Rings and Modules

Labix

May 11, 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 the following are true.

- $\ker(\phi)$ is an ideal of R
- $\text{im}(\phi) \leq S$ is a subring of S

Moreover, we have an isomorphism

$$\frac{R}{\ker(\phi)} \cong \phi(R)$$

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

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

and so we conclude. □

Theorem 1.1.2: The Second Isomorphism Theorem for Rings

Let $A \leq R$ and B an ideal of R. Then the following are true.

- $A + B = \{a + b \mid a \in A, b \in B\}$ is a subring of R
- $A \cap B$ is an ideal of A

Moreover, we have an isomorphism

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

in rings.

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 the set $R \times S = \{(r, s) \in R \times S\}$ together with the binary operations defined element wise.

It is a routine exercise to check that $R \times S$ is indeed a ring in its own right.

A rather unintuitive definition is that of coprime ideals.

Definition 1.2.2: 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 1.2.3

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

$$AB = A \cap B$$

Proof. □

Theorem 1.2.4: Chinese Remainder Theorem

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

$$\phi : R \to \frac{R}{I_1} \times \cdots \times \frac{R}{I_n}$$

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

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

Moreover, if each I_j and I_k are pairwise coprime, then there is an isomorphism

$$\frac{R}{I} \cong \frac{R}{I_1} \times \cdots \times \frac{R}{I_n}$$

given by ϕ.

Proof. Since ϕ is a collection of projections on to each factor, ϕ is a ring homomorphism. It is clear that I is the kernel of the homomorphism. Indeed given $x \in I$, then x lies in each and every I_k for $1 \leq k \leq n$. Thus $\phi(x) = (x + I_1, \ldots, x + I_n) = 0$. Conversely, if $(x + I_1, \ldots, x + I_n)$ is such that applying ϕ gives 0, then $x \in I_1, \ldots, I_n$ so that $x \in I$.

When the ideals are pairwise corpime, consider the elements $e_k = (0, \ldots, 0, x + I_k, 0, \ldots, 0)$ for $1 \leq k \leq n$ (these are called full system of orthogonal central idempotents). Notice that they satisfy the equation $1 = e_1 + \cdots + e_n$ and $e_k^2 = e_k$ for $1 \leq k \leq n$ for $i \neq j$, we have $e_i e_j = 0$. Now since I_i and I_j are coprime, we have that $R = I_i + I_j$ so that $1 = a_j + z_j$ for $a_j \in I_i$ (note the subscript) and $z_j \in I_j$. Define $x_i = z_1 \cdots z_{i-1} \cdot z_{i+1} \cdots z_n$ for each $1 \leq i \leq n$. Write the projection homomorphism as $\psi : R \to R/I_j$. If $i \neq j$, then $\phi_j(x_i) = 0$ because x_i contains the element z_j that lies in I_j. Also, we have that

$$\psi_i(z_j) = \psi_i(1 - a_j) = \psi_i(1) - \psi_i(a_j) = \psi_i(1) = 1$$

in R/I_i since $a_j \in I_i$. Thus we have that

$$\psi_i(x_i) = \psi_i(z_1) \cdots \psi_i(z_n) = 1$$

All this means that $x_i \in R$ is such that $\psi(x_i) = (0, \ldots, 0, 1 + I_i, 0, \ldots, 0)$ for $1 \leq i \leq n$. Now to prove surjectivity, let $(r_1, \ldots, r_n)$ be an element in the product. Then we have that

$$(r_1, \ldots, r_n) = \sum_{j=1}^{n} \psi(r_i) e_i = \sum_{j=1}^{n} \psi(r_i x_i)$$

and so $r_1 x_1 + \cdots + r_n x_n \in R$ is our desired element. And so we are done. □

This is a more generalized version of the Chinese Remainder Theorem in number theory. Indeed, to recover the one in number theory, take $R = \mathbb{Z}$ and $I_k = (n_k)$ for some $n_k \in \mathbb{Z}$ so that I_k is the principal ideal on n_k. Moreover, by choosing each n_k to be pairwise coprime, we obtain the isomorphism which proves that the congruence relation can be solved.

Notice that the proof is instructive. Indeed we can simply follow the steps of the proof to find a solution. Namely, given $(r_1, \ldots, r_n)$ in the product, we can find $r \in R$ such that $\phi(r) = (r_1, \ldots, r_n)$. The steps are as follows.

