Commutative algebra and algebraic geometry

Weiying Guo

December 2021

With utmost sincerity, no difficulty is insurmountable.

These notes are mostly copied from Macdonald-Atiyah's book Communtative algebra and Hartshorne's book Algebraic geometry.

1 Rings and Ring homomorphisms

A ring R is a set with two binary operations with the following conditions

1. R is an abelian group with respect to addition
2. Multiplication is associative i.e.,
$$(xy)z = x(yz)$$
and distributive over addition
$$x(y+z) = xy + xz, \quad (y+z)x = yx + zx$$
3. If $x, y \in R$, then $xy = yx$(ring R is commutative)
4. there exists a unit $1 \in R$ such that $x1 = 1x = x$ for $x \in R$.

Example 1.1. *1. Integers* $\mathbf{Z}$ *is commutative.*

2. The quaternions
$$\mathbb{H} = \{a + ib + jc + kd \mid a, b, c, d \in \mathbb{R}\}$$
with relations
$$i^2 = j^2 = k^2 = ijk = -1$$
is a non-commutative ring with identity.

3. *The zero ring has the multiplicative identity and the addition identity being the same. So we have*

$$x = x1 = x0 = 0.$$

Hence, the zero ring has only one element 0*.*

Definition. A ring homomorphism is

$$f : A \to B$$

satisfies the following conditions

$$\begin{aligned} f(x+y) &= f(x) + f(y) \\ f(xy) &= f(x)f(y) \\ f(1) &= 1 \end{aligned}$$

Moreover, from the first relation, set $x = y = 0$

$$\begin{aligned} f(0+0) &= f(0) + f(0) \\ f(0) &= 2f(0) \\ f(0) &= 0 \end{aligned}$$

Hence, we obtain $f(0) = 0$ and $f(-y+y) = f(-y) + f(y)$. Then we obtain $-f(y) = f(-y)$. Lastly, setting $y = -y$, we obtain $f(x-y) = f(x) - f(y)$.

Definition. A subring of A is a subset of A which contains identity and closed under **addition** and **multiplication**.

Example 1.2. *The integers are subring of the real number or complex number. There are many example of subring we will consider them later on.*

Let

$$\begin{aligned} f &: A \to B \\ g &: B \to C \end{aligned}$$

be ring homomorphims. Then $g \circ f$ is a ring homomoprhism.

1.1 Ideals, quotient rings

An ideal $\mathfrak{a}$ of A is a subring of A which satisfies the following condition

$$A\mathfrak{a} \subset \mathfrak{a}.$$

Example 1.3. *The ideals in the integer ring $\mathbb{Z}$ all takes the form $\mathbb{Z}a = (a)$ where $a \in \mathbb{Z}$. Integers turns out to be a very interesting example to look at for now.*

Example 1.4. *Let*

$$f : A \to B$$

be a ring homomorphism. Then the kernel

$$\ker(f) = \{x \in A \mid f(x) = 0\}$$

is an ideal. To check this is an ideal, assume that $x \in \ker(f)$. Then

$$f(ax) = af(x) = a \cdot 0 = 0.$$

Hence, $\ker(f)$ is an ideal. Moreover, the image

$$\mathrm{Im}(f) = \{y \in B \mid f(x) = y\}$$

is a subring of B.

Definition. Let $\mathfrak{a}$ be an ideal of A. Then the quotient ring is

$$A/\mathfrak{a} \text{ consisting elements } x + \mathfrak{a} \text{ where } x \in A.$$

The multiplication of A is defined as following

$$(x + \mathfrak{a})(y + \mathfrak{a}) = xy + \mathfrak{a}.$$

Example 1.5. *Let $A = \mathbb{Z}$ which is the ring of integers and let $\mathfrak{a} = (2) = 5\mathbb{Z}$ which is the ideal generated by the integer 5. Then the quotient*

$$A/\mathfrak{a} = \mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}.$$

There is a natural mapping

$$\begin{aligned} \phi : A &\to A/\mathfrak{a} \\ x &\mapsto x + \mathfrak{a}. \end{aligned}$$

This map ϕ is surjective and for a give ring homomorphism f, there exists a unique map $\overline{f}$ so that the following communtative diagram

$$\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr, "\phi"'] & & B \\
& A/\mathfrak{a} \arrow[ur, "\exists!\overline{f}"] &
\end{tikzcd},$$

in other word, there exists unique $\overline{f}$ such that $f = f \circ \phi$. The map $\overline{f}$ is often referred to the **descent** of f.

Proposition 1.1 (First isomorphism theorem)**.** *Let $f : A \to B$ be a ring homomoprhism. Then*

$$f/\ker(f) \cong \mathrm{Im}(f).$$

Proof. See Artin's algebra Theorem 11.4.2 on page 335. □

Proposition 1.2 (Correspondence theorem)**.** *There is a one to one correspondence*

$$\{\textit{ideals } \mathfrak{b} \textit{ of } A \textit{ which contains } \mathfrak{a}\} \Longleftrightarrow \{\textit{ideals } \overline{\mathfrak{b}} \textit{ of } A/\mathfrak{a}\}$$

Proof. See Artin's algebra Theorem 11.4.3. □

1.2 Zero divisors, nilpotent elements, unit

Definition. Let A be a ring. Then $x \in A$ is a zero divisor if

$$\text{there exists } y \neq 0 \text{ such that } xy = 0.$$

Example 1.6. *Again we look into the ring*

$$\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}.$$

Then the element $\overline{2}$ and $\overline{3}$ are zero divisors. Since $\overline{2} \times \overline{3} = 0$.

Definition. A ring R has no **zero divisors** is called a integral domain.

