < \infty$.

Let $E \supseteq K \supseteq k$ be the normal hull of K over k (so $E|k$ is a finite Galois extension). By the previous theorem, $\text{rad } R^K = R^K \cap \text{rad}(R^K)^E \subseteq \text{rad}(R^K)^E = \text{rad } R^E$. It therefore suffices to show that if $K|k$ is a finite Galois extension, then $\text{rad } R = \{0\} \Rightarrow \text{rad } R^K = \{0\}$.

Say $G = \text{Gal}(K|k)$. Each $\sigma \in G$ acts on R^K by $1 \otimes \sigma$. In particular, we can identify $\text{Gal}(K|k)$ with a subgroup of $\text{Aut}(R^K)$. Let $\{e_i\}$ be a k -basis for K , and let $z = \sum_i r_i \otimes e_i \in \text{rad } R^K$. Let $\sigma \in G$. Then $\sigma(ze_j) \in \text{rad } R^K$ because $\text{rad } R^K$ is invariant under $\text{Aut}(R^K)$. Now $\sigma(ze_j) = \sum_i r_i \otimes (\sigma(e_i e_j))$.

Consider the trace map $\text{tr} = \sum_{\sigma \in G} \sigma : K \rightarrow k$. (The image of this map lies in k because it is invariant under G , hence lies in $\text{Fix}(\text{Gal}(K|k)) = k$.) This induces a map $\text{tr}_R : R^K \rightarrow R$. Then $\text{tr}(ze_j) = \sum_{\sigma \in G} \sigma(ze_j) \in R \cap \text{rad } R^K \subseteq \text{rad } R = \{0\}$, where the inclusion holds by the previous theorem.

Explicitly, $0 = \text{tr}(ze_j) = \sum_{\sigma \in G} \sum_i r_i \otimes (\sigma(e_i e_j)) = \sum_i r_i \otimes (\sum_{\sigma \in G} \sigma(e_i e_j)) = \sum_i r_i \otimes \text{tr}(e_i e_j) = \sum_i r_i \text{tr}(e_i e_j)$. But the matrix $(\text{tr}(e_i e_j))$ is invertible, so we must have $r_i = 0 \forall i$. Then $z = 0$. Since $z \in \text{rad } R^K$ was arbitrary, we conclude $\text{rad } R^K = \{0\}$. \square

Theorem. If $K|k$ is a separable algebraic field extension, then $\text{rad } R^K = (\text{rad } R)^K$.

Proof. Note that the surjective homomorphism $R \otimes_k K \rightarrow (R/\text{rad } R) \otimes_k K$ given by $r \otimes c \mapsto (r + \text{rad } R) \otimes c$ for $r \in R, c \in K$, establishes the isomorphism $R^K/(\text{rad } R)^K \cong (R/\text{rad } R)^K$. $R/\text{rad } R$ is Jacobson semisimple, so by the above lemma, $(R/\text{rad } R)^K \cong R^K/(\text{rad } R)^K$ is Jacobson semisimple. Then $\{0\} = \text{rad}(R^K/(\text{rad } R)^K) = (\text{rad } R^K)/(\text{rad } R)^K$ (because $(\text{rad } R)^K \subseteq \text{rad } R^K$ by the above theorem). Conclude $\text{rad } R^K = (\text{rad } R)^K$. \square

Exercises for §5

2.5.2. Give an example of a ring R with $\text{rad } R \neq \{0\}$ but $\text{rad } R[t] = \{0\}$.

Proof. Let $S = \mathbb{Q}[x, y]$, $P = (x) \triangleleft S$ the principal ideal generated by x . $S/P \cong \mathbb{Q}[y]$ is a domain, so P is a prime ideal of S . Let $R = S_P$, the localization of S by P . Then R is a local ring and has a unique maximal ideal $M \neq \{0\}$. So $\text{rad } R = M \neq \{0\}$. Since R is commutative, $\text{rad } R[t] = (\text{Nil } R)[t]$. But $R = S_P$ has no nonzero nilpotent elements because S has none. Then $\text{rad } R[t] = (\text{Nil } R)[t] = \{0\}$. \square

2.5.6. For any ring R , show that the Jacobson radical of the power series ring $A = R[[t]]$ is given by $P = \{a + tf(t) : a \in \text{rad } R, f(t) \in A\}$.

2.5.7. For any k -algebra R and any finite field extension $K|k$, show $\text{rad } R$ is nilpotent if and only if $\text{rad } R^K$ is nilpotent.

Proof.

Finite field extensions are algebraic, so we have $\text{rad } R = R \cap \text{rad } R^K$. In particular, $(\text{rad } R)^K \subseteq \text{rad } R^K$. Say $[K : k] = n$. Then we also have $(\text{rad } R^K)^n \subseteq (\text{rad } R)^K$.

Suppose $\text{rad } R$ is nilpotent. Say $(\text{rad } R)^m = \{0\}$. Then $(\text{rad } R^K)^{mn} \subseteq (\text{rad } R \otimes_k K)^n \subseteq (\text{rad } R)^n \otimes_k K^n = \{0\}$, i.e., $\text{rad } R^K$ is nilpotent.

Suppose $\text{rad } R^K$ is nilpotent. Say $(\text{rad } R^K)^m = \{0\}$. Then $(\text{rad } R \otimes_k K)^m \subseteq (\text{rad } R^K)^m = \{0\} \Rightarrow (\text{rad } R \otimes_k 1_K)^m = \{0\} \Rightarrow (\text{rad } R)^m = \{0\}$, i.e., $\text{rad } R$ is nilpotent. \square

2.6 Group Rings and the J -Semisimplicity Problem

Recall the notion of a group ring defined in §1.1.

Definition. Let k be a field. A k -representation of G is a group homomorphism $\phi : G \rightarrow GL_n(k)$. A (left) G -module over k is an ordered pair (V, ρ) consisting of a vector space V and a group homomorphism $\rho : G \rightarrow GL(V)$.

A G -module over k extends to a kG -module via the action

$$\left(\sum_{g \in G} \alpha_g g \right) v = \sum_{g \in G} \alpha_g \rho(g)(v)$$

Conversely, a kG -module ${}_k V$ admits a G -module over k .

Proposition. Let G be an infinite group. Then kG is not semisimple.

Proof. Consider the ring homomorphism $\epsilon : kG \rightarrow k$ (the augmentation map) satisfying $\epsilon|_k = \text{id}_k$, and $\epsilon(g) = 1_G$ for all $g \in G$. Let $A = \ker \epsilon$. Suppose $R = kG$ is semisimple. Then $kG = A \oplus B$ for some left ideal $B \subseteq kG$. Now there exist idempotents $e, f \in kG$ such that $A = Re$, $B = Rf$, $1 = e + f$ and $ef = 0$. For any $\sigma \in G$, $1 - \sigma \in A$. In particular $(1 - \sigma)f \in Ref = \{0\}$. Then $f = \sigma f$. Write $f = \sum_{g \in G} f_h h$ for some $f_h \in k$. Let $\sigma \in G$. The coefficient of 1_G in $f = \sum_{h \in G} f_h h$ is f_1 , but this is also the coefficient of 1_G in $f = \sigma^{-1} f = \sum_{h \in G} f_h (\sigma^{-1} h)$, namely, f_σ . Conclude that $f_h = f_1$ for all $h \in G$. By definition, f is a finite sum. Then we must have $|G| < \infty$, a contradiction to the choice of G . Conclude kG is not semisimple. \square

Theorem (Maschke's Theorem). Let G be a finite group. Then $R = kG$ is semisimple if and only if k is semisimple and $|G| \in \mathcal{U}(k)$.

Proof.

Suppose k is semisimple and $|G| \in \mathcal{U}(k)$. Let W be an R -submodule of the R -module V . By the semisimplicity of k , there exists a k -homomorphism $f : {}_k V \rightarrow {}_k W$ such that $f|_W = \text{id}_W$. Define $\tilde{f} : V \rightarrow V$ by $\tilde{f}(v) = |G|^{-1} \sum_{g \in G} g^{-1} f(gv)$. Since $f(V) \subseteq W$ and W is an R -submodule, we have $\text{im } \tilde{f} \subseteq W$. If $w \in W$, then

$$\tilde{f}(w) = |G|^{-1} \sum_{g \in G} g^{-1} f(gw) = |G|^{-1} \sum_{g \in G} g^{-1} (gw) = |G|^{-1} \sum_{g \in G} w = w$$

i.e., $\tilde{f}|_W = \text{id}_W$. \tilde{f} is automatically a k -homomorphism. If $v \in V$ and $h \in G$, we have

$$\tilde{f}(hv) = |G|^{-1} \sum_{g \in G} g^{-1} f(ghv) = |G|^{-1} h \sum_{g \in G} (gh)^{-1} f(ghv) = h |G|^{-1} \sum_{\tau \in G} \tau^{-1} f(\tau v) = h \tilde{f}(v)$$

so \tilde{f} is an R -homomorphism. Conclude that $V = W \oplus \ker \tilde{f}$.

Suppose kG is semisimple. Let $\epsilon : kG \rightarrow k$ denote the augmentation map. Then $k = \epsilon(R)$ is semisimple. Write $R = Re \oplus Rf$ for orthogonal idempotents $e, f \in R$ satisfying $1 = e + f$,

where $Re = \ker \epsilon$ and Rf is a complimentary left ideal. From before, we have $f = \sum_{g \in G} cg$ for some constant $c \in k$. By the surjectivity of ϵ , we have $\epsilon(Rf) = k$, so $\exists x \in R$ such that $1 = \epsilon(xf) = \epsilon(x)\epsilon(f) = \epsilon(x)c \cdot |G|$. So $|G|$ has a left inverse in k . By a similar argument (considering $\ker \epsilon$ as a right ideal in R and finding orthogonal idempotents $e, f \in R$ such that $\ker \epsilon = eR$ and $R = eR \oplus fR$), $|G|$ has a right inverse in k . Then $|G| \in \mathcal{U}(k)$. \square

Exercises for §6

2.6.1. Let V be a kG -module and H a subgroup of G of finite index n not divisible by $\text{char } k$. Prove that if V is semisimple as a kH -module, then V is semisimple as a kG -module.

Proof.

Let W be a kG -submodule of V . By assumption, V splits as a direct sum of kH -submodules, so there exists a kH -module homomorphism $f : V \rightarrow W$ such that $f|_W = \text{id}_W$.

Let s_1, \dots, s_n be a complete set of right H -coset representatives in G . Note that for any $\tau \in G$, $s_1\tau, \dots, s_n\tau$ is also a complete set of right H -coset representatives in G .

Define $g : V \rightarrow V$ by $g(v) = n^{-1} \sum_{i=1}^n s_i^{-1} f(s_i v)$. g is clearly k -linear. Note that $g(V) \subseteq W$ because $f(V) = W$ and W is a kH -submodule of V . Also, if $v \in W$, then $g(v) = n^{-1} \sum_{i=1}^n s_i^{-1} f(s_i v) = n^{-1} \sum_{i=1}^n s_i^{-1} s_i v = v$, i.e., $g|_W = \text{id}_W$.

Let $\tau \in G$, $v \in V$. For each $1 \leq i \leq n$, write $s_i\tau = h_i s_{\alpha(i)}$ for some $h_i \in H$ and some permutation $\alpha \in S_n$. Then

$$\begin{aligned} g(\tau v) &= n^{-1} \sum_{i=1}^n s_i^{-1} f(s_i \tau v) \\ &= \tau n^{-1} \sum_{i=1}^n (s_i \tau)^{-1} f(s_i \tau v) \\ &= \tau n^{-1} \sum_{i=1}^n (h_i s_{\alpha(i)})^{-1} f(h_i s_{\alpha(i)} v) \\ &= \tau n^{-1} \sum_{i=1}^n s_{\alpha(i)}^{-1} h_i^{-1} h_i f(s_{\alpha(i)} v) \\ &= \tau n^{-1} \sum_{i=1}^n s_{\alpha(i)}^{-1} f(s_{\alpha(i)} v) = \tau g(v) \end{aligned}$$

Conclude that g is a kG -module homomorphism. Then $V = W \oplus \ker g$, and V is a semisimple kG -module. \square

2.6.3. Let k be a ring and G a finite group with $|G| \in k^*$. Let $W \subseteq V$ be left kG -modules.

1. If W is a direct summand of V as k -modules, show that W is a direct summand of V as kG -modules.
2. If V is projective as a k -module, show that V is projective as a kG -module.

Proof.

1. Suppose W is a direct summand of V as k -modules. Then there exists a k -linear map $f : V \rightarrow W$ such that $f|_W = \text{id}_W$. Define $g : V \rightarrow V$ by $g(v) = |G|^{-1} \sum_{\sigma \in G} \sigma^{-1} f(\sigma v)$. Then g is k -linear, $g(V) \subseteq W$, and $g(w) = w$ for all $w \in W$. Let $v \in V$, $\tau \in G$. Then

$$\begin{aligned} g(\tau v) &= |G|^{-1} \sum_{\sigma \in G} \sigma^{-1} g(\sigma \tau v) \\ &= \tau |G|^{-1} \sum_{\sigma \in G} (\sigma \tau)^{-1} g(\sigma \tau v) \\ &= \tau |G|^{-1} \sum_{\sigma' \in G} \sigma'^{-1} f(\sigma' v) = \tau g(v) \end{aligned}$$

So g is a kG -homomorphism. Conclude $V = W \oplus \ker g$.

