Rings and Modules

Labix

April 24, 2024

Abstract

- Abstract Alebra by Thomas W. Judson

Contents

1 More on Rings

1.1 Isomophism Theorem for Rings

The isomorphism theorem for rings is a direct result that extends the group isomorphism theorems.

Their proofs are mostly the same except that we also have to check that multplication is preserved so that the isomorphisms inherited from groups is indeed a ring isomorphism.

Theorem 1.1.1: The First Isomorphism Theorem for Rings

If $\phi : R \to S$ is a homomorphism of rings, then $\ker(\phi)$ is an ideal of R, $\text{im}(\phi) \leq S$ and

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

in rings.

Proof. A group isomorphism $R/\ker(\phi) \cong \phi(R)$ can be established from the first isomorphism theorem for groups. Moreover we know that $\ker(\phi)$ is a normal subgroup. To show that $\ker(\phi)$ is an ideal, notice that for $r \in R$ and $k \in \ker\phi$, $\phi(rk) = \phi(r)\phi(k) = 0$ thus $rk \in \ker(\phi)$. To show that $R/\ker(\phi) \cong \phi(R)$ is a ring isomorphism, suppose that π is the induced group isomorphism. Notice that

$$\begin{aligned}\pi((r_1 + \ker(\phi))(r_2 + \ker(\phi))) &= \pi(r_1 r_2 + \ker(\phi)) \\ &= \phi(r_1 r_2) \\ &= \phi(r_1)\phi(r_2) \\ &= \pi(r_1 + \ker(\phi))\pi(r_2 + \ker(\phi))\end{aligned}$$

□

Theorem 1.1.2: The Second Isomorphism Theorem for Rings

Let $A \leq R$ and B an ideal of R. Then $A + B = \{a + b | a \in A, b \in B\}$ is a subring of R. $A \cap B$ is an ideal of A and

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

Theorem 1.1.3: The Third Isomorphism Theorem for Rings

Let I, J be ideals of R with $I \subset J$. Then J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$

Theorem 1.1.4: The Fourth Isomorphism Theorem for Rings

Let I be an ideal of R. The correspondence between A and A/I is an inclusion preserving bijection between the set of subrings A of R that contain I and the set of subrings of R/I. Furthermore, A is an ideal of R if and only if A/I is an ideal of R/I.

1.2 Chinese Remainder Theorem

In this section we develop the necessary notions in order to illustrate the Chinese Remainder Theorem.

Definition 1.2.1: Direct product of Rings

Let R, S be rings. Define the direct product of R and S to be $R \times S$. Elements of $R \times S$ are of the form (r, s) where $r \in R$ and $s \in S$.

Proposition 1.2.2

Let R, S be rings. Define addition as

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$$

and

$$(r_1, s_1) \cdot (r_2, s_2) = (r_1 r_2, s_1 s_2)$$

and $0 = (0, 0)$ and $1 = (1, 1)$. Then $R \times S$ is a ring. In particular, if $R_1, \ldots, R_n$ are rings. Then $R_1 \times \cdots \times R_n$ is also a ring.

A rather unintuitive definition is that of coprime ideals.

Definition 1.2.3: Coprime Ideals

We say that two ideals A, B in a ring R are coprime if $A + B = R$.

But there is indeed a good reason for the name. Notice that in $\mathbb{Z}$, the prime ideals are exactly the ideals (p) where p is a prime. We also have a nice inclusion of ideals whenever $p|a$ which is $(a) \subseteq (p)$, which we will prove later. This means that in general, the smaller the number a is, the larger the ideal (a) is and indeed, the smaller the number is in $\mathbb{Z}$, the more numbers it can possibly divide. Now recall that if a and b are coprime in $\mathbb{Z}$, then their gcd will be 1. Indeed we will develop the notion of gcd for ideals as well, which is to say that if $d = \gcd(a, b)$ in the usual sense, then $(a) \subseteq (d)$ and $(b) \subseteq (d)$. Then if a and b are coprime, their ideals are both subsets of (1), which is exactly R. This leads to why we say that two ideals are coprime.

Proposition 1.2.4

Let A, B be ideals of a ring R. If A and B are coprime then

$$AB = A \cap B$$

Theorem 1.2.5: Chinese Remainder Theorem

Let $I_1, \ldots, I_n$ be ideals of a ring R. Then the ring homomorphism

$$\phi : A \to A/I_1 \times \cdots \times A/I_n$$

defined by $\phi(x) = (x + I_1, \ldots, x + I_n)$ has kernel

$$I = \bigcap_{k=1}^{n} I_k$$

Lemma 1.2.6: Chinese Remainder Theorem Abstract Form

Let $I_1, \ldots, I_n$ be ideals of a ring R. Let $I = \bigcap_{k=1}^{n} I_k$. If each pair of ideals is coprime, then

$$\phi : R/I \to R/I_1 \times \cdots \times R/I_n$$

is a ring isomorphism. In other words,

$$R/I \cong R/I_1 \times \cdots \times R/I_n$$

Proof. Since $I_1, \ldots, I_n$ are pairwise coprime, we must have $I = I_1 \cdots I_n$. By the first isomorphism theorem for rings, we have that $R/(I_1 \cdots I_n) \cong \phi(R)$ and thus

$$R/I \cong R/I_1 \times \cdots \times R/I_n$$

□

1.3 Graded Rings

Definition 1.3.1: Graded Rings

A graded ring R is a ring such that the underlying additive group is a direct sum of abelian groups R_i, meaning that

$$R = \bigoplus_{n \in \mathbb{N}} R_n$$

and such that for $r_i \in R_i$ and $r_j \in R_j$, $r_i r_j \in R_{i+j}$. A $\mathbb{Z}$ graded ring is a ring graded in $\mathbb{Z}$ instead of $\mathbb{N}$.

Proposition 1.3.2

The following are true for a graded ring $R = \bigoplus_{n \in \mathbb{N}} R_i$.

- R_0 is a subring of R
- R_n is an R_0-module for each n
- R is an R_0-module

Proof.

- R_0 is an abelian group by definition. We also have that $r_0 \in R_0$ and $s_0 \in R_0$ implies $r_0 s_0 \in R_0$ which means that multiplication is closed.
- We have that for $r_0 \in R_0$ and $r_n \in R_n$, $r_0 \cdot r_n \in R_n$
- Since each R_n is a R_0-module, the direct sum R is also an R_0 module.

□

Definition 1.3.3: Homogenous Ideals

An ideal I of a graded ring R is said to be homogenous if for each $a \in I$, the homogenous components of a is in I.

Proposition 1.3.4

If I is an homogenous ideal of a graded ring R, then R/I is also a graded ring.

2 Module Theory

2.1 Introduction to Modules

Definition 2.1.1: Modules

Let R be a ring. A left R-module or a left module over R is a set M together with

- A binary operation $+$ on M under which M is an abelian group
- An action of R on M denoted by $\cdot : R \times M \to M$ and $(r, m) \mapsto r \cdot m$ such that
  - $(r + s) \cdot m = r \cdot m + s \cdot m$ for all $r, s \in R$, $m \in M$
  - $(rs) \cdot m = r \cdot (s \cdot m)$ for all $r, s \in R$, $m \in M$
  - $r \cdot (m + n) = r \cdot m + r \cdot n$ for all $r, s \in R$, $m \in M$
  - $1 \cdot m = m$ for all $m \in M$ if $1 \in R$

A right R-module consists of the same axioms except that the action is on the right, meaning that the action of R on an abelian group M is the map $\cdot : M \times R \to M$.

Notice that while most of the time we exclusively work with left R-modules, all results are valid also to right R-modules because every right R-module is actually a left R^{op} module and vice versa. R^{op} here means that the abelian group is the same: $(R^{\text{op}}, +, \cdot_{R^{\text{op}}})$ is defined to be $(R^{\text{op}}, +) = (R, +)$ and

$$a \cdot_{R^{\text{op}}} b = b \cdot_R a$$

for all $a, b \in R$.

Definition 2.1.2: Submodules

Let R be a ring and let M be an R-module. An R-submodule of M is an abelian subgroup N of M which is closed under the action of ring elements, meaning $rn \in N$ for all $r \in R$, $n \in N$.

Proposition 2.1.3: Submodule Criterion

Let R be a ring and let M be an R-module. A subset N of M is a submodule of M if and only if

- $N \neq \emptyset$
- $x + ry \in N$ for all $r \in R$ and all $x, y \in N$

Proposition 2.1.4: Sum of Submodules

Let M, N be left R-submodules of an R-module K. Then the sum

$$M + N = \{m + n | m \in M, n \in N\}$$

is a left R-submodule of K. Moreover, M, N are both R-submodules of $M + N$.

