Rings and Modules

Labix

May 4, 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
- $\operatorname{im}(\phi) \leq S$ 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

$$\begin{aligned}\pi((r_1 + \ker(\phi))(r_2 + \ker(\phi))) &= \pi(r_1r_2 + \ker(\phi)) \\ &= \phi(r_1r_2) \\ &= \phi(r_1)\phi(r_2) \\ &= \pi(r_1 + \ker(\phi))\pi(r_2 + \ker(\phi))\end{aligned}$$

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 $I_1, \dots, I_n$ 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 $\phi(x) = (x + I_1, \dots, x + I_n)$ 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 $\phi(x) = (x + I_1, \dots, x + I_n) = 0$. Conversely, if $(x + I_1, \dots, x + I_n)$ is such that applying ϕ gives 0, then $x \in I_1, \dots, I_n$ so that $x \in I$.

When the ideals are pairwise corpime, consider the elements $e_k = (0, \dots, 0, x + I_k, 0, \dots, 0)$ 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 $\psi(x_i) = (0, \dots, 0, 1 + I_i, 0, \dots, 0)$ for $1 \leq i \leq n$. Now to prove surjectivity, let $(r_1, \dots, r_n)$ be an element in the product. Then we have that

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

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 $(r_1, \dots, r_n)$ in the product, we can find $r \in R$ such that $\phi(r) = (r_1, \dots, r_n)$. The steps are as follows.

1. Using $R = I_i + R_j$, find $a_j \in R_i$ and $z_j \in R_j$ such that $1 = a_j + z_j$. 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. 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 $n \in \operatorname{im}(\phi)$. 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 $\overline{\phi} : M/\ker(\phi) \to \operatorname{im}(\phi)$ 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.

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

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 $\{b_1, \dots, b_n\} \subseteq B$ 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 definition is reminiscent of a theorem in linear algebra. However note that we require that R to be a division ring. However, 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 $v_1, \dots, v_m \in Z$ and $a_1, \dots, a_m, a \in R$ not all 0 such that

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

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

$$v = -a^{-1}a_1v_1 - \cdots - a^{-1}a_mv_m$$

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. □

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

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

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.

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

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:

$$\begin{tikzcd}
X \arrow[r, hook, "\iota"] \arrow[dr, "f"'] & R\langle X\rangle \arrow[d, dashed, "\exists ! varphi"] \\
& A
\end{tikzcd}$$

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. □

3.4 Amitsur-Schur Lemma

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

Theorem 3.4.1: Amitsur-Schur Lemma

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

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

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

Indeed, suppose that $x \in M$ is non-zero. Consider the map $\pi : A \to M$ defined by $\pi(a) = ax$. Since π is not the zero map and M is simple, by Shur's lemma I we know that $\text{im}(\pi) = M$. By the firs isomorphism theorem, we have that $M \cong \frac{A}{\ker(\pi)}$ and thus the second inequality in dimensions hold. For the first inequality, the linear map $\omega_x : D \to M$ defined by $\omega_x(d) = xd$ is injective because M is simple.

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

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

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

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

Thus we can apply the usual calculations with fractions:

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

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

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

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

The following statement is core to the entire theory of Groups and Representations.

Corollary 3.4.2

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

Proof. The dimension of A is countable since A is a quotient of $\mathbb{C}\langle X \rangle$ by proposition 3.3.3. Since M is simple, it is isomorphic to A/L for some left ideal L. Hence the dimension of M over $\mathbb{C}$ is also countable. This implies that $\dim_{\mathbb{C}}(\text{End}_{\mathbb{C}}(M))$ is countable, and so is the dimension of its subalgebra $\text{End}_A(M)$. But $\mathbb{C}$ is uncountable. Thus every $f \in \text{End}_A(M)$ is algebraic by the Amitsur-Schur lemma. By the fundamental theorem of algebra, the $\mathbb{C}$ is algebraically closed so that the minimal polynomial of f, which is irreducible, has degree 1. Thus the minimal polynomial has root $f \in \mathbb{C}$. □

4 Tensor Products

4.1 Tensor Products of Modules

Definition 4.1.1: Tensor Product of Modules

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

$$A \otimes_R B$$

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

$$\begin{tikzcd} A \times B \arrow[r, "\phi"] \arrow[dr, "\psi"'] & A \otimes_R B \arrow[d, dashed, "\exists!\theta"] \\ & C \end{tikzcd}$$

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 $M_1, \dots, M_n, N$ 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

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

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 $\varphi(m_1, \dots, m_k) = 0$.

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 $B = \{v_1, \dots, v_n\}$. Then the k-tensors

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

with $v_{i_1}, \dots, v_{i_k} \in B$ 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

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

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

Proposition 4.4.6

Let $\{v_1, \dots, v_n\}$ 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

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

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 $\mathbb{F}[x_1, \dots, x_n]$. This isomorphism is also a vector space isomorphism. In particular, $\dim_{\mathbb{F}}(S^k(V)) = \binom{k+n-1}{n-1}$.

4.6 Symmetric and Alternating Tensors

5 Division Rings

Division rings are very closed to being a field. They are just missing commutativity. As one can seen in Field and Galois theory, fields and field homomorphisms are rather rigid objects, so one can expect division rings to be restrictive. Indeed, in this section we will show that any finite division ring must be a field. Moreover, the only finite dimensional division algebra over $\mathbb{R}$ can only take 3 forms, namely $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$. In particular, they have dimension 1, 2 and 4 respectively.

5.1 Properties of Division Rings

Proposition 5.1.1

Let D be a division ring. The following are true regarding the properties of a division ring.

- The only ideals of D are (0) and D.
- If D is an division algebra, then D is a simple D-module.

Proof. Let I be a non-trivial ideal of D. Then by property of an ideal, for $x \in I \setminus \{0\}$, $x^{-1}x \in I$ so that $1 \in I$. Then for any $d \in D$, $d \cdot 1 \in I$ thus $D = I$.

