Rings and Modules

Labix

January 13, 2025

Abstract

- Abstract Alebra by Thomas W. Judson

Contents

1 Basic Module Theory

1.1 Introduction to Modules

Definition 1.1.1: 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 1.1.2: 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 1.1.3: Submodule Criterion

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

- $x + y \in N$ for all $x, y \in N$
- $r \cdot x \in N$ for all $x \in N$ and $r \in R$

Proof. Suppose that N is a left R-submodule. Then the above two conditions are satisfied since N is an R-module in its own right. Conversely, the above two conditions imply that the four conditions for the definition of a module is satisfied. □

Definition 1.1.4: Sum of Submodules

Let R be a ring. 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 1.1.5

Let R be a ring. 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. □

Lemma 1.1.6

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

1.2 Module Homomorphisms

Definition 1.2.1: 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 1.2.2: 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 1.2.3: 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

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

1.3 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 1.3.1: 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 1.3.2: 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 1.3.3: 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 1.3.4: 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.

$$\left\{ \begin{matrix} \text{Submodules of } M \\ \text{containing } N \end{matrix} \right\} \overset{\text{1:1}}{\longleftrightarrow} \left\{ \begin{matrix} \text{Submodules} \\ \text{of } M/N \end{matrix} \right\}$$

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

2 Constructing New Modules

2.1 Direct Sum of Modules

Definition 2.1.1: 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 2.1.2: 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.

Proposition 2.1.3

Let R be a ring. Let I be an indexing set. Let M_i be an R-module for each $i \in I$. Then there is an isomorphism

$$\bigoplus_{i\in I} M_i \cong \prod_{i\in I} M_i$$

given component-wise if and only if $|I| \in \mathbb{N}$.

Let R be a ring. Given a left R-module M, how can we recognize that M is isomorphic to a direct sum? We introduce the notion of internal direct sums to identify direct sums.

Definition 2.1.4: 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 2.1.5

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. □

2.2 Free Modules

Free modules is the module analogue of vector spaces. In general, they can be infinite dimensional.

Definition 2.2.1: 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 2.2.2: 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 admits a basis.

Example 2.2.3

Consider the following abelian groups as $\mathbb{Z}$-modules.

- $\mathbb{Z}[x]$ is a free $\mathbb{Z}$-module isomorphic to $\bigoplus_{n\in\mathbb{N}} \mathbb{Z} \cdot x$.
- $\mathbb{Z}[[x]]$ is not a free $\mathbb{Z}$-module but is isomorphic to $\prod_{n\in\mathbb{N}} \mathbb{Z}$.
- $\mathbb{Q}$ is not a free $\mathbb{Z}$-module.

- $\mathbb{Q}/\mathbb{Z}$ is not a free $\mathbb{Z}$-module.
- $\mathbb{R}$ is not a free $\mathbb{Z}$-module.

Notice that while the countable Cartesian product $\prod_{i\in I} R$ is indeed a left R-module, it is not a free module. Because in the definition of a generating set elements of the direct sum is a finite sum of elements. But elements in $\prod_{i\in I} R$ can have countably many long components.

Lemma 2.2.4

Let R be a ring. Let B be a set. Then the external direct sum

$$\bigoplus_{b\in B} R\cdot b$$

is a free left R-module with basis B.

Proof. Notice that $\{1\cdot b \mid b\in B\}$ is a basis with cardinality B since every element in $\bigoplus_{b\in B} R\cdot b$ only has finitely many non zero components so that it is a unique linear combination of the the set. □

Proposition 2.2.5

Let R be a ring. Let M be a free R-module. Then there is an isomorphism

$$M\cong \bigoplus_{i\in I} R$$

for some indexing set I.

Lemma 2.2.6

Let R be a ring. Let M be a left R-module. If M is free, then M is isomorphic

$$M\cong \frac{\bigoplus_{i\in I} R}{J}$$

to a quotient of a free module for some left R-submodule J.

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 2.2.7

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 $v_1, \ldots, v_m \in T$ and $a_1, \ldots, a_m \in R$ 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 $v_1, \ldots, v_m \in X_m$. 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.

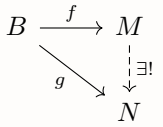
  Suppose that this is false. Then there exists $q \in Q$ such that q is not a linear combination of Z. By a similar argument as above, $Z \cup \{q\}$ is a bigger element of $\mathcal{P}$, contradicting the fact that Z is maximal. Thus we are done.
- Either apply the first point with $S = \emptyset$ or apply the second point with $Q = M$.

This concludes the proof. □

Theorem 2.2.8: Universal Property of Free Modules

Let R be a ring. Let M be an R-module. Let B be a set. Let $f : B \to M$ be a function of sets. Then M is a free module with basis B if and only if the following is true.

For every R-module N and function of sets $g : B \to N$, there exists a unique R-module homomorphism $h : M \to N$ such that the following diagram commutes:



2.3 Finitely Generated Modules

Definition 2.3.1: Finitely Generated Modules

Let R be a ring. Let M be a left R-module. We say that M is finitely generated if M has a finite generating set.

This notion should be somewhat familiar to us. A finitely generated $\mathbb{Z}$-module is just a finitely generated abelian group. We have already classified all finitely generated $\mathbb{Z}$-modules by the fundamental theorem of finitely generated abelian groups.

On the other hand, a finitely generated k-module for a field k is exactly a finite dimensional vector space over k. We have already classified all finitely generated k-modules as they are isomorphic to k^n for some $n \in \mathbb{N}$.

Example 2.3.2

Consider the following abelian groups as $\mathbb{Z}$-modules.