Example 1.7. *The ring $\mathbb{Z}/3\mathbb{Z}$ is an integral domain. More general the ring $\mathbb{Z}/p\mathbb{Z}$ where p is a prime number is an integral domain.*

Definition. An element $x \in A$ is called nilpotent if

$$\text{there exists } n \in \mathbb{Z}_{\geq 1} \text{ such that } x^n = 0.$$

Example 1.8. *It is hard to find nilpotent element in communtantive ring as we will see later that they are contained in the intersection of all prime ideals. But now we will use the matrix ring which is **non-communtantive** in general. The upper-triangluar matrix are nilpotent element in the matrix ring. For instance, let*

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \qquad \textit{then } A^3 = 0.$$

Note that a nilpotent element is a zero divisor. Since if x is nilpotent, then there exists n such that

$$0 = x^n = x^{n-1}x.$$

Definition. Let $x \in A$. Then the ideal **generated by** x is given by

$$(x) = Ax = \{ax \mid a \in A\},$$

we call such ideal a **principal ideal**.

Example 1.9. *For the integer ring, the ideals are all principal.*

Definition. Let A be a ring. Then $x \in A$ is called a **unit** if

$$\text{there exists } y \in A \text{ such that } xy = 1.$$

Example 1.10. *In the integer ring $\mathbb{Z}$, there is only one unit i.e., 1. In the rational ring $\mathbb{Q}$, every element is a unit i.e., an element in $\mathbb{Q}$ takes the form*

$$x = \frac{a}{b}, \ \textit{then } x^{-1} = \frac{b}{a}.$$

Lemma 1.3. *Let $x \in A$. Then*

$$x \textit{ is a unit} \Longleftrightarrow (x) = A = (1).$$

Proof. Assume x is a unit. To show $(x) = A = (1)$. Since x is a unit, there exists $y \in A$ such that $xy = 1$. Since

$$(x) = Ax = \{ax \mid a \in A\},$$

we have $1 \in (x)$. Hence, $(x) = A$. Assume $(x) = A$. Then there exists $y \in A$ such that $xy = 1$. Hence, x is a unit. □

Definition. A field is a ring such that every element is a unit except for 0.

Example 1.11. *The ring of rational numbers $\mathbb{R}$ forms a field and the complex numbers $\mathbb{C}$ is a field. For a counterexample, $\mathbb{Z}$ is not a ring.*

Proposition 1.4. *Let A be a ring which is not the zero ring. Then the following are equivalent:*

1. *A is a field;*
2. *the only ideals in A are 0 and (1);*
3. *every homomorphism of A into a non-zero ring B is injective.*

Proof. Assume A is a field.
To show: the only ideal of A are 0 and (1).
Let $I \in A$ be an ideal.
To show: $I = 0$ or $I = (1)$
Since A is a field, there exists a unit in I.
By Lemma 1.3, we have that $I = A$.
Now we show that $2 \implies 3$.
Let

$$\phi : A \to B$$

be a ring homomorphism.
To show: ϕ is injective.
To show: $\ker(\phi)$ is equal to 0.
Then $\ker(\phi)$ is an ideal.
Since the ideals in A are (0) or (1), we have

$$\ker(\phi) = 0$$

and ϕ is injective.
To show: $3 \implies 1$.
To show: A is a field.
To show: If $x \in A$ and $x \neq 0$, then there exists y such that $xy = 1$.
Assume $x \in A$ and $x \neq 0$ and x is not a unit.
Then the natural map

$$\phi : A \to A/(x)$$

is not only injective but also surjective.
Hence $A \cong A/(x)$.
But this can only happen if $(x) = 0$ which implies that $x = 0$. □

1.3 Prime ideals and maximal ideals

Definition. An ideal $\mathfrak{p}$ in A is prime if $xy \in \mathfrak{p}$, then $x \in \mathfrak{p}$ and $y \in \mathfrak{p}$.

Definition. An ideal A is maximal if $\mathfrak{m} \neq 1$ and if

$$\mathfrak{m} \subseteq \mathfrak{a} \subseteq A,$$

then $\mathfrak{a} = \mathfrak{m}$ or $\mathfrak{a} = A$.

Theorem 1.5. *The following conditions are very useful for checking prime ideals and maximal ideals:*

$$\begin{aligned} \mathfrak{p} \textit{ is prime } &\iff A/\mathfrak{p} \textit{ is an integral domain },\\ \mathfrak{m} \textit{ is maximal } &\iff A/\mathfrak{m} \textit{ is a field.}\end{aligned}$$

Remark 1.6. Since fields are integral domains, maximal ideals are prime ideals by Theorem 1.5.

Let S be a non-empty partially ordered set. Then a subset T of S is a **chain** if $x, y \in T$, then either $x \leq y$ or $y \leq x$.

Lemma 1.7 (Zorn's lemma)**.** *Let S be a partially ordered set with partial ordering $\leq$. If every chain T of S has a upper bound in S, then S has at least one maximal element.*

Theorem 1.8. *Let $A \neq 0$ be a ring. Then A has at least one maximal ideal.*

Proof. Now let Σ be the set of all ideals in A. Then Σ is a partially order set with partial order $\subseteq$. Let (a_α) be a chain of ideals in A and let

$$\mathfrak{a} = \bigcup_\alpha \mathfrak{a}_\alpha.$$

In order to verify $\mathfrak{a}$ is an ideal, let $x \in \mathfrak{a}$ and $y \in A$. Then $x \in \mathfrak{a}_\alpha$ for some α. Since $\mathfrak{a}_\alpha$ is an ideal, $yx \in \mathfrak{a}_\alpha \subseteq \mathfrak{a}$. Hence, $\mathfrak{a}$ is an ideal. It is also an upper bound of the chain T. By Zorn's lemma, there exists at least one maximal ideal in A. □

Corollary 1.9. *Let $\mathfrak{a} \neq A$ be an ideal of A. Then there exists a maximal ideal containing $\mathfrak{a}$.*

Proof. Recall from Proposition 1.2(Correspondence theorem) that there is a one to one correspondence between the ideals $\mathfrak{b}$ containing $\mathfrak{a}$ and the ideals $\overline{\mathfrak{b}}$ in $A/\mathfrak{a}$. From theorem 1.8, we know that there is a maximal ideal for each ring A. Consider the ring $A/\mathfrak{a}$, there is a maximal ideal call it $\overline{m_\mathfrak{a}}$. Hence, the ideal $m_\mathfrak{a}$ in A under the correspondence map contains $\mathfrak{a}$ and it is also a maximal ideal. □

Corollary 1.10. *Every non-unit of A is contained in a maximal ideal.*

Proof. Let $x \in A$ be a non-unit. Then it generated an ideal (x). Hence, it is contained in some maximal ideal by Corolloary .9. □

One interesting ring that we will be interested is so called the **local ring** which is a ring contains a unique maximal ideal. Since local ring has unique maximal ideal, we call the quotient $A/\mathfrak{m}$ the **residue field** of A, where $\mathfrak{m}$ is the unique maximal ideal of A. Now we procceed to investigate when the ring will be local.