2. Suppose V is projective as a k -module. Let $f : A \rightarrow B$ be a surjective kG -module homomorphism, and suppose $g : V \rightarrow B$ is kG -module homomorphism. By assumption, there exists a k -module homomorphism $h : V \rightarrow A$ such that $f \circ h = g$. Define $\tilde{h} : V \rightarrow A$ by $\tilde{h}(v) = |G|^{-1} \sum_{\sigma \in G} \sigma^{-1} h(\sigma v)$. Check as above that \tilde{h} is a kG -module homomorphism. Let $v \in V$. Then

$$\begin{aligned} (f \circ \tilde{h})(v) &= f \left(|G|^{-1} \sum_{\sigma \in G} \sigma^{-1} h(\sigma v) \right) \\ &= |G|^{-1} \sum_{\sigma \in G} f(\sigma^{-1} h(\sigma v)) \\ &= |G|^{-1} \sum_{\sigma \in G} \sigma^{-1} (f \circ h)(\sigma v) \\ &= |G|^{-1} \sum_{\sigma \in G} \sigma^{-1} g(\sigma v) \\ &= |G|^{-1} \sum_{\sigma \in G} g(v) = g(v) \end{aligned}$$

Conclude that $f \circ \tilde{h} = g$, hence V is projective as a kG -module. □

2.6.7. Show that if k_0 is any finite field and G is any finite group, then $(k_0G/\text{rad } k_0G) \otimes_{k_0} K$ is semisimple for any field extension $K \supseteq k_0$. (For this Exercise, we assume Wedderburn's Theorem that finite division rings are commutative.)

Proof.

We know that $k_0G/\text{rad } k_0G$ is semisimple, so we can write $k_0G/\text{rad } k_0G \cong \prod_{i=1}^r M_{n_i}(D_i)$ for some $n_i \in \mathbb{N}$ and some finite-dimensional k_0 -division rings D_i . By Wedderburn's Theorem, each D_i is in fact a finite field extension of k_0 .

Now $(k_0G/\text{rad } k_0G) \otimes_{k_0} K \cong \prod_{i=1}^r M_{n_i}(D_i) \otimes_{k_0} K \cong \prod_{i=1}^r M_{n_i}(D_i \otimes_{k_0} K)$. It now suffices to show that each $D_i \otimes_{k_0} K$ is isomorphic to a direct product of fields, for then $(k_0G/\text{rad } k_0G) \otimes_{k_0} K$ will be isomorphic to a direct product of matrix rings over fields, hence will be semisimple.

Write $D = D_i$. Recall that finite fields are perfect, so the finite field extension D/k_0 is separable. We can thus write $D = k_0(\alpha)$ for some $\alpha \in D$. Let $f \in k_0[x]$ denote the minimal polynomial of α over k_0 . Then $D \cong k_0[x]/(f)$. Over K , we have a factorization $f = f_1 \cdots f_m$ for pairwise nonassociate irreducible polynomials $f_j \in K[x]$. Then $D \otimes_{k_0} K \cong k_0[x]/(f) \otimes_{k_0} K \cong K[x]/(f) \cong \prod_{j=1}^m K[x]/(f_j)$, a direct product of fields. \square

2.6.8. Let $k \subseteq K$ be two fields and G a finite group. Show $\text{rad } KG = (\text{rad } kG) \otimes_k K$.

Proof.

If $\text{char } k = 0$, then kG and KG are semisimple by Maschke's Theorem, and the result follows trivially.

Suppose $\text{char } k = p > 0$, and let \mathbb{F}_p denote the finite field of order p . Since $\dim_{\mathbb{F}_p} \mathbb{F}_p G = |G| < \infty$, we have $\mathbb{F}_p G \cap \text{rad } kG = \text{rad } \mathbb{F}_p G$, hence $\text{rad } \mathbb{F}_p G \otimes_k k \subseteq \text{rad } kG$. Note that $(\mathbb{F}_p G \otimes_{\mathbb{F}_p} k)/(\text{rad } \mathbb{F}_p G \otimes_{\mathbb{F}_p} k) \cong (\mathbb{F}_p G / \text{rad } \mathbb{F}_p G) \otimes_{\mathbb{F}_p} k$, which is semisimple by Exercise 2.6.7. Conclude that $\text{rad } kG = \text{rad } \mathbb{F}_p G \otimes_{\mathbb{F}_p} k$. By a similar argument, $\text{rad } KG = \text{rad } \mathbb{F}_p G \otimes_{\mathbb{F}_p} K$.

Now $\text{rad } kG \otimes_k K = [\text{rad } \mathbb{F}_p G \otimes_{\mathbb{F}_p} k] \otimes_k K = \text{rad } \mathbb{F}_p G \otimes_{\mathbb{F}_p} K = \text{rad } KG$. \square

2.6.9. Let $k \subseteq K$ be two fields and G a finite group. Show that a kG -module M is semisimple if and only if the KG -module $M^K = M \otimes_k K$ is semisimple.

Proof.

(\Rightarrow): Suppose M^K is semisimple. Let $N \subseteq M$ be a kG -submodule. Then there exists a KG -module homomorphism $f : M^K \rightarrow N^K$ such that $f|_{N^K} = \text{id}_{N^K}$. Let $\{e_i : i \in I\}$ be a k -basis for K . Then $M^K = \bigoplus_i M \otimes_k e_i$. Now given $m \in M$, $f(m \otimes 1) = \sum_i g_i(m) \otimes e_i$ for uniquely determined k -linear maps $g_i : M \rightarrow N$.

Let $r \in kG$. On the one hand, $f(rm \otimes 1) = \sum_i g_i(rm) \otimes e_i$. On the other hand, $f(rm \otimes 1) = f((r \otimes 1)(m \otimes 1)) = (r \otimes 1)f(m \otimes 1) = (r \otimes 1) \sum_i g_i(m) \otimes e_i = \sum_i r g_i(m) \otimes e_i$. Conclude that each g_i is a kG -module homomorphism. Assume that $e_{i_0} = 1 \in k$. Now $f|_{N^K} = \text{id}_{N^K} \Rightarrow g_{i_0} : M \rightarrow N$ is surjective and $g_{i_0}|_N = \text{id}_N$. Then $M = N \oplus \ker g_{i_0}$. Conclude that M is semisimple.

(\Leftarrow): Suppose M is semisimple. Then M is a direct sum of simple kG -modules, $M = \bigoplus_{j \in J} M_j$ for some index set J . Now $M^K = \bigoplus_{i \in I} M \otimes e_i = \bigoplus_{i \in I} \left(\bigoplus_{j \in J} M_j \right) \otimes e_i$, a direct sum of simple kG -modules, so M^K is semisimple as a KG -module.

Let $W \subseteq M^K$ be a KG -submodule. In particular, W is a kG -submodule of M^K . Write $W = \bigoplus_i N_i \otimes e_i$ for some kG -submodules $N_i \subseteq M$. For any $i, i' \in I$, we have $N_i \otimes e_{i'} = (e_{i'} e_i^{-1})(N_i \otimes e_i) \subseteq (e_{i'} e_i^{-1})W \subseteq W$. Conclude $N_i = N_{i'}$ for all $i, i' \in I$. So $W = \bigoplus_i N \otimes e_i = N^K$ for some kG -submodule $N \subseteq M$. Say $M = N \oplus N'$. Then $M^K = N^K \oplus (N')^K = W \oplus (N')^K$. Conclude that M^K is a semisimple KG -module. \square

Chapter 3

Introduction to Representation Theory

3.7 Modules over Finite-Dimensional Algebras

In this section we assume that R is a finite-dimensional k -algebra.

R is left (right) artinian, because ideals are k -subspaces of bounded dimension. Then $\bar{R} = R/\text{rad } R$ is artinian and Jacobson semisimple, hence semisimple. By the Wedderburn–Artin theory of semisimple modules, we can write $\bar{R} \cong B_1 \times \cdots \times B_r$ where $B_i = M_{n_i}(D_i)$ for some $n_i \in \mathbb{N}$ and some (finite-dimensional) division k -algebra D_i . If M_i denotes the unique simple left B_i -module, then $\{M_1, \dots, M_r\}$ is a complete list of isomorphism classes of simple left \bar{R} -modules and $\bar{R}\bar{R} = \bigoplus_{i=1}^r n_i M_i$. Moreover, we have the following:

- $D_i = \text{End}(B_i M_i) = \text{End}({}_R M_i)$ and $B_i \cong \text{End}(M_i D_i)$ (Double Centralizer Property)
- The natural map $R \rightarrow \text{End}(M_i D_i)$ is surjective.
- $\dim_k M_i = n_i \cdot \dim_k D_i$ (since $M_i \cong D_i^{n_i}$)
- $\dim_k R = \dim_k \text{rad } R + \sum_{i=1}^r n_i^2 \dim_k D_i$
- If $\bar{k} = k$ (i.e., k is algebraically closed), then $D_i = k$.

Lemma (Burnside’s Lemma). Let M be a finite-dimensional right k -vector space, and let A be a k -subalgebra of $\text{End}(M_k)$ such that ${}_A M$ is simple. Assume that $\text{End}({}_A M) = k$. Then $A = \text{End}(M_k)$.

Proof. This follows from the above observations with $R = A$ and $D = k$. □

Example. When does $\text{End}({}_R M) = k$ for simple M ?

1. Let $k = \mathbb{R}$, $R = \mathbb{C}$ an \mathbb{R} -algebra, and ${}_R M = {}_R R = \mathbb{C}$. Then $\text{End}({}_R M) = \mathbb{C} \neq k$.
2. Let $K|k$ be a field extension, $K \neq k$. Then $\text{End}({}_k K) = K \neq k$.

3. Let

$$R = \begin{bmatrix} k & k \\ & k \end{bmatrix}, \quad M = k^2 = \begin{bmatrix} k \\ k \end{bmatrix}$$

so M is a left R -module. M is not simple: $\begin{bmatrix} k \\ 0 \end{bmatrix}$ is a proper R -submodule of M . Now

$$\begin{aligned} \text{End}({}_R M) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(k) : \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} \delta & \epsilon \\ & \tau \end{pmatrix} \right] = 0, \forall \delta, \epsilon, \tau \in k \right\} \\ &= \{aI : a \in k\} \cong k \end{aligned}$$

Definition. Let R be a k -algebra, $K|k$ a field extension. Define the scalar extension of R to K by $R^K = R \otimes_k K$. If M is a left R -module, define the scalar extension of M to K by $M^K = M \otimes_k K$.

R^K is a K -algebra, and R can be identified with $R = R \otimes_k k \subseteq R^K$. M^K is a left R^K module via the action $(r \otimes c_1)(m \otimes c_2) = (rm) \otimes (c_1 c_2)$ for $c_i \in K$, $r \in R$, $m \in M$.

Lemma. Let R be a k -algebra (not necessarily finite-dimensional), and let M, N be left R -modules, $\dim_k M < \infty$. Let $K|k$ be a field extension. Then the natural map $\theta : (\text{Hom}_R(M, N))^K \rightarrow \text{Hom}_{R^K}(M^K, N^K)$ is a k -vector space isomorphism.

Proof. Fix a k -basis $\{a_i : i \in I\}$ of K . Let $f \in \text{Hom}_{R^K}(M^K, N^K)$. Then $f(m \otimes 1) = \sum_{i \in I} g_i(m) \otimes a_i \in N \otimes_k K$ for uniquely determined k -linear maps $g_i : M \rightarrow N$. Now for $r \in R$, we have

$$\begin{aligned} \sum_{i \in I} g_i(rm) \otimes a_i &= f(rm \otimes 1) \\ &= f((r \otimes 1)(m \otimes 1)) \\ &= (r \otimes 1)f(m \otimes 1) \\ &= (r \otimes 1) \left(\sum_{i \in I} g_i(m) \otimes a_i \right) \\ &= \sum_{i \in I} r g_i(m) \otimes a_i \end{aligned}$$

Conclude that $g_i \in \text{Hom}_R(M, N)$. Moreover, only finitely many of the g_i can be nonzero: Fix a k -basis $\{m_1, \dots, m_n\}$ for M . For each $1 \leq j \leq n$, let $I_j \subset I$ consist of those indices i such that $g_i(m_j) \neq 0$. Then each I_j is a finite set, because every element of N^K is a finite sum of simple tensors. Now $I' = \bigcup_1^n I_j$ is a finite set, and $g_i \equiv 0$ for all $i \notin I'$ because the m_j span M .

Set $g = \sum_{i \in I} g_i \otimes a_i \in (\text{Hom}_R(M, N))^K$ (this sum makes sense by the above comment). Then $\theta(g) = f$, since in particular they agree on simple tensors $m \otimes 1 \in M^K$. Conclude that θ is surjective.

Let $f = \sum_{i \in I} f_i \otimes a_i \in (\text{Hom}_R(M, N))^K$, and suppose $\theta(f) = 0$. Then for each $m \in M$, $0 = f(m \otimes 1) = \sum_{i \in I} f_i(m) \otimes a_i$. Conclude that $f_i(m) = 0$ for all $m \in M$ and $f = \sum_{i \in I} f_i \otimes a_i = 0$. \square

Theorem. Let R be a finite dimensional k -algebra, and let M be a simple left R -module, $\dim_k M < \infty$. Then the following are equivalent:

1. $\text{End}({}_R M) = k$
2. The natural map $\pi : R \rightarrow \text{End}(M_k)$ is surjective.
3. For all field extensions $K|k$, M^K is a simple R^K -module.
4. For an algebraically closed field $E \supseteq k$, M^E is a simple R^E -module.

Under these equivalent conditions, say the R -module M is absolutely simple or absolutely irreducible over k .

Proof.

(1) \Rightarrow (2): Let $A = \text{im } \pi$. Then M is a simple left A -module, and by Burnside's Lemma, $A = \text{End}(M_k)$, i.e., π is surjective.

(2) \Rightarrow (3): By the surjectivity of π , we may replace R by $\text{End}(M_k)$. Now $M \cong k^n$ for some $n \in \mathbb{N}$, so $R \cong M_n(k)$. Then $M^K \cong K^n$, and $R^K \cong M_n(K)$. Then M^K is a simple R^K algebra.

(3) \Rightarrow (4): Trivial.