1. Fix $1 \leq i \leq n$. Using $R = I_i + I_j$, find $a_j \in I_i$ and $z_j \in I_j$ such that $1 = a_j + z_j$ for each j. This can be done for example by Bezout's lemma in $R = \mathbb{Z}$.
2. Define $x_i = z_1 \cdots z_{i-1} \cdot z_{i+1} \cdots z_n$ for $1 \leq k \leq n$.
3. Do the same for each $1 \leq i \leq n$. The solution is then $r = r_1 x_1 + \cdots + r_n x_n$.

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 an abelian group $(M, +)$ together with an action of R on M denoted by $\cdot : R \times M \to M$ such that

- $r \cdot (m + n) = r \cdot m + r \cdot n$ for all $r, s \in R$, $m \in M$
- $(rs) \cdot m = r \cdot (s \cdot m)$ for all $r, s \in R$, $m \in M$
- $(r + s) \cdot m = r \cdot m + s \cdot m$ 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 $r \in R$, $n \in N$.

Submodules of a ring R are well known objects. They are just the ideals of R.

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 $x, y \in N$

Definition 2.1.4: Sum of Submodules

Let M, N be left R-submodules of an R-module K. Define the sum of M and N to be the set

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

together with a ring operation $\cdot : R \times M + N \to M + N$ defined by

$$(r, m + n) = r \cdot (m + n) = r \cdot m + r \cdot n$$

Lemma 2.1.5

Let M and N be left R-submodules of an R-module K. Then $M + N$ is an R-submodule of K.

Proof. Notice that since the underlying group of K is abelian, we have that $M + N$ is a

group. Also it is clear by definition of the ring operation on $M+N$ that the operation is closed. Thus $M+N$ is an R-submodule of K. □

Proposition 2.1.6: 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 $\text{im}(\phi) = \{n \in N | n = \phi(m) \text{ for some } m\}$

Definition 2.2.3: Quotient Module

Let M be an R-module and N a submodule of M. Define the quotient module of M and N to be the abelian quotient group

$$\frac{M}{N} = \{m + N \mid m \in M\}$$

together with the left ring operation $\cdot : R \times \frac{M}{N} \to \frac{M}{N}$ defined by

$$(r, m+N) = r \cdot (m+N) = rm + N$$

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

Moreover, we have an isomorphism

$$\frac{M}{\ker(\phi)} \cong \phi(M)$$

of modules.

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 the following are true.

- A and B are submodules of $A + B$
- $A \cap B$ is a submodule of A and B

Moreover, we have the following isomorphism

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

of quotient R-modules.

Proof. It is clear that A and B are subgroups of $A + B$. Moreover, the left R-action on A and B is closed since they are left R-submodules. Thus A and B are submodules of $A + B$. The proof for $A \cap B$ is similar.

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.

$$\left\{\begin{smallmatrix}\text{Submodules of } M \\ \text{containing } N\end{smallmatrix}\right\} \xleftrightarrow{1:1} \left\{\begin{smallmatrix}\text{Submodules} \\ \text{of } M/N\end{smallmatrix}\right\}$$

The correspondence is given by sending A to A/N for all $A \supseteq N$.

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

$$\text{End}_R(M) = \{\phi : M \to M \mid \phi \text{ is an isomorphism of } M\}$$

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. □

The following lemma shows that endomorphisms of R as an R-module consists of precisely the left multiplications of R by each element in R (Thus also having an isomorphism on right multiplication).

Moreover, the ring structures are compatible so that it is not just a bijection.

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: Direct Product of Modules

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

$$\prod_{i \in I} M_i = \left\{ (m_i)_{i \in I} \,\middle|\, m_i \in M_i \right\}$$

together with the left R-module structure inherited component wise.

Definition 2.5.2: External Direct Sum of Modules

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

the family of modules to be

$$\bigoplus_{i\in I} M_i = \left\{ (m_i)_{i\in I} \in \prod_{i\in I} M_i \;\middle|\; m_i \neq 0 \text{ for finitely many } i \right\}$$

There is no different between finite direct sum and finite direct products. However when I is an infinite indexing set, there is a big difference. For instance, a direct product of rings is still a ring but infinite direct product of rings is not a ring.

Definition 2.5.3: Internal Direct Sum of Modules

Let I be an indexing set and $\{N_i \mid i \in I\}$ be a family of submodules of a left R-module M. Define

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

If the external direct product is isomorphic to

$$\bigoplus_{i\in I} N_i \cong \sum_{i\in I} N_i$$

then we call $\sum_{i\in I} N_i$ the internal direct sum and denote it with $\bigoplus_{i\in I} N_i$ instead. If $M \cong \bigoplus_{i\in I} N_i$ then we say that M is the internal direct sum.