Proposition 2.1.5: Intersection of Modules

Let M, N be left R-modules. Then the intersection $M \cap N$ is a left R-submodule of both M and N.

2.2 Module Homomorphisms

Definition 2.2.1: R-Module Homomorphisms

Let R be a ring and let M and N be left R-modules. A map $\phi : M \to N$ is an R-module homomorphism if

- $\phi : M \to N$ is a homorphism of the underlying abelian group
- $\phi(am) = a\phi(m)$ for $a \in R$ and $m \in M$

We say that ϕ is a R-module isomorphism if it is bijective.

Definition 2.2.2: Kernel and Image

Let R be a ring and let M and N be R-modules. Let $\phi : M \to N$ be a R-module homomorphism. Define

- the kernel of ϕ to be $\ker(\phi) = \{m \in M | \phi(m) = 0\}$
- the image of ϕ to be $\text{im}(\phi) = \{n \in N | n = \phi(m) \text{ for some } m\}$

Proposition 2.2.3: Quotient Module

Let R be a ring. Let M be a left R-module and let N be a submodule of M. Then the quotient group M/N is a left R-module.

2.3 Isomorphism Theorem for Modules

Similar to the isomorphism theorem for rings, the isomorphism theorem for modules extends the definition of the original isomorphism for groups. Therefore most of the time we just have to check the compatibility of the isomorphism theorems with the ring action on the abelian group.

Theorem 2.3.1: First isomorphism Theorem for Modules

Let M, N be left R-modules and let $\psi : M \to N$ be an R-mdoule homomorphism. Then the following are true.

- $\ker(\phi)$ is a submodule of M
- $\text{im}(\phi)$ is a submodule of N
- $M/\ker(\phi) \cong \phi(M)$

Proof. We have seen all these statements for groups. We just have to show that the statements are compatible with the left action of the left R-module structure.

- Let $r \in R$ and $m \in \ker(\phi)$. Then $\phi(r \cdot m) = r \cdot \phi(m) = 0$ and thus $r \cdot m \in \ker(\phi)$
- Let $r \in R$ and $n \in \text{im}(\phi)$. Then $r \cdot \phi(n) = \phi(r \cdot n)$ implies $r \cdot n$ lies in the image of ϕ
- Let $r \in R$ and $m + \ker(\phi) \in M/\ker(\phi)$. Denote the group isomorphism $\overline{\phi} : M/\ker(\phi) \to \text{im}(\phi)$ defined by $m + \ker(\phi) \mapsto \phi(m)$. Then we have

$$\begin{aligned} \overline{\phi}(r \cdot (m + \ker(\phi))) &= \overline{\phi}(r \cdot m + \ker(\phi)) \\ &= \phi(r \cdot m) \\ &= r \cdot \phi(m) \end{aligned}$$

Thus they all are compatible with left multiplication. □

Theorem 2.3.2: Second isomorphism Theorem for Modules

Let A, B be left R-submodules of an R-module M. Then we have the following isomorphism of quotient R-modules:

$$\frac{A+B}{B} \cong \frac{A}{A \cap B}$$

Proof. Consider the composition of R-module homomorphisms $\phi : A \to A + B \to \frac{A+B}{B}$ defined by $a \mapsto a + B$. It is a homomorphism since it is the composition of the inclusion and the quotient map. This maps is surjective since for any $(a + b) + B$, we have that $(a + b) + B = a + B$ and thus $a \in A$ maps to this element.

I claim that $\ker(\phi) = A \cap B$. If $a \in \ker(\phi)$ then $a + B = B$ implies that $a \in A$. Thus $a \in A \cap B$. If $a \in A \cap B$ then clearly $\phi(a) = a + B = B$. By the first isomorphism theorem, we have that

$$\frac{A+B}{B} \cong \frac{A}{A \cap B}$$

and we are done. □

Theorem 2.3.3: Third isomorphism Theorem for Modules

Let M be a left R-module. Let A be an R-submodule of M and B an R-submodule of A. Then we have the following isomorphism of quotient R-modules:

$$\frac{M/B}{A/B} \cong \frac{M}{A}$$

Theorem 2.3.4: Correspondence Theorem for Modules

Let N be a submodule of the R-module M. There is a bijection between the submodules of M which contain N and the submodules of M/N. The correspondence is given by A to A/N for all $A \supseteq N$. This correspondence commutes with the processes of taking sums and intersections.

2.4 The Endomorphism Ring

Definition 2.4.1: Endomorphisms of a Module

Let R be a ring and M a left R-module. An endomorphism of M is a homomorphism $\phi : M \to M$. Denote the set of all R-endomorphisms by $\text{End}_R(M)$.

Proposition 2.4.2

Let R be a ring and M a left R-module. Then $\text{End}_R(M)$ is a ring.

Proof. Let $\phi, \psi \in \text{End}_R(M)$. Define $\phi + \psi : M \to M$ by $m \mapsto \phi(m) + \psi(m)$. We first show that $\text{End}_R(M)$ is a group.

- Since M is associative as an additive group, associativity follows
- Clearly the zero map $0 \in \text{End}_R(M)$ acts as the additive inverse since for any $\phi \in \text{End}_R(M)$, we have that $\phi(m) + 0 = 0 + \phi(m) = \phi(m)$ since 0 is the additive identity for M
- For every $\phi \in \text{End}_R(M)$, the map taking m to $-\phi(m)$ also lies in $\text{End}_R(M)$. Since $-\phi(m)$ is the inverse of $\phi(m)$ in M, we have that $-\phi$ is the inverse of ϕ

Now define $\phi \cdot \psi \in \text{End}_R(M)$ by $m \mapsto \phi(\psi(m))$. We show the remaining axioms for a ring.

- Since composition of functions is associative, associativity follows
- The identity map id acts as the identity since composition of any map with identity is itself
- Since $\phi \in \text{End}_R(M)$ is a module homomorphism, we have

$$\phi((\psi + \varphi)(m)) = \phi(\psi(m) + \varphi(m)) = \phi(\psi(m)) + \phi(\varphi(m))$$

  and thus distributivity is satisfied.

Thus we are done. □

Lemma 2.4.3

Let R be a ring. Then R is a left R-module. Moreover, $\text{End}_R(R) \cong R$.

Proof. Clearly R is a left R-module where the left action is just left multiplication.

Define a map $\phi : R \to \text{End}_R(R)$ by $r \mapsto \phi(r)(x) = x \cdot r$. We check that ϕ is a ring homomorphism.

- ϕ preserves addition since

$$\begin{aligned} \phi(r+s)(x) &= x \cdot (r+s) \\ &= x \cdot r + x \cdot s \\ &= \phi(r)(x) + \phi(s)(x) \end{aligned}$$

- ϕ preserves identity since $\phi(1)(x) = x \cdot 1 = x$ is just the identity map
- ϕ preserves multiplication since

$$\begin{aligned} \phi(rs) &= x \cdot (rs) \\ &= (x \cdot r) \cdot s \\ &= \phi(s)(x \cdot r) \\ &= \phi(s)(\phi(r)(x)) \end{aligned}$$

We also show that ϕ is bijective.

- The kernel ϕ is 0 because letting $r \in \ker(\phi)$, we have $\phi(r) = 0$. But we also know that $\phi(r)(1_R) = 1_R \cdot r$. Equating gives $r = 0$.
- Let $\eta \in \text{End}_R(R)$. Let $x \in R$. Then we have

$$\begin{aligned} \eta(x) &= \eta(x \cdot 1_R) \\ &= x \cdot \eta(1_R) && (\eta \text{ is a module homomorphism}) \\ &= \phi(\eta(1_R))(x) \end{aligned}$$

Thus ϕ is a ring isomorphism. □

2.5 Direct Sum of Modules

Definition 2.5.1: External Direct Sum of Modules

Let I be an indexing set and $\{M_i | i \in I\}$ be a family of R-modules. Define the direct sum of the family of modules to be

$$\prod_{i \in I} M_i = \{(m_i)_{i \in I} | m_i \in M_i \text{ and } m_i \neq 0 \text{ for finitely many } i\}$$

Definition 2.5.2: Internal Direct Sum of Modules

Let I be an indexing set and $\{N_i | i \in I\}$ be a family of submodules of a left R-module M. The internal direct sum of the family of submodules is defined to be

$$\sum_{i \in I} N_i = \{a_1 + \cdots + a_n | a_i \in N_i\}$$

If $M = \sum_{i \in I} N_i$ then we say that M is the internal direct sum.