- $\mathbb{Z}[x]$ is not a finitely generated $\mathbb{Z}$-module.
- $\mathbb{Z}[[x]]$ is not a finitely generated $\mathbb{Z}$-module.
- $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}$-module.
- $\mathbb{Q}/\mathbb{Z}$ is not a finitely generated $\mathbb{Z}$-module.
- $\mathbb{R}$ is not a finitely generated $\mathbb{Z}$-module.

Proposition 2.3.3

Let R be a ring. Let M be a left R-module. Then M is finitely generated if and only if there exists a surjective homomorphism $R^n \to M$ for some $n \in \mathbb{N}$.

While free modules mimic the notion of a vector space, finitely generated free modules mirror the notion of finite dimensional vector spaces.

Proposition 2.3.4

Let R be a ring. Let M be an R-module. If M if finitely generated and free, then there is an isomorphism

$$M \cong R^n \cong R^{\oplus n}$$

for some $n \in \mathbb{N}$.

2.4 The Module of Homomorphisms

Definition 2.4.1: The Set of Homomorphisms

Let R be a ring. Let M, N be R-modules. Define the homomorphism ring of R to be the set

$$\text{Hom}_R(M, N) = \{\phi : M \to N \mid \phi \text{ is an } R\text{-module homomorphism}\}$$

of all R-module homomorphisms from M to N.

Proposition 2.4.2

Let R be a ring. Let M, N be R-modules. Then $\text{Hom}_R(M, N)$ is a $Z(R)$-module with the following binary operations.

- For $\phi, \varphi : M \to N$ two R-module homomorphisms, define $\phi + \varphi : M \to N$ by $(\phi + \varphi)(m) = \phi(m) + \varphi(m)$ for all $m \in M$
- For $\phi : M \to N$ an R-module homomorphism and $r \in Z(R)$, define $r\phi : M \to N$ by $(r\phi)(m) = r \cdot \phi(m)$ for all $m \in M$.

In particular, it is an abelian group.

Proof. We first show that the addition operation gives the structure of a group.

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

We now show that

- Let $r, s \in R$, we have that $((sr)\phi)(m) = (sr) \cdot \phi(m) = s \cdot (r \cdot \phi(m)) = s(r(\phi))(m)$ and hence we showed associativity.
- It is clear that $1_R \in R$ acts as the identity of the operation.

Thus we are done. □

2.5 The Endomorphism Ring

Definition 2.5.1: 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 2.5.2

Let R be a ring and M a left R-module. Define two binary operations on $\text{End}_R(M)$ as follows.

- Let $\phi, \psi \in \text{End}_R(M)$. Define $\phi + \psi : M \to M$ by $m \mapsto \phi(m) + \psi(m)$.
- Let $\phi, \psi \in \text{End}_R(M)$. Define $\phi \cdot \psi \in \text{End}_R(M)$ by $m \mapsto \phi(\psi(m))$.

Then $\text{End}_R(M)$ is a ring with the above operations.

Proof. 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

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.

Proposition 2.5.3

Let R be a ring. Then we have an isomorphism

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

Proof.
Define a map $\phi : R \to \text{End}_R(R)$ by

$$r \mapsto \begin{pmatrix} \phi(r) : R \to R \\ x \mapsto x \cdot r \end{pmatrix}$$

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. □

Notice that in the proof it might be more natural to show first that $R^{\text{op}} \cong \text{End}_R(R)$ and then to show that $R^{\text{op}} \cong R$. The first isomorphism is naturally isomorphic but the second one is not. Naturality refers to category theory.

2.6 Tensor Products of Modules

Definition 2.6.1: Bilinear Maps

Let R be a ring. Let A, B, C be R-modules. We say that an R-module homomorphism

$$\varphi : A \times B \to C$$

is bilinear if the following are true.

- Linearity in the first variable:

$$\varphi(sa_1 + ta_2, b) = s\varphi(a_1, b) + t\varphi(a_2, b)$$

  for all $a_1, a_2 \in A$, $b \in B$ and $s, t \in R$.
- Linearity in the second variable:

$$\varphi(a, sb_1 + tb_2) = s\varphi(a, b_1) + t\varphi(a, b_2)$$

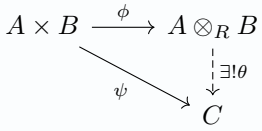
  for all $a \in A$, $b_1, b_2 \in B$ and $s, t \in R$.

Definition 2.6.2: 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 the following universal property as satisfied. For any other R-bilinear map $\psi : A \times B \to C$, there is a unique R-linear map $\theta : A \otimes_R B \to C$ such that the following diagram commutes:



Proposition 2.6.3

Let R be a ring. Let A, B be R-modules. There is a one-to-one correspondence

$$\{\varphi : A \times B \to R \mid \varphi \text{ is bilinear}\} \overset{1:1}{\longleftrightarrow} \text{Hom}_R(A \otimes_R B, R)$$

given by the universal property. Explicitly, denote $\varphi : A \times B \to A \otimes_R B$ the universal map. For each $f \in \text{Hom}_R(A \otimes_R B, R)$, it is mapped to $f \circ \varphi$.

The universal property makes it very abstract and hard to visualize the tensor product. There are a number of explicit ways to think about the tensor product.

Lemma 2.6.4

Let R be a ring. Let A, B be R-modules. Let F be the module over R with basis $(a, b) \in A \times B$. Also let L be the ideal of F generated by the elements of F of the form

- $(a_1 + a_2, b) - (a_1, b) - (a_2, b)$
- $(a, b_1 + b_2) - (a, b_1) - (a, b_2)$
- $(sa, b) - s(a, b)$

- $(a, sb) - s(a, b)$

for $a, a_1, a_2 \in A$, $b, b_1, b_2 \in B$ and $s \in R$. Then the tensor product of A and B is given by

$$A \otimes_R B = \frac{F}{L}$$

Proposition 2.6.5

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 2.6.6

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 2.6.7

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

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

Recall that any abelian group A can also be thought of as a $\mathbb{Z}$-module. The tensor product over $\mathbb{Z}$ or any of its quotient modules are significantly easier to compute.