Thus there is no distinction in external and internal direct sum of modules, just that whether our view point starts with the larger module M or with the collection $\{M_i \mid i \in I\}$.

Lemma 2.5.4

Let I be an indexing set and $\{N_i \mid i \in I\}$ be a family of submodules of a left R-module M. Define $\phi : \bigoplus_{i\in I} N_i \to M$ by

$$\phi\left((m_i)_{i\in I}\right) = \sum_{i\in I} m_i$$

Then the following are true.

- $\text{im}(\phi) = \sum_{i\in I} N_i$
- If ϕ is injective then $\sum_{i\in I} N_i$ is the internal direct sum
- ϕ is bijective then M is the internal direct sum of $\{N_i \mid i \in I\}$

Proof. Firstly, it is clear that $\text{im}(\phi) = \sum_{i\in I} N_i$ by definition of ϕ. If ϕ is injective then we obtain an isomorphism $\bigoplus_{i\in I} N_i \cong \sum_{i\in I} N_i$ by the first isomorphism theorem of modules. Finally if ϕ is also surjective then we have $M = \sum_{i\in I} N_i \cong \bigoplus_{i\in I} N_i$ and so we are done. □

2.6 Free Modules

Definition 2.6.1: Basis of a Module

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.

By considering r_b being dependent on $b \in B$, we can define

$$\text{Fun}_f(B, R) = \{f : B \to R \mid f(b) = 0_R \text{ for all but finitely many } b \in B\}$$

then we can rewrite the definition of generating sets to be if for every $m \in M$, there exists $f \in \text{Fun}_f(B, R)$ such that $m = \sum_{b \in B} f(b) \cdot b$. We can also define linear independence in a similar fashion.

Basis for a module is similar to a basis for vector spaces. Indeed every field is a ring so one can think of modules as a generalization for vector spaces. However, not every module admits a basis just like the theory in vector spaces. When they do admit a basis, we call the module a free module.

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.

Conversely, every set of elements forms the basis for a free R-module. This is what it means for the R-module to be free, as a universal property.

Lemma 2.6.3

For every set B there is a free left R-module

$$\bigoplus_{b \in B} R = \left\{ (r_1, r_2, \dots) \in \prod_{b \in B} R \mid \text{ All but finitely many } r_i \text{ is } 0 \right\}$$

with basis of cardinality $|B|$.

Proof. $\prod_{b \in B} R$ inherits the structure of an R-module be defining component wise addition and left R-action. Notice that $\{(1, 0, \dots,), (0, 1, 0, \dots), \dots\}$ is then a basis with cardinality B since every element in $\bigoplus b \in BR$ only has finitely many non zero components so that it is a unique linear combination of the the set.

Alternatively, notice that $\prod_{b \in B} R = \text{Fun}(B, R)$ the set of all functions from B to R together with addition and left R-action defined on elements. Then $\bigoplus_{b \in B} R = \text{Fun}_f(B, R)$ and that the delta functions

$$\delta_b(x) = \begin{cases} 1 & \text{if } x = b \\ 0 & \text{if } x \neq b \end{cases}$$

form a basis for $\bigoplus_{b \in B} R$. □

Notice that while the countable Cartesian product $\prod_{b \in B} R$ is indeed a left R-module, it is not a free module. Because in the definition of a generating set we always require it to be finite. But elements in $\prod_{b \in B} R$ can have countably many long components.

Lemma 2.6.4

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

Proof. Let M be an R-module. Choose a generating set $B \subseteq M$. This is always possible because trivially we can choose $B = M$. Define a map $\pi_B : \bigoplus_{b \in B} R \to M$ by

$$\pi_B(r_1, r_2, \dots) = \sum_{b \in B} r_b \cdot b$$

Note that the sum is finite since elements of $\bigoplus_{b \in B} R$ has finitely many non-zero components. It is clear that it is an R-module homomorphism. It is also surjective by definition of a generating set. By the first isomorphism theorem for module, we have that

$$\frac{\bigoplus_{b \in B} R}{\ker(\pi_B)} \cong M$$

and so we conclude. □

The following is reminiscent of a theorem in linear algebra. However note that we require that R to be a division ring. Because we only dealt with finite dimensional vector spaces in Linear Algebra, we will need Zorn's lemma to deal with the case that the basis set has countable cardinality. Recall Zorn's lemma: If $(\mathcal{P}, \preceq)$ is a non empty poset such that every chain $P_1 \preceq P_2 \preceq \cdots$ has an upper bound, then $(\mathcal{P}, \preceq)$ contains a maximal element.