Since the submodules of D are precisely the ideals of D, we conclude that D is a simple D-module. □

Lemma 5.1.2

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

- $Z(D)$ is a field and D is a $Z(D)$-algebra
- $C_D(x)$ is a division ring and a $Z(D)$-subalgebra

Proof. $Z(D)$ as a subdivision ring is also a division ring in its own right. Since $Z(D)$ consists of all commuting elements, $Z(D)$ is commutative and so is a field. Thus D is a $Z(D)$-algebra by multiplication.

It is clear that $0, 1 \in C_D(x)$. Let $a, b \in C_D(x)$. Then

$$(a - b)x = ax - bx = xa - xb = x(a - b)$$

so that $a - b \in C_D(x)$. Also $abx = axb = xab$ implies that $ab \in C_D(x)$. Finally, $ax = xa$ implies that $x = a^{-1}xa$ so that $xa^{-1} = a^{-1}x$ and that $a^{-1} \in D$. Thus $C_D(x)$ is a sub division ring. Since $C_R(x)$ contains $Z(R)$, $C_R(x)$ is thus a $Z(D)$-algebra. □

5.2 The Structure of Quaternions

Recall in Group theory that we have encountered the quaternion group. We can turn it into a vector space over $\mathbb{R}$ by allowing coefficients on the quaternion group.

Definition 5.2.1: Quaternions

Define the quaternions as the quotient algebra

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

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

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

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

Proposition 5.2.2

The quaternions satisfy the following multiplication table:

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

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

Proposition 5.2.3

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

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

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

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

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

Proposition 5.2.4

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

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

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

and cross product

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

Proposition 5.2.5

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

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

Proof. By $\mathbb{R}$-bilinearity, we have that we have that

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

A simple calculation yields $\mathbf{h}_1\mathbf{h}_2 = -\mathbf{h}_1 \cdot \mathbf{h}_2 + \mathbf{h}_1 \times \mathbf{h}_2$ using multiplication rules of quaternions. Thus we are done. □

Definition 5.2.6: Conjugate and Norm

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

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

Also define the norm of x to be

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

Proposition 5.2.7

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

- $xx^* = \|x\|^2$
- $(xy)^* = y^*x^*$
- $\|xy\| = \|x\|\|y\|$

Proof.

- Write $x = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$. Then by considering the purely imaginary quaternions as a 3 dimensional vector space, we have that

$$\begin{aligned} xx^* &= \left(a^2 - \begin{pmatrix} b \\ c \\ d \end{pmatrix} \cdot \begin{pmatrix} -b \\ -c \\ -d \end{pmatrix}\right) + \left(a\begin{pmatrix} b \\ c \\ d \end{pmatrix} - a\begin{pmatrix} b \\ c \\ d \end{pmatrix} - \begin{pmatrix} b \\ c \\ d \end{pmatrix} \times \begin{pmatrix} b \\ c \\ d \end{pmatrix}\right) \\ &= a^2 + b^2 + c^2 + d^2 \\ &= \|x\|^2 \end{aligned}$$

- Again write $x = a_1 + \mathbf{h}_1$ and $y = a_2 + \mathbf{h}_2$, then by a similar method, we have that

$$\begin{aligned} y^*x^* &= (a_2a_1 + \mathbf{h}_2 \cdot \mathbf{h}_1) + (-a_1\mathbf{h}_2 - a_2\mathbf{h}_1 + \mathbf{h}_2 \times \mathbf{h}_1) \\ &= (a_2a_1 + \mathbf{h}_2 \cdot \mathbf{h}_1) - (a_1\mathbf{h}_2 + a_2\mathbf{h}_1 + \mathbf{h}_1 \times \mathbf{h}_2) \\ &= (xy)^* \end{aligned}$$

by using the fact that $-\mathbf{x}\times\mathbf{y}=\mathbf{y}\times\mathbf{x}$.

- Using the above two identity, we have that

$$\begin{aligned}\|xy\|^2&=(xy)(xy)^*\\&=xyy^*x^*\\&=x\|y\|^2x^*\\&=xx^*\|y\|^2\\&=\|x\|^2\|y\|^2\end{aligned}$$

And so we are done. □

Proposition 5.2.8

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

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

Similar to the real and complex counter part, we can form all kinds of special groups for quaternions, beginning with the unitary group.

Definition 5.2.9: The Quaternionic Unitary Group

Define the quaternionic unitary group to be the subgroup

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

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

Note that this is different from the quaternion group since the quaternion group only consists of the basis vectors and their inverses.

Proposition 5.2.10

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

Proof. Define $\phi:\mathbb{R}_+^\times\times U(\mathbb{H})\to\mathbb{H}$ by $\phi(r,x)=rx$. It is clear that this is a group homomorphism. Moreover, its kernel is trivial since scalar multiplication is equal to 0 if and only if $x=0$. Also it is surjective. Indeed any vector x can be written as $\|x\|\frac{x}{\|x\|}$ where $\frac{x}{\|x\|}$ now lies in the unitary group. Thus ϕ is a bijective homomorphism. □

By writing every quaternion group as a scalar multiplied by an element of the unitary group, we obtain a polar coordinate representation similar to that of the complex numbers in terms of the argument and magnitude.

Proposition 5.2.11: Quaternionic Euler's Formula

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

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

Proof. If $q = a + b\mathbf{x}$ then notice that q lies in the two dimensional $\mathbb{R}$-subalgebra $\mathbb{R}(x) = \mathbb{R} + \mathbb{R}\mathbf{x}$. This is isomorphic to $\mathbb{C}$ so in particular, all partial sums

$$\sum_{k=0}^{n} \frac{\mathbf{x}^n}{n!}$$

also lie in $\mathbb{R}(x) \cong \mathbb{C}$ and quaternionic Euler's formula follows from the usual Euler's formula. □

However, note that in general since quaternions do not commutate, $e^{X+Y} \neq e^X e^Y$. This is true only if $X, Y \in \mathbb{R}(x)$. This is because then $XY = YX$ so that $e^{X+Y} = e^X e^Y$.