Proposition 2.6.8

Let A be an abelian group. Then the following are true.

- $\mathbb{Z} \otimes_{\mathbb{Z}} A \cong A$
- $\mathbb{Z}/p\mathbb{Z} \otimes_{\mathbb{Z}} A \cong A/pA$
- $\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/\gcd(m, n)\mathbb{Z}$

2.7 Tensor Products of Vector Spaces

Let $R = k$ be a field and let V, W be finite dimensional vector spaces. Because they are finite dimensional, V and V^* are isomorphic and similarly for W. We can then obtain an interpretation of the tensor product using bilinear maps.

Corollary 2.7.1

Let V, W be finite dimensional vector spaces over a field k. Then there is an isomorphism

$$V \otimes W = \{\varphi : V^* \times W^* \to k \mid \varphi \text{ is multilinear}\}$$

given as follow by the above theorem and the fact that finite dimensional vector spaces are isomorphic to their dual.

Proof. We have that

$$\begin{aligned} \{\varphi : V^* \times W^* \to k \mid \varphi \text{ is multilinear}\} &\cong \mathrm{Hom}_k(V^* \otimes W^*, k) && \text{(thm 3.3.4)} \\ &= (V^* \otimes W^*)^* \\ &\cong V^{**} \otimes W^{**} \\ &\cong V \otimes W \end{aligned}$$

and so we conclude. □

Let V be a vector space over a field k. In particular this means that V is a module over k and all the theory on tensor products apply to V. Because of the importance of the dual space there is more general notion of tensors for vector spaces.

Definition 2.7.2: The Space of Tensors

Let V be a vector space over a field. Let $m, n \in \mathbb{N}$. A type (m, n) tensor of V is an element of the tensor product

$$T_n^m(V) = V^{\otimes m} \otimes (V^*)^{\otimes n}$$

We call $T_n^m(V)$ the space of tensors of V.

Repeatedly applying 3.4.1 gives the following.

Theorem 2.7.3

Let V be a finite dimensional vector space over a field k. Then there is an isomorphism

$$T_n^m = \left\{\varphi : (V^*)^{\times m} \times V^{\times n} \to k \mid \varphi \text{ is multilinear}\right\}$$

given by applying 3.4.1 repeatedly.

3 Some Properties of Modules

3.1 Invariant Basis Number Property

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 3.1.1: 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 3.1.2

Every division ring is an IBN-ring.

Proposition 3.1.3

Every commutative ring is an IBN-ring.

Proposition 3.1.4

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 3.1.5

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.

3.2 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 3.2.1: 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 3.2.2

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 3.2.3

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 3.2.4

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 3.2.5: 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, $\text{im}(\phi) = N$. Thus ϕ is a bijection. □

Corollary 3.2.6: 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 3.2.7: 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. □

4 Exact Sequences of Modules

4.1 Introduction to Exact Sequences

Exact sequences give a compact way of expressing a sequence of homomorphisms and modules.

Definition 4.1.1: Long Exact Sequences

Let R be a ring. Let M_k be a left R-module for each $k \in \mathbb{Z}$. Let $f_k : M_k \to M_{k-1}$ be R-module homomorphisms for each $k \in \mathbb{Z}$. We say that the sequence

$$\cdots \longrightarrow M_1 \xrightarrow{f_{k+1}} M_k \xrightarrow{f_k} M_{k+1} \longrightarrow \cdots$$

is exact if $\text{im}(f_{k+1}) = \ker(f_k)$ for all $k \in \mathbb{Z}$.

We are particularly interested in a special type of long exact sequences: Those that has 3 consecutively non-negative terms.

Definition 4.1.2: Short Exact Sequences

Let R be a ring. A short exact sequence of R-modules is a long exact sequence consisting of 3 consecutive non-zero terms in the sequence. Explicitly, it is given by

$$0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$$

for M_1, M_2, M_3 being R-modules and $f : M_1 \to M_2$ and $g : M_2 \to M_3$ being R-module homomorphisms.

Lemma 4.1.3

Let R be a ring. Let M_1, M_2, M_3 be R-modules. Let $f : M_1 \to M_2$ and $g : M_2 \to M_3$ be R-module homomorphisms. Then the sequence

$$0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$$

is exact if and only if the following are true.

- f is injective.
- g is surjective.
- $\text{im}(f) = \ker(g)$.

Lemma 4.1.4

Let R be a ring. Let M_1, M_2, M_3 be R-modules. Let $f : M_1 \to M_2$ and $g : M_2 \to M_3$ be R-module homomorphisms such that

$$0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$$

is a short exact sequence. Then the following are true.

- $M_1 \cong \ker(g)$
- $M_3 \cong \text{coker}(f) = \frac{M_2}{\text{im}(f)}$

Proof. Since f is injective, by the first isomorphism theorem we conclude that $A \cong \text{im}(f)$. By exactness, $\text{im}(f) = \ker(g)$ so that $A \cong \ker(g)$.