Proposition 1.11. *Let A be a ring and $\mathfrak{m} \neq (1)$ an ideal of A such that $x \in A - \mathfrak{m}$ is a unit in A. Then A is a local ring.*

Proof. Since every ideal contains units are equal to A, for proper ideals it must be contained in $\mathfrak{m}$. So $\mathfrak{m}$ is a maximal ideal and it is also a unique maximal ideal. □

Proposition 1.12. *Let A be a ring and $\mathfrak{m}$ a maximal ideal of A such that every element of $1 + \mathfrak{m}$ is a unit in A. Then A is a local ring.*

Proof. Assume $x \in A - \mathfrak{m}$. Since $\mathfrak{m}$ is maximal, the ideal

$$\langle x, \mathfrak{m} \rangle = A.$$

Hence, there exists $y \in A$ and $t \in \mathfrak{m}$ such that

$$xy + t = 1.$$

Hence, $xy = 1 - t \in 1 + \mathfrak{m}$ and it is a unit. Therefore, x is a unit. Hence, A is a local ring by Prop 1.11. □

Example 1.12. *Let $A = k[x_1, \dots, x_n]$ be a polynomial ring, with k being a field. If f is a irreducible polynomial, then the ideal generated by (f) is a prime ideal.*

Example 1.13. *Let $A = \mathbb{Z}$ be the integer ring. Then every ideal in $\mathbb{Z}$ is principal and the prime ideals are the ones generated by the prime numbers.*

Example 1.14. *A* ***principal ideal domain*** *is an integral domain with every ideal being a principal. In a principal ideal domain, we have every non-zero prime ideal is a maximal ideal. To see this, let $(x) \neq 0$ be a prime ideal and let $(x) \subseteq (y)$. To show $(y) = A$ or $(y) = (x)$. Since $(x) \subseteq (y)$, we have $x = yz$ for some $x \in A$. Hence, $yz \in (x)$. Since $z \notin$*

2 Nilradical and Jacobson radical

The following section gives the nilradical and Jacobson radical. Let A be a communtative ring and

$$\mathfrak{R} = \{\text{all nilpotent elements in a ring } A\}.$$

The ideal $\mathfrak{R}$ is called the nilradical of A.

Proposition 2.1. *The set $\mathfrak{R}$ is an ideal and $A/\mathfrak{R}$ has no non-trivial nilpotent element.*

Proof. To show: $\mathfrak{R}$ is an ideal.
To show:

1. $A\mathfrak{R} \subset \mathfrak{R}$,

2. $\mathfrak{R}$ is a subring.

Case 1:Assume $x \in \mathfrak{R}$. Then $ax \in \mathfrak{R}$ for all $a \in A$.
Case 2:Let $x, y \in \mathfrak{R}$. Then

$$x^m = 0 \quad \text{and} \quad y^n = 0.$$

By the binomial theorem,

$$(x+y)^{m+n-1} = \sum_{i=1}^{m+n-1} \binom{m+n-1}{i} x^i y^{m+n-1-i}.$$

Let $s = i$ and $r = m+n-1-i$. Then $s+r = m+n-1$. Hence, we cannot have both $r < m$ and $s < n$. Therefore, we have

$$(x+y)^{m+n-1} = 0.$$

Hence, $\mathfrak{R}$ is closed under addition and it is clear that $\mathfrak{R}$ is closed under multiplication. Hence, $\mathfrak{R}$ is a subring and therefore an ideal. Now we will show that $A/\mathfrak{R}$ has no nilpotent element.
To show: $A/\mathfrak{R}$ has no nilpotent element.
To show: If $\overline{x} \in A/\mathfrak{R}$ is a nilpotent element, then $\overline{x} = 0$.
Assume $\overline{x} \in A/\mathfrak{R}$ and $\overline{x}$ is a nilpotent element.
Then there exists $n > 0$ such that

$$\overline{x}^n = 0.$$

Since $\overline{x}^n = 0$, we have $x^n \in \mathfrak{R}$. Hence, there exists $k > 0$ such that $(x^n)^k = 0$. Therefore, $x \in \mathfrak{R}$ and $\overline{x} = 0$. □

The following proposition can also be another interptation of the nilradical.

Proposition 2.2. *Let $\mathfrak{N}$ be the nilradical of A. Then*

$$\mathfrak{N} = \bigcap_{\mathfrak{p} \text{ prime ideal } \subset A} \mathfrak{p}$$

Proof. Assume $\mathfrak{N}' = \bigcap_{\mathfrak{p} \text{ prime ideal } \subset A} \mathfrak{p}$.
To show: $\mathfrak{N} = \mathfrak{N}'$.
To show: $\mathfrak{N} \subseteq \mathfrak{N}'$ and $\mathfrak{N}' \subseteq \mathfrak{N}$.
To show: $\mathfrak{N} \subseteq \mathfrak{N}'$.
Assume $f \in A$ and f is a nilpotent element.
To show: $f \in \mathfrak{N}'$.
To show: $f \in \mathfrak{p}$ for all prime ideals $\mathfrak{p}$ in A.
Since f is nilpotent, there exists $n > 0$ such that $f^n = 0$.
Since $0 \in \mathfrak{p}$ for all $\mathfrak{p}$, $f^n \in \mathfrak{p}$.
Since $\mathfrak{p}$ is prime, $f \in \mathfrak{p}$ for all prime $\mathfrak{p}$.
To show: $\mathfrak{N}' \subseteq \mathfrak{N}$.
Assume f is not nilpotent.
To show: f is not in $\mathfrak{N}'$.
Let

$$\Sigma = \{\mathfrak{a} \text{ ideals } \mid \text{ there exists } n > 0 \text{ such that } f^n \in \mathfrak{a}\}.$$