(4) \Rightarrow (1): Suppose M^E is a simple R^E -module for an algebraically closed field $E \supseteq k$. $\text{End}({}_{R^E} M^E)$ is a division algebra by Schur's Lemma. In particular, it is a finite-dimensional division E -algebra, so $\text{End}({}_{R^E} M^E) \cong E$. But $\text{End}({}_{R^E} M^E) \cong (\text{End}({}_R M))^E$ by the above lemma. Conclude $\text{End}({}_R M) \cong k$. \square

Definition. Let R be a finite-dimensional k -algebra. A field $K|k$ is called a splitting field for R and we say that R splits over K if every irreducible R^K -module is absolutely irreducible.

The algebraic closure E of k is always a splitting field for R .

Proposition. Let R be a k -algebra, $K|k$ a field extension. Then $K|k$ is a splitting field for R if and only if $K|k$ is a splitting field for $\bar{R} = R/\text{rad } R$.

Proof. We established in §2.5 that $(\text{rad } R)^K \subseteq \text{rad } R^K$ and $(R/\text{rad } R)^K \cong R^K/(\text{rad } R)^K$. From this it follows that $\text{rad } \bar{R}^K \cong \text{rad}(R^K)/(\text{rad } R)^K$, hence $\bar{R}^K/\text{rad } \bar{R}^K \cong R^K/\text{rad}(R^K)$.

Let M be an irreducible \bar{R}^K -module. Then M is an irreducible $\bar{R}^K/\text{rad } \bar{R}^K$ -module, hence an irreducible $R^K/\text{rad } R^K$ -module by the above observation, hence an irreducible R^K -module. The reverse implications are all also valid. Conclude that M is absolutely irreducible over k as an \bar{R}^K -module if and only if it is absolutely irreducible over k as an R^K -module. Thus $K|k$ is a splitting field for R if and only if $K|k$ is a splitting field for \bar{R} . \square

Proposition. Let k be a field, R a finite-dimensional k -algebra, $\{M_i\}$ a complete set of simple left R -modules. Then the following are equivalent:

1. R splits over k .
2. $\bar{R} = R/\text{rad } R$ splits over k .

3. $\overline{R} \cong M_{n_1}(k) \times \cdots \times M_{n_r}(k)$ for some $n_i \in \mathbb{N}$.

4. $\dim_k R = \dim_k(\text{rad } R) + \sum_{i=1}^r (\dim_k M_i)^2$.

Proof.

(1) \iff (2): This is the previous proposition.

(2) \iff (3): This is immediate from the definition of a splitting field and the observations made at the beginning of the section.

(3) \iff (4): The implication (3) \Rightarrow (4) is immediate. Suppose $\dim_k R = \dim_k(\text{rad } R) + \sum_{i=1}^r (\dim_k M_i)^2$. We know that $\overline{R} \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$ for some division k -algebras D_i and $n_i \in \mathbb{N}$ satisfying $\dim_k M_i = n_i \dim_k D_i$. It follows that

$$\sum_{i=1}^r n_i^2 (\dim_k D_i)^2 = \sum_{i=1}^r (\dim_k M_i)^2 = \sum_{i=1}^r n_i^2 (\dim_k D_i)$$

For this equality to hold, we must have $\dim_k D_i = 1$, $1 \leq i \leq r$. Conclude $D_i = k$ and $\overline{R} \cong M_{n_1}(k) \times \cdots \times M_{n_r}(k)$. \square

Example.

1. Let $k = \mathbb{Q}$, $R = \mathbb{Q}[x]$ or $\mathbb{Q}[x]/(x^2 + 1)$. Let $M = \mathbb{Q}^2$, and let x act on M by

$$x \mapsto \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

Because x has no real eigenvectors, M is an irreducible left R -module. We have

$$\text{End}({}_R M) = \mathbb{Q}I + \mathbb{Q} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \cong \mathbb{Q}[x]/(x^2 + 1)$$

So M is not absolutely irreducible.

2. Let $K = \mathbb{C}$, $R^K = \mathbb{C}[x]$ or $\mathbb{C}[x]/(x^2 + 1)$. M^K is reducible, $M^K \cong \mathbb{C}v_1 + \mathbb{C}v_2$ for eigenvectors v_1, v_2 of x . Then $\text{End}({}_{R^K} M^K) \cong \mathbb{C} \oplus \mathbb{C}$.

Proposition. A field extension $K|k$ is a splitting field for $R = k[t]/(f)$ if and only if K is a splitting field for $f(t) \in k[t]$.

Proof. Write $f = f_1^{n_1} \cdots f_r^{n_r}$ as a product of irreducible polynomials in $K[t]$, $f_i \neq f_j$ for $i \neq j$. Then $R^K = K[t]/(f_1^{n_1} \cdots f_r^{n_r}) \cong K[t]/(f_1^{n_1}) \times \cdots \times K[t]/(f_r^{n_r})$, and $\text{rad } R^K = (\overline{f_1}) \times \cdots \times (\overline{f_r})$, where the bar denotes passage to the quotient. Note that $R^K / \text{rad } R^K \cong K[t]/(f_1) \times \cdots \times K[t]/(f_r)$, and $K[t]/(f_i)$ is a field extension of K of degree $\deg f_i$.

Now K is a splitting field for R if and only if $R^K / \text{rad } R^K$ is isomorphic to a direct product of matrix algebras over K . This is true if and only if $\deg f_i = 1$ for each $1 \leq i \leq r$. But $\deg f_i = 1$ for all $1 \leq i \leq r$ if and only if K is a splitting field for f . \square

Recall that a field k is called perfect if every algebraic extension of k is separable. Recall that all fields of characteristic zero are perfect, and a field k of characteristic $p > 0$ is perfect if and only if $k^p = k$.

Proposition. Every k -algebra R over a perfect field has a splitting field K with $[K : k] < \infty$.

Proof. Since $K|k$ is a splitting field for R if and only if it is a splitting field for $R/\text{rad } R$, we may assume that R is semisimple. Let $E = \bar{k}$ be the algebraic closure of k . Then E is separable. Moreover, by a theorem of §2.5, we have $\text{rad } R^E = (\text{rad } R)^E = (0)^E = \{0\}$. Then R^E is semisimple.

Now $R^E \cong \prod_{i=1}^r M_{n_i}(E)$ for some $r \in \mathbb{N}$, $n_i \in \mathbb{N}$, by a previous observation that the algebraic closure of k is always a splitting field for R . Let $E_{ab}^{(i)}$ denote the ab matrix unit of if i -th factor $M_{n_i}(E)$. Say $E_{ab}^{(i)}$ has preimage under the above isomorphism $\sum_l r_l \otimes e_l^{(a,b,i)}$. Let $K = k \left(\left\{ e_l^{(a,b,i)} : 1 \leq a, b \leq i, 1 \leq i \leq r \right\} \right)$. Then $[K : k] < \infty$, and $R^K \cong \prod_{i=1}^r M_{n_i}(K)$. Conclude that K is a splitting field for k . \square

Proposition. Let k be a field, $K|k$ a field extension, and R a k -algebra.

1. If M_1 and M_2 are nonisomorphic simple left R -modules, then M_1^K and M_2^K have no common composition factors.
2. Every simple R^K -module V is a composition factor of M^K for some simple left R -module M .

Proof.

1. Let $\pi : \bar{R} = R \rightarrow R/\text{rad } R = \prod_i B_i$ denote the projection map, the B_i the simple components of \bar{R} . We may assume that M_1 is the unique simple module of B_1 , and M_2 is the unique simple module of B_2 . From the direct product decomposition $\bar{R} = \prod_i B_i$, we obtain idempotents $e_i \in B_i$ such that $B_i = Re_i$.

Let $x \in R$ such that $\pi(x) = e_1$. Then $x \otimes 1 \in R^K$ acts as the identity on any composition factor V_1 of M_1^K , and acts as zero on any composition factor V_2 of M_2^K . Then $V_1 \not\cong V_2$.

2. Let $0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_m = {}_R R$ be a composition series for R . Then $0 \subsetneq I_1^K \subsetneq I_2^K \subsetneq \cdots \subsetneq I_m^K = R^K$ is a filtration of R^K (not necessarily still a composition series). Let V be a simple left R^K -module. Then V must be a composition factor of I_{i+1}^K/I_i^K for some i . But $I_{i+1}^K/I_i^K \cong (I_{i+1}/I_i)^K$. Set $M = I_{i+1}/I_i$. Then M is a simple left R -module, and V is a composition factor of M^K . \square

Proposition. Let k be a field, R a k -algebra. Let $K|k$ and $L|K$ be field extensions, with K a splitting field for R . Then L is a splitting field for R . More explicitly, if $\{V_1, \dots, V_m\}$ is a complete set of pairwise nonisomorphic simple left R^K -modules, then $\{V_1^L, \dots, V_m^L\}$ is a complete set of pairwise nonisomorphic simple left R^L -modules.

Proof. Since K is a splitting field and by part (1) of the above proposition, V_1^L, \dots, V_m^L are pairwise nonisomorphic simple left R^L -modules. By part (2) of the above proposition, this is a complete list of simple left R^L -modules. Now each V_i^L is absolutely irreducible because each field extension $F|L$ is in particular a field extension of K , so $(V_i^L)^F = (V_i^K)^F$ is a simple left $(R^L)^F = (R^K)^F$ -module. \square

If K is a splitting field for R , the number of simple left R -modules is less than or equal to the number of simple left R^K -modules, and if $L|K$ is a field extension, then the number of simple left R^L modules equals the number of simple left R^K -modules.

Lemma. Let k be a commutative ring, $R = M_n(k)$. For $a, b \in R$, let $[a, b] = ab - ba$ denote the additive commutator, $[R, R]$ the additive subgroup generated by all such $[a, b]$. Then $[R, R] = \{M \in M_n(k) : \text{tr}(M) = 0\}$.

Proof. The inclusion $[R, R] \subseteq \{M \in M_n(k) : \text{tr}(M) = 0\}$ is clear. For the reverse inclusion, note that $\{M \in M_n(k) : \text{tr}(M) = 0\}$ is spanned by the collection of $E_{ii} - E_{jj} = [E_{ij}, E_{ji}]$ and $E_{ij} = [E_{ii}, E_{ij}]$, $i \neq j$. \square

From now on, let k be a field, R a finite-dimensional k -algebra, and $T(R) = \text{rad } R + [R, R]$, a k -subspace of R .

Theorem. Assume that R splits over k . Then the number of simple left R -modules equals $\dim_k R/T(R)$. Furthermore, $T(R)$ contains all nilpotent elements in R .

Proof. Let $\bar{R} = R/\text{rad } R$. By the Wedderburn–Artin Theorem and since R splits over k , $\bar{R} = M_{n_1}(k) \times \cdots \times M_{n_r}(k)$ for some $n_i \in \mathbb{N}$. Then there are precisely r simple left R -modules.

Let $A_i = M_{n_i}(k)$. Now $A_i A_j = \{0\}$ for $i \neq j \Rightarrow [\bar{R}, \bar{R}] \cong \prod_{i=1}^r [A_i, A_i]$. Then $\bar{R}/[\bar{R}, \bar{R}] \cong \prod_{i=1}^r A_i/[A_i, A_i] \cong \prod_{i=1}^r k$, since $A_i/[A_i, A_i]$ is isomorphic as a k -algebra to the collection of scalar diagonal matrices in A_i . Then $\dim_k \bar{R}/[\bar{R}, \bar{R}] = r$. Since $[R, R]$ maps onto $[\bar{R}, \bar{R}]$ under the projection map $R \rightarrow \bar{R}$, we now have $\dim_k R/T(R) = \dim_k \bar{R}/[\bar{R}, \bar{R}] = r$.

If $x \in R$ is nilpotent, then $\bar{x} \in \bar{R}$ is a sum of nilpotent matrices in $\prod_{i=1}^r A_i$. Then $\bar{x} \in [\bar{R}, \bar{R}]$, so $x \in \text{rad } R + [R, R] = T(R)$. \square

Corollary. Let R be a k -algebra which splits over $K \supseteq k$. Let r be the number of simple left R -modules, and let r' be the number of simple left R^K -modules. Then $r \leq r' \leq \dim_k R/T(R)$.

Proof. The first inequality follows from a previous observation. As for the second inequality, we have by the previous theorem that $r' = \dim_K R^K/T(R^K)$. The inclusion $[R, R]^K \subseteq [R^K, R^K]$ is clear, while the inclusion $(\text{rad } R)^K \subseteq \text{rad } R^K$ follows from a theorem of §2.5, so $T(R)^K \subseteq T(R^K)$. Then $r' = \dim_K R^K/T(R^K) \leq \dim_K R^K/T(R)^K = \dim_k R/T(R)$. \square

Definition. Let R be a finite-dimensional k -algebra, and let M be a left R -module of finite dimension over k with left R -action given by $\rho : R \rightarrow \text{End}(M)$. Call the map $\chi_M : R \rightarrow k$ given by $x \mapsto \text{tr } \rho(x)$ the character associated with the left R -module M .

Remark. Let M_1, M_2, M be finite-dimensional k -vector spaces with left R -actions ρ_1, ρ_2, ρ . Suppose $0 \rightarrow M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \rightarrow 0$ is a short exact sequence of R -modules. Say $\dim_k M_1 = n_1$ and $\dim_k M_2 = n_2$. Choose an ordered k -basis for M such that the first n_1 basis vectors span $\text{im } f$ and the last n_2 basis vectors span $\ker g$. Then with respect to this basis, each $\rho(x)$, $x \in R$, is represented by a block upper-triangular matrix:

$$\rho(x) \sim \left[\begin{array}{c|c} \rho_1(x) & * \\ \hline 0 & \rho_2(x) \end{array} \right]$$

Conclude $\text{tr } \rho = \text{tr } \rho_1 + \text{tr } \rho_2$, and thus $\chi_M = \chi_{M_1} + \chi_{M_2}$. In particular, the composition factors of a module M , counted with multiplicities, completely determine χ_M .

Theorem. Let k be a field of characteristic zero. Let M be a left R -module of finite dimension over k . Then χ_M determines the composition factors of M . Explicitly, if $\chi_M = \chi_N$ for left R -modules M, N of finite dimension over k , then M, N have the same composition factors, counted with multiplicity. Furthermore, if M, N are semisimple, then $\chi_M = \chi_N \Rightarrow M \cong N$.