Since g is surjective, by the first isomorphism theorem we conclude that $\frac{B}{\ker(g)} \cong C$. By exactness, $\text{im}(f) = \ker(g)$ and so we conclude. □

From the above we can deduce that whenever we see the following sequences:

$$0 \longrightarrow \ker(g) \overset{\iota}{\hookrightarrow} B \overset{g}{\longrightarrow} C \longrightarrow 0$$

$$0 \longrightarrow A \overset{f}{\longrightarrow} B \overset{q}{\twoheadrightarrow} \frac{B}{\text{im}(f)} \longrightarrow 0$$

are exact by definition.

4.2 Split Exact Sequences

Definition 4.2.1: Split Exact Sequence

Let R be a ring. Let the following be an exact sequence of R-modules.

$$0 \longrightarrow M_1 \overset{f}{\longrightarrow} M_2 \overset{g}{\longrightarrow} M_3 \longrightarrow 0$$

We say that the sequence is split exact if $M_2 \cong M_1 \oplus M_3$.

The following is an important equivalent characterization of split exact sequence.

Proposition 4.2.2: The Splitting Lemma

Let R be a ring. Let the following be an exact sequence of R-modules.

$$0 \longrightarrow A \overset{f}{\longrightarrow} B \overset{g}{\longrightarrow} C \longrightarrow 0$$

Then the following are equivalent.

- The short exact sequence is a split exact sequence
- There exists an R-module homomorphism $p : B \to A$ such that $p \circ f = \text{id}_A$
- There exists an R-module homomorphism $s : C \to B$ such that $g \circ s = \text{id}_C$

Proof.

- (1) $\implies$ (2), (3): Suppose that $B \cong A \oplus C$. Then the projection map $p : A \oplus C \to A$ and the inclusion map $s : C \to A \oplus C$ is such that $p \circ f = \text{id}_A$ and $g \circ s = \text{id}_C$.
- (2) $\implies$ (1): For any $b \in B$, write $b = f(p(b)) + (b - f(p(b)))$. Then $f(p(b)) \in \text{im}(f)$ and $b - f(p(b)) \in \ker(p)$ since $p(b - f(p(b))) = p(b) - p(b) = 0$. Now I claim that $\ker(p) \cap \text{im}(f) = 0$. Indeed if $b \in \ker(p) \cap \text{im}(f)$, then there exists $a \in A$ such that $f(a) = b$. Then
$$a = p(f(a)) = p(b) = 0$$
Thus $b = f(0) = 0$. This shows that $B \cong \ker(p) \oplus \text{im}(f)$.

  Consider the restricted $g|_{\ker(p)} : \ker(p) \to C$. I want to show that g is an isomorphism. Let $b \in \ker\left(g|_{\ker(p)}\right)$. By exactness, there exists $a \in A$ such that $f(a) = b$. Then $a = p(f(a)) = p(b) = 0$ since $b \in \ker(p)$. Thus $b = f(0) = 0$ so that $b \in \ker\left(g|_{\ker(p)}\right)$. For surjectivity, let $c \in C$. By exactness, g is surjective so there exists $b \in B$ such that $g(b) = c$. Since $B \cong \ker(p) \oplus \text{im}(f)$, we can write $b = f(a) + k$ for some $a \in A$ and $k \in \ker(p)$. Then we have that
$$c = g(b) = g(f(a) + k) = g(k)$$
which means that there exists $k \in \ker(p)$ such that $g|_{\ker(p)}(k) = c$. Thus $\ker(p) \cong C$. Since f is injective, $im(f) = f(A) \cong A$. Thus we have that $B \cong \text{im}(f) \oplus \ker(p) \cong A \oplus C$.
- (3) $\implies$ (1): For any $b \in B$, write $b = (b - s(g(b))) + s(g(b))$. Then $s(g(b)) \in \text{im}(s)$ and $g(b) = g(b) - g(s(g(b)) = 0$ so that $b - s(g(b)) \in \ker(g)$. Now I claim that

$\ker(g) \cap \text{im}(s) = 0$. Indeed if $b \in \ker(g) \cap \text{im}(s)$, then there exists $c \in C$ such that $s(b) = c$ and

$$c = g(s(c)) = g(b) = 0$$

since $b \in \ker(g)$ so that $c = 0$. This shows that $B \cong \ker(g) \oplus \text{im}(s)$.

Since $\ker(g) = \text{im}(f)$ by exactness, f being injective also implies that $A \cong \text{im}(f) = \ker(g)$. Since also we have that $g \circ s = \text{id}_C$, we have that s is injective so that $\text{im}(s) \cong C$. Thus we conclude that $B \cong \ker(g) \oplus \text{im}(s) \cong A \oplus C$.

Thus we conclude. □

Proposition 4.2.3

Let R be a ring. Let the following be an exact sequence of R-modules.

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

If C is a free R-module then it is a split exact sequence.

Proof. Since C is a free R-module, there exists a basis $X = \{c_1, \ldots, c_n\}$ such that $C = \bigoplus_{i=1}^n Rc_i$. Since g is surjective, we can find $b_1, \ldots, b_n \in B$ such that $g(b_i) = c_i$ for $1 \leq i \leq n$. By the universal property of free R-modules, there exists an R-module homomorphism $s : C \to B$ such that $s(c_i) = b_i$ for $1 \leq i \leq n$. Now notice that for $c \in C$, we can write $c = \sum_{i=1}^n k_i c_i$ for some $k_i \in \mathbb{Z}$. Since s is an R-module homomorphism, we have that $s\left(\sum_{i=1}^n k_i c_i\right) = \sum_{i=1}^n k_i b_i$. Then we have that

$$g(s(c)) = g\left(\sum_{i=1}^n k_i b_i\right) = \sum_{i=1}^n k_i c_i$$

Thus $g \circ s = \text{id}_C$. By the splitting lemma, we conclude that $B \cong A \oplus C$. □

The following two lemmas are very intuitive and straight forward to remember.