Since $0 \notin \mathfrak{a}$, Σ is not empty.
Hence, applying Zorn's lemma, there exists a maximal element in Σ ordered by inclusion. Define $\mathfrak{p}$ to be the maximal element in Σ.
To show: $\mathfrak{p}$ is a prime ideal.
Assume $x, y \notin \mathfrak{p}$.
Since $x, y \notin \mathfrak{p}$,

$$\mathfrak{p} \subseteq \mathfrak{p} + (x) \quad \text{and} \quad \mathfrak{p} \subseteq \mathfrak{p} + (y)$$

strictly contain $\mathfrak{p}$. Therefore $\mathfrak{p} + (x) \notin \Sigma$ and $\mathfrak{p} + (y) \notin \Sigma$.
Hence, there exists m, ℓ such that

$$f^m \in \mathfrak{p} + (x) \quad f^\ell \in \mathfrak{p} + (y)$$

for some m, n. Hence,

$$f^{m+\ell} \in \mathfrak{p} + (xy).$$

Therefore, $\mathfrak{p} + (xy) \notin \Sigma$ and $(xy) \notin \mathfrak{p}$. Hence, $xy \notin \mathfrak{p}$. □

The **Jacobson radical** $\mathfrak{J}$ of A is defined as

$$\mathfrak{J} = \bigcap_{\mathfrak{m} \text{ maximal idea of } A} \mathfrak{m},$$

The following Proposition give a characterization of the Jacobson ideal.

Proposition 2.3. *The elements in the Jacobson ideal has the following correspondence*

$$x \in \mathfrak{J} \iff 1 - xy \text{ is a unit in } A \text{ for all } y \in A.$$

Proof. □

Modules

Definition. Let A be a ring. An A-module is a abelian group M with the following conditions satisfied:

$$\begin{aligned} a(x+y) &= ax + ay \\ (a+b)x &= ax + bx \\ (ab)x &= a(bx) \\ 1x &= x \end{aligned}$$

There is also an equivalent definition which is the following

Definition. Let A be a ring. Then an A-module M is a ring homomorphism

$$f : A \to \mathrm{End}(M).$$

There are several interesting examples for module. Let's have a look.

Example 2.1.

1. *If A is a field, then A-module is simply a vector space. So a vector sapce is a speical case of module.*

2. *Let $A = \mathbb{Z}$. Then A-module is the same as an abelian group.*

3. *Let $A = k[x]$. Then A-module is a k-vector space with a linear(????) transformation.*

4. *Let G be a finite group and let $A = k[G]$ which is the group algebra over k. Then A-module is a k-representation of G.*

Definition. Let M, N be A-module and let $a \in A$, $x, y \in M$. Then an A-module homomorphism is a function

$$f : M \to N$$

such that

$$\begin{aligned} f(x+y) &= f(x) + f(y) \\ f(ax) &= af(x) \end{aligned}$$

The first condition means taht f is a homomrphism of abelian groups and the second means that f is an A linear map.

Similarly to the ring homomorphism that composition of A-module homomorphism is also an A-module homomoprhism.

Definition. Define the set of all A-module homomorphisms to be

$$\mathrm{Hom}_A(M,N) = \{f : M \to N \mid (f+g)(x) = f(x)+g(x), \quad (af)(x) = a \cdot f(x)\}$$

Definition. Let $u : M' \to M$ and $v : N \to N''$. Then u, v induces maps

$$\begin{aligned} \overline{u} : \mathrm{Hom}(M,N) &\to \mathrm{Hom}(M',N) \\ f &\mapsto f \circ u \\ \overline{v} : \mathrm{Hom}(M,N) &\to \mathrm{Hom}(M,N'') \\ f &\mapsto v \circ f \end{aligned}$$

The following is an important relation between the modules and the maps of modules.

Lemma 2.4. *Let A be a ring and M be a A module. Then*

$$\mathrm{Hom}(A,M) \cong M.$$

Proof. Let $f \in \mathrm{Hom}(A,M)$. Define

$$\begin{aligned} M &\to \mathrm{Hom}(A,M) \\ x &\mapsto f(1) = x. \end{aligned}$$

It is clear that this is an isomorphism. □

Definition. A **submodule** N of an A-module M satisfies

1. $N \subseteq M$ is a subgroup,

2. If $a \in A$ and $n \in N$, then $a \cdot n \in N$.

Definition. Let M be an A-module and let M' be an submodule of M. Then M/M' defines an A-module with the following scalar multiplication

$$a(x + M') = ax + M'.$$

We call the A-module M/M' the quotient of M by M'.

Samiliarly to the quotient of the rings, there is the natural map

$$\begin{aligned} \varphi : M &\to M/M' \\ x &\mapsto x + M' \end{aligned}$$

which is an A-module homomorphism. Likewise in the ring case, we have the following correspondence theorem

Theorem 2.5. *(correspondence theorem) Let M' be a submodule of M. Then we have the following correspondence theorem*

$$\left\{ \textit{ submodule of } M \textit{ containing } M' \right\} \Longleftrightarrow \left\{ \textit{ submodule of } M/M' \right\}$$