Proof. Write $\bar{R} = \prod_i S_i$, S_i the simple components of R , and let $\pi : R \rightarrow \bar{R}$ denote the projection map. Let M_i denote the simple left S_i -module, so $\{M_i\}$ is a complete list of simple left R -modules. Suppose M_i has multiplicity m_i as a composition factor for M . Then $\chi_M = \sum_i m_i \chi_{M_i}$, and M completely determines χ_M (cf. previous remark).

Take $a_j \in R$ such that $\pi(a_j)$ is the identity of S_j . Then a_j acts as δ_{ij} on M_i . Now $\chi_M = \sum_i m_i \chi_{M_i} \Rightarrow \chi_M(a_j) = \sum_i m_i \chi_{M_i}(a_j) = m_j \dim_k M_j$. So $m_j = \chi_M(a_j) / \dim_k M_j$, and χ_M completely determines the composition factors of M . \square

Example. Let k be a field of prime characteristic $p > 0$, R a k -algebra, and M an R -module. Then $\chi_{pM} = p\chi_M \equiv 0 \equiv \chi_{\{0\}}$, but pM and $\{0\}$ have different composition factors.

Proposition. Let M, N be left R -modules, N absolutely irreducible. Assume that either (1) $\dim_k M = \dim_k N$, or else (2) M is irreducible. Then $\chi_M = \chi_N \Rightarrow M \cong N$.

Proof. Let $\pi : R \rightarrow \bar{R}$ denote the usual projection, and write $\bar{R} = \prod_{i=1}^r S_i$, S_i the simple components of R . Let M_i be the unique simple left S_i -module, so that $\{M_i : 1 \leq i \leq r\}$ is a complete list of simple left R -modules.

Say $N = M_1$. By an equivalent characterization of absolute irreducibility, the natural map $R \rightarrow S_1 = \text{End}(N_k)$ is surjective. Let $a \in R$ such that $\pi(a) \in S_1$ has trace 1. Then $\chi_N(a) = 1$. Write $\chi_M = \sum_{i=1}^r m_i \chi_{M_i}$. Now if $\chi_M = \chi_N$, we have $1 = \chi_N(a) = \chi_M(a) = \sum_{i=1}^r m_i \chi_{M_i}(a) = m_1 \chi_{M_1}(a) = m_1$. Then by assumptions (1),(2), we must have $m_2 = \dots = m_r = 0$, hence $M \cong N$. \square

Corollary. Let R be a finite-dimensional k -algebra, and suppose R splits over k . Then two simple R -modules are isomorphic if and only if they have the same characters.

Proof. This is immediate from the previous proposition. \square

Exercises for §7

3.7.1. Let M, N be finite-dimensional modules over a finite-dimensional k -algebra R . For any field $K \supseteq k$, show M^K and N^K have a common composition factor as R^K -modules if and only if M and N have a common composition factor as R -modules.

Proof.

Let $\{0\} \subset M_1 \subset \dots \subset M_m = M$ and $\{0\} \subset N_1 \subset \dots \subset N_n = N$ be composition series for M, N , respectively.

(\Rightarrow): Suppose as R^K -modules M^K and N^K have a common composition factor V . Then for some $0 \leq i \leq m-1$ and some $0 \leq j \leq n-1$, V is a common composition factor of $M_{i+1}^K/M_i^K \cong (M_{i+1}/M_i)^K$ and $N_{j+1}^K/N_j^K \cong (N_{j+1}/N_j)^K$. Note that M_{i+1}/M_i and N_{j+1}/N_j are simple left R -modules, so by an above proposition we must have $M_{i+1}/M_i \cong N_{j+1}/N_j$, i.e., M and N have a common composition factor.

(\Leftarrow): Suppose M and N have a common composition factor. Without loss of generality, we may assume $M_1 \cong N_1$. Then $M_1^K \cong N_1^K$, and M^K and N^K share the composition factors of $M_1^K \cong N_1^K$. \square

3.7.2. Let R be a finite-dimensional k -algebra which splits over k . Show that for any field $K \supseteq k$, $\text{rad}(R^K) = (\text{rad } R)^K$.

Proof. Since $\dim_k R < \infty$, we have automatically $(\text{rad } R)^K \subseteq \text{rad } R^K$. Note that $R/\text{rad } R$ is a semisimple, hence a direct sum of simple left R -modules. Since R splits over k , all simple R -modules remain simple upon scalar extension to K . Then $(R/\text{rad } R)^K \cong R^K/(\text{rad } R)^K$ is a semisimple R^K -module, so $(\text{rad } R^K) \cdot R^K/(\text{rad } R)^K = \{0\} \Rightarrow \text{rad } R^K \subseteq (\text{rad } R)^K$. Conclude $\text{rad } R^K = (\text{rad } R)^K$. \square

3.7.4. Let R be a left artinian ring and $C \subseteq Z(R)$ a subring. Show that $\text{Nil } C = C \cap \text{rad } R$. If R is a finite-dimensional algebra over a subfield $k \subseteq C$, show $\text{rad } C = C \cap \text{rad } R$.

Proof. Since R is left artinian, $\text{rad } R$ is a nil ideal in R , so $C \cap \text{rad } R \subseteq \text{Nil } C$. Let $c \in \text{Nil } C$. Then Rc is a (two-sided) ideal in R . Say $c^n = 0$. Then for $r \in R$, $(rc)^n = r^n c^n = 0$. Conclude that Rc is a nil ideal, hence $Rc \subseteq \text{rad } R$. In particular, $c \in C \cap \text{rad } R$. Conclude $\text{Nil } C = C \cap \text{rad } R$.

Suppose R is finite-dimensional over a subfield $k \subseteq C$ (in particular, R is left artinian). Then C is a finitely generated k -algebra $\Rightarrow \text{rad } C = \text{Nil } C = C \cap \text{rad } R$. \square

3.7.5. Let R be a finite-dimensional k -algebra which splits over k . Show that any subalgebra $C \subseteq Z(R)$ also splits over k .

Proof. Since R splits over k , $R/\text{rad } R \cong \prod_{i=1}^r M_{n_i}(k)$ for some $n_i, r \in \mathbb{N}$. Then $C/\text{rad } C = C/(C \cap \text{rad } R) \cong (C + \text{rad } R)/\text{rad } R$ is a subring of $Z(R/\text{rad } R) \cong \prod_{i=1}^r k$. Now $C/\text{rad } C$ is a commutative semisimple ring, so $C/\text{rad } C \cong \prod_{j=1}^s K_j$ for some finite field extensions $K_j|k$ and some $s \leq r$.

Consider $\prod_{j=1}^s K_j$ as a subalgebra of $\prod_{i=1}^r k$, and let e_j denote the identity element of K_j . Let $\pi_i : \prod_{i=1}^r k \rightarrow k$ denote the i -th projection homomorphism. Then $\pi_i(e_j) \neq 0$ for some $1 \leq i \leq r$. Now $\pi_i(e_j) = \pi_i(e_j e_j) = \pi_i(e_j) \pi_i(e_j) \Rightarrow \pi_i(e_j) = 1$. Restricting π_i to K_j , we have a k -algebra homomorphism $\pi_i : K_j \rightarrow k$, and conclude $K_j \cong k$.

Then $C/\text{rad } C \cong \prod_{j=1}^s k$ splits over k . \square

3.7.8. Let R be a finite-dimensional k -algebra, and let $L \supseteq K \supseteq k$ be fields. Assume that L is a splitting field for R . Show that K is a splitting field for R if and only if for every simple left R^L -module M , there exists a (simple) left R^K -module U such that $U^L \cong M$.

Proof.

Suppose K is a splitting field for R , and let M be a simple left R^L -module. Let $\{V_i : 1 \leq i \leq n\}$ be a complete set of pairwise nonisomorphic simple left R^K -modules. Then $\{V_i^L : 1 \leq i \leq n\}$ is a complete set of pairwise nonisomorphic simple left R^L -modules, and $M \cong V_j^L$ for some $1 \leq j \leq n$.

Conversely, suppose the given condition on simple left R^L -modules holds. Let V be a simple left R^K -module. It suffices to show that V^F is a simple R^F -module for all field extensions $F|K$. In fact, it suffices to show that V^L is a simple R^L -module, for then if

$\{0\} \neq V_1 \subsetneq V^F$ were a proper nonzero R^F -submodule of V^F , we'd have $\{0\} \neq V_1^L \subsetneq (V^F)^{FL} = (V^L)^{FL}$, i.e., V_1^L is a proper nonzero submodule of the simple R^{FL} -module $(V^L)^{FL}$, a contradiction.

Let $W \subseteq V^L$ be a simple R^L -module. By assumption, there exists a simple left R^K -module U such that $W \cong U^L$. Since V^L and U^L share a common composition factor (namely $W \cong U^L$), we conclude that $V \cong U$ since U, V are both simple R^K -modules. Hence $V^L \cong U^L \cong W$ a simple R^L -module, and the result follows. \square

3.7.9. If $K \supseteq k$ is a splitting field for a finite-dimensional k -algebra R , does it follow that K is also a splitting field for any quotient algebra \overline{R} of R ?

Proof. Yes. We may assume $K = k$. Let $\varphi : R \rightarrow \overline{R}$ denote the projection map to the quotient algebra \overline{R} , and let V be a simple left \overline{R} -module. Then R acts on V via φ , and V becomes a simple left R -module. For any field extension $L|K$, V^L remains simple as a left R -module, hence simple as a \overline{R} -module as well. Conclude that V is absolutely irreducible, so K is a splitting field for \overline{R} . \square

3.8 Representations of Groups

In this section we assume that G is a finite group, unless noted otherwise.

Let k be a field, and let G be a finite group. Recall that the group ring kG is semisimple if and only if $\text{char } k \nmid |G|$. Restating previous results in the context of the group ring kG , we have:

- $kG/\text{rad } kG \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$ for some $n_i \in \mathbb{N}$ and division algebras D_i
- As left G -modules, $kG/\text{rad } kG \cong \bigoplus_{i=1}^r n_i M_i$ where $M_i \cong D_i^{n_i}$.
- $|G| = \dim_k(\text{rad } kG) + \sum_{i=1}^r n_i^2 \dim_k D_i$.
- If k is a splitting field for G , then there are $\dim_k kG/[kG, kG]$ simple kG -modules.

Definition. Say that a field k is a splitting field for the group G if the group algebra kG splits over k .

Theorem. Let k be a field, G a finite group. Then there exists a finite field extension $K|k$ such that K is a splitting field for G .

Proof. If $\text{char } k = 0$, then k is perfect and such a K exists by a result of §3.7. Suppose k is of prime characteristic $p > 0$. Then $\overline{k} \supseteq k \supseteq \mathbb{F}_p$. \mathbb{F}_p is a perfect field, so by a result of §3.7, there exists a finite extension $k_1|\mathbb{F}_p$ such that G splits over k_1 . Let K denote the unique smallest field extension of \mathbb{F}_p containing both k and k_1 . Then $[K : k] < \infty$, and $k_1 \subseteq K \Rightarrow K$ is a splitting field for G . \square

Example.

1. Let G be an abelian group. Then necessarily $kG/\text{rad } kG \cong D_1 \times \cdots \times D_r$ for some finite field extensions $D_i|k$. If in addition G splits over k , then $D_i = k$ for all $1 \leq i \leq r$ and the dimension of every irreducible kG -module is one.

2. Let $G = C_n = \langle g \rangle$ the cyclic group of order n . Then $kG \cong k[x]/(x^n - 1)$.

- (a) Suppose $k = \mathbb{C}$ or $k = \mathbb{Q}(\zeta)$, ζ a primitive n -th root of unity. Then $k[x]/(x^n - 1) \cong \prod_{i=1}^n k[x]/(x - \zeta^i) \cong \prod_{i=1}^n k$.
- (b) Suppose $k = \mathbb{Q}$. Let $\Phi_d(x)$ denote the d -th cyclotomic polynomial. Recall that $\Phi_d(x)$ is a degree $\varphi(d)$ irreducible polynomial over \mathbb{Q} , and $\prod_{d|n} \Phi_d(x) = x^n - 1$. Then

$$\mathbb{Q}[x]/(x^n - 1) \cong \prod_{d|n} \mathbb{Q}[x]/(\Phi_d(x)) \cong \prod_{d|n} \mathbb{Q}(\zeta_d)$$

g acts on $\mathbb{Q}(\zeta_d)$ as multiplication by a primitive d -th root of unity ζ_d .

- (c) Suppose $k = \mathbb{R}$. If $n = 2m + 1$, then

$$\mathbb{R}[x]/(x^n - 1) \cong \mathbb{R} \times \prod_{i=1}^m \mathbb{R}[x]/\left((x - \zeta^i)(x - \bar{\zeta}^i)\right)$$

There is a unique one-dimensional module with trivial G action, and m two-dimensional simple modules, with g acting as multiplication by ζ^j , i.e., as a rotation by the angle $2\pi j/n$. If $n = 2m$, then

$$\mathbb{R}[x]/(x^n - 1) \cong \mathbb{R} \times \mathbb{R} \times \prod_{i=1}^{m-1} \mathbb{R}[x]/\left((x - \zeta^i)(x - \bar{\zeta}^i)\right)$$

There are two one-dimensional modules, with g acting as 1 and -1 , respectively, and $m - 1$ two-dimensional simple modules, with g acting as multiplication by ζ^j , i.e., as a rotation by the angle $2\pi j/n$.