Proposition 5.2.12: Quaternionic De Moivre's Formula

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

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

Proof. We have that

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

and so we are done. □

5.3 3D Rotations using Quaternions

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

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

Proposition 5.3.1

Let $M \in \text{SO}_3(\mathbb{R})$ be a special orthogonal transformation. Then there exists an orthonormal basis of $\mathbb{R}^3$ such that the matrix decomposes into the direct sum $(1) \oplus R_\alpha$, where

$$R_\alpha = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$$

is a rotation in $\mathbb{R}^2$.

Proof. Since M is a bijective linear transformation, M has at least 1 real eigenvector $\mathbf{v}$ with eigenvalue $\alpha \in \mathbb{R}$. Note that since M is also in the special orthogonal group, $a = \pm 1$. Let W be the plane orthogonal to $\mathbf{v}$. Note that $M\mathbf{w} \in W$ for any $\mathbf{w} \in W$ because M is bijective and that

$$\mathbf{v} \cdot M\mathbf{w} = M(\alpha^{-1}\mathbf{v}) \cdot (M\mathbf{w}) = \alpha^{-1}\mathbf{v} \cdot \mathbf{w} = 0$$

so that $M\mathbf{w} \in W$. Thus the linear transformation of M restricted to W is an orthogonal transformation. But orthogonal transformations in $\mathbb{R}^2$ is exactly given by R_α for some angle α, or a reflection S_α along an angle.

If $\alpha = 1$, we must have that M restricted to the orthogonal plane is a rotation R_α. Then we are done by choosing the ordered basis $\mathbf{v}$ and any orthonormal basis e_2 and e_3 of W. If $\alpha = -1$, then M restricted to the orthogonal plane is a reflection S_α. But S_α then has eigenvalues 1 and -1. We can then return to the start of the proof and choose the eigenvector corresponding to the eigenvalue 1. Thus then we will arrive at the case of $\alpha = 1$. □

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

Lemma 5.3.2

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

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

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

Proof. Choose $\mathbf{y} \in \mathbb{H}_0$ an orthogonal vector to $\mathbf{x}$ that is a unit vector. Let $\mathbf{z} = \mathbf{x} \times \mathbf{y}$. By proposition 5.1.5, we have that $\mathbf{x}^2 + \mathbf{y}^2 + \mathbf{z}^2 = -1$ and

$$\begin{aligned} \mathbf{xy} &= -\mathbf{yx} = \mathbf{z} \\ \mathbf{yz} &= -\mathbf{zy} = \mathbf{x} \\ \mathbf{zx} &= -\mathbf{xz} = \mathbf{y} \end{aligned}$$

so that $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$ forms a basis for $\mathbb{H}_0$. It suffices to check the equation on basis vectors since the rotation is a linear map. Notice that $e^{-\theta \mathbf{x}} = \cos(\theta) - \mathbf{x}\sin(\theta)$. Now we have that

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

Now also,

$$\begin{aligned} e^{\theta \mathbf{x}} \mathbf{y} e^{-\theta \mathbf{x}} &= (\cos(\theta) + \mathbf{x}\sin(\theta))\mathbf{y}(\cos(\theta) - \mathbf{x}\sin(\theta)) \\ &= (\mathbf{y}\cos(\theta) + \mathbf{z}\sin(\theta))(\cos(\theta) - \mathbf{x}\sin(\theta)) \\ &= ((\cos(\theta))^2 - (\sin(\theta))^2)\mathbf{y} + (2\cos(\theta)\sin(\theta))\mathbf{z} \\ &= \mathbf{y}\cos(2\theta) + \mathbf{z}\sin(2\theta) \\ &= R_{\mathbf{x}}^{2\theta}(\mathbf{y}) \end{aligned}$$

Finally we have that

$$\begin{aligned} e^{\theta \mathbf{x}} \mathbf{z} e^{-\theta \mathbf{x}} &= (\cos(\theta) + \mathbf{x}\sin(\theta))\mathbf{z}(\cos(\theta) - \mathbf{x}\sin(\theta)) \\ &= (\mathbf{z}\cos(\theta) - \mathbf{y}\sin(\theta))(\cos(\theta) - \mathbf{x}\sin(\theta)) \\ &= ((\cos(\theta))^2 - (\sin(\theta))^2)\mathbf{z} - (2\cos(\theta)\sin(\theta))\mathbf{y} \\ &= \mathbf{z}\cos(2\theta) - \mathbf{y}\sin(2\theta) \\ &= R_{\mathbf{x}}^{2\theta}(\mathbf{z}) \end{aligned}$$

and so we conclude. □

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

Theorem 5.3.3

The conjugation action map

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

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

5.4 Division Rings over Real and Complex Numbers

Proposition 5.4.1

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

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

Proposition 5.4.2

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

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

In order to proof the grand result, we need the notion of the trace map from Linear Algebra.

Definition 5.4.3: Trace Map

Let D be a real division algebra of finite dimension over $\mathbb{R}$. Define the trace map $\text{Tr}_D : D \to \mathbb{R}$ by

$$\text{Tr}_D(a) = \text{Tr}(L_a)$$

where $L_a : D \to D$ is the left multiplication map $L_a(d) = ad$.

Lemma 5.4.4

Let A be a finite dimensional algebra over a field $\mathbb{F}$. If $a \in A$ then the minimal polynomial of L_a is equal to μ_a.

Proof. Notice that we have $L_a^n(b) = a^n b = L_{a^n}(b)$ so that

$$f(L_a)(b) = f(a)b = L_{f(a)}(b)$$

for each polynomial $f(x)$ and $b \in A$. If $f(a) = 0$, then $f(L_a) = 0$. If $f(L_a) = 0$, then $f(a) = f(a) \cdot 1 = f(L_a)(1) = 0$. Thus the minimal polynomial of L_a and a are the same. □

Theorem 5.4.5: Frobenius Theorem

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

Proof. Let D be a finite dimensional division algebra over $\mathbb{R}$.