2.6 Free Modules

Definition 2.6.1: Basis

Let R be a ring and M a left R-module. Let $B \subseteq M$.

- We say that B is linearly independent if for every $\{b_1, \ldots, b_n\} \subseteq B$ such that

  $$\sum_{i=1}^{n} r_i b_i = 0_M$$

  we have that $r_1 = \cdots = r_n = 0_R$
- We say that B is a generating set of M if for all $m \in M$,

  $$m = \sum_{b \in B} r_b \cdot b$$

  for finitely many non zero r_b
- We say that B is a basis of M if B is both linearly independent and is a generating set of M.

Definition 2.6.2: Free R-Module

Let R be a ring and M a left R-module. We say that M is a free R-module if M has a basis.

Lemma 2.6.3

For every set B there is a free left R-module, denoted $\oplus_B R$ with basis of cardinality $|B|$.

Lemma 2.6.4

Every left R-module is isomorphic to a quotient of a free module.

Theorem 2.6.5

Let R be a division ring. Let M be a left R-module. Then

- M is a free R-module

- Every linearly independent subset $S \subseteq M$ can be extended to a basis
- Every generating set $Q \subseteq M$ contains a basis

2.7 Simple Modules

Definition 2.7.1: Simple Module

A left R-module M is simple if $M \neq 0$ and that 0 and M are the only submodules of M.

Lemma 2.7.2

If L is a maximal left ideal, then the left R-module R/L is simple.

Proof. By the correspondence theorem, ideals of R/L are in 1-1 correspondence to ideals of R that contains L. Since L is maximal, there exists no such ideals. Thus R/L has no ideals and thus no R-submodule. □

In particular, this means that every field $\mathbb{F}$ is a simple $\mathbb{F}$-module.

Theorem 2.7.3

Let R be a non-zero ring. Then R has a maximal left ideal.

Corollary 2.7.4

Every non-zero ring R has a simple left R-module.

Proof. Since every ring R has a maximal left ideal L, R/L is a non-trivial simple R-module by lemma 2.6.2. □

Proposition 2.7.5: Schur's Lemma I

Let $\phi : M \to N$ be a homomorphism of simple left R-modules. Then either $\phi = 0$ or ϕ is an isomorphism.

Proof. Suppose that $\phi \neq 0$. Since $\ker(\phi)$ is a submodule of M and M is simple, we must have that $\ker(\phi) = 0$. Then we must have that $\text{im}(\phi)$ is a non-trivial submodule of N. But since N is simple, $\text{im}(\phi) = M$. Thus ϕ is a bijection. □

Corollary 2.7.6: Schur's Lemma II

If M is a simple left R-module, then $\text{End}_R(M)$ is a division ring.

Proof. Let $\phi \in \text{End}_R(M)$ be non-zero. Since M is simple, Schur's lemma I tells us that ϕ is an isomorphism. Then it has an inverse. □

Theorem 2.7.7: Baby Artin-Wedderburn Theorem

Let R be a non-zero ring. Then every left R-module is free if and only if R is a division ring.

Proof. If R is a division ring, then every left R-module has basis by theorem 2.5.5. Now suppose that R is a non-zero ring such that every left R-module is free. By corollary 2.6.4, there exists a simple left R-module M. Let x be a basis element of M.

Consider the homomorphism $\pi : R \to M$ defined by $\pi(r) = rx$. Then $\ker(\pi) = 0$ otherwise there would be a linear dependency on the basis element x. Since $\text{im}(\pi)$ is a non-zero submodule of M, a simple module, $\text{im}(\pi) = M$. By the first isomorphism theorem, $M \cong R$ as left R-modules. By lemma 2.4.3, we have an isomorphism

$$\text{End}_R(M) \cong \text{End}_R(R) \cong R$$

of rings. By Schur's lemma II, we have that $\text{End}_R(M) \cong R$ is a division ring. □

3 Associative Algebras

3.1 Algebras over a Ring

Definition 3.1.1: Associative Algebras

Let R be a commutative ring. An R-algebra is a ring $(A, +, \times)$ such that $(A, +)$ is an R-module and that the following distributivity law is satisfied:

$$r \cdot (x \times y) = (r \cdot x) \times y = x \times (r \cdot y)$$

for all $r \in R$ and $x, y \in A$.

Here A is not required to be commutative.

Proposition 3.1.2

Let R be a ring. Then the following are equivalent characterizations of an R-algebra.

- A is an R-algebra.
- A is a ring together with a ring homomorphism $f : R \to A$ such that $f(R) \subseteq Z(A)$.

Lemma 3.1.3

Let F be a field and R be a commutative ring. Then R is an F-algebra if and only if R is a vector space over F.

Definition 3.1.4: R-Algebra Homomorphism

Let R be a commutative ring and A, B be both R-algebras. We say that a map of sets $f : A \to B$ is an R-algebra homomorphism if the following are satisfied:

- f is an R-linear map: $f(rx + sy) = rf(x) + sf(y)$ for $x, y \in A$ and $r, s \in R$
- f is a ring homomorphism: $f(xy) = f(x)f(y)$ for $x, y \in A$

Proposition 3.1.5

Let A be an R-algebra. Then any left, right or two-sided ideals of A is an R-subalgebra of A.

Definition 3.1.6: Graded Algebra

A graded algebra A over R is an algebra that is also a graded ring.

3.2 Commutative Algebras

Definition 3.2.1: Commutative Algebras

Let R be a commutative ring. A commutative R-algebra is an R-algebra A that is commutative.

Proposition 3.2.2

Let R be a commutative ring. Then the following are equivalent characterizations of a commutative R-algebra.

- A is a commutative R-algebra

- A is a commutative ring together with a ring homomorphism $f : R \to A$

Proof. Suppose that A is an R-algebra. Then define a map $f : R \to A$ by $f(r) = r \cdot 1$ where $r \cdot 1$ is the module operation on A. Then clearly this is a ring homomorphism.

Suppose that A is a commutative ring together with a ring homomorphism $f : R \to A$. Define an action $\cdot : R \times A \to A$ by $r \cdot a = f(r)a$. Then this action clearly allows A to be an R-module. □

3.3 Free Algebras

Proposition 3.3.1

Let $\mathbb{F}$ be a field. Then the polynomial ring $\mathbb{F}[x]$ is an $\mathbb{F}$ algebra. Its vector space structure has basis $\{x^n | n \in \mathbb{N}\}$.

Definition 3.3.2: Free Algebra

Let $\mathbb{F}$ be a field. Let $X = \{x_1, \ldots, x_k\}$. The free algebra $\mathbb{F}\langle X\rangle = \mathbb{F}\langle x_1, \ldots, x_k\rangle$ is the free R-module with a basis consisting of all words over X together with multiplication rule defined as follows: for $x_{i_1} \cdots x_{i_n}$ and $y_{j_1} \cdots y_{j_m}$ words of $\mathbb{F}\langle X\rangle$,

$$(x_{i_1} \cdots x_{i_n})(y_{j_1} \cdots y_{j_m}) = x_{i_1} \cdots x_{i_n} \cdot y_{j_1} \cdots y_{j_m}$$

Proposition 3.3.3

If X is a non-empty countable set, then the dimension $\dim_{\mathbb{F}}(\mathbb{F}\langle X\rangle)$ is countable.

We use the notion of free algebras to define the universal property of R-algebras.

Proposition 3.3.4: Universal Property

Let A be an R-algebra. For every $f : X \to A$ a map of sets, there exists a unique homomorphism of algebras $\varphi : \mathbb{F}\langle X\rangle \to A$ such that $\varphi(x_i) = f(x_i)$ for each $x_i \in X$.

3.4 Amitsur-Schur Lemma

Recall that we say $a \in \mathbb{F}$ a field is an algebraic element over $\mathbb{F}$ if there exists some polynomial in $f \in \mathbb{F}[x]$ for which $f(a) = 0$. Moreover, the minimal polynomial μ_a is monic and of smallest degree amongst all f for which $f(a) = 0$.

Theorem 3.4.1: Amitsur-Schur Lemma

Let A be an $\mathbb{F}$-algebra for $\mathbb{F}$ a field, such that A has vector space dimension less than $|\mathbb{F}|$. If M is a simple left A-module, then every element of the division $\mathbb{F}$-algebra $\mathrm{End}_A(M)$ is algebraic.