3. Let $G = S_n$, the symmetric group on n letters.

- (a) Let $k = \mathbb{Q}$. S_n acts on $\mathbb{Q}^n = \mathbb{Q}\langle e_1, \dots, e_n \rangle$ by permuting the basis elements.
- $M_1 = \mathbb{Q}$ the trivial module, $\chi_{M_1} \equiv 1$.
 - $M_2 = \mathbb{Q}^n/M_1 \cong \{\sum_{i=1}^n a_i e_i : \sum_{i=1}^n a_i = 0\}$ (We will prove later that M_2 is an absolutely irreducible $\mathbb{Q}S_n$ -module.)
 - One-dimensional sign representation, $\text{sgn} : S_n \xrightarrow{\rho} GL_n(\mathbb{Q}) \xrightarrow{\det} \{\pm 1\}$, where $\rho : S_n \rightarrow GL_n(\mathbb{Q})$ denotes the inclusion of S_n into $GL_n(\mathbb{Q})$ as monomial matrices.

Note that $\chi_\rho(\sigma) =$ the number of one-cycles in σ .

From the decomposition $\mathbb{Q}^n = M_1 \oplus M_2$, it follows that $\chi_{M_2} = \chi_\rho - \chi_{M_1} = \chi_\rho - 1$.

- (b) Let $n = 3$, $k = \mathbb{F}_2$. $\mathbb{F}_2 S_3$ is not semisimple by Maschke's Theorem.
- $M_1 = \mathbb{F}_2$ trivial module.
 - $M_2 = \mathbb{F}_2^2/M_1$ two-dimensional module.

Check that M_2 is an absolutely irreducible $\mathbb{F}_2 S_3$ -module by checking dimensions:

$$6 = |S_3| = \underbrace{\dim(\text{rad } \mathbb{F}_2 S_3)}_{\geq 1} + 1^2 + 2^2 \dim D + \dots$$

For some field extension $D|\mathbb{F}_2$. Conclude that $D = \mathbb{F}_2$, $\dim(\text{rad } \mathbb{F}_2 S_3) = 1$, and $\{M_1, M_2\}$ is a complete list of simple $\mathbb{F}_2 S_3$ -modules, \mathbb{F}_2 is a splitting field for S_3 . Check that $\text{rad } \mathbb{F}_2 S_3 = \mathbb{F}_2 (\sum_{\sigma \in S_3} \sigma)$.

(c) Let $n = 3$, $k = \mathbb{F}_3$. $\mathbb{F}_3 S_3$ is not semisimple by Maschke's Theorem.

- $M_1 = \mathbb{F}_3$ trivial module.
- sgn sign representation.

The normal Sylow 3-subgroup $\langle (123) \rangle$ acts trivially on an irreducible S_3 -module (to be proved later). Then the irreducible representations of S_3 are the same as those of $S_3/\langle (123) \rangle \cong S_2$.

From the equation $|G| = \dim_k(\text{rad } kG) + \sum_{i=1}^r n_i^2 \dim_k D_i$ we infer that S_2 has at most two irreducible representations. Conclude that $\{M_1, \text{sgn}\}$ is a complete list of irreducible $\mathbb{F}_3 S_3$ -modules, S_3 splits over \mathbb{F}_3 , and $\dim(\text{rad } \mathbb{F}_3 S_3) = 4$.

Theorem (Clifford). Let $H \trianglelefteq G$, and let V be a simple kG -module. Then ${}_k H V$ is a semisimple kH -module.

Proof. Let M be a simple kH -submodule of V . Then for all $g \in G$, gM is again a kH -submodule of V , $hgM = g(g^{-1}hg)M \subseteq gM$ by normality of H . Moreover, gM is a simple kH -submodule, for if M' were a proper kH -submodule of gM , then $g^{-1}M'$ would be a proper submodule of M .

Now $\sum_{g \in G} gM$ is a kG -submodule of V , hence $V = \sum_{g \in G} gM$ by the simplicity of V . So V is a sum of simple kH -submodules. Conclude that V is semisimple as a kH -module. \square

Theorem. Let k be a field of prime characteristic $p > 0$, and let H be a normal p -subgroup of G . Then:

1. H acts trivially on every simple kG -module, and the simple kG -modules correspond bijectively to the simple $k(G/H)$ -modules. If G itself is a p -group, then the only simple left kG -module is k itself, with trivial G -action.
2. kH has a unique simple module, namely, the trivial module k .

Proof.

1. This follows from (2), since by Clifford's Theorem every simple kG -module is a direct sum of simple kH -modules.
2. Argue by way of induction on $|H|$, the case $|H| = 1$ being trivial. Assume that $|H| > 1$ and let M be a simple kH -module. Recall that H has a nontrivial center, so let $1 \neq h \in Z(H)$. Say $|h| = p^n$. Then in kH , we have $(h - 1)^{p^n} = h^{p^n} - 1 = 1 - 1 = 0$, so $h - 1$ acts as a nilpotent endomorphism of M . Then $\ker(h - 1) \neq \{0\}$ and $M_0 := \{m \in M : hm = m\} \neq \{0\}$. M_0 is a left kH -submodule because $h \in Z(H)$. Conclude that $M_0 = M$ by the simplicity of M . Now M is a simple $k(H/\langle h \rangle)$ -module. But $|H/\langle h \rangle| < |H|$, so induction applies and we conclude that M is the trivial module. \square

Definition. Given a finite group G , define $O_p(G)$ to be the intersection of all Sylow p -subgroups of G .

Lemma. $O_p(G)$ is the largest normal p -subgroup of G .

Proof. $O_p(G) = \bigcap \{P : P \in \text{Syl}_p(G)\} \trianglelefteq G$, since for each $g \in G$, we have $gO_p(G)g^{-1} = \bigcap \{gPg^{-1} : P \in \text{Syl}_p(G)\} = \bigcap \{P : P \in \text{Syl}_p(G)\} = O_p(G)$ by the conjugacy of Sylow p -subgroups of G . And any normal p -subgroup of G is certainly contained in $O_p(G)$ because every p -subgroup of G is contained in a Sylow p -subgroup, and all Sylow p -subgroups of G are conjugate. \square

Corollary. Let k be a field of prime characteristic $p > 0$. Then $O_p(G)$ is the subgroup of G acting trivially on every simple kG -module. Equivalently, $O_p(G) = \{h \in G : h - 1 \in \text{rad } kG\}$.

Proof. Let H be the subgroup of G acting trivially on all simple left kG -modules. By the previous theorem, $O_p(G) \leq H$. Let $h \in H$. The left regular module kG is a finite-dimensional k -vector space, hence has a composition series. From this we infer that $h - 1$ acts kG as a nilpotent endomorphism.

Say $(h - 1)^{p^n} = 0$ for some $n > 0$. But $(h - 1)^{p^n} = h^{p^n} - 1$ in kG , so we conclude that $|h|$ is a p -power, and H is a p -subgroup of G . It's clear that $H \trianglelefteq G$, since if M is a simple left kG -module and $g \in G$, gM is a simple left kG -module and for $m \in M$, $(g^{-1}hg)m = g^{-1}h(gm) = g^{-1}(gm) = m$, i.e., $g^{-1}hg \in H$. Conclude $H \leq O_p(G) \Rightarrow H = O_p(G)$. \square

Corollary (Wallace). Let k be a field of prime characteristic $p > 0$. Suppose G has a normal Sylow p -subgroup H . Then $\text{rad } kG = \sum_{h \in H} kG(h - 1)$. In particular, $\dim_k \text{rad } kG = [G : H](|H| - 1)$.

Proof. Let $I = \sum_{h \in H} kG(h - 1)$. I is clearly a left ideal of kG . Since $(h - 1)g = g(g^{-1}hg - 1)$ and $H \trianglelefteq G$, conclude that I is a two-sided ideal of kG . Now $I \subseteq \text{rad } kG$ by the previous corollary.

Note that the surjective k -linear map $kG \rightarrow k(G/H)$ satisfying $g \mapsto gH, \forall g \in G$ factors through a map $\phi : kG/I \rightarrow k(G/H)$, while the surjective k -linear map $\psi : k(G/H) \rightarrow kG/I$ satisfying $gH \mapsto g + I$ is well defined, since for all $g \in G, h \in H$, we have $gh + I = gh - g(h - 1) + I = g + I$. Conclude that these maps are isomorphisms, establishing $kG/I \cong k(G/H)$.

Now $p \nmid |G/H|$, so $k(G/H)$ is semisimple by Maschke's Theorem. Conclude $\text{rad } kG = I$. Finally, from the isomorphism $kG/I \cong k(G/H)$ we obtain $|G| - \dim_k \text{rad } kG = |G/H|$, i.e., $\dim_k \text{rad } kG = |G| - |G/H| = [G : H](|H| - 1)$. \square

Recall the augmentation map $\epsilon : kG \rightarrow k$ mapping $g \mapsto 1$ for all $g \in G$.

Corollary. Let k be a field of prime characteristic $p > 0$. Let G be a p -group, and set $J = \text{rad } kG$. Then:

1. $J = \ker \epsilon = \sum_{g \in G} k(g - 1)$
2. $J^{|G|} = \{0\}$.
3. If G is generated by g_1, \dots, g_n , then J is generated by $g_1 - 1, \dots, g_n - 1$ as a left ideal.

Proof.

1. Apply the previous corollary with $H = G$. Then $J = \sum_{g \in G} kG(h-1)$. Note that for $g \in G$, $h \in H$, we have $g(h-1) = (gh-1) - (g-1)$. Conclude that $J = \sum_{g \in G} k(g-1)$. It is now clear that $\ker \epsilon \subseteq J$. But $\dim_k(\ker \epsilon) = |G| - 1 = \dim_k J$, so we conclude $J = \ker \epsilon = \sum_{g \in G} k(g-1)$.
2. kG is a finite-dimensional k -vector space, hence has a composition series. Because G is a p -group, the only simple left kG -module is k with trivial G -action (cf. previous theorem). Conclude that G must have $|G|$ composition factors. Now because J acts trivially on all composition factors of G , we must have $J^{|G|} = \{0\}$.
3. This follows from part (a), the observation that if $g, g' \in G$, then $gg' - 1 = g(g' - 1) + (g - 1)$, and induction on the length of words in G . \square

Theorem. Let k be a field with $\text{char } k \nmid |G|$. Suppose k is a splitting field for G . Then the number of simple left kG -modules equals the number of conjugacy classes in G .

Proof. Since $\text{char } k \nmid |G|$, kG is semisimple by Maschke's Theorem. Write $kG \cong M_{n_1}(k) \times \cdots \times M_{n_r}(k)$ for some $n_i \in \mathbb{N}$, so kG has precisely r simple left kG -modules (up to isomorphism). Under this decomposition of kG , observe that $Z(kG) \cong \prod_{i=1}^r k$ and $\dim_k Z(kG) = r$. Let $\{\mathcal{C}_1, \dots, \mathcal{C}_s\}$ be a complete list of conjugacy classes of G . For $1 \leq i \leq s$, let $c_i = \sum_{g \in \mathcal{C}_i} g$. Then $c_i \in Z(kG)$. The c_i are clearly linearly independent, hence form a k -basis for $Z(kG)$. Then $s = \dim_k Z(kG) = r$. \square

Definition. Let G be a group, p a prime. Say $g \in G$ is p -regular (or a p' -element) if $p \nmid |g|$. Say that $g \in G$ is p -singular (or a p -element) if $|g| = p^j$ for some $j \in \mathbb{N}$. Say a conjugacy class \mathcal{C} of G is p -regular if any $g \in \mathcal{C}$ is p -regular. (By convention, say that every element of G is 0-regular.)

Lemma. Let G be a finite group. For each $g \in G$, there exist unique $g_p, g_{p'} \in G$ such that g_p is p -singular, $g_{p'}$ is p -regular, and $g = g_p g_{p'} = g_{p'} g_p$.

Proof. Say $|g| = p^k n$ with $p \nmid n$. Then $rp^k + sn = 1$ for some $r, s \in \mathbb{Z}$. Let $g_p = g^{sn}$, and let $g_{p'} = g^{rp^k}$. Then g_p is p -singular, $g_{p'}$ is p -regular, and $g = g_p g_{p'} = g_{p'} g_p$.

Suppose $g = h_p h_{p'} = h_{p'} h_p$ is another such decomposition of g . Note that $h_p, h_{p'}$ each commute with g , hence commute with each of $g_p, g_{p'}$. Now $g_p h_p^{-1} = g_{p'}^{-1} h_{p'}$, $g_p h_p^{-1}$ is p -singular, and $g_{p'}^{-1} h_{p'}$ is p -regular. Conclude $g_p h_p^{-1} = 1 = g_{p'}^{-1} h_{p'}$ and $g_p = h_p$, $g_{p'} = h_{p'}$. \square

Recall that if $R = kG$ splits over the field k , then the number of simple left R -modules is equal to $\dim_k R/T(R)$, where $T(R) = \text{rad } R + [R, R]$. We showed that $T(R)$ contains all nilpotent elements of R .

Lemma. Let R be a ring of prime characteristic $p > 0$. Then:

1. For all $a_1, \dots, a_n \in R$ and $r \geq 1$, $(a_1 + \cdots + a_n)^{p^r} = a_1^{p^r} + \cdots + a_n^{p^r} \pmod{[R, R]}$.
2. If $s \in [R, R]$, then $s^{p^r} \in [R, R]$.

Proof.