Step 1: $D = \mathbb{R} \oplus \ker(\text{Tr}_D)$.
The trace map is defined to be linear over the components of the matrix. Moreover, the second one follows from the fact that $L_a : D \to D$ is given by the matrix aI_n. Finally, it is clear that the kernel of the trace map is $n - 1$ dimensional. Moreover it is surjective and that $\mathbb{R} \cap \ker(\text{Tr}_D) = 0$.

Step 2: If $a \in \ker(\text{Tr}_D)$ then $a^2 \in \mathbb{R}$ and $a^2 \leq 0$.
Now let $a \in D$ lie in the kernel. If $a \in \mathbb{R}$ then since D is the direct sum of $\mathbb{R}$ and the kernel, we must have that $a = 0$. So suppose that $a \notin \mathbb{R}$. Then since any irreducible polynomial in $\mathbb{R}[x]$ must either be linear or quadratic with discriminant less than 0. Since $a \notin \mathbb{R}$, the minimal polynomial μ_a of a must be quadratic:

$$\mu_a(x) = x^2 + \alpha x + \beta$$

where $\alpha^2 - 4\beta < 0$. By the above corollary, L_a also has μ_a as the minimal polynomial. The characteristic polynomial $c_{L_a}(x)$ of L_a has the same roots as μ_a. Since μ_a is irreducible, c_{L_a} must be a power of μ_a. It follows that

$$c_{L_a}(x) = \mu_a(x)^{n/2} = (x^2 + \alpha x + \beta)^{n/2} = x^n + \frac{n\alpha}{2}x^{n-1} + \cdots + \beta^{n/2}$$

From Linear Algebra, we know that the trace appears as the first coefficient of the characteristic polynomial. By definition of $\ker(\text{Tr}_D)$, we have that $\text{Tr}_D(a) = 0$. It follows that $\alpha = 0$, $\beta > 0$ and $\alpha^2 + \beta = 0$. Thus $\alpha^2 = -\beta < 0$. We then conclude that $a^2 \leq 0$.

Write $D_0 = \ker(\text{Tr}_D)$. We now have a function $q : D_0 \to \mathbb{R}$ defined by

$$q(a) = -a^2$$

This is a positive definite quadratic form. We can polarize it to obtain $\tau : D_0 \times D_0 \to \mathbb{R}$ defined by

$$\tau(a, b) = -\frac{1}{2}(ab + ba)$$

Step 3: (D_0, τ) is a finite dimensional Euclidean space.
It is clear that τ is symmetric since $\tau(a, b) = \tau(b, a)$. τ is bilinear since

$$\begin{aligned}\tau(a + b, c) &= -\frac{1}{2}((a + b)c + c(a + b)) \\ &= -\frac{1}{2}(ac + ca) - \frac{1}{2}(bc + cb) \\ &= \tau(a, c) + \tau(b, c)\end{aligned}$$

and the property that $\tau(\lambda a, b) = \lambda\tau(a, b)$ for $\lambda \in \mathbb{R}$ is clear. Thus τ is a bilinear form. It is positive definite by step 2 since $\tau(a, a) = -a^2 > 0$.

By Gram-schimdt, we obtain an orthonormal basis for D_0, namely $e_1, \dots, e_{n-1}$.

Step 4: $e_i^2 = -1$ and $e_i \cdot e_j = -e_j \cdot e_i$ for all $1 \leq i \neq j \leq n - 1$. Also, $e_k = \pm(e_i \cdot e_j)^{-1}$ for $1 \leq i < j < k \leq n - 1$.
As the basis is orthonormal, we have that $\tau(e_i, e_i) = 1$ and $\tau(e_i, e_j) = 0$ for all $i \neq j$. The results then follow from the definition of τ. Also, let $u = e_i e_j e_k$. We have that

$$\begin{aligned}u^2 &= (e_i e_j)e_k e_i e_j e_k \\ &= -e_j(e_i e_k)e_i e_j e_k \\ &= e_j e_k(e_i e_i)e_j e_k \\ &= -(e_j e_k)e_j e_k \\ &= e_j e_j e_k e_k \\ &= 1\end{aligned}$$

Thus $u^2 = 1$ implies $(u - 1)(u + 1) = 0$. Since D is a division algebra, $e_i e_j e_k = u = \pm 1$. Hence we conclude.
Step 5: Conclusion.
By analzing the dimension n, we have the following:

- If $n = 1$, then we must have $D = \mathbb{R}$.
- If $n = 2$, then $e_1^2 = 1$ so that $D \cong \mathbb{C}$.
- If $n = 3$, then it is impossible by proposition 5.4.2.
- If $n = 4$, then $D = \mathbb{R} \oplus \mathbb{R}e_1 \oplus \mathbb{R}e_2 \oplus \mathbb{R}e_3$. Let $i = e_1$, $j = e_2$ and $k = e_1e_2$. Then by step 4, we have that $i^2 = j^2 = k^2 = -1$ and $ijk = kk = -1$. Thus $D \cong \mathbb{H}$.
- If $n = 5$, then it is impossible by step 4. Indeed we have that $e_3 \pm (e_1e_2)^{-1}$ and $e_4 = \pm(e_1e_2)^{-1}$ so that $e_4 = \pm e_3$. This contradicts the fact that $e_1, \dots, e_{n-1}$ is a basis.

□

Together with Amitsur-Schur lemma, we can prove a stronger statement.

Theorem 5.4.6

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

Proof. Let D be a countable generated $\mathbb{R}$-division algebra. Then D is a simple module and $\text{End}_D(D) \cong D$ by lemma 2.4.3. Moreover, by Amitsur-Schur lemma, every element $d \in D$ is algebraic. The algebra $\mathbb{R}(d)$ generated by d is a finite dimensional field. If $d \notin \mathbb{R}$, then by Frobenius theorem, $\mathbb{R}(d) \cong \mathbb{C}$ and the minimal polynomial is quadratic. Write it as $\mu_d = x^2 + \alpha_d x + \beta_d$. If $\mathbb{R}(d) = D$, then we are done.