Theorem 2.6.5

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

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

Proof.

- Let S be a linearly independent set. Let $(\mathcal{P}, \subseteq)$ be the poset ordered by inclusion, where elements are subsets $S \subseteq X \subseteq M$ and that X is linearly independent. $\mathcal{P}$ is non empty since $S \in \mathcal{P}$. Let $\mathcal{C}$ be a chain in $\mathcal{P}$. If $\mathcal{C}$ is empty, then any $X \in \mathcal{P}$ is an upper bound. So assume that $\mathcal{C}$ is non-empty. Consider the set

  $$T = \bigcup_{X \in \mathcal{C}} X$$

  Clearly $X \subseteq T$ for all $X \in \mathcal{C}$. It remains to show that $T \in \mathcal{P}$.

  Clearly $S \subseteq T$. We now want to show that T is a linearly independent set. Let $v_1, \dots, v_m \in T$ and $a_1, \dots, a_m \in R$ such that

  $$\sum_{k=1}^{m} a_k v_k = 0$$

  Since T is the union of $X \in \mathcal{C}$, each v_j belongs to some $X_j \in \mathcal{C}$. Since $\mathcal{C}$ is a chain, one of these sets, X_m contains all the other X_j. Thus $v_1, \dots, v_m \in X_m$. Since $X_m \in \mathcal{P}$, we conclude that $a_1 = \cdots = a_m = 0$. Thus T is linearly independent so that $T \in \mathcal{P}$.

  By Zorn's lemma, $\mathcal{P}$ has a maximal element Z. Suppose that Z does not span M. Then there exists $v \in M$ that is not a finite linear combination of elements of Z. Since Z is

maximal, $Z \cup \{v\}$ does not belong to $\mathcal{P}$ and hence is linearly dependent. Thus there are $v_1, \ldots, v_m \in Z$ and $a_1, \ldots, a_m, a \in R$ not all 0 such that

$$\sum_{k=1}^{m} a_k v_k + av = 0$$

If $a = 0$ then we have linear dependence among $v_1, \ldots, v_m$, a contradiction. Thus $a \neq 0$. Since R is a division ring, a has an inverse a^{-1}. Hence

$$v = -a^{-1}a_1 v_1 - \cdots - a^{-1}a_m v_m$$

This is a contradiction. Thus Z is a basis.

- Suppose that $(\mathcal{P}, \subseteq)$ is the poset under inclusion with elements of $\mathcal{P}$ being subsets $X \subseteq Q$ and X is linearly independent. Notice that $\emptyset \in \mathcal{P}$ so $\mathcal{P}$ is non empty. By a similar argument as above, we can conclude that $\mathcal{P}$ has an upper bound. By Zorn's lemma, $\mathcal{P}$ has a maximal element Z. It is linearly independent and is contained in Q. Now Z is a basis once we have shown that Z generates M. Since every $v \in M$ is a finite linear combination of elements of Q, we just have to express every $q \in Q$ as a linear combination of Z.

  Suppose that this is false. Then there exists $q \in Q$ such that q is not a linear combination of Z. By a similar argument as above, $Z \cup \{v\}$ is a bigger element of $\mathcal{P}$, contradicting the fact that Z is maximal. Thus we are done.

- Either apply the first point with $S = \emptyset$ or apply the second point with $Q = M$.

This concludes the proof. □

It is not a coincidence that we require R to be a division ring. Every division ring is an invariant basis number (IBN) ring.

Definition 2.6.6: Invariant Basis Number Property

Let R be a ring. We say that R has the invariant basis number (IBN) property if every free R-module has equal cardinality for basis.

Proposition 2.6.7

Every division ring is an IBN-ring.

Proposition 2.6.8

Every commutative ring is an IBN-ring.

Proposition 2.6.9

Let R be a ring. Then R is an IBN-ring if and only if $R^m \cong R^n$ implies that $m = n$.

Proposition 2.6.10

Let $f : R \to S$ be a surjective non zero ring homomorphism. Let S be an IBN-ring. Then R is also an IBN-ring.

2.7 Simple Modules

The first structural result on Modules is the baby Artin-Wedderburn theorem. It relies on another powerful lemma called Schur's lemma, which has a fundamental application in Representation theory. We begin with the notion of 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.