1. We have $(a_1 + \cdots + a_n)^{p^r} = \sum a_{i_1} \cdots a_{i_{p^r}}$ where the sum is taken over all words of length p^r in the symbols a_1, \dots, a_n . The cyclic group C_{p^r} of order p^r acts on these words by cyclic permutations, and two words in the same C_{p^r} orbit are congruent modulo $[R, R]$. (This is clear since $a_{i_1} a_{i_2} \cdots a_{i_{p^r}} = a_{i_2} \cdots a_{i_{p^r}} a_{i_1} + [a_{i_1}, a_{i_2} \cdots a_{i_{p^r}}]$, and distinct elements in a C_{p^r} orbit are obtained through a sequence of such cyclic permutations.) There are precisely n singleton C_{p^r} orbits, namely those of $a_1^{p^r}, \dots, a_n^{p^r}$, and all other orbits are of cardinality p^r . Conclude that, modulo $[R, R]$, our sum takes the form

$$(a_1 + \cdots + a_n)^{p^r} = \sum a_{i_1} \cdots a_{i_{p^r}} \equiv a_1^{p^r} + \cdots + a_n^{p^r} + p^r(\cdots) = a_1^{p^r} + \cdots + a_n^{p^r} \pmod{[R, R]}$$

2. It suffices to prove the case $r = 1$. Write $s = \sum (a_i b_i - b_i a_i)$ for some $a_i, b_i \in R$. Then

$$\begin{aligned} s^p &\equiv \sum (a_i b_i - b_i a_i)^p \pmod{[R, R]} \\ &\equiv \sum ((a_i b_i)^p - (b_i a_i)^p) \pmod{[R, R]} \\ &\equiv \sum (a_i (b_i a_i)^{p-1} b_i - (b_i a_i)^{p-1} b_i a_i) \\ &\equiv \sum [a_i, (b_i a_i)^{p-1} b_i] \equiv 0 \pmod{[R, R]} \end{aligned}$$

i.e., $s^p \in [R, R]$. □

Lemma. Let k be a field, G a finite group, and set $R = kG$. Then $\alpha \in [R, R]$ if and only if the sum of its coefficients over each conjugacy class of G is zero.

Proof.

(\Rightarrow): Let $\alpha \in [R, R]$. It suffices to consider the case $\alpha = ab - ba$ for some $a, b \in R$. Write $a = \sum_{g \in G} \alpha_g g$, $b = \sum_{h \in H} \beta_h h$. Then $\alpha = \sum_{g, h \in G} \alpha_g \beta_h (gh - hg)$. But gh, hg are conjugate in G , $hg = g^{-1}(gh)g$, so in this case it is clear that the sum of the coefficients of α over each conjugacy class of G is zero.

(\Leftarrow): Let $g_1, g_2 \in G$ be conjugate, with say $g_2 = h^{-1}g_1h$. Then $g_1 - g_2 = hh^{-1}g_1 - h^{-1}g_1h = [h, h^{-1}g_1] \in [R, R]$. Now let $\mathcal{C} = \{g_1, \dots, g_n\}$ be a conjugacy class of G , and let $\alpha = \sum_{i=1}^n a_i g_i$. If $\sum_{i=1}^n a_i = 0$, then by the previous observation we have $\alpha = \sum_{i=1}^n a_i g_i \equiv \sum_{i=1}^n a_i g_1 \equiv 0 \pmod{[R, R]}$, i.e., $\alpha \in [R, R]$. □

Corollary. Let $R = kG$ as above, and let $\{a_i : i \in I\}$ be a complete set of conjugacy class representatives of the group G . Then $\{a_i + [R, R] : i \in I\}$ is a k -basis for $R/[R, R]$.

Proof. Let $\mathcal{B} = \{a_i + [R, R] : i \in I\}$. \mathcal{B} is a spanning set for $R/[R, R]$ by the previous observation that conjugate elements of G are equivalent modulo $[R, R]$, and it is linearly independent by the previous lemma. Conclude that \mathcal{B} is a basis for $R/[R, R]$. □

Lemma. Let $R = kG$ as above, k a field of characteristic $p \geq 0$, and let $J \subseteq I$ be such that $\{a_j : j \in J\}$ is a complete set of the p -regular conjugacy class representatives of G . Suppose that k is a splitting field for G . Then $\{a_j + T(R) : j \in J\}$ is a k -basis for $R/T(R)$.

Proof. If $p = 0$, then $\text{rad } R = 0$ and $T(R) = [R, R]$. All conjugacy classes are 0-regular by convention, so in this case $J = I$ and we are done by the previous corollary.

Suppose $p > 0$. Let $g \in G$. By a previous lemma, $g = g_p g_{p'} = g_{p'} g_p$ for uniquely determined $g_p, g_{p'} \in G$, with $g_{p'}$ a p -regular element and g_p a p -singular element. Say $|g_{p'}| = p^k$. Then

$$(g - g_{p'})^{p^k} = g^{p^k} - g_{p'}^{p^k} = (g_p g_{p'})^{p^k} - g_{p'}^{p^k} = g_p^{p^k} g_{p'}^{p^k} - g_{p'}^{p^k} = g_{p'}^{p^k} - g_{p'}^{p^k} = 0$$

So $g - g_{p'}$ is a nilpotent element of R , hence is an element of $T(R)$ by a result of §3.7. So $g \equiv g_{p'} \pmod{T(R)}$. We already established that conjugate elements of G are equivalent modulo $[R, R]$. Conclude that $\{a_j + T(R) : j \in J\}$ is a spanning set for $T(R)$.

Suppose $\sum_{j \in J} \epsilon_j a_j \in T(R)$. Say $\sum_{j \in J} \epsilon_j a_j = r + b$ for some $r \in \text{rad } R$, $b \in [R, R]$. Set $m = \text{lcm}\{|a_j| : j \in J\}$. Necessarily $p \nmid m$, i.e., $p \in \mathbb{Z}_m^*$, so $\exists N \in \mathbb{N}$ such that $p^N \equiv 1 \pmod{m}$. Set $q = p^N$. Then $a_j^q = a_j$ for each $j \in J$. Choose n large enough so that $r^q = 0$ (possible since $r \in \text{rad } R$ is nilpotent).

By a previous lemma $b^q \in [R, R]$. Now

$$\begin{aligned} 0 = r^q &= \left(\sum_j \epsilon_j a_j - b \right)^q \\ &\equiv \sum_j \epsilon_j^q a_j^q - b^q \\ &\equiv \sum_j \epsilon_j^q a_j \pmod{[R, R]} \end{aligned}$$

Then $\epsilon_j = 0, \forall j \in J$ by the previous lemma. Conclude that $\{a_j + T(R) : j \in J\}$ is a linearly independent subset of $T(R)$, hence is a k -basis for $T(R)$. \square

Theorem (Brauer). Let k be a field of characteristic $p \geq 0$. Suppose k is a splitting field for the group G . Then the number of simple kG -modules equals the number of p -regular conjugacy classes of G .

Proof. Let $R = kG$ as above. The case $\text{char } k = 0$ has already been established. Suppose $\text{char } k = p > 0$. We proved in §3.7 that the number of simple left kG -modules equals $\dim_k R/T(R)$. The result now follows from the previous lemma. \square

We now develop further the character theory for G . From now on, assume that k is a splitting field for G , and that $\text{char } k \nmid |G|$. For a kG -module M , let $\rho : kG \rightarrow \text{End}(M)$ denote the given representation. Recall that χ_M is defined by $\chi_M(g) = \text{tr } \rho(g)$ for all $g \in G$. We make the immediate observation that if $g, h \in G$, then

$$\chi(hgh^{-1}) = \text{tr } \rho(hgh^{-1}) = \text{tr } \rho(g)\rho(h)\rho(g^{-1}) = \text{tr } \rho(h)\rho(g^{-1})\rho(g) = \text{tr } \rho(hg^{-1}g) = \chi(h)$$

i.e., χ is constant on conjugacy classes of G .

Let $R = kG$ as above, and recall the notations from the beginning of this section. By our assumption that $\text{char } k \nmid |G|$ and that k is a splitting field for G , we have $D_i = k$ and $n_i = \dim_k M_i$ for all $1 \leq i \leq r$. Write $\chi_i = \chi_{M_i}$. Let $\{e_i : 1 \leq i \leq r\}$ be the central idempotents in R giving the decomposition of R into its simple components, $R \cong Re_1 \times \cdots \times Re_r$. Then e_i acts on M_j as δ_{ij} .

Remark. Let $\{\mathcal{C}_i : 1 \leq i \leq r\}$ be a complete list of the conjugacy classes of G , and let $c_i = \sum_{g \in \mathcal{C}_i} g$. Then $\{c_i : 1 \leq i \leq r\}$ and $\{e_i : 1 \leq i \leq r\}$ are two k -bases for $Z(kG)$.

Remark. The character of the left regular module kG is given by $\chi_{reg} = \sum_{i=1}^r n_i \chi_i$. For $g \in G$, we have

$$\chi_{reg}(g) = \begin{cases} |G| & g = 1 \\ 0 & g \neq 1 \end{cases}$$

Theorem. With the notations as above,

1. $e_i = |G|^{-1} n_i \sum_{g \in G} \chi_i(g^{-1})g$. (So $\text{char } k \nmid n_i, \forall 1 \leq i \leq r$.)
2. $c_g = |\mathcal{C}_g| \sum_{i=1}^r \chi_i(g) \frac{1}{n_i} e_i$ (where \mathcal{C}_g denotes the conjugacy class of g in G).

Proof.

1. Let $g \in G$. Write $e_i = \sum_{h \in G} a_h h$ for some $a_h \in k$. Now

$$a_g |G| = \chi_{reg}(g^{-1} e_i) = \sum_{j=1}^r n_j \chi_j(g^{-1} e_i) = n_i \chi_i(g^{-1})$$

by the previous remark that $\chi_{reg} = \sum_{i=1}^r n_i \chi_i$ and the fact that e_i acts on M_j as δ_{ij} .

2. Write $c_g = \sum_{i=1}^r b_i e_i$ for some $b_i \in k$. Now

$$|\mathcal{C}_g| \chi_j(g) = \chi_j(c_g) = \chi_j \left(\sum_{i=1}^r b_i e_i \right) = b_j n_j$$

by the previous remark that characters are constant on conjugacy classes of G , and that e_i acts on M_j as δ_{ij} . \square

We make the following notational convention: Given a character χ of kG and a conjugacy class \mathcal{C} of G , define $\chi(\mathcal{C}) = \chi(g)$ for any $g \in \mathcal{C}$. (This makes sense by a previous observation.)

Theorem (Character Orthogonality). With the notations as above,

1. $|G|^{-1} \sum_{g \in G} \chi_i(g^{-1}) \chi_j(g) = \delta_{ij}$
2. Let $\mathcal{C}, \mathcal{C}'$ be conjugacy classes of G . Then

$$\sum_{i=1}^r \chi_i(\mathcal{C}) \chi_i(\mathcal{C}') = \begin{cases} |G|/|\mathcal{C}| & \mathcal{C} = \mathcal{C}' \\ 0 & \mathcal{C} \neq \mathcal{C}' \end{cases}$$

Proof.

1. This follows by applying χ_j to the expression $e_i = |G|^{-1} n_i \sum_{g \in G} \chi_i(g^{-1})g$.

2. Combining the results of the previous theorem, we have

$$\begin{aligned} c_g &= |\mathcal{C}_g| \sum_{i=1}^r \chi_i(g) \frac{1}{n_i} \left(|G|^{-1} n_i \sum_{h \in G} \chi_i(h^{-1}) h \right) \\ &= \frac{|\mathcal{C}_g|}{|G|} \sum_{h \in G} \left(\sum_{i=1}^r \chi_i(g) \chi_i(h^{-1}) \right) h \end{aligned}$$

and the result follows. \square

Fix a set of representatives $\{a_j : 1 \leq j \leq r\}$ for the conjugacy classes of a group G . We construct an $r \times r$ matrix with ij entry equal to $\chi_i(a_j)$, and call it the character table of G (with respect to the splitting field k). If we let $a_1 = 1_G$, then the first column of the character table will always list the dimensions of the irreducible representations of G .

Example.

1. Let $G = S_3$. Let M_1 denote the trivial representation, $M_2 = k\langle e_1, \dots, e_n \rangle / k\langle e_1 + \dots + e_n \rangle$ as before, and sgn the sign representation. Recall that $\chi_{M_2}(g)$ is one less than the number of one-cycles in g .

χ	$\{1\}$	$\{(12)\}$	$\{(123)\}$
χ_{M_1}	1	1	1
χ_{M_2}	2	0	-1
χ_{sgn}	1	-1	1

2. Let $G = \langle g \rangle = C_n$, the cyclic group of order n . Note that each $g^i \in G$, $1 \leq i \leq n-1$ is its own conjugacy class. Fix a primitive n -th root of unity $\zeta \in \mathbb{C}$, and let $\rho_j : G \rightarrow \mathbb{C}$ denote the representation mapping $g \mapsto \zeta^j$ (so $\rho_j(g^i) = \zeta^{ij}$). Then $\{\rho_1, \dots, \rho_n\}$ is a complete list of irreducible $\mathbb{C}C_n$ -representations.

Definition. A function $\mu : G \rightarrow k$ is called a class function if $\mu(hgh^{-1}) = \mu(g), \forall g, h \in G$.

Let $F_k(G)$ denote the collection of class functions on G . Then $F_k(G)$ is a k -vector space of k -dimension r , r the number of conjugacy classes in G . Define a symmetric bilinear form on $F_k(G)$ by

$$\langle \mu, \nu \rangle = \frac{1}{|G|} \sum_{g \in G} \mu(g^{-1}) \nu(g)$$

Theorem. Let $\{\chi_i : 1 \leq i \leq r\}$ denote the collection of irreducible characters of G . Then $\{\chi_i : 1 \leq i \leq r\}$ is an orthonormal basis for $F_k(G)$ with respect to the inner product $\langle \cdot, \cdot \rangle$.

Proof. We certainly have $\{\chi_i : 1 \leq i \leq r\} \subseteq F_k(G)$ by the previous observation that class functions are constant on conjugacy classes of G . Moreover, we have that the χ_i are orthonormal with respect to the inner product $\langle \cdot, \cdot \rangle$ by the previous theorem, hence form a linearly independent set. Since $|\{\chi_i : 1 \leq i \leq r\}| = r = \dim_k F_k(G)$, we conclude that $\{\chi_i : 1 \leq i \leq r\}$ is an orthonormal basis for $F_k(G)$. \square

Note that $F_k(G)$ and $Z(kG)$ are dual with respect to the pairing $(\mu, \alpha) \mapsto \mu(\alpha)$, $\mu \in F_k(G)$, $\alpha \in Z(kG)$. Furthermore, $\{n_i^{-1}\chi_i : 1 \leq i \leq r\}$ and $\{e_i : 1 \leq i \leq r\}$ are dual bases with respect to this pairing.