Let $f : M \to N$ be an A-module homomorphism. Then the kernel of f is the set

$$\mathrm{Ker}(f) = \{x \in M \mid f(x) = 0\}$$

and kernel is a submodule of M. Now the image

$$\mathrm{Im}(f) = f(M)$$

is a submodule of N. Now we define the cokernel to be

$$\mathrm{Coker}(f) = N/\,\mathrm{Im}(f),$$

which is a quotient module of N. Similarly to the ring case, we have the following isomorphism theorem

$$M/\ker(f) \cong \mathrm{Im}(f).$$

2.1 Operations on submodules

Let $(M_i)_{i\in I}$ be a family of submodules of M. Define **sum of** modules

$$\sum_{i\in I} M_i = \left\{ \sum_{i\in I} x_i \mid x_i \in M_i \text{ for all } i \in I \right\},$$

where only finite many of the x_is are non-zero. Note that

$$\sum_{i\in I} M_i \quad \text{is the } \textbf{smallest} \text{ submodule of } M \text{ which contains all } M_i.$$

Remark 2.6. Let $(M_i)_{i\in I}$ be a family of A-modules. Consider the following intersection

$$B = \bigcap_{i\in I} M_i,$$

we will show that B is indeed a A-module. Let $x \in B$. Then

$$a \cdot x \quad \text{is well-defined.}$$

Let N be a submodule of A-moudle M. Then the quotient

$$M/N = \{x + N \mid x \in M\},$$

is a A-module with actions

$$a(x + N) = ax + N.$$

The next proposition is some useful identities

Proposition 2.7. *Let $N \subseteq M \subseteq L$ be A-modules. Then*

$$(L/N)/(M/N) \cong L/M.$$

Secondly, if M_1, M_2 are submodules of M, then

$$(M_1 + M_2)/M_1 \cong M_2/(M_1 \cap M_2).$$

Proof. Define

$$\begin{aligned} \theta : L/N &\to L/M \\ x + N &\mapsto x + M. \end{aligned}$$

Now if we act A on θ, we obtain that

$$\theta(a(x+N)) = \theta(ax+N) = ax+M = a\theta(x+M).$$

Now we want to show that

$$\ker(\theta) = M/N.$$

Firstly, we show that $\ker(\theta) \subseteq M/N$, then we show that $M/N \subseteq \ker(\theta)$. Assume that $x+N \in \ker(\theta)$ and $x \in L$.
To show: $x \in M$.
Then

$$0+N = \theta(x+N) = x+M.$$

Since $N \subseteq M$, we have $x \in M$. Now we show that $M/N \subseteq \ker(\theta)$. Assume that

$$x+N \in M/N \quad \text{ where } x \in M.$$

Then

$$\theta(x+N) = x+M = 0+M.$$

Hence, $\ker(\theta) = M/N$. For the second part of proposition, we consider the following sequence of maps

$$\begin{aligned} f : M_2 &\xrightarrow{\iota} M_1 + M_2 \xrightarrow{\pi} (M_1+M_2)/M_1, \\ m_2 &\mapsto 0 + m_2 \mapsto m_2 + M_1 \end{aligned}$$

where ι is the inclusion map and π is the projection map. Now we will show that this map is indeed surjective. Assume

$$(m_1+m_2)+M_1 \in (M_1+M_2)/M_1, \quad \text{ where } m_1 \in M_1 \text{ and } m_2 \in M_2.$$

Then

$$(m_1+m_2)+M_1 = m_2+M_1.$$

Hence, the map f is surjective. Now we will show that

$$\ker(f) = M_1 \cap M_2.$$

But this is clear from the series of decompositions of maps. □

Let $\mathfrak{a}$ be an ideal of A, and let M be an A-module. Define the **product**

$$\mathfrak{a}M = \left\{ \sum_{i \in I} a_i x_i \mid a_i \in \mathfrak{a} \text{ and } x_i \in M \right\}.$$

It is clear that $\mathfrak{a}M \subseteq M$ and if $a \in A$ and $x \in \mathfrak{a}M$, then $a \cdot x \in \mathfrak{a}M$. Hence, $\mathfrak{a}M$ is a A-submodule of M.
Let N, P be submodules of M. Define

$$(N : P) = \{a \in A \mid aP \subseteq N\}.$$

Since N is an A-module, $(N : P) \subseteq A$ is an ideal of A. Now if we set $N = (0)$, then

$$(0 : P) = \{a \in A \mid aM = 0\} := \mathrm{Ann}(M),$$

we call $\mathrm{Ann}(M)$ the set of annihilator of M.

Remark 2.8. Let $\mathfrak{a} \subseteq \mathrm{Ann}(M)$ be an ideal of A. Then an A-module M can become an $A/\mathfrak{a}$-module via

$$\overline{x} \cdot m := (x + \mathfrak{a})m = x \cdot m.$$

Let M be an A-module. If $\mathrm{Ann}(M) = 0$, then M is called **faithful**. If $\mathrm{Ann}(M) = \mathfrak{a}$, then M is faithful as $A/\mathfrak{a}$-module.

Proposition 2.9. *Let M, N be A-modules. Then*

$$\begin{aligned} \mathrm{Ann}(M + N) &= \mathrm{Ann}(M) \cap \mathrm{Ann}(N) \\ (N : P) &= \mathrm{Ann}((N + P)/N). \end{aligned}$$

Proof. Let $a \in \mathrm{Ann}(M + N)$. Then

$$a \cdot (m + n) = a \cdot m + a \cdot n = 0 \quad \text{for all } m \in M \text{ and } n \in N.$$

So

$$a \cdot m = 0 \quad \text{and} \quad a \cdot n = 0$$

therefore $a \in \mathrm{Ann}(M) \cap \mathrm{Ann}(N)$. Assume $a \in \mathrm{Ann}(M) \cap \mathrm{Ann}(N)$. Then $a \in \mathrm{Ann}(M)$ and $a \in \mathrm{Ann}(N)$. So

$$a \cdot (m + n) = 0.$$

Assume $a \in (N : P)$. Then $aP \subseteq N$. To show

$$a(n + p + N) = 0 \text{ for } a \in A \text{ and } n + p + N \in (N + P)/N.$$

Since

$$an + ap + N = an + N = 0 + N,$$

so $x = n + p + N \in \mathrm{Ann}(N + P)/N$. Assume $n + p + N \in \mathrm{Ann}(N + P)/N$. Then

$$0 + N = a(n + p + N) = p + N,$$

hence, $p \in N$. □

The submodule generated by x is defined as

$$(x) := Ax = \{ax \mid a \in A\}.$$

If

$$M = \sum_{i \in I} Ax_i,$$

then $\{x_1, \ldots, x_n\}$ is the set of **generators** of M. If the set of **generators** is finite, then M is said to be **finitely generated**.