Proof. Let $\mathcal{P}$ be the set of all proper left ideals of R ordered by inclusion. Since R is non-zero, the ideal (0) is proper and so belongs to $\mathcal{P}$. Thus $\mathcal{P} \neq \emptyset$. Let $\mathcal{C}$ be a chain in $\mathcal{P}$. Define

$$Z = \bigcup_{X \in \mathcal{C}} X$$

If $\mathcal{C}$ is empty then $Z = \{0\}$. We show that Z is a left ideal. Clearly $0 \in Z$. If $a \in Z$ and $r \in R$, then $a \in X$ for some $X \in \mathcal{C}$ so that $ra \in X \subseteq Z$. Now suppose that $a, b \in Z$. Then $a \in X$ and $b \in Y$ for some $X, Y \in \mathcal{C}$. Since $\mathcal{C}$ is a chain, without loss of generality assume that $X \subseteq Y$. Then $a \in Y$ so that $a + b \in Y \subseteq Z$. Thus Z is a left ideal.

Since all $X \in \mathcal{C}$ are proper ideals with $1 \notin X$, then $1 \notin Z$. Then Z is proper and $Z \in \mathcal{P}$. Z is then an upper bound of $\mathcal{C}$. By Zorn's lemma, $\mathcal{P}$ has a maximal element. Then the maximal element is a maximal left ideal of R. □

As a result, we can prove the existence of a simple left R-module for any ring R.

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 2.7.2. □

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 2.6.5. Now suppose that R is a non-zero ring such that every left R-module is free. By corollary 2.7.4, 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 Algebras over a Ring

3.1 Associative Algebras

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 $x, y \in A$.

A prototypical example of an algebra would be a ring itself. Indeed for a ring R, R is a left R-module via the action of left multiplication.

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 $f(R) \subseteq Z(A)$.

This establishes a one-to-one correspondence

$$\left\{ (A, R) \;\middle|\; A \text{ is an } R\text{-algebra} \right\} \overset{1:1}{\longleftrightarrow} \left\{ \phi : R \to A \;\middle|\; \begin{array}{c} \phi \text{ is a ring homomorphism} \\ \text{such that } f(R) \subseteq Z(A) \end{array} \right\}$$

Notice that when R is a field, the algebra A becomes a vector space over R.

Lemma 3.1.3

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

Proof. If A is an F-algebra, then it is clear that properties of a vector space holds. Indeed A is an abelian group and F is a left action on A such that distributivity, associativity and identity is satisfied. Conversely, if A is a vector space over F, then the distributivity law is satisfied by definition of a vector space. Moreover F satisfies associativity and identity so that F is a ring action on A. □

Definition 3.1.4: R-Subalgebra

Let A be an R-algebra. An R-subalgebra of A is a subring of A which is also an R-algebra in its own right.

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: 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 $x, y \in A$

Definition 3.1.7: 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. □

Under the correspondence of associative algebra, the above proposition gives a another correspondence between the first one.

$$\left\{ (A, R) \;\middle|\; \begin{array}{c} A \text{ is a commutative} \\ R\text{-algebra} \end{array} \right\} \overset{1:1}{\longleftrightarrow} \left\{ \phi : R \to A \;\middle|\; \begin{array}{c} \phi \text{ is a ring homomorphism} \\ \text{such that } f(R) \subseteq Z(A) = A \end{array} \right\}$$

In particular, the construction above are inverses of each other so that it gives the one-to-one correspondence.

3.3 Free Algebras

The polynomial rings defined in Group and Rings enjoy much more structure than just being a ring. In fact, the prototypical example of an algebra is the polynomial ring $R[x]$ for a ring R. It is in fact a free R-module with basis $\{1, x, x^2, \dots\}$. While $R[x]$ can be decomposed into a direct sum of R-modules, $R[x]$ itself is also an R-module so that $R[x]$ becomes a commutative algebra.

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 $\{x^n \mid n \in \mathbb{N}\}$.

If we do not allow the basis elements of $R[x]$ to commute, we obtain a free algebra.

Definition 3.3.2: Free Algebra

Let R be a ring. Let $X = \{x_1, \dots, x_k\}$. The free algebra $R\langle X \rangle = \mathbb{F}\langle x_1, \dots, x_k \rangle$ 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 $\mathbb{F}\langle X \rangle$,

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

For $X = \{x\}$ to be a set of one element, then $\mathbb{F}\langle X\rangle$ has vector space basis $\{1, x, x^2, \dots\}$ which coincides with $\mathbb{F}[x]$. Thus $\mathbb{F}[x] = \mathbb{F}\langle x\rangle$. However, if $X = \{x, y\}$ is a set of two elements, then the basis of $\mathbb{F}\langle X\rangle$ as a vector space over $\mathbb{F}$ is

$$\{1, x, y, x^2, xy, yx, y^2, \dots\}$$

Compare it to that of $\mathbb{F}[x, y]$ which has basis

$$\{1, x, y, x^2, xy = yx, y^2, \dots\}$$

Since $\mathbb{F}\langle X\rangle$ not commuting, the cardinality of the basis becomes large. Fortunately, the size of the basis is still countable.