If $\mathbb{R}\langle d\rangle \neq D$, pick $c \in D \setminus \mathbb{R}\langle d\rangle$. Then subalgebra $A = \mathbb{R}(c, d)$ generated by d and c is a division algebra because each element $r \notin R$ can be inverted from $r^2 + \alpha_r + \beta_r = 0$. Indeed we have that $(r + \alpha_r)r = -\beta_r$ so that $r^{-1} = -\beta_r^{-1}(r + \alpha_r)$. Note that $\beta_r \neq 0$ since $\mu_r(x)$ is irreducible.

Now we have that

$$(c + d)^2 + \alpha_{c+d}(c + d) + \beta_{c+d} = c^2 + cd + dc + d^2 + \alpha_{c+d}(c + d) + \beta_{c+d}$$

This is the minimal polynomial of $c + d$, and so it is 0. It follows that

$$\begin{aligned} dc &= -c^2 - cd - d^2 - \alpha_{c+d}(c + d) - \beta_{c+d} \\ &= \alpha_c c + \beta_c - cd + \alpha_d d + \beta_d - \alpha_{c+d}(c + d) - \beta_{c+d} \end{aligned}$$

Thus every element of $\mathbb{R}\langle c, d\rangle$ is an $\mathbb{R}$-linear combination of $1, c, d, cd$. By Frobenius theorem, we have that $\mathbb{R}\langle c, d\rangle \cong \mathbb{H}$. If $\mathbb{R}\langle c, d\rangle = D$ then we are done.

Suppose that $\mathbb{R}\langle c, d\rangle \neq D$. Pick $b \in D \setminus \mathbb{R}\langle c, d\rangle$. Consider the subalgebra $\mathbb{R}\langle b, c, d\rangle$ generated by b, c, d. By the same argument as above, $\mathbb{R}\langle b, c, d\rangle$ is a division algebra. By the argument with the minimal polynomials of b, r and $b + r$ for some $r \in \mathbb{R}\langle c, d\rangle$, we can write every element as an $\mathbb{R}$-linear combination of $1, c, d, cd, b, cb, db$ and cdb. Thus $\mathbb{R}\langle b, c, d\rangle$ is a finite dimensional division algebra over $\mathbb{R}$ of dimension at least 5. This contradicts Frobenius theorem. □

However this is no longer true for division algebras over $\mathbb{R}$ of uncountable dimension. For example, the ring of Laurent series $\mathbb{R}((x))$, $\mathbb{C}((x))$ and $\mathbb{H}((x))$ are all examples of such.

5.5 Finite Division Rings

Corollary 5.5.1

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

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

Proof. We know that $Z(D)$ is a field. Since D is finite, $Z(D)$ is finite. Every finite field is of the form $\mathbb{F}_{p^n}$ from Field and Galois theory. Since D is a $Z(D)$-algebra and D is finite, we must have $\dim_{Z(D)} D$ is finite. The final point also follows. □

Proposition 5.5.2

Let D be a finite division ring and $\dim_{Z(D)}(D) = m$ for $Z(D) \cong \mathbb{F}_{p^n}$ for some prime p and $n \in \mathbb{N} \setminus \{0\}$. Then there exists positive integers $d_1, \dots, d_k$ such that $d_i | m$, $d_i < m$ and

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

Proof. The group $D^\times$ acts on D by conjugation. By the class equation, we have that

$$q^m = |D| = |Z(R)| + \sum_{i=1}^{k} |\text{Orb}_{D^\times}(x_i)|$$

for $Z(R), \text{Orb}_{D^\times}(x_1), \dots, \text{Orb}_{D^\times}(x_k)$ the distinct orbits of the action.

If D is a field, then $Z(D) = D$ and $m = 1$. All orbits moreover have size 1 since D is commutative. Thus we have that $q = q$ for the identity.

Now suppose that D is not a field. There exists orbits of size greater than 1 since in general. $xyx^{-1} \neq y$. Thus $k \geq 1$. Let $\text{Orb}_{D^\times}(y_1), \dots, \text{Orb}_{D^\times}(y_k)$ be the distinct orbits of size at least 2. Notice that

$$\begin{aligned} \text{Stab}_{D^\times}(y_i) &= \{g \in D^\times \mid g y_i g^{-1} = y_i\} \\ &= \{g \in D^\times \mid g y_i = y_i g\} \\ &= C_D(y_i) \setminus \{0\} \end{aligned}$$

Since $C_D(y_i)$ is a division algebra, its dimension d_i must be finite since D is finite. It is also strictly less than m since $C_D(y_i)$ is a $Z(R)$-subalgebra of D. The orbit stabilizer theorem together with the class equation gives

$$\begin{aligned} q^m &= |D| \\ &= |Z(R)| + \sum_{i=1}^{k} |\text{Orb}_{D^\times}(x_i)| \\ &= q + \sum_{i=1}^{k} \frac{|D^\times|}{|C_D(y_i) \setminus \{0\}|} \\ &= q + \sum_{i=1}^{k} \frac{q^m - 1}{q^{d_i} - 1} \end{aligned}$$

and so we conclude. □

Theorem 5.5.3: Little Wedderburn's Theorem

A finite division ring is a field.

Proof. Firstly, the function $h(x) = \frac{x^m-1}{x^{d_i}-1}$ is a polynomial since d_i divides m. Any factor $x - \zeta^k$ where $\zeta = e^{2\pi i/m}$ of the cyclotomic polynomial $\Psi_m(x)$ divides $x^m - 1$ but not $x^{d_i} - 1$ and hence it divides $h(x)$. Thus $\Psi_m(x)$ divides $h(x)$ and $\Psi_m(q)$ divides the right hand side of

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

Hence $\Psi_m(q)$ divides $q - 1$. But this is a contradiction since $|\Psi_m(q)| > q - 1$. Indeed, we have that

$$\begin{aligned} |\Psi_m(q)| &= \prod_{t=1,\gcd(t,m)=1}^{m-1} |q - \zeta^t| \\ &> (q-1)^{\deg(\Psi_m(x))} \\ &\geq q - 1 \end{aligned}$$

where the first inequality $|q - \zeta^t| > q - 1$ is clear since $\zeta^t \neq 1$ and on the complex plane, $q - 1$ is the distinct from the real point q to 1 and $|q - \zeta^t|$ is the distance from q to ζ^t which is on the unit circle and thus is further away from q than 1. □