Proof. By Schur's Lemma II, $D = \mathrm{End}_A(M)$ is a division ring. Clearly, D is an $\mathbb{F}$-algebra by defining the ring homomorphism $\phi : \mathbb{F} \to D$ by $\phi(\alpha)(m) = \alpha m$. Then the dimensions of the three vector spaces satisfy

$$\dim_{\mathbb{F}}(D) \leq \dim_{\mathbb{F}}(M) \leq \dim_{\mathbb{F}}(A) < |\mathbb{F}|$$

Indeed, suppose that $x \in M$ is non-zero. Consider the map $\pi : A \to M$ defined by $\pi(a) = ax$. Since π is not the zero map and M is simple, by Shur's lemma I we know that $\mathrm{im}(\pi) = M$. By

the firs isomorphism theorem, we have that $M \cong \frac{A}{\ker(\pi)}$ and thus the second inequality in dimensions hold. For the first inequality, the linear map $\omega_x : D \to M$ defined by $\omega_x(d) = xd$ is injective because M is simple.

Any element $\alpha \in \mathbb{F} \subseteq D$ is clearly algebraic: Just choose $\mu_\alpha(x) = x - \alpha$. Now consider $d \in D \setminus \mathbb{F}$. Then for each $\alpha \in \mathbb{F}$, the element $d - \alpha$ is non-zero. Since D is a division ring, we get $|\mathbb{F}|$ number of non-zero elements $(d-\alpha)^{-1}$. Their number exceeds the dimension of D. Hence we have a non-trivial linear dependence

$$\sum_{i=1}^{k} \beta_i (d - \alpha_i)^{-1} = 0$$

for any $k \geq 1$. All elements $d - \alpha_i$ commutes because $\alpha_i \in \mathbb{F} \subseteq Z(D)$. Furthermore, $d - \alpha_i$ commutes with $(d - \alpha_j)^{-1}$ because

$$\begin{aligned} ab = ba &\implies ab^{-1} = b^{-1}bab^{-1} = b^{-1}abb^{-1} = b^{-1}a \\ &\implies a^{-1}b^{-1} = b^{-1}a^{-1} \end{aligned}$$

Thus we can apply the usual calculations with fractions:

$$0 = \sum_{i=1}^{k} \beta_i \frac{1}{d - \alpha_i} = \frac{f(d)}{(d-\alpha_1)\cdots(d-\alpha_k)}$$

where $f(d) = \sum_{j=1}^{k} \prod_{i=1}^{k} \frac{\beta_j}{x-\alpha_j}(x - \alpha_i)$. Multiplying by the denominator, we get $f(d) = 0$. Notice that

$$f(\alpha_1) = \beta_1(\alpha_1 - \alpha_2)\cdots(\alpha_1 - \alpha_k) \neq 0$$

so that $f(x) \neq 0$ and thus d is algebraic. □

The following statement is often referred to as Schur's lemma in representation theory.

Corollary 3.4.2

Let A be a countable generated $\mathbb{C}$-algebra. Let M is a simple left A-module. Then $\mathrm{End}_A(M) = \mathbb{C}$.

4 Tensor Products

4.1 Tensor Products of Modules

Definition 4.1.1: Tensor Product of Modules

Let R be a ring. Let A, B be R-modules. The tensor product of A and B over R is an R-module

$$A \otimes_R B$$

together with an R-bilinear map $\phi : A \times B \to A \otimes_R B$ such that for any other R-bilinear map $\psi : A \times B \to C$, there is a unqiue R-linear map $\theta : A \otimes_R B \to C$ such that $\psi = \theta \circ \phi$. In other words, the following diagram commutes:

$$\begin{array}{ccc} A \times B & \xrightarrow{\phi} & A \otimes_R B \\ & \searrow^{\psi} & \downarrow{\scriptstyle \exists! \theta} \\ & & C \end{array}$$

Lemma 4.1.2

Let R be a ring. The tensor product of two modules over R always exists and is unique.

Proposition 4.1.3

Let R be a ring and A, B, C be R-modules. Then the following properties hold for the tensor product.

- Associativity: $(A \otimes_R B) \otimes_R C \cong A \otimes_R (B \otimes_R C)$
- Commutativity: $A \otimes_R B \cong B \otimes_R A$
- Identity: $A \otimes_R R \cong A$
- Distributivity: $(A \oplus B) \otimes_R C \cong (A \otimes_R C) \oplus (B \otimes_R C)$

Proposition 4.1.4

Let R be a ring and I, J be ideals of R. Then

$$\frac{R}{I} \otimes_R \frac{R}{J} \cong \frac{R}{I+J}$$

Proposition 4.1.5

Let M be an R-module and I an ideal of R. Then

$$M \otimes \frac{R}{I} \cong \frac{M}{IM}$$

4.2 Multilinear Maps

Definition 4.2.1: Multilinear Map

Let $M_1, \ldots, M_n, N$ be R-modules. A map $\varphi : M_1, \times \cdots \times M_n \to N$ is multlinear map if for each fixed i and fixed elements $m_j \in M_j$ for $j \neq i$, the map $M_i \to N$ defined by

$$x \mapsto \varphi(m_1, \ldots, m_{i-1}, x, m_{i+1}, \ldots, m_n)$$

is an R-module homomorphism.

Definition 4.2.2: Alternating Map

A multilinear map $\varphi : M \times \cdots \times M \to N$ is called symmetric if interchanging m_i and m_j does not change the value of φ for any i, j.

Definition 4.2.3: Alternating Map

A multilinear map $\varphi : M \times \cdots \times M \to N$ is called alternating if $m_i = m_{i+1}$ for some i implies $\varphi(m_1, \ldots, m_k) = 0$.

4.3 Tensor Algebra

In this section, R is a commutative ring with identity and we assume that the left and right action on every R-module is the same.

Definition 4.3.1: kth Tensor Power

Let M be an R-module. Let $k \in \mathbb{N}$. Define the kth tensor power of M to be the tensor product

$$M^{\otimes k} = M \otimes M \cdots \otimes M$$

where the tensor product over M is taken k times.

By convention, define $M^{\otimes 0}$ to be R.

Definition 4.3.2: Tensor Algebra

Let M be an R-module. Define the tensor algebra over V to be the direct sum

$$T(M) = \bigoplus_{k=0}^{\infty} M^{\otimes k}$$

Define multiplication in $T(M)$ to be the map $M^{\otimes k} \otimes M^{\otimes l} \to V^{\otimes k+l}$, defined by

$$(m_1 \otimes \cdots \otimes m_i)(m'_1 \otimes \cdots \otimes m'_j) = m_1 \otimes m_i \otimes m'_1 \otimes \cdots \otimes m'_j$$

and then extended by linearity to all of $T(M)$.

Proposition 4.3.3

Let M be an R-module. Then $T(M)$ is a graded R-algebra with the above defined multiplication rule.

Proposition 4.3.4: Universal Property

The tensor algebra $T(M)$ of an R-module M satisfies the following universal property. Let A be any R-algebra and $\varphi : M \to A$ an R-module homomorphism. Then there is a unique R-algebra homomorphism $\psi : T(M) \to A$ such that $\psi|_M = \varphi$.

Proposition 4.3.5

Let V be a finite dimensional vector space over $\mathbb{F}$ with basis $B = \{v_1, \ldots, v_n\}$. Then the k-tensors

$$v_{i_1} \otimes \cdots \otimes v_{i_k}$$

with $v_{i_1}, \ldots, v_{i_k} \in B$ are a basis for $T^k(V)$ over $\mathbb{F}$. In particular, $\dim_{\mathbb{F}}(T^k(V)) = n^k$.

4.4 Exterior Algebra

Definition 4.4.1: Alternating Quotient

Let M be an R-module. The alternating quotient is the ideal

$$A(M) = \langle m \otimes m | m \in M \rangle$$

of $T(M)$.

Lemma 4.4.2

The ideal $A(M)$ is a homogenous ideal.

Definition 4.4.3: Exterior Algebra

Let M be an R-module. Define the exterior algebra of V to be the quotient

$$\Lambda(M) = T(V)/A(M)$$

Elements of the form $m_1 \otimes m_2$ are written as $m_1 \wedge m_2$ by convention.

Proposition 4.4.4

Let M be an R-module. Then the following are true regarding the symmetric algebra.

- $\Lambda(M)$ is a graded ring with homogenous components $\Lambda^k(M) = T^k(M)/A^k(M)$ called the kth exterior power
- $\Lambda^0(M) = R$
- $\Lambda^1(M) = M$
- $\Lambda(M)$ is an R-algebra.