Proposition 3.3.3

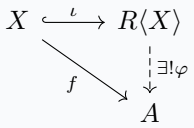
If X is a non-empty countable set, then the dimension $\dim_{\mathbb{F}}(\mathbb{F}\langle X\rangle)$ is countable.

Proof. Relabel elements of X as $X = \{x_1, x_2, \dots\}$. The monomials x_i form a basis of $\mathbb{F}\langle X\rangle$. For each d, the monomials of degree d are finite. Thus the basis of X is a countable union of finite sets. Thus the basis is countable. □

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

Proposition 3.3.4: Universal Property

The free algebra $R\langle X\rangle$ over a ring R satisfies the following universal property. If A is an R-algebra, then for every $f : X \to A$ a map of sets, there exists a unique homomorphism of algebras $\varphi : R\langle X\rangle \to A$ such that $\varphi(x_i) = f(x_i)$ for each $x_i \in X$. In other words, the following diagram commutes:



where $\iota : X \to R\langle X\rangle$ is the inclusion.

Proof. Consider the set of monomials over elements of X. They form a basis of $R\langle X\rangle$ as an R-module. For a monomial $x_{i_1} \cdots x_{i_m}$, define

$$\varphi(x_{i_1} \cdots x_{i_m}) = f(x_{i_1}) \cdots f(x_{i_m})$$

and extend it by R-linearity. Then it is clear that φ is a well defined algebra homomorphism that satisfies the theorem. Any other homomorphism as in the theorem must satisfy the above conditions thus φ is unique. □

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 Radicals

5.1 The Radical of a Module

Definition 5.1.1: Cosimple

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

Lemma 5.1.2

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.

Proof. If N is cosimple then M/N has no non-trivial submodules. By the correspondence theorem this implies that there are not submodules of M containing N. Thus N is a maximal proper submodule of M. If N is a maximal proper submodule of M, then by the correspondence theorem, M/N has no submodules and so is simple. □

Definition 5.1.3: 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.

We can draw a connection between the radical and the socle. Consider $\mathbb{Z}$ as a $\mathbb{Z}$-module. It is clear that $\mathbb{Z}$ has no simple submodules. Indeed for any $k \in \mathbb{Z}$, $k\mathbb{Z}$ has a submodule $(2k)\mathbb{Z}$. Since $\mathbb{Z}$ is a principal ideal domain this concludes all possible ideals. Thus

$$\text{soc}(\mathbb{Z}) = 0$$

As for the radical, notice that quotient modules of $\mathbb{Z}$ are modules of the form $\mathbb{Z}/k\mathbb{Z}$. It does not have a subgroup exactly when $k = p$ is a prime. The intersection of all such groups is then 0 so that

$$\text{rad}(\mathbb{Z}) = 0$$

There is a duality between the radical and the socle as follows. For $n \in \mathbb{N}$, consider $\mathbb{Z}/n\mathbb{Z}$ as a $\mathbb{Z}$-module. Clearly we have that its simple modules are exactly the submodules $\mathbb{Z}/(n/k)\mathbb{Z}$ when n/k is a prime number. Similarly, $\mathbb{Z}/n\mathbb{Z}$ has a cosimple submodule of the form $\mathbb{Z}/(n/p)\mathbb{Z}$ when p is a prime.

The notion of a radical is reminiscent to the radical of a number. In number theory, the radical of $n = p_1^{a_1} \cdots p_k^{a_k} \in \mathbb{N}$ is defined by $\text{rad}(n) = p_1 \cdots p_k$. Write $r = \text{rad}(n)$. It is easy to see that

$$\text{soc}(\mathbb{Z}/n\mathbb{Z}) = \frac{n}{r}\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/r\mathbb{Z} \cong \frac{\mathbb{Z}/n\mathbb{Z}}{\text{rad}(\mathbb{Z}/n\mathbb{Z})}$$

and that

$$\text{rad}(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/(n/r)\mathbb{Z}$$

5.2 The Nilradical Ideal

Definition 5.2.1: Nilpotents

Let R be a ring. An element $x \in R$ is said to be nilpotent if $x^n = 0$ for some $n \in \mathbb{N}$.

Definition 5.2.2: Nil Ideals and Nilpotent Ideals

Let R be a ring. An ideal I is said to be nil if all $x \in I$ is nilpotent. I is said to be nilpotent if $I^n = 0$ for some $n \in \mathbb{N}$.