Lemma 4.2.4: Five Lemma

Let R be a ring. Consider the commutative diagram

$$\begin{array}{ccccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} & D & \xrightarrow{j} & E \\ \downarrow{\scriptstyle l} & & \downarrow{\scriptstyle m} & & \downarrow{\scriptstyle n} & & \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle q} \\ A' & \xrightarrow{r} & B' & \xrightarrow{s} & C' & \xrightarrow{t} & D' & \xrightarrow{u} & E' \end{array}$$

where all the objects are R-modules. Suppose that the following are true.

- The two rows are exact
- $m : B \to B'$ and $p : D \to D'$ are isomorphisms
- $l : A \to A'$ is surjective
- $q : E \to E'$ is injective

Then n is an isomorphism.

Proof. For injectivity,
Let $c \in \ker(n)$. Then $n(c) = 0$. By commutativity, we have that

$$p(h(c)) = t(n(c)) = t(0) = 0$$

Since p is an isomorphism, then $h(c) = 0$ and $c \in \ker(h)$. By exactness, we have that $c \in \ker(h) = \text{im}(g)$. Thus there exists $b \in B$ such that $g(b) = c$. Now by commutativity, we

have that

$$s(m(b)) = n(g(b)) = n(c) = 0$$

so that $m(b) \in \ker(s)$. By exactness, we have that $m(b) \in \ker(s) = \text{im}(r)$. Thus there exists $a' \in A'$ such that $r(a') = m(b)$. By surjectivity of l, there exists $a \in A$ such that $l(a) = a'$. By commutativity, we have that

$$m(f(a)) = r(l(a)) = r(a') = m(b)$$

Since m is an isomorphism, $f(a) = b$. Then by exactness, $\ker(g) = \text{im}(f)$ implies

$$0 = g(f(a))g(b) = c$$

Thus $c = 0$ and so n is injective.

For surjectivity,
Let $c' \in C'$. By exactness, we have that $u(t(c')) = 0$. Since p is an isomorphism, there exists $d \in D$ such that $p(d) = t(c')$. By commutativity, we have that

$$q(j(d)) = u(p(d)) = u(t(c')) = 0$$

Since q is injective, $j(d) = 0$. So $d \in \ker(j)$. By exactness, $d \in \ker(j) = \text{im}(h)$. Thus there exists $c \in C$ such that $h(c) = d$. By commutativity, we have that

$$t(n(c)) = p(h(c)) = p(d) = t(c')$$

Thus $t(n(c) - c') = 0$ and $n(c) - c' \in \ker(t)$. By exactness, $n(c) - c' \in \ker(t) = \text{im}(s)$. So there exists $b' \in B'$ such that $s(b') = n(c) - c'$. Since m is an isomorphism, there exists $b \in B$ such that $m(b) = b'$. By commutativity, we have that

$$n(g(b)) = s(m(b)) = n(c) - c'$$

Now $n(g(b) - c) = c'$ and so we have proven surjectivity. □

The proof is long but is rather straight forward. In every step there is only one possible way to advance, and so one eventually arrives at the conclusion.

Lemma 4.2.5: Snake Lemma

Let R be a ring. Consider the commutative diagram

$$\begin{array}{ccccccccc} & & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & & \end{array}$$

where all the objects are R-modules. If the two rows are exact, then there is an exact sequence relating the kernels and cokernels of a, b, c

$$\ker(a) \longrightarrow \ker(b) \longrightarrow \ker(c) \xrightarrow{d} \text{coker}(a) \longrightarrow \text{coker}(b) \longrightarrow \text{coker}(c)$$

where d is called the connecting homomorphism.

Proof. We construct the function d as follows.

- Let $k \in \ker(c)$.
- By exactness, g is surjective. Thus there exists $l \in B$ such that $g(l) = k$.
- But $g'(b(l)) = c(g(l)) = c(k) = 0$ which means that $b(l) \in \ker(g')$. By exactness, there exists $m \in A'$ such that $f'(m) = b(l)$ since $\text{im}(f') = \ker(g')$. This m is unique since f' is

injective. In particular, $[m] \in \text{coker}(a)$.
We then define $d : \ker(c) \to \text{coker}(a)$ by $d(k) = m$.

We need to show that d is well defined. Suppose that l' is another element in B such that $g(l') = k$. Then $g(l - l') = 0$ so that $l - l' \in \ker(g)$. By exactness, $\text{im}(f) = \ker(g)$ so there is some $n \in A$ such that $f(n) = l - l'$. By a similar argument as the first paragraph, one can find $m' \in A'$ such that $f'(m') = b(l')$. Then

$$f'(a(n)) = b(f(n)) = b(l - l') = b(l) - b(l') = f'(m) - f'(m')$$

Since f' is injective by exactness, we have that $a(n) = m - m'$ so that $m - m' \in \text{im}(a)$ and hence $[m] = [m']$. Thus d is a well defined map.

Since all operations above are R-module homomorphisms, d is also an R-module homomorphism.

It remains to show exactness of the sequence. □

Lemma 4.2.6

Let the following be an exact sequence of abelian groups.

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

Then $\text{rank}(B) = \text{rank}(A) + \text{rank}(C)$.

Lemma 4.2.7

Let the following be an exact sequence of vector spaces.

$$0 \longrightarrow V \xrightarrow{f} W \xrightarrow{g} U \longrightarrow 0$$

Then $\dim(W) = \dim(V) + \dim(U)$.

5 Algebras over a Ring

5.1 Associative Algebras

Definition 5.1.1: 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 5.1.2

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 5.1.3

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. □

Lemma 5.1.4

Let R be a ring. Then R is an algebra over $\mathbb{Z}$.