2.2 Direct sum and product

Let M, N be A-modules. Define the **direct sum** to be

$$M \bigoplus N = \{(x, y) \mid x \in M, y \in N\},$$

where the addition and scalar multiplication is defined as

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2),$$
$$a(x, y) = (ax, ay)$$

Let $(M_i)_{i \in I}$ be a set of A-modules. Define the direct sum to be

$$M = \bigoplus_{i \in I} M_i = \{(x_i)_{i \in I} \text{ such that} x_i \in M_i \text{ for } i \in I\},$$

where almost all x_i are 0. If the restriction on the number of non-zero x's is dropped, then the direct sum become a **direct product**

$$M = \bigoplus_{i \in I} M_i = \prod_{i=1}^{n} M_i.$$

Remark 2.10. If the index set I is finite, then the direct sum and the direct product are the same.

Let

$$A = \prod_{i=1}^{n} A_i = \{(a_1, \ldots, a_n) \mid x_i \in A_i\}.$$

Let

$$b_i = (0, \ldots, 0, a_i, 0, \ldots, 0).$$

Then $Ab_i = (b_i)$ is an ideal of A. Then

$$A = (b_1) \oplus (b_2) \oplus \cdots \oplus (b_n).$$

Conversely, let

$$A = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n$$

of A as a direct sum of ideals. Define the A-submodule

$$\mathfrak{b}_i = \bigoplus_{j \neq i} \mathfrak{a}_j.$$

Then there is a map

$$\begin{gathered} \iota : \mathfrak{b}_i \to A \\ (a_1, \ldots, a_{j-1}, a_{j+1}, \ldots, a_n) \mapsto (a_1, \ldots, a_{j-1}, 0, a_{j+1}, \ldots, a_n). \end{gathered}$$

This map is clearly a A-module homomorphism. It is an isomoprhism onto the image. Hence, we can identify each of the A-module $\mathfrak{b}_i$ with a submodule in A. Now we show that $\mathfrak{b}_i \cong A/\mathfrak{a}_i$ is an isomorphism of modules. Consider the following

$$f : \mathfrak{b}_i \to A \to A/\mathfrak{a}_i.$$

The kernel of this map is $\mathfrak{a}_i \cap \mathfrak{b}_i$. But $\mathfrak{a}_i \cap \mathfrak{b}_i = \{0\}$. Hence, f is injective. Moreover, f is also surjective. Since composition of module homomorphisms is a module homomorphism. The identity(?????) element e_i of $\mathfrak{a}_i$ is an idempotent(????) and $\mathfrak{a}_i = (e_i)$.

2.3 Finitely generated modules

Let M be a A-module. Then M is **finitely generated** if there exists a generating set $\{m_1, \ldots, m_n\}$ such that for $x \in M$, there exists $a_1, \ldots, a_n$ such that

$$x = a_1 m_1 + a_2 m_2 + \cdots + a_n m_n.$$

A **free** A module M is

$$M = \bigoplus_{i \in I} M_i, \qquad \text{where } M_i \cong A,$$

where I can be an infinite set A **finitely generated** free A-module M is

$$M \cong \bigoplus_{i=1}^{n} A.$$

Proposition 2.11. *Let M be an A-module. Then*

M is finitely generated A module $\iff$ $M \cong A^n/N$ for some integer $n > 0$.

Proof. Assume M is a finitely generated module. Then there exists $\{m_1, \dots, m_n\}$ and $a_1, \dots, a_n$ such that if $x \in M$, then

$$x = a_1 m_1 + a_2 m_2 \cdots + a_n m_n.$$

Let

$$e_i = (0, \dots, 0, 1, \dots, 0)$$

be the i-th component of A^n. Then

$$\begin{aligned} f : A^n &\to M \\ e_i &\mapsto m_i, \end{aligned}$$

is surjective. But f is not nesscessary injective. So $\ker(f) \neq \{0\}$ and we decent to an isomomorphism

$$\overline{f} : A^n/\ker(f) \to M.$$

Hence, $A^n/\ker(f) \cong M$. Conversely, assume $M \cong A^n/N$ for some integer $n \in \mathbb{Z}_{>0}$ and some ideal N. Define the generating set of A^n/N to be

$$G = \{e_1 + N, e_2 + N, \dots, e_n + N\}.$$

Then any element of A^n/N can be expressed in terms of the elements of G. Hence, we are done by the isomophirsm. □

The following is a general version of Cayley-Hamilton theorem for modules.

Theorem 2.12. *(Carmer's rule) Let A be an $n \times n$ matrix with entries in a field $\mathbb{F}$. Then*

$$A \operatorname{adj}(A) = \operatorname{adj}(A) A = \det(A) I,$$

where $\operatorname{adj}(A)$ is the adjoint matrix and I is the identity matrix.

Proposition 2.13. *(Cayley-Hamilton) Let M be a finitely generated A-module and let $\mathfrak{a}$ be an ideal of A. Moreover, let*

$$\phi : M \to M \quad \textit{such that} \quad \phi(M) \subseteq \mathfrak{a}M (What is this condition),$$

where ϕ is a A-module homomorphism. Then ϕ satisfies

$$\phi^n + a_1 \phi^{n-1} + \cdots + a_n = 0,$$

where the a_i are in $\mathfrak{a}$.