Lemma 5.2.3

Let R be a ring. Then every nilpotent ideal is nil.

Not every nil ideal is nilpotent.

Definition 5.2.4: Quasiregular

Let R be a ring. An element $x \in R$ is said to be quasiregular if $1 + x$ is invertible. An ideal I in R is said to be quasiregular if every $x \in I$ is quasiregular.

Lemma 5.2.5

Every nilpotent element is quasiregular. Moreover, every nil ideal of a ring R is quasiregular.

Proof. If $x^n = 0$, then

$$(1 + x)(1 - x + x^2 - \cdots + (-1)^{n-1}x^{n-1}) = 1 + (-1)^{n-1}x^n = 1$$

Thus we have constructed an inverse. It follows that every nil ideal is quasiregular. □

The converse is in general false. Consider the matrix ring $M_n(\mathbb{F})$ over a field $\mathbb{F}$. A matrix is nilpotent if and only if 0 is the only eigenvalue. A matrix is quasiregular if and only if -1 is not an eigenvalue. These are not strict implications on one another.

For the statement for ideals, consider $\mathbb{C}[[x]]$ the ring of formal power series and the subring $\mathbb{C}((x))$ of Laurent power series. The ideal

$$(x) = \{f \in \mathbb{C}((x)) \mid a_0 = 0\}$$

is quasiregular but not nil. Indeed $x \in (x)$ is not nilpotent but every $z \in (x)$ is of the form $a_1x + a_2x^2 + \ldots$ so that $1 + z = 1 + a_1x + a_2x^2 + \ldots$ is invertible.

Proposition 5.2.6

Suppose that R is a ring such that I and J are nilpotent. Then $I + J$ is nilpotent.

Proof. Suppose that $I^n = 0$ and $J^m = 0$. For any $x_i \in I$ and $y_j \in J$, we have that

$$\prod_{i=1}^{n}(x_i + y_i) = x_1x_2 \cdots x_n + \text{ terms involving at least one } y_i$$

so that

$$(I + J)^{nm} = ((I + J)^n)^m \subseteq (I^n + J)^m = J^m = 0$$

□

5.3 Annihilator

Definition 5.3.1: Annihilators

Let R be a ring and M an R-module. Let $m \in M$. Define the annihilator of m to be

$$\text{Ann}_R(m) = \{r \in R \mid rm = 0\}$$

Define the annihilator of M to be

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

Right annihilators are defined similarly.

When R is commutative left annihilators and right annihilators are the same.

Lemma 5.3.2

Let R be a ring and M an R-module. Let $m \in M$. Then $\text{Ann}_R(m)$ and $\text{Ann}_R(M)$ are left ideals of R. Moreover, $\text{Ann}_R(m)$ is a maximal ideal of R.

5.4 The Jacobson Radical

Definition 5.4.1: Jacobson Radical

Let R be a ring. The Jacobson radical of R is the radical of R as a left R-module. This is denoted as

$$J(R) = \text{rad}(R)$$

Theorem 5.4.2

Let R be a ring. The following are equal for R as a left R-module.

- The Jacobson radical $J(R) = \text{rad}(R)$
- The intersection
$$J_1 = \bigcap_{\substack{I \text{ is a maximal} \\ \text{ideal of } R}} I$$
of maximal ideals
- The intersection
$$J_2 = \bigcap_{M \text{ is simple}} \text{Ann}_R(M)$$
of all annihilators of simple modules
- The largest quasiregular two-sided ideal J_3.

Proof.

- $J(R) \subseteq J_2$: Let $x \in J(R)$ and M a simple R-module. For each $m \in M$ non zero, $\text{Ann}_R(m)$ is a maximal left ideal of R, in other words it is a cosimple submodule of R as a left R-module. Thus $x \in \text{Ann}_R(m)$ and $xm = 0$. It follows that $xM = 0$ and $x \in J_2$.
- $J_2 \subseteq J_1$: Let $x \in J_2$ and let I be a maximal left ideal of R. Then R/I is a simple left module so $x(R/I) = 0$. It follows that $x + I = x(1 + I) = I$. Thus $x \in I$ and $x \in J_1$.

- J_1 is a quasiregular ideal. Let $x \in J_1$. Notice that $R(1+x) = R$ because if not, then $R(1+x)$ is contained in a maximal ideal L. Then both $x \in L$ and $1+x \in L$, thus $1 \in L$ and $L = R$. Thus $1+x$ has an inverse in R, say $1+y$. Then $(1+y)(1+x) = 1$ so that $y+x+yx = 0$ and so that $y = -x - yx \in J_1$. Hence $1+y$ also has a left inverse z. Thus

$$z = z(1+y)(1+x) = 1+x$$

  and that x is quasiregular.