Definition 5.1.5: 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 5.1.6

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

Definition 5.1.7: 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 $x, y \in A$

5.2 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 5.2.1

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 5.2.2: 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 5.2.3

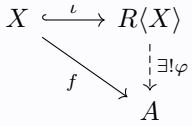
If X is a non-empty countable set, then the dimension $\dim_{\mathbb{F}}(\mathbb{F}\langle X\rangle)$ is countable.

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 5.2.4: Universal Property

Let X be a set. 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. □

5.3 Derivations of Algebras

Definition 5.3.1: Derivations

Let A be a ring and B an A-algebra. Let M be a B-module. An A-derivation of B into M is an A-module homomorphism $d : B \to M$ such that the Leibniz rule holds:

$$d(b_1 b_2) = b_1 d(b_2) + d(b_1) b_2$$

for $b_1, b_2 \in B$. Denote the set of all A-derivations from B to M by

$$\mathrm{Der}_A(B, M) = \{d : B \to M \mid d \text{ is an } A \text{ derivation } \}$$

This is reminiscent of properties of a derivative. Indeed, from the above definition, take $A = \mathbb{R}$ and $B = M = \mathbb{R}[x_1, \ldots, x_n]$. Then the formal partial derivatives $\frac{\partial}{\partial x_i} : \mathbb{R}[x_1, \ldots, x_n] \to \mathbb{R}[x_1, \ldots, x_n]$ defined by

$$\left(f(x) = \sum_{k_1, \ldots, k_n} a_{k_1, \ldots, k_n} x_1^{k_1} \cdots x_i^{k_i} \cdots x_n^{k_n} \right) \mapsto \left(\frac{\partial f}{\partial x_i} = \sum_{k_1, \ldots, k_n} a_{k_1, \ldots, k_n} k_i x_1^{k_1} \cdots x_i^{k_i - 1} \cdots x_n^{k_n} \right)$$

(provided $k_i \geq 1$, otherwise the derivative is constant on that term) is $\mathbb{R}$-linear and satisfies the Leibniz rule. These are the two fundamental properties that a derivative should possess.

Definition 5.3.2: The Module of Derivations

Let A be a ring and B an A-algebra. Let M be a B-module. Define the B-module of derivations to be the set

$$\mathrm{Der}_A(B, M) = \{d : B \to M \mid d \text{ is a derivation of } A\}$$

together with the following operations:

- Addition is defined by sending $d_1, d_2 : B \to M$ to $(d_1 + d_2) : B \to M$ that maps b to $d_1(b) + d_2(b)$.
- Left action is defined by $\cdot : B \times \mathrm{Der}_A(B, M) \to \mathrm{Der}_A(B, M)$ that sends $b \in B$ and $d : B \to M$ to $(bd) : B \to M$ defined by $u \mapsto b \cdot d(u)$.

Lemma 5.3.3

Let A be a ring and B an A-algebra. Let M be a B-module. Then $\mathrm{Der}_A(B, M)$ is indeed a B-module with the given operations.

Proof. Firstly, $\text{Der}_A(B, M)$ is an abelian group. We check the group axioms.

- Closure: Let $a \in A$ and $b_1, b_2 \in B$. $d_1 + d_2 : B \to M$ is an A-module homomorphism because

$$\begin{aligned}(d_1 + d_2)(ab_1 + b_2) &= d_1(ab_1 + b_2) + d_2(ab_1 + b_2) \\ &= ad_1(b_1) + d_1(b_2) + ad_2(b_1) + d_2(b_2) \\ &= a(d_1 + d_2)(b_1) + (d_1 + d_2)(b_2)\end{aligned}$$

  Finally, the Leibniz rule is satisfied because

$$\begin{aligned}(d_1 + d_2)(b_1b_2) &= d_1(b_1b_2) + d_2(b_1b_2) \\ &= b_1d_1(b_2) + d_1(b_1)b_2 + b_1d_2(b_2) + d_2(b_1)b_2 \\ &= b_1(d_1 + d_2)(b_2) + (d_1 + d_2)(b_1)b_2\end{aligned}$$

- Associativity: Follows from the fact that M is a group
- Identity: The zero map is the identity since for any $d : B \to M$, $d + 0 : B \to M$ sends b to $d(b)$ and thus $d + 0 = d$.
- Inverse: For each $d : B \to M$ the maps sending b to $-d(b)$ is an inverse
- Abelian: Follows from the fact that M is abelian.

Finally, left action is defined by $\cdot : B \times \text{Der}_A(B, M) \to \text{Der}_A(B, M)$ that sends $b \in B$ and $d : B \to M$ to $(bd) : B \to M$ defined by $u \mapsto b \cdot d(u)$. Associativity and identity is clear. □

Derivatives in analysis also satisfy the quotient rule and the fact that constant maps have 0 derivative. The following lemma shows that instead of defining derivatives for it so that constant maps have 0 derivative, it is in fact a consequence of linearity and Leibniz rule.

Lemma 5.3.4

Let A be a ring and B an A-algebra Let M be a B-module. Let $d : B \to M$ be an A-derivation. Then $d(a) = 0$ for all $a \in A$.

Proof. Since $d : B \to M$ is an A-module homomorphism, $d(a \cdot 1) = a \cdot d(1)$. We also have, by the Leibniz rule that $d(1) = 1 \cdot d(1) + d(1) \cdot 1 = 2d(1)$ which implies $d(1) = 0$. Thus $d(a \cdot 1) = a \cdot d(1) = 0$. □

As mentioned above, derivatives in analysis also satisfy the quotient rule. However, one must be careful in the question of existence of the quotient rule given the Leibniz rule because first of all B and M may not formally have quotients since they are not fields. Instead, what one can do is to pass on the derivative to the fraction field so that quotients are well defined. Interested readers are referred to [**?**].