Proof. Let $x_1, \dots, x_n$ be the set of generators of M. To obtain the result, we want see the action of ϕ on each of the generators x_i,

$$\phi(x_i) = \sum_{j=1}^{n} a_{ij} x_j \implies \sum_{j=1}^{n} (\delta_{ij}\phi - a_{ij}) x_j = 0, \quad \text{for } i \in \{1, \dots, n\}.$$

where δ_{ij} is the Kronecker delta. Let $n = 3$, we form the matrix of the system of linear equations

$$\begin{pmatrix} \phi - a_{11} & -a_{12} & -a_{13} \\ -a_{21} & \phi - a_{22} & -a_{23} \\ -a_{31} & -a_{32} & \phi - a_{33} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Let

$$A = \begin{pmatrix} \phi - a_{11} & -a_{12} & -a_{13} \\ -a_{21} & \phi - a_{22} & -a_{23} \\ -a_{31} & -a_{32} & \phi - a_{33} \end{pmatrix}$$

Then

$$\operatorname{adj}(A) = \begin{pmatrix} ??? \end{pmatrix}.$$

Applying Carmer's rule

$$\operatorname{adj}(A)A = \begin{pmatrix} \det(A) & 0 & 0 \\ 0 & \det(A) & 0 \\ 0 & 0 & \det(A) \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Hence,

$$\det(A) x_i = 0, \quad \text{for } i \in \{1, \dots, n\}$$

Then expanding the determinant of A, we will obtain the equation as stated. □

Corollary 2.14. *Let M be a finitely generated A-module and let $\mathfrak{a}$ be an ideal of A such that $\mathfrak{a}M = M$. Then*

$$\textit{there exists } x \equiv 1 (\textit{mod } \mathfrak{a}) \textit{ such that } xM = 0.$$

Proof. Let $\phi = \mathrm{Id}$. Then

$$x := 1 + a_1 + \cdots + a_n \equiv 1 (\mathrm{mod}\ \mathfrak{a}).$$

By Proposition 2.12, $xM = 0$. □

The following proposition is the well-known theorem by Nakayama.

Proposition 2.15. *(Nakayama's lemma) Let M be a finitely generated A-module and $\mathfrak{a} \subseteq \mathfrak{R}$ be an ideal contained in the Jacobson radical. Then $\mathfrak{a}M = M$ implies $M = 0$.*

Proof. From Corollary 2.14, there exists $x \equiv 1 \mod \mathfrak{R}$ such that

$$xM = 0.$$

Recall from Proposition 2.3, if $\mathfrak{R}$ is a Jacobson radical, then

$$x \in \mathfrak{R} \iff 1 - xy \text{ is a unit in } A \text{ for all } y \in A.$$

Since $x \equiv 1 \mod \mathfrak{R}$, we have $x - 1 \in \mathfrak{R}$. Choose $y = -1$. Then $1 - x(-1) = x$ is a unit. So

$$M = x^{-1}xM = 0.$$

□

Apperently, there is another proof of the Nakayama's lemma. But why is it interesting(???).

Proof. Let $M \neq 0$. Since M is finitely generated, there exists a minimal set of genreators of M i.e.,

$$M = A - \text{span}\{u_1, \ldots, u_n\}.$$

Since $\mathfrak{a}M = M$, $u_n \in \mathfrak{a}M$. Hence, there exists $a_1, \ldots, a_n$ such that

$$u_n = a_1u_1 + \cdots + a_nu_n, \qquad \text{where } a_i \in \mathfrak{a}. \tag{2.1}$$

Now rearranging (2.1) gives

$$(1 - a_n)u_n = a_1u_1 + \cdots + a_{n-1}u_{n-1}.$$

Since $a_i \in \mathfrak{a}$ and $\mathfrak{a} \subseteq \mathfrak{R}$, $a_n \in \mathfrak{R}$. Again by Proposition 2.3, we can choose $y = 1$ such that $1 - a_n$ is a unit. Hence, u_n is generated by $\{u_1, \ldots, u_{n-1}\}$. This is a contradiction because we have choosen a minimal generating set at the start. □

The following maybe some important proposition we might need later on(???).

Corollary 2.16. *Let M be a finitely generated A-module, N a submodule of M and $\mathfrak{a} \subseteq \mathfrak{R}$ an ideal in the Jacobson radical. Then*

$$\textit{if} \quad M = \mathfrak{a}M + N, \ \textit{then} \quad M = N.$$

Proof. Applying Nakayama lemma on the quotient

$$M/N = \{m + N \mid m \in M\}.$$

To show:

$$\mathfrak{a}(M/N) = M/N,$$

firstly, we construct the following isomorphism

$$f : \mathfrak{a}M + N \to \mathfrak{a}(M/N)$$
$$(a_1m_1 + a_2m_2 + \cdots + a_nm_n + n) \mapsto a_1(m_1 + N) + a_2(m_2 + N) + \cdots + a_n(m_n + N).$$

It will be remained to be in the appendix to show that $\ker(f) = N$. Hence, we have the following isomorphism

$$\frac{\mathfrak{a}M + N}{N} \cong \mathfrak{a}\left(\frac{M}{N}\right).$$

Since $\mathfrak{a}M + N = M$, the result follows. □

The following proposition is about local rings. Let A be a local ringt. Then

A has a unique maximal ideal with $k = A/\mathfrak{m}$ being its residue field.

Let M be a finitely generated A-module. Then $M/\mathfrak{m}M$ is a annihilated by $\mathfrak{m}$. Hence, it is a $A/\mathfrak{m}$ module which is a k vector space. So $M/\mathfrak{m}$ is a finite dimension vector space over k. Now we investigate a little bit into the vector space structure of $M/\mathfrak{m}M$.