- For any quasiregular ideal I, $I \subseteq J(R)$. Suppose the contrary. Then there exists a quasiregular ideal I not in $J(R)$. Since $J(R) \subseteq J_2 \subseteq J_1$ and J_1 is the intersection of maximal left ideals, there exists a maximal left ideal L and $x \in I$ such that $x \notin L$. Then $L + Rx = R$ and $1 = k + rx$ for some $k \in L$ and $r \in R$. But then $k = 1 - rx = 1 + (-r)x$ is invertible since $-rx \in I$. This implies that $L = R$, which is a contradiction.

- J_2 is a two sided ideal. It is clear that J_2 is an additive subgroup. Let $x \in J_2$ and $r \in R$ and M a simple R-module. We know that $xM = 0$. But also we have that $xrM \subseteq xM = 0$ and $rxM \subseteq r\{0\} = 0$. Thus J_2 is a two sided-ideal.

- Conclusion: By the fist four points, $J(R) \subseteq J_2 \subseteq J_1 \subseteq J(R)$ so that they all are equal. Moreover, $J(R)$ contains every quasiregular ideal so $J(R) = J_3$.

□

In particular, the last equivalent characterization means that $J(R)$ is a two sided ideal so that all the above equivalent characterizations also work when considering R as a right R-module.

One can imagine the Jacobson radical to work well in commutative algebra. Indeed it is a two sided ideal so that when everything is commutative, the notion of the Jacobson radical still makes sense. We will see more of the Jacobson radical in Commutative Algebra.

Lemma 5.4.3

Let R be a ring. Then we have

$$J\left(\frac{R}{J(R)}\right) = 0$$

6 Chain Conditions

6.1 Noetherian Rings and Modules

Definition 6.1.1: Ascending Chain Condition

An R-module M is said to satisfy the ascending chain condition if for any $M_1, M_2, \ldots$ submodule of M such that

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$$

is an ascending chain, then there is a positive integer n such that $M_i = M_n$ for all $i \geq n$.

Definition 6.1.2: Noetherian Rings and Modules

Let R be a ring. Let M be a left R-module. We say that M is left (right) Noetherian if M satisfies the ascending chain condition. We say that a ring R is left (right) Noetherian if R is Noetherian when viewed as an R-module.

An R-module or a ring is said to be Noetherian if it is both left and right Noetherian.

The Noetherian property depends on the left / right module structure. For example,

$$R = \begin{pmatrix} \mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix}$$

is right Noetherian but not left Noetherian.

Proposition 6.1.3

Let R be a ring and M an R-module. Then the following are equivalent.

- M is Noetherian
- Every submodule of M is finitely generated
- Every non empty collection of submodules of M has a maximal element

Proposition 6.1.4

Let N be an R-submodule of M. Then M is Noetherian if and only if N and M/N are Noetherian.

6.2 Artinian Rings and Modules

Definition 6.2.1: Descending Chain Condition

An R-module M is said to satisfy the descending chain condition if for any $M_1, M_2, \ldots$ submodules of M such that

$$M_1 \supseteq M_2 \supseteq M_3 \supseteq \cdots$$

is an ascending chain, then there is a positive integer n such that $M_i = M_n$ for all $i \geq n$.

Definition 6.2.2: Artinian Rings and Modules

Let R be a ring. Let M be a left R-module. We say that M is left (right) Artinian if M satisfies the descending chain condition. We say that a ring R is left (right) Artinian if R is Artinian when viewed as an R-module.

An R-module or a ring is said to be Artinian if it is both left and right Artinian.

Proposition 6.2.3

Let R be a ring and M an R-module. Then the following are equivalent.

- M is Artinian
- Every non empty collection of submodules of M has a minimal element

Proposition 6.2.4

Let N be an R-submodule of M. Then M is Artinian if and only if N and M/N are Artinian.

Theorem 6.2.5

If R is a left artinian ring, then $J(R)$ is nilpotent.

Recall that an ideal I of a ring is nilpotent if $I^n = 0$ for some $n \in \mathbb{N}$.

Corollary 6.2.6

Let R be a left artinian ring. Then the following are equivalent.

- $J(R)$ is the largest nilpotent two sided ideal of R
- $J(R)$ is the largest nilpotent left ideal of R
- $J(R)$ is the largest nilpotent right ideal of R.