Theorem 4.4.5

Let M be an R-module. Let

$$I = \langle m_1 \otimes \cdots \otimes m_k | m_1, \ldots, m_k \in M, m_i = m_j \text{ for some } i \neq j \rangle$$

Then $\Lambda^k(M) = T^k(M)/I$.

Proposition 4.4.6

Let $\{v_1, \ldots, v_n\}$ be a basis of the vector space V. Then

$$\{v_{i_1} \wedge \cdots \wedge v_{i_r} | 1 \leq i_1 < \cdots < i_r \leq n\}$$

is a basis of $\Lambda^r(V)$ and

$$\dim(\Lambda^r(V)) = \binom{n}{r}$$

Corollary 4.4.7

Let V be vector space over $\mathbb{F}$ of dimension n. For $k > n$, $\Lambda^k(M) = 0$.

Lemma 4.4.8

Let M be an R-module. Then the following are true regarding the exterior algebra $\Lambda(M)$.

- Alternating: $m \wedge m = 0$ for all $m \in M$
- $m_1 \wedge m_2 = -m_2 \wedge m_1$ for any $m_1, m_2 \in M$
- $m_1 \wedge m_2 = (-1)^{rs} m_2 \wedge m_1$ for any $m_1 \in \Lambda^r(M)$ and $m_2 \in \Lambda^s(M)$

4.5 Symmetric Algebra

Definition 4.5.1: Symmetric Quotient

Let M be an R-module. The symmetric quotient is the ideal

$$C(M) = \langle m_1 \otimes m_2 - m_2 \otimes m_1 | m_1, m_2 \in M \rangle$$

of $T(M)$ generated by commutativity.

Lemma 4.5.2

The ideal $C(M)$ is a homogenous ideal.

Definition 4.5.3: Symmetric Algebra

Let M be an R-module. Define the symmetric algebra of M to be the quotient

$$S(M) = T(M)/C(M)$$

Elements of the form $m_1 \otimes m_2$ are written as $m_1 m_2$ by convention.

Again here we are quotienting out symmetric objects so that we can treat them as the same thing.

Proposition 4.5.4

Let M be an R-module. Then the following are true regarding the symmetric algebra.

- $S(M)$ is a graded ring with homogenous components $S^k(M) = T^k(M)/C^k(M)$ called the kth symmetric power
- $S^0(M) = R$
- $S^1(M) = M$
- $S(M)$ is an R-algebra.

Theorem 4.5.5

Let M be an R-module. Let

$$I = \langle m_1 \otimes \cdots \otimes m_k - m_{\sigma(1)} \otimes \cdots \otimes m_{\sigma(k)} | m_1, \ldots, m_k \in M, \sigma \in S_k \rangle$$

Then $S^k(M) = T^k(M)/I$.

Theorem 4.5.6: Universal Property

The symmetric algebra $S(M)$ for an R-module M satisfies the following universal property: Let A be any commutative R-algebra and $\varphi : M \to A$ an R-module homomorphism. Then there exists a unique R-algebra homomorphism $\psi : S(M) \to A$ such that $\psi|_M = \varphi$.

Corollary 4.5.7

Let V be an n-dimensional vector space over $\mathbb{F}$. Then $S(V)$ is isomorphic as a graded $\mathbb{F}$-algebra to $\mathbb{F}[x_1, \ldots, x_n]$. This isomorphism is also a vector space isomorphism. In particular, $\dim_{\mathbb{F}}(S^k(V)) = \binom{k+n-1}{n-1}$.

4.6 Symmetric and Alternating Tensors

5 Division Rings

5.1 The Structure of Quaternions

Definition 5.1.1: Quaternions

Define the quaternions as the quotient algebra

$$\mathbb{H} = \frac{\mathbb{R}\langle x_1, x_2, x_3\rangle}{I}$$

where $I = (x_1^2 + 1, x_2^2 + 1, x_3^2 + 1, x_1x_2x_3 + 1)$.

Elements of $\mathbb{H}$ are of the form $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ for $a, b, c, d \in \mathbb{R}$ and by writing $\mathbf{i} = x_1 + I$, $\mathbf{j} = x_2 + I$ and $\mathbf{k} = x_3 + I$.

A quaternion is said to be real if $b = c = d = 0$. It is said to be imaginary if $a = 0$. Denote the set of all imaginary quaternions by $\mathbb{H}_0$.

Proposition 5.1.2

The quaternions satisfy the following multiplication table:

$\cdot$	1	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
1	1	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
$\mathbf{i}$	$\mathbf{i}$	-1	$\mathbf{k}$	$-\mathbf{j}$
$\mathbf{j}$	$\mathbf{j}$	$-\mathbf{k}$	-1	$\mathbf{i}$
$\mathbf{k}$	$\mathbf{k}$	$\mathbf{j}$	$-\mathbf{i}$	-1

Proof. We only need to consider products that does not involve 1. It clear for $t = 1, 2, 3$, $x_t^2 + 1 \in I$. This means that $x_t^2 + I = -1 + I$ and thus $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^1 = -1$. Similarly, we have that $x_1x_2x_3 + I = -1 + I$ and thus $\mathbf{ijk} = -1$. Multiplying this expression by $-\mathbf{i}$ on the left gives $\mathbf{jk} = \mathbf{i}$. We can also multiply the expression by $-\mathbf{k}$ on the right to get $\mathbf{ij} = \mathbf{k}$. Now multiply $\mathbf{i}$ to the left of the equation $\mathbf{ij} = \mathbf{k}$ to get $-\mathbf{j} = \mathbf{ik}$. We can also multiply $\mathbf{ij} = \mathbf{k}$ by $\mathbf{j}$ on the right gives $-\mathbf{i} = \mathbf{kj}$. Finally we have $\mathbf{j}(\mathbf{i} = \mathbf{jk}) \implies \mathbf{ji} = -\mathbf{k}$ and $(\mathbf{ji} = -\mathbf{k})(-\mathbf{i}) \implies \mathbf{j} = \mathbf{ki}$. □

Proposition 5.1.3

The elements $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$ form a basis for the $\mathbb{R}$-algebra $\mathbb{H}$.

Proof. It is clear that $1, x_1, x_2, x_3, x_1x_2, x_1x_3, x_2, x_3, \ldots$ span $\mathbb{H}$. By writing x_1, x_2, x_3 each in terms of $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$ respectively, we have can see that $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$ span $\mathbb{H}$. It remains to show that they are linearly independent.

Consider the $\mathbb{R}$-algebra homomorphism $f : \mathbb{R}\langle x_1, x_2, x_3\rangle \to M_{2\times 2}(\mathbb{C})$ defined by $f(x_1) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $f(x_2) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $f(x_3) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. It is clear that $I \subseteq \ker(f)$ since $f(x_1^2 + 1) = f(x_2^2 + 1) = f(x_3^2 + 1) = f(x_1x_2x_3 + 1) = 0$. By the first and third isomorphism theorem for modules, we have that

$$\frac{\mathbb{H}}{\ker(f)/I} \cong \frac{\mathbb{R}\langle x_1, x_2, x_3\rangle}{\ker(f)} \cong \mathrm{im}(f)$$

This means that $\dim_{\mathbb{R}}(\mathbb{H}) \geq \dim_{\mathbb{R}}(\mathrm{im}(f))$. Since the matrices $f(x_1), f(x_2), f(x_3)$ and 1 are all linearly independent over $\mathbb{R}$, we have that $\mathrm{im}(f)$ is at least 4-dimensional. Hence the four spanning elements of $\mathbb{H}$ must be linearly independent. □

Proposition 5.1.4

The imaginary quaternions $\mathbb{H}_0$ form a three dimensional vector subspace of $\mathbb{H}$. The real quaternions form a subalgebra $\mathbb{R}$ of $\mathbb{H}$.