Remark. Over $k = \mathbb{C}$, one can show that $\chi_i(g^{-1}) = \overline{\chi_i(g)}$, $\forall g \in G$, and the bilinear form $\langle \cdot, \cdot \rangle$ can be replaced by the Hermitian inner product $\langle \mu, \nu \rangle = |G|^{-1} \sum_{g \in G} \overline{\mu(g)} \nu(g)$.

Assume now that $\text{char } k = 0$. In this case kG is semisimple, and the character χ of a left kG -module M completely determines the composition factors of M .

Corollary. Let $\chi \in F_k(G)$ be the character of some kG -module M . Then $\langle \chi, \chi \rangle = 1$ if and only if χ is irreducible.

Proof. Write $\chi = \sum_{i=1}^r n_i \chi_i$. Then $1 = \langle \chi, \chi \rangle = \sum_{i=1}^r n_i^2$ if and only if $n_i = 1$ for some $1 \leq i \leq r$ and $n_j = 0$ for $i \neq j$, i.e., $\chi = \chi_i$ is irreducible. \square

Corollary. Two G -modules M, N are isomorphic if and only if $\chi_M = \chi_N$.

Proof. This is immediate. \square

Remark. There are several ways to produce new kG -modules.

1. Given a kG -module V , the dual space $V^* = \text{Hom}_k(V, k)$ becomes a G -module under the action $x \cdot f(v) = f(x^{-1}v)$, $\forall f \in V^*, x \in G, v \in V$.
2. Let G, H be finite groups, V a G -module, W an H -module. Then $V \otimes W$ becomes a $G \times H$ -module via the action $(g, h) \cdot (v \otimes w) = gv \otimes hw$ on simple tensors ($g \in G, h \in H, v \in V, w \in W$), and extending linearly.

Lemma. Let G, H be finite groups, V a G -module, W an H -module. The character of $V \otimes W$, denoted $\chi_V \otimes \chi_W$, is given by $(\chi_V \otimes \chi_W)(g, h) = \chi_V(g)\chi_W(h)$.

Proof. This follows from the definition of how $G \times H$ acts on $V \otimes W$. \square

Theorem. Let G, H be finite groups.

1. If V is an irreducible G -module, and W is an irreducible H -module, then $V \otimes W$ is an irreducible $G \times H$ -module.
2. If $\{V_i : 1 \leq i \leq r\}$ is a complete list of irreducible G -modules, and $\{W_j : 1 \leq j \leq s\}$ is a complete list of irreducible H -modules, then $\{V_i \otimes W_j : 1 \leq i \leq r, 1 \leq j \leq s\}$ is a complete list of irreducible $G \times H$ -modules.

Proof.

1. Observe that

$$\begin{aligned}
\langle \chi_V \otimes \chi_W, \chi_V \otimes \chi_W \rangle &= \frac{1}{|G \times H|} \sum_{(g,h) \in G \times H} \chi_V \otimes \chi_W((g, h)^{-1}) \cdot \chi_V \otimes \chi_W(g, h) \\
&= \frac{1}{|G \times H|} \sum_{(g,h) \in G \times H} \chi_V(g^{-1})\chi_W(h^{-1})\chi_V(g)\chi_W(h) \\
&= \left(\frac{1}{|G|} \sum_{g \in G} \chi_V(g^{-1})\chi_V(g) \right) \left(\frac{1}{|H|} \sum_{h \in H} \chi_W(h^{-1})\chi_W(h) \right) \\
&= \langle \chi_V, \chi_V \rangle \langle \chi_W, \chi_W \rangle = 1
\end{aligned}$$

Conclude that $V \otimes W$ is irreducible.

2. Let $\mathcal{B} = \{V_i \otimes W_j : 1 \leq i \leq r, 1 \leq j \leq s\}$ Mimicking the previous calculation, we have

$$\langle \chi_{V_i} \otimes \chi_{W_j}, \chi_{V_k} \otimes \chi_{W_l} \rangle = \delta_{ik} \delta_{jl}$$

so the elements of \mathcal{B} are mutually nonisomorphic irreducible $G \times H$ -modules. But there are precisely rs conjugacy classes in $G \times H$, so we conclude that \mathcal{B} is a complete list of irreducible $G \times H$ -modules. □

Corollary. Let G be a group, V an irreducible representation of G , V_1 a one-dimensional representation of G . Then $V \otimes V_1$ is an irreducible representation of G .

Proof. Note that since V_1 is a one-dimensional representation, we must have $\chi_{V_1}(g^{-1}) = \chi_{V_1}(g)^{-1}, \forall g \in G$. Then

$$\begin{aligned} \langle \chi_V \otimes \chi_{V_1}, \chi_V \otimes \chi_{V_1} \rangle &= \frac{1}{|G|^2} \sum_{g,h \in G} \chi_V \otimes \chi_{V_1}((g,h)^{-1}) \cdot \chi_V \otimes \chi_{V_1}(g,h) \\ &= \frac{1}{|G|^2} \sum_{g,h \in G} \chi_V(g^{-1}) \chi_{V_1}(h^{-1}) \chi_V(g) \chi_{V_1}(h) \\ &= \frac{1}{|G|^2} \sum_{g,h \in G} \chi_V(g^{-1}) \chi_V(g) \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_V(g^{-1}) \chi_V(g) \\ &= \langle \chi_V, \chi_V \rangle = 1 \end{aligned}$$

Conclude that $V \otimes V_1$ is irreducible. □

Example. Let $G = S_4$. Let M_1 denote the trivial module, $M_2 = k\langle e_1, \dots, e_n \rangle / k\langle e_1 + \dots + e_n \rangle$ as above.

χ	$\{1\}$	$\{(12)\}$	$\{(123)\}$	$\{(1234)\}$	$\{(12)(34)\}$
M_1	1	1	1	1	1
sgn	1	-1	1	-1	1
	2	0	-1	0	2
M_2	3	1	0	-1	-1
$M_2 \otimes \text{sgn}$	3	-1	0	1	-1

The entries of the unmarked row can be inferred from the character orthogonality relations, and the fact that the squares of the first column entries must sum to $24 = |S_4|$.

Let G be a group, $H \leq G$. A kG -module V may also be viewed as a kH -module by restricting the representation $\rho : G \rightarrow GL(V)$ to H . We call this the restriction of V to H , and denote it by $\text{Res}_H^G V = \text{Res}_H V$. Restriction induces a map $\text{res}_H^G : F_k(G) \rightarrow F_k(H)$, which simply restricts elements of $F_k(G)$ to kH .

Definition. Let H be a subgroup of the finite group G , and let V be a kH -module affording the representation ρ of H . The kG -module $\text{Ind}_H^G V = \text{Ind}^G V = kG \otimes_{kH} V$ is called the induced module of V and the representation of G it affords is called the induced representation of ρ . If ψ is the character afforded by V , then the character of the induced representation is called the induced character, and is denoted by $\text{Ind}_H^G(\psi)$.

Proposition. Retain the notations from above. Then:

1. Let k denote the trivial G -module. Then $\text{Ind}_{\{1\}}^G k \cong kG$, the left regular module.
2. Denote by 1_H the trivial kH -module. Then $\text{Ind}_H^G 1_H \cong k(G/H)$, the left coset representation of G .
3. Let L be a group, $H \leq G \leq L$, and let W be a kH -module. Then

$$\text{Ind}_G^L (\text{Ind}_H^G W) \cong \text{Ind}_H^L W$$

Theorem. Let V be a kH -module affording the matrix representation $\rho : H \rightarrow GL_n(k)$, and let g_1, \dots, g_m be representatives for the distinct left cosets of H in G . There exists a basis for the induced module $W = \text{Ind}_H^G V = kG \otimes_{kH} V$ of dimension $n \cdot [G : H]$ over k such that W affords the representation $\Phi : G \rightarrow GL_{n[G:H]}(k)$ defined for each $g \in G$ by the block matrix

$$\Phi(g) = [\rho(g_i^{-1}gg_j)]$$

where $\rho(g_i^{-1}gg_j)$ is an $n \times n$ block appearing in the ij block position of $\Phi(g)$, and where $\rho(g_i^{-1}gg_j)$ is defined to be the zero block whenever $g_i^{-1}gg_j \notin H$.

(Note that $\Phi(g)$ is a block permutation matrix in the sense that there is exactly one nonzero block in each row and column.)

Proof. Note that kG is a free right kH -module and $kG = g_1kH \oplus \dots \oplus g_mkH$. Then $W = kG \otimes_{kH} V \cong (g_1 \otimes V) \oplus \dots \oplus (g_m \otimes V)$. Let v_1, \dots, v_n be a basis of V affording the matrix representation $\rho : H \rightarrow GL_n(k)$. Then

$$\{g_1 \otimes v_1, g_1 \otimes v_2, \dots, g_1 \otimes v_n, g_2 \otimes v_1, \dots, g_2 \otimes v_n, \dots, g_m \otimes v_n\}$$

is an ordered basis for $W = \text{Ind}_H^G V$.

Fix $g \in G$, $1 \leq j \leq m$. Say $gg_j = g_i h$ for some $1 \leq i \leq m$ and $h \in H$, and say $\rho(h) = (a_{pq}) \in GL_n(k)$. Then for $1 \leq k \leq n$, we have

$$\begin{aligned} g(g_j \otimes v_k) &= (gg_j) \otimes v_k = g_i \otimes hv_k \\ &= \sum_{t=1}^n a_{tk}(g_i \otimes v_t) \end{aligned}$$

So $\Phi(g)$ maps the j -th block of basis vectors $g_j \otimes v_1, \dots, g_j \otimes v_n$ to the i -th block of basis vectors $g_i \otimes v_1, \dots, g_i \otimes v_n$, and then has the matrix $\rho(h)$ in that block. Since $h = g_i^{-1}gg_j$, this is precisely the action described by the matrix $\Phi(g)$. \square

Corollary. If ψ is the character afforded by V , then the induced character is given by

$$\text{Ind}_H^G(\psi) = \frac{1}{|H|} \sum_{x \in G} \psi(x^{-1}gx)$$

where $\psi(y) = 0$ if $y \notin H$.

Proof. Let $g \in G$. By the previous theorem,

$$\begin{aligned} \text{Ind}_H^G(\psi)(g) &= \sum_{i=1}^m \text{tr } \rho(g_i^{-1}gg_i) = \sum_{i=1}^m \psi(g_i^{-1}gg_i) \\ &= \frac{1}{|H|} \sum_{i=1}^m \sum_{h \in H} \psi(h^{-1}g_i^{-1}gg_i h) \\ &= \frac{1}{|H|} \sum_{x \in G} \psi(x^{-1}gx) \end{aligned}$$

because $g_i h$ ranges over G as (i, h) ranges over $\{1, \dots, m\} \times H$. \square

Theorem (Frobenius Reciprocity). Let H be a subgroup of the finite group G . Let $\psi \in F_k(H)$, $\varphi \in F_k(G)$. Then

$$\langle \text{Ind}_H^G \psi, \varphi \rangle_G = \langle \psi, \text{Res}_H^G \varphi \rangle_H$$

Proof. By the previous corollary we have

$$\begin{aligned} \langle \text{Ind}_H^G \psi, \varphi \rangle_G &= \frac{1}{|G|} \sum_{g \in G} \text{Ind}_H^G(\psi)(g) \varphi(g^{-1}) \\ &= \frac{1}{|G|} \sum_{g \in G} \frac{1}{|H|} \sum_{x \in G} \psi(x^{-1}gx) \varphi(g^{-1}) \\ &= \frac{1}{|G||H|} \sum_{x, y \in G} \psi(y) \varphi(xy^{-1}x^{-1}) \quad y = x^{-1}gx \\ &= \frac{1}{|G||H|} \sum_{\substack{y \in H \\ x \in G}} \psi(y) \varphi(y^{-1}) \\ &= \frac{1}{|H|} \sum_{y \in H} \psi(y) \varphi(y^{-1}) = \langle \psi, \text{Res}_H^G \varphi \rangle_H \end{aligned}$$

i.e., $\langle \text{Ind}_H^G \psi, \varphi \rangle_G = \langle \psi, \text{Res}_H^G \varphi \rangle_H$. \square

Example. Let $k = \mathbb{C}$, and let $D_n = \langle x, y : x^n = y^2 = 1, yx = x^{-1}y \rangle$ denote the Dihedral group of order $2n$. Note that $C_n = \langle x \rangle \triangleleft D_n$. Suppose n is even. We have the following

one-dimensional characters of D_n :

χ	x	y
ψ_1	1	1
ψ_2	1	-1
ψ_3	-1	1
ψ_4	-1	-1

Let $\epsilon = e^{2\pi i/n}$. Define $\rho^h : D_n \rightarrow GL_n(\mathbb{C})$ ($0 \leq h \leq n$) by

$$\rho^h(x^k) = \begin{bmatrix} e^{hk} & 0 \\ 0 & e^{-hk} \end{bmatrix}, \quad \rho^h(yx^k) = \begin{bmatrix} 0 & e^{-hk} \\ e^{hk} & 0 \end{bmatrix}$$

We have the following character table of D_n (n even):

χ	$\{1\}$	$\{x^{n/2}\}$	$\{x^{\pm k}\}$	$\{yx^{2i} : \forall i\}$	$\{yx^{2i+1} : \forall i\}$
ψ_1	1	1	1	1	1
ψ_2	1	1	1	-1	-1
ψ_3	1	$(-1)^{n/2}$	$(-1)^k$	1	-1
ψ_4	1	$(-1)^{n/2}$	$(-1)^k$	-1	1
ρ^h	2	$2(-1)^h$	$\epsilon^{hk} + \epsilon^{-hk}$	0	0

where in the third column we let $1 \leq k \leq \frac{n}{2} - 1$, and in the last row we let $1 \leq h \leq \frac{n}{2} - 1$.