6 Semisimplicity

6.1 Semisimple Modules

Definition 6.1.1: Semisimple Modules

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

Definition 6.1.2: Socle of a Module

Let M be a left R-module. The socle of M is defined by

$$\text{soc}(M) = \sum_{\substack{S \text{ is a simple} \\ \text{submodule}}} S$$

Lemma 6.1.3

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

Proof. Suppose that M is semisimple. Then M is a direct sum of simple submodules so that $M = \text{soc}(M)$. Now suppose that $\text{soc}(M) = M$. Suppose that $M = \sum_{i\in I} S_i$ is the internal direct product of some submodules of M. Consider the poset

$$\mathcal{P} = \left\{ X \subseteq I \;\middle|\; \sum_{i\in X} S_i \text{ is a direct sum} \right\}$$

ordered by inclusion. In particular, recall from Rings and Modules that $X \in \mathcal{P}$ if and only if $\phi : \bigoplus_{i\in X} S_i \to M$ defined by $\phi\left((m_i)_{i\in X}\right) = \sum_{i\in X} m_i$ is injective. The kernel of ϕ is given by

$$\begin{aligned} \ker(\phi) &= \left\{ (m_i)_{i\in X} \mid \sum_{i\in X} m_i = 0 \right\} \\ &= \left\{ (m_i)_{i\in X} \;\middle|\; \text{for all } i_1, \dots i_k \in X \text{ we have } m_{i_1} + \cdots + m_{i_k} = 0 \right\} \end{aligned}$$

The kernel being trivial is equivalent to the condition that for all $i_1, \dots, i_k \in X$ and all $m_{i_t} \in S_{i_t}$, we have $m_{i_1} + \cdots + m_{i_k} = 0$ implies $m_{i_1} = \cdots = m_{i_k} = 0$. Let $\mathcal{C}$ be a chain in $\mathcal{P}$. It is clear that $T = \bigcup_{Z\in\mathcal{C}} Z$ is an upper bound of $\mathcal{C}$. Indeed if the above condition fails, then it fails on some finitely many elements x_i which are contained in $X \subseteq Z \subseteq T$. By Zorn's lemma, $\mathcal{P}$ has a maximal element J. We know that $N = \sum_{i\in J} S_i$ is a direct sum. It remains to show that $N = M$. If this is false, then there exists S_k not a subset of N. In particular, $k \neq J$. Consider the set $J \cup \{k\}$. In particular the above condition fails and such a failure must contain a non-zero element $x_k \in S_k$ since the condition holds before k was introduced to J. Then $x_k = -\sum_{j\neq k} x_j \in N$ and $N \cap S_k$ is non-zero. Since S_k is simple, $N \cap S_k = S_k$ and thus $N \supseteq S_k$, which is a contradiction. □

Corollary 6.1.4

A quotient module of a semisimple module is semisimple.

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

Recall the radical

Lemma 6.1.5

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

Proof. Suppose that M is semisimple. Then $M = \bigoplus_{i \in I} S_i$ for S_i simple submodules of M. Define

$$M_i = \bigoplus_{j \in I \setminus \{i\}} S_j$$

for each $i \in I$. Since $M/M_i \cong S_i$, we have that M_i is cosimple. Then

$$\text{rad}(M) = \bigcap_{\substack{N \leq M \\ N \text{ is cosimple}}} N \subseteq \cap_{i \in I} M_i = 0$$

Thus $\text{rad}(M) = 0$. □

6.2 Maschke's Theorem

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

Definition 6.2.1: Completely Reducible Modules

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

Proposition 6.2.2

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

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

of R-modules.

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

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

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

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

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

Lemma 6.2.3

A submodule of a completely reducible module is reducible.

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

$$M = P \oplus K$$

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

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

so that we conclude. □

Lemma 6.2.4

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

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

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

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

Theorem 6.2.5

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

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

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

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

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

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

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

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

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

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

$\psi(n)+\sum_{i\in J}\psi(s_i)=0$ together with $n\in\ker(\psi)$ to imply that

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

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

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

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

Corollary 6.2.6

A submodule of a semisimple module is semisimple.

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

Using the notion of completely reducible, we can prove that the decomposition of a semisimple module into simple modules is essentially unique.

Proposition 6.2.7

Let M be a semisimple left R-module with two decompositions

$$M=\bigoplus_{i=1}^n S_i \quad\text{and}\quad M=\bigoplus_{j=1}^m T_j$$

into simple modules. Then $n=m$ and the simple modules S_i and T_j are isomorphic up to reordering.

Proof. We proceed by induction on n. If $n=1$, then, M is simple and we are done.

Suppose that it is true for $n-1$. Let $K=\bigoplus_{i=1}^{n-1}S_i$. Consider the quotient homomorphism $\psi:M\to M/K$. Clearly we have that

$$\frac{M}{K}=\psi(M)=\psi\left(\sum_{j=1}^m T_j\right)=\sum_{j=1}^m\psi(T_j)$$

Then each $\psi(T_j)$ is either 0 or simple and isomorphic to T_j so that we can reduce the indexing set so that we exclude the $j\in J$ for which $\psi(T_j)=0$. Now we have that $M=K\oplus\left(\bigoplus_{j\in J}T_j\right)$. By proposition 2.2.2, we have that S_n and $\left(\bigoplus_{j\in J}T_j\right)$ are isomorphic. Thus $\bigoplus_{j\in J}T_j$ is actually just a single element. Without loss of generality, take $J=\{m\}$. Both $\bigoplus_{i=1}^{n-1}S_i$ and $\bigoplus_{j=1}^{m-1}T_j$ are direct complements of T_m. They are isomorphic by proposition 2.2.2. By the induction hypothesis, we conclude. □