We treat the imaginary quaternions $\mathbb{H}_0$ as the standard 3-space with dot product

$$(b_1\mathbf{i} + c_1\mathbf{j} + d_1\mathbf{k}) \cdot (b_2\mathbf{i} + c_2\mathbf{j} + d_2\mathbf{k}) = b_1b_2 + c_1c_2 + d_1d_2$$

and cross product

$$\begin{aligned}(b_1\mathbf{i} + c_1\mathbf{j} + d_1\mathbf{k}) \times_c (b_2\mathbf{i} + c_2\mathbf{j} + d_2\mathbf{k}) &= (c_1d_2 - c_2d_1)\mathbf{i} + (d_1b_2 - d_2b_1)\mathbf{j} + (b_1c_2 - c_2b_1)\mathbf{k} \\ &= \begin{vmatrix} \mathbf{i} & \mathbf{j} & \mathbf{k} \\ b_1 & c_1 & d_1 \\ b_2 & c_2 & d_2 \end{vmatrix}\end{aligned}$$

Proposition 5.1.5

Let $a_1 + \mathbf{h}_1$ and $a_2, \mathbf{h}_2$ be quaternions such that $a_1, a_2 \in \mathbb{R}$ and $\mathbf{h}_1, \mathbf{h}_2 \in \mathbb{H}_0$. Then

$$(a_1 + \mathbf{h}_1)(a_2 + \mathbf{h}_2) = (a_1a_2 - \mathbf{h}_1 \cdot \mathbf{h}_2) + (a_1\mathbf{h}_2 + a_2\mathbf{h}_1 + \mathbf{h}_1 \times_c \mathbf{h}_2)$$

Definition 5.1.6: Conjugate and Norm

Let $x = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathbb{H}$ be a quaternion. Define the conjugate of x to be

$$x^* = a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$$

Also define the norm of x to be

$$\|x\| = \sqrt{a^2 + b^2 + c^2 + d^2}$$

Proposition 5.1.7

Let $x, y \in \mathbb{H}$ be quaternions. The following are true regarding the conjugate and norm of the quaternions:

- $xx^* = \|x\|$
- $(xy)^* = y^*x^*$
- $\|xy\| = \|x\|\|y\|$

Proof. □

Proposition 5.1.8

$\mathbb{H}$ is a division ring.

Proof. Let $x \in \mathbb{H}$. By the above proposition, we have that $x\frac{x^*}{\|x\|} = 1$ which means we have found an inverse $\frac{x^*}{\|x\|}$ of x. □

5.2 The Multiplicative Group of Quaternions

Definition 5.2.1: The Quaternionic Unitary Group

Define the quaternionic unitary group to be the subgroup

$$U(\mathbb{H}) = \{x \in \mathbb{H} \mid \|x\| = 1\}$$

of $\mathbb{H}^\times$.

Proposition 5.2.2

The multiplicative group $\mathbb{H}^\times$ is isomorphic to $\mathbb{R}_+^\times \times U(\mathbb{H})$, where $\mathbb{R}_+^\times$ is the multiplicative group of non-zero real numbers.

Proof. □

Proposition 5.2.3: Quaternionic Euler's Formula

Write a quaternion into the form $q = a + b\mathbf{x} \in \mathbb{H}$ where $a, b \in \mathbb{R}$ and $\mathbf{x} \in \mathbb{H}_0$ is purely imaginary such that $\|\mathbf{x}\| = 1$. Then

$$e^q = e^a(\cos(b) + \mathbf{x}\sin(b))$$

Proposition 5.2.4: Quaternionic De Moivre's Formula

Let $\mathbf{x} \in H_0$ be purely imaginary such that $\|\mathbf{x}\| = 1$. Let $n \in \mathbb{Z}$. Then

$$(\cos(b) + \mathbf{x}\sin(b))^n = \cos(nb) + \mathbf{x}\sin(nb)$$

5.3 3D Rotations using Quaternions

Recall the special orthogonal group in 3-dimensions is the group

$$\mathrm{SO}_3(\mathbb{R}) = \{M \in \mathrm{GL}_3(\mathbb{R}) | \det(M) = 1\}$$

Proposition 5.3.1

Let $M \in \mathrm{SO}_3(\mathbb{R})$ be a special orthogonal transformation. Then there exists an orthonormal basis of $\mathbb{R}^3$ such that the matrix decomposes into the direct sum $(1) \oplus R_\alpha$, where $R_\alpha = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$ is a rotation in $\mathbb{R}^2$.

Now we know that every special orthogonal transformation is just a rotation in the plane orthogonal to e_1. In generality, we write $R_{\mathbf{x}}^\alpha$ for the anti-clockwise rotation in angle α in the plane orthogonal to $\mathbf{x} \in \mathbb{R}^3$. We can use the quaternions to write out a formula for applying the special orthogonal transformation to a vector.

Lemma 5.3.2

Let $\mathbf{x} \in \mathbb{H}_0 \cap U(\mathbb{H})$ be an imaginary unit. Let $\theta \in \mathbb{R}$. Then

$$R_{\mathbf{x}}^{2\theta}(\mathbf{w}) = e^{\theta\mathbf{x}}\mathbf{w}e^{-\theta\mathbf{x}}$$

for all $\mathbf{w} \in \mathbb{H}_0$.

This leads tot he fundamental fact behind the theory of spinors in Geometry and Physics.

Theorem 5.3.3

The conjugation action map

$$\phi : U(\mathbb{H}) \to \mathrm{SO}(\mathbb{H}_0) \cong \mathrm{SO}_3(\mathbb{R})$$

defined by $\phi(x)(\mathbf{z}) = x\mathbf{z}x^{-1}$ for $\mathbf{z} \in \mathbb{H}_0$ and $x \in U(\mathbb{H})$ is a surjective two to one group homomorphism.

5.4 Division Rings over Real and Complex Numbers

Proposition 5.4.1

The only finite dimensional $\mathbb{C}$-division algebra is $\mathbb{C}$.

Proof. Let D be a finite dimensional $\mathbb{C}$-division algebra. Then in particular, $\mathbb{C} \subseteq D$. Suppose that $a \in D$. Then the minimal polynomial $\mu_a(x)$ is an irreducible element of $\mathbb{C}[x]$. By the fundamental theorem of algebra, $\mu_a(x) = x - \alpha$ with $\alpha \in \mathbb{C}$. This means that $a = \alpha \in \mathbb{C}$ and thus $D = \mathbb{C}$. □

Proposition 5.4.2

The only odd dimensional $\mathbb{R}$-division algebra is $\mathbb{R}$.

Proof. Let D be an $\mathbb{R}$-division algebra of odd dimension n. Then in particular, $\mathbb{R} \subseteq D$. Let $a \in D$. In linear algebra we know that the $\mathbb{R}$-linear map $L : D \to D$ defined by $L(d) = ad$ admits a real eigenvalue $\alpha \in D$ and eigenvector v. Then $av = \alpha v$ implies that $(a - \alpha)v = 0$. Since D is a division algebra, we have that $a = \alpha \in \mathbb{R}$. Thus $\mathbb{R} = D$. □

Theorem 5.4.3: Frobenius Theorem

A finite dimensional division algebra over $\mathbb{R}$ is isomorphic to $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$.

Theorem 5.4.4

The only countably generated division algebra over $\mathbb{R}$ up to isomorphism is either $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$.

5.5 Finite Division Rings

Lemma 5.5.1

Let R be a division ring. Then $Z(R)$ is a field. Moreover, R is a $Z(R)$-algebra.

Corollary 5.5.2

Let D be a finite division ring. Then the following statements are true regrading D.

- $Z(D)$ is a finite field $\mathbb{F}_{p^n}$ for some $n \in \mathbb{N} \setminus \{0\}$
- The dimension of D, $m = \dim_{Z(D)} D$ over $Z(D)$ is finite
- $|D| = p^{nm}$

Lemma 5.5.3

Let R be a division ring and $x \in R$. Then $C_R(x)$ is a division ring and a $Z(R)$-subalgebra.

Proposition 5.5.4

Let D be a finite division ring of dimension m over its center $Z(D) = \mathbb{F}_q$, where $q = p^n$ for some prime p and $n \in \mathbb{N} \setminus \{0\}$. Then there exists positive integers $d_1, \ldots, d_k$ such that $d_i | m$, $d_i < m$ and

$$q^m = q + \sum_{i=1}^{k} \frac{q^m - 1}{q^{d_i} - 1}$$

Theorem 5.5.5: Little Wedderburn's Theorem

A finite division ring is a field.

5.6 Laurent Series

Definition 5.6.1: Laurent Series

Let R be a ring. A Laurent series in variable x with coefficients in a ring R is an expression of the form

$$\sum_{n=m}^{\infty} a_n x^n$$

for $m \in \mathbb{Z}$ and $a_n \in R$. Denote the set of Laurent series in x by

$$R((x))$$

Lemma 5.6.2

Let R be a ring. Then $R((x))$ is also a ring. If R is a field, then $R((x))$ is also a field.

Lemma 5.6.3

The center of $\mathbb{H}((x))$ is precisely $\mathbb{R}((x))$.