Exercises for §8

3.8.1. Give an example of a pair of finite groups G, G' such that for some field k , $kG \cong kG'$ as k -algebras, but $G \not\cong G'$ as groups.

Proof. Let $k = \mathbb{C}$. Let $G = C_4$ the cyclic group of order 4, and let $G' = V_4$ the Klein 4-group. Then $kG \cong \bigoplus_{i=1}^4 \mathbb{C} \cong kG'$, but $G \not\cong G'$. \square

3.8.2. Let k be a field whose characteristic is prime to the order of the finite group G . Show that the following statements are equivalent:

1. Each irreducible kG -module has k -dimension 1.
2. G is abelian, and k is a splitting field for G .

3.8.5. For any field k and for any normal subgroup H of a group G , show that $kH \cap \text{rad } kG = \text{rad } kH$.

Proof.

Let $\{g_i : i \in I\}$ be a complete set of right coset representatives for H in G , with $g_{i_0} = 1$. Let $I' = I \setminus \{i_0\}$. Then as a left kH -module, $kG = kH \oplus (\bigoplus_{i \in I'} kH g_i)$, i.e., kH is a direct summand of kG as a kH -module. Then $kH \cap \text{rad } kG \subseteq \text{rad } kH$.

Let V be a simple left kG -module. By Clifford's Theorem, V is semisimple as a left kH -module. Say $V = \bigoplus_j M_j$ for simple left kH -modules M_j . Then $(\text{rad } kH) \cdot V = \bigoplus_j (\text{rad } kH) \cdot M_j = \{0\}$. Then $\text{rad } kH \subseteq kH \cap \text{rad } kG$. Conclude $\text{rad } kH = kH \cap \text{rad } kG$. \square

Exercise. Let $k = \mathbb{C}$, $D_n = \langle x, y : x^n = y^2 = 1, yx = x^{-1}y \rangle$ the dihedral group of order $2n$, and $\epsilon = e^{2\pi i/n}$. D_n contains the cyclic group $C_n = \langle x \rangle$ as a subgroup. Denote by σ^h ($0 \leq h \leq n$) the one-dimensional irreducible representation of the cyclic group C_n defined by $\sigma^h(x) = e^h$. Define $\rho^h : D_n \rightarrow GL_n(\mathbb{C})$ ($0 \leq h \leq n$) by

$$\rho^h(x^k) = \begin{bmatrix} e^{hk} & 0 \\ 0 & e^{-hk} \end{bmatrix}, \quad \rho^h(yx^k) = \begin{bmatrix} 0 & e^{-hk} \\ e^{hk} & 0 \end{bmatrix}$$

Show that

1. ρ^h is a representation of D_n .
2. $\rho^h \cong \text{Ind}_{C_n}^{D_n} \sigma^h$
3. $\rho^h \cong \rho^{n-h}$

Below in (4) and (5) we assume that n is even.

4. ρ^h is irreducible unless $h = 0, n/2$.
5. $\rho^0 = \psi_1 + \psi_2$ and $\rho^{n/2} = \psi_3 + \psi_4$ where ψ_i are the four one-dimensional representations of D_n defined in the lectures.
6. For D_n with n odd, formulate similar statements as in (4),(5), and determine the character table.

Chapter 7

Local Rings, Semilocal Rings, and Idempotents

7.19 Local Rings

Theorem. The following are equivalent for a ring R :

1. R has a unique maximal left ideal.
2. R has a unique maximal right ideal.
3. $R/\text{rad } R$ is a division ring.

If R satisfies any of these conditions, call R a local ring.

Proof. It suffices to prove (1) \Leftrightarrow (3). The equivalence (2) \Leftrightarrow (3) will follow by symmetry.

(1) \Rightarrow (3): If R has a unique maximal left ideal M , then $\text{rad } R = M$ and $R/\text{rad } R$ has precisely two left ideals: $\{0\}$ and $R/\text{rad } R$. Conclude that $R/\text{rad } R$ is a division ring.

(3) \Rightarrow (1): Suppose $R/\text{rad } R$ is a division ring. $R/\text{rad } R$ has precisely two left ideals, $\{0\}$ and $R/\text{rad } R$, so $\text{rad } R$ must be a maximal left ideal of R . But $\text{rad } R$ is the intersection of all maximal left ideals in R , so we conclude that $\text{rad } R$ is the only maximal left ideal in R . \square

Properties of a Local Ring R :

1. R has a unique maximal left ideal $M = \text{rad } R = R \setminus \mathcal{U}(R)$.
2. R has no nontrivial idempotents: Suppose $e \in R$ is an idempotent. If $e \in R^*$, then $e = e(ee^{-1}) = ee^{-1} = 1$. If $e \notin R^*$, then $e \in \text{rad } R \Rightarrow 1 - e \in R^* \Rightarrow e(1 - e) = 0 \Rightarrow e = 0$.

Example. Let k be a field, V an n -dimensional k -vector space, $R = \bigwedge(V)$ the exterior algebra on V . Then R is a local ring with unique maximal left ideal $M = \text{rad } R = \bigwedge^1(V) \oplus \cdots \oplus \bigwedge^n(V)$.

Lemma (Fitting Decomposition). Let R be a ring, and let M be a left R -module that admits a composition series. Let $f \in \text{End}({}_R M)$. Then $M = \ker f^r \oplus \text{im } f^r$ for some $r \gg 0$.

Proof. Since ${}_R M$ admits a composition series, it has the ACC and DCC on submodules. Consider the chains $\ker f \subseteq \ker f^2 \subseteq \dots$ and $\operatorname{im} f \supseteq \operatorname{im} f^2 \supseteq \dots$. Choose $r \in \mathbb{N}$ large enough that both chains stabilize. Then for all $x \in M$, $f^r(x) = f^{2r}(y)$ for some $y \in M$. Now $x = f^r(y) + (x - f^r(y)) \in \operatorname{im} f^r + \ker f^r$. Suppose $f^r(x) \in \ker f^r$. Then $0 = f^{2r}(x) \rightarrow x \in \ker f^{2r} = \ker f^r \Rightarrow f^r(x) = 0$. Conclude that the decomposition $M = \ker f^r + \operatorname{im} f^r$ is direct, i.e., $M = \ker f^r \oplus \operatorname{im} f^r$. \square

Lemma. Let R be a ring, and let ${}_R M$ be an indecomposable left R -module that admits a composition series. Then $\operatorname{End}({}_R M)$ is a local ring.

Proof. Let I be a maximal left ideal of $E = \operatorname{End}({}_R M)$. Let $a \in E \setminus I$. Then $E = Ea + I$ by the maximality of I . Write $1 = ga + f$ for some $g \in E$, $f \in I$. Since $f \in I$, f cannot be an isomorphism of M . In particular, f and hence also f^r is not surjective. By Fitting's Lemma, $\exists r \in \mathbb{N}$ such that $M = \ker f^r \oplus \operatorname{im} f^r$. Since $\operatorname{im} f^r \neq M$, we conclude $\ker f^r = M$ and $\operatorname{im} f^r = \{0\}$ by the indecomposability of M . Now $ga = 1 - f$ and $(1 + f + \dots + f^{r-1})ga = 1$, i.e., a is left invertible. Conclude that I is the unique maximal left ideal of E and $E = \operatorname{End}({}_R M)$ is a local ring. \square

Proposition. Let R be a ring and M a left R -module whose submodules satisfy either the ACC or the DCC. Then there exists a decomposition of M into a finite direct sum of indecomposable submodules $M = M_1 \oplus \dots \oplus M_m$. Call such a decomposition of M a Krull–Schmidt decomposition of M . In particular, any finitely generated module over a left artinian ring has a Krull–Schmidt decomposition.

Proof. Call a submodule $N \subseteq M$ “good” if it has a Krull–Schmidt decomposition, and call a submodule “bad” if it does not. Note that the zero submodule is good, as is any indecomposable submodule. If $N, N' \subseteq M$ are good and $N \cap N' = \{0\}$, then $N + N' = N \oplus N'$ is good.

Suppose M is bad. Then in particular M itself is not indecomposable, and we can write $M = M_1 \oplus M'_1$ for some submodules $M_1, M'_1 \neq \{0\}$ of M . Now at least one of M_1, M'_1 must be bad, say M_1 . Then $M_1 = M_2 \oplus M'_2$ for some submodules $M_2, M'_2 \neq \{0\}$ of M_1 . Repeating this process we obtain infinite chains of submodules

$$M \supsetneq M_1 \supsetneq M_2 \supsetneq M_3 \supsetneq \dots \quad \text{and} \quad \{0\} \subsetneq M'_1 \subsetneq M'_1 \oplus M'_2 \subsetneq M'_1 \oplus M'_2 \oplus M'_3 \subsetneq \dots$$

in contradiction to the fact that the submodules of M satisfy either the ACC or the DCC. Conclude that M is good, i.e., M has a Krull–Schmidt decomposition. \square

Theorem (Krull–Schmidt). Let R be a ring, and let M be a left R -module that admits a composition series. Suppose M has two Krull–Schmidt decompositions

$$M = M_1 \oplus \dots \oplus M_m = M'_1 \oplus \dots \oplus M'_n$$

Then $m = n$, and after reordering, $M_i \cong M'_i$ for all $1 \leq i \leq m$.

Proof.

We argue by way of induction on m , the case $m = 1$ being trivial. Note that if M admits a composition series, then so do each M_i, M'_j , so $\operatorname{End}({}_R M_i), \operatorname{End}({}_R M'_j)$ are local rings by the previous lemma.

Consider the projections $\alpha_i : M \rightarrow M_i$, $\beta_j : M \rightarrow M'_j$ in $\text{End}({}_R M)$. Then $1 = \alpha_1 + \cdots + \alpha_m = \beta_1 + \cdots + \beta_n$, so $\alpha_1 = \alpha_1\beta_1 + \cdots + \alpha_1\beta_n$. Restricting to M_1 , $\text{id}_{M_1} = \sum_{j=1}^n \alpha_1\beta_j|_{M_1}$. Now some $\alpha_1\beta_j|_{M_1}$, say $\alpha_1\beta_1|_{M_1}$ must be a unit in $\text{End}({}_R M_1)$, for otherwise each $\alpha_1\beta_j|_{M_1} \in \text{rad } \text{End}({}_R M_1)$ (because $\text{End}({}_R M_1)$ is a local ring), which implies that $\text{id}_{M_1} = \sum_{j=1}^n \alpha_1\beta_j|_{M_1} \in \text{rad } \text{End}({}_R M_1)$, a contradiction.

To say that $\alpha_1\beta_1|_{M_1}$ is a unit in $\text{End}({}_R M_1)$ is to say that $\alpha_1\beta_1 : M_1 \rightarrow M_1$ is an automorphism. Then $\beta_1 : M_1 \rightarrow M'_1$ is a split monomorphism (i.e., an injection with a left inverse). Conclude by the indecomposability of M'_1 that $\beta_1 : M_1 \rightarrow M'_1$ is an isomorphism.

Since $\beta_1 : M_1 \rightarrow M'_1$ is an isomorphism, M_1 has trivial intersection with $\ker \beta_1 = M'_2 \oplus \cdots \oplus M'_n$. Let $a \in M'_1$ and write $a = \beta_1(b)$ for some $b \in M_1$. Then $\beta_1(a - b) = a - \beta_1(b) = a - a = 0$, i.e., $a - b \in \ker \beta_1 = M'_2 \oplus \cdots \oplus M'_n$. Then $a \in M_1 \oplus M'_2 \oplus \cdots \oplus M'_n$. Conclude $M = M_1 \oplus M'_2 \oplus \cdots \oplus M'_n$.

Now $M_2 \oplus \cdots \oplus M_m \cong M/M_1 \cong M'_2 \oplus \cdots \oplus M'_n$. Applying the induction hypothesis, $m = n$ and the M_i are unique up to ordering. \square

7.21 The Theory of Idempotents

Let R be a ring.

Definition. An idempotent $e \in R$ is called primitive if it is not a sum of orthogonal idempotents.

Recall that $1 = e_1 + \cdots + e_n$ for orthogonal idempotents $e_i \in R$ if and only if the left regular module ${}_R R$ decomposes as a direct sum of left ideals $R = Re_1 \oplus \cdots \oplus Re_n$. The idempotent e_i is primitive if and only if Re_i is an indecomposable left ideal.

Lemma. Let M be a left R -module, and let $e \in R$ be an idempotent.

1. There exists an additive group isomorphism $eM \cong \text{Hom}_R(Re, M)$.
2. There exists a ring anti-isomorphism $eRe \cong \text{End}({}_R Re)$.

Proof.

1. Define $f : eM \rightarrow \text{Hom}_R(Re, M)$ by $em \mapsto f_{em}$ where $f_{em} : Re \rightarrow M$ is defined by $f_{em}(ae) = aem$. It is clear that f is an additive map, while $f_{em} : Re \rightarrow M$ is an R -module homomorphism. Define $g : \text{Hom}_R(Re, M) \rightarrow eM$ by $g(\alpha) = \alpha(e) = \alpha(ee) = e\alpha(e) \in eM$. It is clear that g is an additive map.

Let $m \in M$, $\alpha \in \text{Hom}_R(Re, M)$. Then $(g \circ f)(em) = g(f_{em}) = f_{em}(e) = e(em) = m$ and $(f \circ g)(\alpha) = f(\alpha(e)) = f_{\alpha(e)} = \alpha$, since for $r \in R$, $f_{\alpha(e)}(re) = re\alpha(e) = \alpha(re) = \alpha(re)$. Conclude that f, g are inverse isomorphisms.

2. It suffices to show that f is a ring anti-homomorphism in the case $M = Re$. Let $r, s, a \in R$. Then

$$f((ere)(ese))(ae) = f_{eres}(ae) = (ae)(eres) = f_{ese}(aere) = f_{ese}(f_{ere}(ae))$$

i.e., $f((ere)(ese)) = f(ese)f(ere)$, so f is a ring anti-isomorphism. \square