The set of all derivations itself also has an extra structure of being a B-module in its own right.

We can see that $\text{Der}_{\mathbb{R}}(\mathbb{R}[x_1, \ldots, x_n], \mathbb{R}[x_1, \ldots, x_n])$ has more than just the standard partial derivatives from the module structure. For examples, the sum of partial derivatives

$$\frac{\partial}{\partial x_i} + \frac{\partial}{\partial x_j} : \mathbb{R}[x_1, \ldots, x_n] \to \mathbb{R}[x_1, \ldots, x_n]$$

defined by $f \mapsto \frac{\partial f}{\partial x_i} + \frac{\partial f}{\partial x_j}$.

However, second order derivatives (which are compositions of the first order partial derivatives) are not

derivations! Indeed they satisfy not the Leibniz property but instead, we have that

$$\frac{\partial(fg)}{\partial x_i x_j} = \frac{\partial}{\partial x_i}\left(\frac{\partial f}{\partial x_j}g + f\frac{\partial g}{\partial x_j}\right) = \frac{\partial^2 f}{\partial x_i x_j} + \frac{\partial f}{\partial x_j}\frac{\partial g}{\partial x_i} + \frac{\partial f}{\partial x_i}\frac{\partial g}{\partial x_j} + \frac{\partial^2 g}{\partial x_i x_j}$$

which is way more complicated!

Finally, there is one more example of derivations. While we have done a completely general treatment of partial derivatives above, we can in fact evaluate the derivative at a chosen point and it will again be an $\mathbb{R}$-derivation. Writing $f(p) = \text{ev}_p(f)$ where ev is the evaluation homomorphism, the $\mathbb{R}$-derivation $\mathbb{R}[x_1, \ldots, x_n] \to \mathbb{R}[x_1, \ldots, x_n]$ defined by

$$f \mapsto \frac{\partial f}{\partial x_i}g(p) + f(p)\frac{\partial g}{\partial x_i}$$

is also a derivation!

6 Graded Structures

6.1 Graded Rings

Definition 6.1.1: Graded Rings

Let R be a ring. We say that R is graded if the following are true.

- The abelian group structure of R decomposes into a direct sum

$$R = \bigoplus_{k=0}^{\infty} R_k$$

  where each R_k is an abelian group
- For $r_i \in R_i$ and $r_j \in R_j$, $r_i r_j \in R_{i+j}$.

We say that an element $r \in R$ is homogenous if $r \in R_k$ for some $k \in \mathbb{N}$.

Proposition 6.1.2

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 6.1.3: Graded Commutative Rings

Let $R = \bigoplus_{k=0}^{\infty} R_k$ be a graded ring. We say that R is graded commutative if for all $r \in R_i$ and $r \in R_j$,

$$r \cdot s = (-1)^{ij} s \cdot r$$

Definition 6.1.4: Homomorphism of Graded Rings

Let R, S be graded rings. Let $\varphi : R \to S$ be a ring homomorphism. We say that ϕ is a graded ring homomorphism if

$$\phi(R_i) \subseteq S_i$$

for each $i \in \mathbb{N}$.

Definition 6.1.5: Isomorphism of Graded Rings

Let R, S be graded rings. Let $\varphi : R \to S$ be a ring homomorphism. We say that ϕ is a graded ring isomorphism if it is a graded ring homomorphism and an isomorphism of rings.

6.2 Homogeneous Ideals

Definition 6.2.1: Homogeneous Ideals

Let R be a graded ring. Let I be an ideal of R. We say that I is a homogeneous ideal if for all $a \in I$, each homogeneous components of a lies in I.

Lemma 6.2.2

Let R be a graded ring. Let I be an ideal of R. Then I is homogeneous if and only if for all $f \in I$ with homogeneous decomposition $f = \sum_{k=0}^{d} f_k$, each $f_k \in I$.

Lemma 6.2.3

Let R be a graded ring. Let I, J be homogeneous ideals of R. Then the following are true.

- $I + J$ is a homogeneous ideal
- IJ is a homogeneous ideal
- $I \cap J$ is a homogeneous ideal
- $\sqrt{I}$ is a homogeneous ideal

Proposition 6.2.4

Let R be a graded ring. Let I be a homogeneous ideal of R. Then R/I is also a graded ring with decomposition given by

$$\frac{R}{I} = \bigoplus_{k=0}^{\infty} \frac{R_k}{R_k \cap I}$$

6.3 Graded Modules

Definition 6.3.1: Graded Modules over a Ring

Let R be a ring. Let M be an R-module. We say that M is a graded module over R if there is a decomposition

$$M = \bigoplus_{k=0}^{\infty} M_k$$

into R-modules such that $m_i + m_j \in M_{i+j}$ for $m_i \in M_i$ and $m_j \in M_j$.

Definition 6.3.2: Graded Modules over a Graded Ring

Let R be a graded ring. Let M be an R-module. We say that M is a graded module over R if there is a decomposition

$$M = \bigoplus_{k=0}^{\infty} M_k$$

into abelian groups and $R_i M_j \subseteq M_{i+j}$.