6 Semisimplicity

6.1 Semisimple Modules

Definition 6.1.1: Semisimple Modules

A left R-module M is semisimple if M is a direct sum of simple modules.

Definition 6.1.2: Socle of a Module

Denote $\mathcal{SM}(M) = \{S \leq M | S \text{ is simple}\}$. A socle of a left R-module M is a submodule

$$\text{soc}(M) = \sum_{S \in \mathcal{SM}(M)} S$$

Lemma 6.1.3

A module M is semisimple if and only if $\text{soc}(M) = M$.

Corollary 6.1.4

A quotient module of a semisimple module is semisimple.

Proof. Suppose that M is semisimple. Then $M = \bigoplus_{i \in I} S_i$ where S_i are simple modules. Consider a quotient M/N and the quotient homomorphism $\psi : M \to M/N$. Clearly, $M/N = \psi(M) = \sum_{i \in I} \psi(S_i)$ and each $\psi(S_i)$ is either 0 or simple. Then $\text{soc}(M/N) = M/N$ and M/N is semisimple. □

6.2 Peirce Decomposition for Modules

Definition 6.2.1: Idempotents

Let R be a ring. We say that $e \in R$ is idempotent if $e^2 = e$.

Definition 6.2.2: Orthogonal Idempotents

Let R be a ring. We say that two idempotent elements $e, f \in R$ is orthogonal if $ef = fe = 0$.

Definition 6.2.3: Full System of Orthogonal Idempotents

Let R be a ring. A full system of orthogonal idempotents is a finite collection of non-zero pairwise orthogonal idempotent elements $e_1, \ldots, e_n \in R$ such that $e_1 + \cdots + e_n = 1$.

Proposition 6.2.4

Let M be an R-module. Then there is a bijection between the set of all finite direct sum decompositions $M = \bigoplus_{i=1}^n M_i$ with all $M_i \neq 0$ and the set of all full orthogonal system of idempotents in $\text{End}_R(M)$.

Proof. A decomposition $M = \bigoplus_{i=1}^n M_i$ gives a system of idempotents through its component maps $e_k : M \to M$ defined by $(x_1, \ldots, x_n) \mapsto (0, \ldots, 0, x_i, 0, \ldots, 0)$. This map is an endomorphism since it is the composition of the projection with to M_k with the inclusion to M. It is clear that they form a full system of orthogonal idempotents for $\text{End}_R(M)$.

Now suppose that we have a full orthogonal system of idempotents $e_1, \ldots, e_n$ in $\text{End}_R(M)$. Define $M_k = Me_k = \text{im}(e_k)$ for $1 \leq k \leq n$. $\phi : \bigoplus_{i=1}^n M_i \to M$ defined by $(m_1, \ldots, m_n) \mapsto \sum_{i=1}^n m_i$ is surjective because each $m \in M$ can be written as

$$\begin{aligned} \text{id}_{\text{End}_R(M)}(m) &= (e_1 + \cdots + e_n)(m) \\ &= e_1(m) + \cdots + e_n(m) \\ &= \phi(e_1(m), \ldots, e_n(m)) \end{aligned}$$

It is injective because if $\phi(x) = 0$ for $x = (e_1(m_1), \ldots, e_n(m_n))$ implies that

$$\begin{aligned} 0 &= e_k(\phi(x)) \\ &= e_k(e_1(m_1) + \cdots + e_n(m_n)) \\ &= \sum_{i=1}^n e_k(e_i(m_i)) \\ &= e_k(m_k) \end{aligned}$$

This implies that $m_k = 0$ for $1 \leq k \leq n$ and so $x = 0$.

It is clear that these constructions are inverse functions between the stated sets. □

Note that in particular, we can also take M to just be R to get a decomposition on idempotents by ideals of R. This means that for $\{e_1, \ldots, e_n\}$ a full orthogonal system of idempotents, we have a decomposition

$$R = Re_1 \oplus \cdots \oplus Re_n$$

Proposition 6.2.5

Let $e, f, g \in R$ be idempotents of a ring. Then the map $\psi : eRf \to \text{Hom}_R(Re, Rf)$ defined by

$$\psi(erf) : Re \to Rf$$

to be the map $se \mapsto serf$ is an isomorphism of abelian groups such that $\psi(erf)\psi(fsg) = \psi(erfsg)$. In particular, if $e = f$, then ψ is a ring isomorphism.

Theorem 6.2.6: Peirce Decompositions

A full system of orthogonal idempotents in R gives a direct sum decomposition of R and M into $\mathbb{Z}$-modules that can be written in matrix forms

$$R = \bigoplus_{i,j=1}^n e_i R e_j = \begin{pmatrix} e_1Re_1 & \cdots & e_1Re_n \\ \vdots & \ddots & \vdots \\ e_nRe_1 & \cdots & e_nRe_n \end{pmatrix}$$

and

$$M = \bigoplus_{i=1}^n e_i M = \begin{pmatrix} e_1M \\ \vdots \\ e_nM \end{pmatrix}$$

that satisfies the following:

- If R is an $\mathbb{F}$-algebra, all e_iRe_j and e_iM are $\mathbb{F}$-vector subspaces
- The multiplication in R defines the structure of a ring on each e_iRe_j. This ring is non-zero.
- The R-module action on M defines a structure of e_iRe_i-module on e_iM
- In the matrix interpretation, the multiplication in R and the R action on M satisfies the standard matrix rules

Proof. □

6.3 Artin-Wedderburn Theorem

Theorem 6.3.1: Artin-Wedderburn Theorem

Let R be a ring. Then the following are equivalent characterizations of semisimplicity.

- Every left R-module is semisimple
- The ring R as a left R-module is semisimple
- There exists $n_1, \ldots, n_k \in \mathbb{N}$ and division rings $D_1, \ldots, D_k$ such that R is isomorphic to the direct product $\prod_{i=1}^{k} M_{n_i}(D_i)$

Proof.

- (1) $\implies$ (2) is obvious because R is also a left R-module.
- (2) $\implies$ (1): Let M be an R-module. Choose a generating set B of M. Then M is a quotient of the free module $\bigoplus_{b\in B} Rb$. Since R is semisimple, RB is also semisimple. By corollary 6.1.4, M is also a semisimple module.
- (2) $\implies$ (3): Write the R-module R as a direct sum of simple modules $R = \bigoplus_{i\in I} S_i$. Note that the set I is finite because $1 = \sum_{i\in I} s_i$ for $s_i \in S_i$ and so we can remove the 0 in the sum to get $1 = s_1, \ldots, s_m$. Then each element $r \in R$ can be written as $r = rs_1 + \cdots + rs_m$. Hence $R = \bigoplus_{i=1}^{m} S_i$.

  Let $L_1, \ldots, L_k$ be distinct simple modules among the S_i. By Schur's lemma, $D_i = \mathrm{End}_R L_i$ is a division ring. Reorder the summands so that we can group them as following:

$$R = \underbrace{S_1 \oplus \cdots \oplus S_{n_1}}_{\text{each } S_i \cong L_1} \oplus \cdots \oplus \underbrace{S_{n_1+\cdots+n_{k-1}+1} \oplus \cdots \oplus S_m}_{\text{each } S_i \cong L_k}$$

  Replace each S_i with the corresponding L_j together with lemma 2.4.3 to get

$$R \cong \mathrm{End}_R \cong \mathrm{End}_R \left(\underbrace{L_1 \oplus \cdots \oplus L_1}_{n_1} \oplus \cdots \oplus \underbrace{L_{i_k} \oplus \cdots \oplus L_k}_{n_k} \right) = \mathrm{End}_R \left(\bigoplus_{j=1}^{k} L_j^{n_j} \right)$$

  Now let $e_1, \ldots, e_m$ be the full system of orthogonal idempotents corresponding to the above decomposition by proposition 6.2.4. Consider e_j in the jth group and e_s in the tth group. By proposition 6.2.5, we have

$$e_j R e_s \cong \mathrm{Hom}_R(L_j, L_t) = \begin{cases} 0 & \text{if } j \neq t \\ D_j & \text{if } j = t \end{cases}$$

  Then by the Peirce decomposition,

$$R = \begin{pmatrix} D_1 & \cdots & D_1 & 0 & \cdots & 0 & \cdots \\ \vdots & & \vdots & \vdots & & \vdots & \\ D_1 & \cdots & D_1 & 0 & \cdots & 0 & \cdots \\ 0 & \cdots & 0 & D_2 & \cdots & D_2 & \cdots \\ \vdots & & \vdots & \vdots & & \vdots & \\ 0 & \cdots & 0 & D_2 & \cdots & D_2 & \cdots \\ \vdots & & \vdots & \vdots & & \vdots & \end{pmatrix} = M_{n_1}(D_1) \times M_{n_2}(D_2) \times \cdots \times M_{n_k}(D_k)$$

- (3) $\implies$ (2): Let $R = \prod_{i=1}^{k} M_{n_i}(D_i)$. Then elementary matrix $E_{i,i}^{t} \in M_{n_t}(D_t)$ form a full system of orthogonal idempotents. Then the R-module $RE_{i,i}^{t}$ is simple because it is isomorphic to the column module $D_t^{n_t}$. Thus $R = \bigoplus_{i,t} RE_{i,i}^{t}$ is a direct sum of semisimple modules.