Theorem 6.2.8: Maschke's Theorem

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

Proof. Suppose that $\mathbb{F}G$ is semisimple. Consider $\mathbb{F}$ as the trivial $\mathbb{F}G$-module defined by $g \cdot x = x$ for all $x \in \mathbb{F}$ and $g \in G$ and extend it by linearity. Then there is a homomorphism of $\mathbb{F}G$-modules $\psi : \mathbb{F}G \to \mathbb{F}$ defined by

$$\psi\left(\sum_{g\in G} \lambda_g g\right) = \sum_{g\in G} \lambda_g$$

Since $\mathbb{F}G$ is semisimple, $\ker(\psi)$ has a direct complement L. By proposition 2.2.2, and the first isomorphism theorem for modules, we have that $L \cong \mathbb{F}$. Since $L \cong \mathbb{F}$, $hx = x$ for all $h \in G$. Thus

$$\sum_{g\in G} \lambda_g(hg) = \sum_{g\in G} \lambda_g g$$

for all $h \in G$. Thus all λ_g are equal. Hence $L =\cong \mathbb{F}z$ where $z = \sum_{g\in G} g$. If G is infinite then z is not well defined. Finally, if $n = |G|$ is finite and $p \mid n$, then $\psi(z) = n = 0_{\mathbb{F}}$ and $\psi : L \to \mathbb{F}$ is not surjective, contradicting proposition 2.2.2. Thus p does not divide n.

Now suppose the contrary. Since p does not divide n, we can choose $\lambda \in \mathbb{F}$ such that $n\lambda = 1_{\mathbb{F}}$. Let N be an $\mathbb{F}G$-submodule of an $\mathbb{F}G$-module M. Then N is a vector subspace of M and so we can choose a vector space complement L such that $M = N \oplus L$ in the sense of Linear Algebra. This gives a projection map $p : M \to M$ such that $\ker(p) = L$, $\text{im}(p) = N$ and $p^2 = p$ and is linear. Define $q : M \to M$ a linear map by

$$q(x) = \lambda \sum_{g\in G} g \cdot p(g^{-1}(x))$$

By definition, $N \supseteq \text{im}(q)$. Moreover, for each $x \in N$, we have that $g^{-1}x \in N$ so that

$$q(x) = \lambda_{g\in G} g \cdot (g^{-1}x) = \lambda \sum_{g\in G} x = \lambda n x = x$$

Thus q is another idempotent $N = \text{im}(q)$. Moreover, $q \in \text{End}_{\mathbb{F}G}(M)$ since for $x \in M$ and $h \in G$, we have that

$$\begin{aligned} q(hx) &= \lambda \sum_{g\in G} g \cdot (g^{-1}hx) \\ &= \lambda \sum_{g,k\in G, gk=h} g \cdot (kx) \\ &= \lambda \sum_{g\in G} hg \cdot (g^{-1}kx) \\ &= hq(x) \end{aligned}$$

so that $\ker(q)$ is a direct complement and so we conclude. □

6.3 Peirce Decomposition for Modules

Definition 6.3.1: Idempotents

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

Definition 6.3.2: Full System of Orthogonal Idempotents

Let R be a ring. Two idempotents e, f are orthogonal if $ef = fe = 0$. A full system of orthogonal idempotents is a finite collection of non-zero pairwise orthogonal idempotent elements $e_1, \dots, e_n \in R$ such that $e_1 + \cdots + e_n = 1$.

Such a system always exists and may not be unique up even just up to the size $n \in \mathbb{N}$. Indeed one such trivial system is to take the identity 1.

Proposition 6.3.3

Let M be an R-module. Then there is a bijection

$$\left\{\substack{\text{Finite direct sum}\\ \text{decompositions } M=\bigoplus_{i=1}^n M_i}\right\} \xleftrightarrow{1:1} \left\{\substack{\text{Full orthogonal system}\\ \text{of idempotentes in } \mathrm{End}_R(M)}\right\}$$

between the set of all finite direct sum decompositions $M = \bigoplus_{i=1}^n M_i$ with all $M_i \neq 0$ and the set of all full orthogonal system of idempotents in $\mathrm{End}_R(M)$.

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

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

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

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

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

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

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

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

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

Definition 6.3.4: Peirce Decompositions

Let M be an R-module. A finite direct sum decomposition

$$M = \bigoplus_{i=1}^n M_i$$

arising from a full orthogonal system of idempotents are called Peirce decompositions.

For two idempotents e and f, eRf loses the structure of a ring and is just an abelian group. We give a useful interpretation of eRf as follows.

Proposition 6.3.5

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

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

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

By collecting all the abelian groups eRf in a matrix, we can recover the ring R itself.

Theorem 6.3.6: Two-Sided Peirce Decompositions

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

$$R = \bigoplus_{i,j=1}^{n} e_iRe_j = \begin{pmatrix} e_1Re_1 & \cdots & e_1Re_n \\ \vdots & \ddots & \vdots \\ e_nRe_1 & \cdots & e_nRe_n \end{pmatrix} \quad \text{and} \quad M = \bigoplus_{i=1}^{n} e_iM = \begin{pmatrix} e_1M \\ \vdots \\ e_nM \end{pmatrix}$$

that satisfies the following:

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

Proof. Let $e_1, \dots, e_n$ be the given full orthogonal system of idempotents of the ring R. Then by proposition 2.2.4 we obtain a finite direct sum decomposition

$$R = \bigoplus_{i=1}^{n} e_iR \quad \text{and} \quad M = \bigoplus_{i=1}^{n} e_iM$$

Each e_iR is an R-module since they are left ideals. Thus we can apply proposition 2.2.4 to obtain $e_iR = \bigoplus_{i=1}^{n} e_iRe_j$ so that we obtain the required decompositions for R and M.

Let $\lambda \in \mathbb{F}$ and $x \in e_iRe_j$. Then $x = e_iye_j$ for some $y \in R$. Then

$$\lambda x = \lambda e_iye_j = e_i(y\lambda)e_j \in e_iRe_j$$

since R is an $\mathbb{F}$-algebra. Since e_iRe_j is an abelian subgroup, it follows that e_iRe_j is an $\mathbb{F}$-vector subspace. The proof for e_iM is similar.