Proposition 6.3.3

Let R be a graded ring. Let M, N be graded R-modules. Then the tensor product $M \otimes_R N$ is also a graded R-module, with grading given by

$$(M \otimes_R N)_n = \frac{\bigoplus_{i+j=n} M_i \otimes_{\mathbb{Z}} N_j}{\left\langle rm \otimes n - m \otimes rn \mid \substack{m \in M_a, n \in N_b, r \in R_c \\ \text{such that } a+b+c=n} \right\rangle}$$

Proposition 6.3.4

Let R, S be graded rings considered as graded $\mathbb{Z}$-modules. Then the graded $\mathbb{Z}$-module $R \otimes_{\mathbb{Z}} S$ is also a graded ring, with multiplication defined by

$$(r_1 \otimes s_1)(r_2 \otimes s_2) = (-1)^{|s_1||r_2|}(r_1 r_2 \otimes s_1 s_2)$$

Lemma 6.3.5

Let R, S be graded rings. If R and S are graded commutative, then $R \otimes_{\mathbb{Z}} S$ is also graded commutative.

6.4 Graded Algebras

Definition 6.4.1: Graded Algebra

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

Proposition 6.4.2

Let R be a graded ring. Let A, B be graded R-algebras. Then the tensor product $A \otimes_R B$ is also a graded R-algebra, with grading given by

$$(A \otimes_R B)_n = \frac{\bigoplus_{i+j=n} A_i \otimes_{\mathbb{Z}} B_j}{\left\langle rm \otimes n - m \otimes rn \mid \begin{smallmatrix} m \in A_a, n \in B_b, r \in R_c \\ \text{such that } a+b+c=n \end{smallmatrix} \right\rangle}$$

and multiplication given by

$$(r_1 \otimes s_1)(r_2 \otimes s_2) = (-1)^{|s_1||r_2|}(r_1 r_2 \otimes s_1 s_2)$$

7 Tensor Algebras

7.1 Multilinear Maps of R-Modules

Definition 7.1.1: Multilinear Map

Let $M_1, \ldots, M_n, N$ be R-modules. An R-module homomorphism $\varphi : M_1 \times \cdots \times M_n \to N$ is said to be multilinear if the following is true. For $1 \leq k \leq n$ and all $m_i \in M_i$ for $i \neq k$, the map $M_i \to N$ defined by

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

is an R-module homomorphism. Denote the set of all multilinear maps from $M_1 \times \cdots \times M_n$ to N by

$$\mathrm{Hom}^n(M_1 \times \cdots \times M_n; N)$$

Definition 7.1.2: Symmetric 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 7.1.3: 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 $\varphi(m_1, \ldots, m_k) = 0$.

7.2 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 7.2.1: 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 7.2.2: 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 7.2.3

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

Proposition 7.2.4: 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 7.2.5

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, $\dim_{\mathbb{F}}(T^k(V)) = n^k$.

7.3 Exterior Algebra

Definition 7.3.1: 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 7.3.2

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

Definition 7.3.3: 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 7.3.4

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 7.3.5

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 7.3.6

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 7.3.7

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

Lemma 7.3.8

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 $m_2 \in \Lambda^s(M)$

7.4 Symmetric Algebra

Definition 7.4.1: 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 7.4.2

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

Definition 7.4.3: 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 7.4.4

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 7.4.5

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 7.4.6: 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 7.4.7

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, $\dim_{\mathbb{F}}(S^k(V)) = \binom{k+n-1}{n-1}$.

8 Radicals

8.1 The Radical of a Module

Definition 8.1.1: Cosimple

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

Lemma 8.1.2

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 8.1.3: 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.

8.2 Nilpotent Elements

Definition 8.2.1: 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 8.2.2: 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 8.2.3

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

Not every nil ideal is nilpotent.

Definition 8.2.4: 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 8.2.5

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 8.2.6

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

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

□

8.3 The Annihilator of an Element

Definition 8.3.1: 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 8.3.2

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.

8.4 The Jacobson Radical

Definition 8.4.1: 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 8.4.2

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
$$J_1 = \bigcap_{I \text{ is a maximal ideal of } R} I$$
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 8.4.3

Let R be a ring. Then we have

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

9 Chain Conditions

9.1 Noetherian Rings and Modules

Definition 9.1.1: 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 9.1.2: 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 9.1.3

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 9.1.4

Let R be a ring. Let M_1, M_2, M_3 be R-modules. Let $f : M_1 \to M_2$ and $g : M_2 \to M_3$ be R-module homomorphisms such that

$$0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$$

is a short exact sequence. Then M_2 is Noetherian if and only if M_1 and M_3 are Noetherian.

Corollary 9.1.5

Let R be a ring. Let M be a left R-module. Then the following are true.
- If N is an R-submodule of M, then M is Noetherian if and only if N and M/N is Noetherian
- If N is an left R-module, then $M \oplus N$ is Noetherian if and only if M and N are Noetherian
- If R is Noetherian and I is a left ideal of R, then R/I is Noetherian.

Corollary 9.1.6

Let R be a Noetherian ring. Let M be a left R-module. Then M is Noetherian if and only if M is a finitely generated R-module.

9.2 Artinian Rings and Modules

Definition 9.2.1: 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 9.2.2: 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 9.2.3

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 9.2.4

Let R be a ring. Let M_1, M_2, M_3 be R-modules. Let $f : M_1 \to M_2$ and $g : M_2 \to M_3$ be R-module homomorphisms such that

$$0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$$

is a short exact sequence. Then M_2 is Artinian if and only if M_1 and M_3 are Artinian.

Corollary 9.2.5

Let R be a ring. Let M be a left R-module. Then the following are true.
- If N is an R-submodule of M, then M is Artinian if and only if N and M/N is Artinian
- If N is an left R-module, then $M \oplus N$ is Artinian if and only if M and N are Artinian
- If R is Artinian and I is a left ideal of R, then R/I is Artinian.

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

Theorem 9.2.6

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

Corollary 9.2.7

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.