□

Similarly, there is a decomposition for right semisimple rings.

Corollary 6.3.2

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

Proposition 6.3.3

The following are true regarding semisimple algebras over fields.

- A semisimple $\mathbb{C}$-algebra of finite or countable dimension is isomorphic to

$$\prod_{i=1}^{k} M_{k_i}(\mathbb{C})$$

- A semisimple $\mathbb{R}$-algebra of finite or countable dimension is isomorphic to

$$\prod_{i=1}^{k} M_{k_i}(\mathbb{R}) \times \prod_{i=1}^{n} M_{n_i}(\mathbb{C}) \times \prod_{i=1}^{t} M_{t_i}(\mathbb{H})$$

- A finite dimensional semisimple $\mathbb{F}_q$ algebra is isomorphic to

$$\prod_{i=1}^{k} M_{k_i}(\mathbb{F}_q^{t(i)})$$

6.4 Maschke's Theorem

For Maschke's theorem, we would need an equivalent definition of semisimplicity of modules.

Definition 6.4.1: Completely Reducible Modules

Let M be an R-module. M is said to be completely reducible if for every submodule N of M, there exists a submodule L of M such that $M = N \oplus L$.

Proposition 6.4.2

Let M be an R-module such that $M = N \oplus L$. Then there is an isomorphism

$$L \cong \frac{M}{N}$$

of R-modules.

Proof. Consider the quotient map $\psi : M \to M/N$. This restricts to a homomorphism $\overline{\psi} : L \to M/N$. This map is injective since

$$\ker(\overline{\psi}) = L \cap \ker(\psi) = L \cap N = 0$$

The map is surjective since every $m \in M$ can be written as $m = l + n$ for $l \in L$ and $n \in N$.

Then

$$\psi(l) = \psi(l+n) = \psi(m) = m + N$$

so that ψ is surjective and so is $\overline{\psi}$. □

Lemma 6.4.3

A submodule of a completely reducible module is reducible.

Proof. Let N be a submodule of a completely reducible module M. Let P be a submodule of P. Then it has a direct complement

$$M = P \oplus K$$

together with the corresponding idempotents π of $\mathrm{End}_R(M)$ and p of P for which $\pi(p+k) = p$. The image of π is equal to P, which is a subset of N. This allows us to restrict the idempotent and use proposition 6.2.4 to obtain $\phi = \pi|_N \in \mathrm{End}_R(M)$ and

$$N = \mathrm{im}(\phi) \oplus \ker(\phi) = P \oplus K'$$

so that we conclude. □

Lemma 6.4.4

A non-zero completely reducible module contains a simple submodule.

Proof. Let M be a completely reducible R-module. Pick a non-zero element $x \in M$. Then left R-module homomorphism $\pi_x : R \to M$ defined by $\pi_x(r) = r \cdot x$ is non-zero because $\pi_x(1) = x \neq 0$. Since every ring has a maximal left ideal, $\ker(\pi_x)$ as an ideal also lies in some maximal ideal L. Notice that $Rx \cong \frac{R}{\ker(\pi_x)}$. This gives a surjective R-module homomorphism

$$\psi : \frac{R}{\ker(\pi_x)} \to \frac{R}{L}$$

defined by $\psi(r + \ker(\pi_x)) = r + L$. The module Rx is a submodule of M, and hence completely reducible by the above lemma. This means that there exists a submodule N of Rx such that $Rx = N \oplus \ker(\psi)$. The homomorphism $\psi|_N : N \to R/L$ is an isomorphism by proposition 6.4.2. Since R/L is simple, N is a simple submodule of M and so we conclude. □

Theorem 6.4.5

Let M be an R-module. Then M is semisimple if and only if M is completely reducible.

Proof. Suppose that M is completely reducible. By the above lemma, it is clear that $\mathrm{soc}(M)$ is non-empty. If $M = \mathrm{soc}(M)$ we are done. So suppose not. By complete reducibility, there exists a submodule K such that $M = \mathrm{soc}(M) \oplus K$. Since K is a submodule of M, K is completely reducible. By the above lemma, K contains a simple submodule S. Then $S \subseteq \mathrm{soc}(M)$, which is a contradiction.

Now assume that M is semisimple. Let $M = \bigoplus_{i \in I} S_i$ for simple modules S_i. Let N be a submodule of M. If $\psi : M \to M/N$ is the quotient homomorphism, then

$$M/N = \psi(M) = \sum_{\in I} \psi(M)$$

with each $\psi(S_i) = \frac{S_i}{S_i \cap N}$. In particular, each $\psi(S_i)$ is either zero or simple and isomorphic to S_i. Since quotient of semisimple modules are semisimple, we have that M/N is semisimple and

one can choose a subset J of I indices such that

$$M/N = \bigoplus_{i \in J} S_i$$

with $\psi(S_i) \cong S_i$ for all i.

We claim that $M = N \oplus \left(\bigoplus_{i \in J} S_i\right)$. To prove it, consider the natural R-module homomorphism

$$\varphi : N \oplus \left(\bigoplus_{i \in J} S_i\right) \to M$$

defined by $\varphi(n, (s_i)_{i \in J}) = n + \sum_{i \in J} s_i$. It is injective since for $(n, (s_i)_{i \in J}) \in \ker(\varphi)$, we have $\psi(n) + \sum_{i \in J} \psi(s_i) = 0$ together with $n \in \ker(\psi)$ to imply that

$$\sum_{i \in J} \psi(s_i) = 0$$

Using the direct sum $M/N = \bigoplus_{i \in J} S_i$, we have that each $\psi(s_i) = 0$. Since $\psi : S_i \to \psi(S_i)$ is an isomorphism, we have that $s_i = 0$. This means that we have $n + \sum_{i \in J} s_i = 0$ together with $s_i = 0$ to imply that $n = 0$. So we are done with injectivity. For surjectivity, we have for each $m \in M$, we can write a finite sum $\psi(m) = \sum_{i \in J} \psi(s_i)$ for some $s_i \in S_i$ all but finitely many non-zero. Then $m - \sum_{i \in J} s_i \in \ker(\psi) = N$ and we have that

$$\varphi\left(m - \sum_{i \in J} s_i, (s_i)_{i \in J}\right) = m$$

This show that we have an isomorphism so that M is now completely reducible. □

Corollary 6.4.6

A submodule of a semisimple module is semisimple.

Proof. If M is semisimple, then M is completely reducible. Submodule of completely reducible modules are completely reducible. Then by the above theorem, the submodule is semisimple. □

Theorem 6.4.7: Maschke's Theorem

Let G be a group, $\mathbb{F}$ a field of characteristic p. Then the group algebra $\mathbb{F}G$ is semisimple if and only if G is of finite order n with p not dividing n.

6.5 Radical

Definition 6.5.1: Cosimple

Let M be an R-module. We say that a submodule N of M is cosimple if $\frac{M}{N}$ is simple.

Lemma 6.5.2

Let M be an R-module and N a submodule of M. Then N is cosimple if and only if N is a maximal proper submodule of M.

Definition 6.5.3: Radical

Let M be an R-module. Define the radical of M to be the intersection

$$\text{rad}(M) = \bigcap_{\substack{S \leq M \\ S \text{ is cosimple}}} S$$

of all cosimple submodules of M.

Lemma 6.5.4

Let M be an R-module. If M is semisimple, then $\text{rad}(M) = 0$.

Definition 6.5.5: Artinian Modules

A left R-module M is said to be Artinian if for every descending chain of submodules

$$N_1 \supseteq N_2 \supseteq \cdots \supseteq N_n \supseteq \cdots$$

there exists $m \in \mathbb{N}$ such that $N_n = N_m$ for all $n > m$.

Theorem 6.5.6

Let M be an Artinian left R-module. Then M is semisimple if and only if $\text{rad}(M) = 0$.