Multiplication in R is given by $(e_ixe_i) \cdot (e_iye_i) = e_ixye_i$ so that multiplication is closed. Moreover, $1_{e_iRe_i} = e_i$ is not equal to 0 so that the ring is non-zero.

Similarly, $(e_ixe_i) \cdot (e_im) = e_ixm \in e_iM$ so that e_iM is closed under the ring action. Thus e_iM becomes an e_iRe_i-module.

It is easy to check that multiplication defined in the matrix way makes sense. □

Note component wise multiplication only defines a group isomorphism between $R = \bigoplus_{i,j=1}^n e_iRe_j$ To obtain a ring isomorphism, one needs to consider multiplication as matrices.

6.4 Artin-Wedderburn Theorem

Theorem 6.4.1: Artin-Wedderburn Theorem

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

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

Proof.

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

  Let $L_1, \dots, L_k$ be distinct simple modules among the S_i. By Schur's lemma, $D_i = \text{End}_R L_i$ is a division ring. Reorder the summands so that we can group them as following:
  $$R = \underbrace{S_1 \oplus \cdots \oplus S_{n_1}}_{\text{each } S_i \cong L_1} \oplus \cdots \oplus \underbrace{S_{n_1+\cdots+n_{k-1}+1} \oplus \cdots \oplus S_m}_{\text{each } S_i \cong L_k}$$
  Replace each S_i with the corresponding L_j together with lemma 2.4.3 to get
  $$R \cong \text{End}_R \cong \text{End}_R\left(\underbrace{L_1 \oplus \cdots \oplus L_1}_{n_1} \oplus \cdots \oplus \underbrace{L_{i_k} \oplus \cdots \oplus L_k}_{n_k}\right) = \text{End}_R\left(\bigoplus_{j=1}^k L_j^{n_j}\right)$$
  Now let $e_1, \dots, e_m$ be the full system of orthogonal idempotents corresponding to the above decomposition by proposition 6.2.4. Consider e_j in the jth group and e_s in the tth group. By proposition 6.2.5, we have
  $$e_jRe_s \cong \text{Hom}_R(L_j, L_t) = \begin{cases} 0 & \text{if } j \neq t \\ D_j & \text{if } j = t \end{cases}$$
  Then by the Peirce decomposition,
  $$R = \begin{pmatrix} D_1 & \cdots & D_1 & 0 & \cdots & 0 & \cdots \\ \vdots & & \vdots & \vdots & & \vdots & \\ D_1 & \cdots & D_1 & 0 & \cdots & 0 & \cdots \\ 0 & \cdots & 0 & D_2 & \cdots & D_2 & \cdots \\ \vdots & & \vdots & \vdots & & \vdots & \\ 0 & \cdots & 0 & D_2 & \cdots & D_2 & \cdots \\ \vdots & & \vdots & \vdots & & \vdots & \end{pmatrix} = M_{n_1}(D_1) \times M_{n_2}(D_2) \times \cdots \times M_{n_k}(D_k)$$

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

□

Similarly, there is a decomposition for right semisimple rings.

Corollary 6.4.2

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

Proof. R is a right R-module if and only if it is a left R^{op}-module. Moreover $M_n(D^{\text{op}}) \cong M_n(D^{\text{op}})$ so that we conclude by Artin-Wedderburn theorem. □

It thus makes sense to just say that a ring is semisimple instead of distinguishing left and right.

Proposition 6.4.3

The following are true regarding semisimple algebras over fields.

- A semisimple $\mathbb{C}$-algebra of countable dimension is isomorphic to
$$\prod_{i=1}^k M_{k_i}(\mathbb{C})$$
- A semisimple $\mathbb{R}$-algebra of countable dimension is isomorphic to
$$\prod_{i=1}^k M_{k_i}(\mathbb{R}) \times \prod_{i=1}^n M_{n_i}(\mathbb{C}) \times \prod_{i=1}^t M_{t_i}(\mathbb{H})$$
- A finite dimensional semisimple $\mathbb{F}_q$ algebra is isomorphic to
$$\prod_{i=1}^k M_{k_i}(\mathbb{F}_{q^{t_i}})$$

Proof. If R is an $\mathbb{F}$-algebra that is semisimple, we have that
$$R = \prod_{i=1}^k M_{n_i}(D_i)$$
by Artin-Wedderburn theorem. In particular, each $M_{n_i}(D_i)$ is also an $\mathbb{F}$-algebra. Moreover, by identifying D in any one component of M_{n_i}, we can see that D is also an $\mathbb{F}$-algebra. Each D_i is a finite dimensional $\mathbb{F}$-vector space if and only if R is finite dimensional. Then we have the following.

- If $\mathbb{F} = \mathbb{C}$ then D_i can only possibly be $D_i = \mathbb{C}$
- If $\mathbb{F} = \mathbb{R}$ then D_i is either $\mathbb{R}$ or $\mathbb{C}$ or $\mathbb{H}$ by Frobenius theorem and theorem 1.4.6.
- If $\mathbb{F} = \mathbb{F}_q$ then $D_i = \mathbb{F}_{q^{t_i}}$ for some $t_i \in \mathbb{N}$ by Little Wedderburn's theorem.

Thus we conclude. □

7 Radicals

7.1 The Radical of a Module

Definition 7.1.1: Cosimple

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

Lemma 7.1.2

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 7.1.3: 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

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

7.2 The Nilradical Ideal

Definition 7.2.1: 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 7.2.2: 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 7.2.3

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

Not every nil ideal is nilpotent.

Definition 7.2.4: 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 7.2.5

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 $a_1x + a_2x^2 + \dots$ so that $1 + z = 1 + a_1x + a_2x^2 + \dots$ is invertible.

Proposition 7.2.6

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

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

□

7.3 Annihilator

Definition 7.3.1: 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 7.3.2

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.

7.4 The Jacobson Radical

Definition 7.4.1: 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 7.4.2

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 7.4.3

Let R be a ring. Then we have
$$J\left(\frac{R}{J(R)}\right) = 0$$