Proposition 2.17. *Let*

$$\pi : M \to M/\mathfrak{m}M$$
$$m \mapsto m + \mathfrak{m}M$$

and let $\{x_i \mid i \in \{1, \ldots, n\}\}$ be the set of elements in M so that

$$\pi(x_i) \text{ forms a basis of } M/\mathfrak{m}M.$$

Proof. Let N be the submodule of M generated by x_i. Consider the following series of maps

$$f : N \xrightarrow{\iota} M \xrightarrow{\pi} M/\mathfrak{m}M$$
$$n \mapsto n \mapsto n + \mathfrak{m}M.$$

Then the above map is surjective, because the elements x_i forms a basis of $M/\mathfrak{m}M$. Indeed, if $m + \mathfrak{m}M$, then there exists $k_i \in A/\mathfrak{m}$ and $x_i \in N$ such that

$$\begin{aligned} m + \mathfrak{m}M &= k_1 f(x_1) + k_2 f(x_2) + \cdots + k_N f(x_N) \\ &= f(k_1 x_1) + f(k_2 x_2) + \cdots + f(k_N x_N), \end{aligned}$$

where the second equality is due to the fact that any A-module homomomrphism(????A-module or A/m?) is also an $A/\mathfrak{m}$ A-module homomorphism. Next we would like to show that

$$N = M.$$

Since A is a local ring, the Jacobson radical is just $\mathfrak{a}$. Hence, by corollary 2.16, we only need to show that

$$M + \mathfrak{m}M + N.$$

Now it is clear that

$$N + \mathfrak{m}M \subseteq M.$$

Conversely, since the map f is surjective, there exists $n \in N$ such that

$$f(n) = x + \mathfrak{m}M,$$

for $x + \mathfrak{m}M \in M/\mathfrak{m}M$. □

3 Exact sequences

A sequence of A-modules and A-homomorphisms

$$\cdots \to M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \to \cdots$$

is said to be **exact** if

$$\mathrm{Im}(f_i) = \mathrm{Ker}(f).$$

The sequence is **exact** if it is exact at each M_i. In particular:

$$0 \to M' \xrightarrow{f} M \text{ is exact } \iff f \text{ is injective ;} \tag{3.1}$$

$$M \xrightarrow{g} M'' \to 0 \text{ is exact } \iff g \text{ is surjective ;} \tag{3.2}$$

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0 \text{ is exact } \iff f \text{ is injective, } g \text{ is surjective} \tag{3.3}$$

The map g in the last statement induces and isomorphism

$$g' : M/f(M') \to M''$$

via the first isomorphism theorem. A sequence

$$0 \to N_i \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} N_{i+1} \to 0$$

is called a **short exact sequences**: if

$$N_i = \mathrm{Im}(f_i) = \ker(f_{i+1}).$$

Every long exact sequence can be split up into set of short exact sequence in this fashion.

Proposition 3.1. *Let*

$$M' \xrightarrow{u} M \xrightarrow{v} 0 \tag{3.4}$$

be a sequence of A-module and homomorphism. Then the sequence (3.4) *is exact if and only if the sequence*

$$0 \to \mathrm{Hom}(M'', N) \xrightarrow{\overline{v}} \mathrm{Hom}(M, N) \xrightarrow{\overline{u}} \mathrm{Hom}(M', N)$$

is exact.

Proof. NEED TO BE DONE.(!!!!!!!!!!!!!!!!!) □

Proposition 3.2. *Let*

$$0 \to N' \xrightarrow{u} N \xrightarrow{v} N'' \tag{3.5}$$

be a sequence of A-modules and homomomrphisms. Then the sequence (3.5) *is exact if and only if*

$$0 \to \mathrm{Hom}(M, N') \xrightarrow{\overline{u}} \mathrm{Hom}(M, N) \xrightarrow{\overline{v}} \mathrm{Hom}(M, N'')$$

is exact.

Proof. NEED TO BE DONE.(!!!!!!!!!!!!!!!) □

Proposition 3.3 (snake lemma)**.** *Let*

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "u"] \arrow[d, "f'"] & M \arrow[r, "v"] \arrow[d, "f"] & M'' \arrow[r] \arrow[d, "f''"] & 0 \\
0 \arrow[r] & N' \arrow[r, "u'"] & N \arrow[r, "v'"] & N'' \arrow[r] & 0
\end{tikzcd}$$

be a commutative diagram of A-modules and homomorphisms. Then the following diagram

$$\begin{tikzcd}
0 \arrow[r] & \ker(f') \arrow[r, "\overline{u}"] \arrow[d, "\iota'"] & \ker(f) \arrow[r, "\overline{v}"] \arrow[d, "\iota"] & \ker(f'') \arrow[d, "\iota''"] & \\
0 \arrow[r] & M' \arrow[r, "u"] \arrow[d, "f'"] & M \arrow[r, "v"] \arrow[d, "f"] & M'' \arrow[r] \arrow[d, "f''"] & 0 \\
0 \arrow[r] & N' \arrow[r, "u'"] \arrow[d, "\pi'"] & N \arrow[r, "v'"] \arrow[d, "\pi"] & N'' \arrow[r] \arrow[d, "\pi''"] & 0 \\
 & \mathrm{Coker}(f') \arrow[r, "\overline{u}"] & \mathrm{Coker}(f) \arrow[r, "\overline{v}"] & \mathrm{Coker}(f'') \arrow[r] & 0
\end{tikzcd}$$

where $\overline{u}, \overline{v}$ are restrictions of u, v and $\overline{u}', \overline{v}'$ are induced by u', v'

Proof. The proof is diagram chasing and needs to be done(!!!!!!!!). □

Remark 3.4. The homomorphism d is normally called the **boundary homomorphism**.

Let C be a class of A-modules and let λ be a function on C with values in $\mathbb{Z}$. The function λ is **additive** if, for each short exact sequence

$$0 \to M' \to M \to M'' \to 0$$

where $M, M', M'' \in C$, then

$$\lambda(M') - \lambda(M) + \lambda(M'') = 0.$$

Example 3.1. *Let $A = k$ be a field and let C be the class of all finite-dimensional k-vector spaces V. Then the function*

$$\begin{aligned} \lambda : C &\to \mathbb{Z} \\ V &\mapsto \dim(V) \end{aligned}$$

is an additive function on C. The proof of this is the fact that every short exact sequence of finite-dimensional k-vector spaces splits i.e., if the following sequence

$$0 \to V' \to V \to V'' \to 0$$

is exact, then we have

$$V \cong V'' \oplus V'.$$

Hence

$$\dim(V) = \dim(V'') + \dim(V') \implies \dim(V'') + \dim(V') - \dim(V) = 0.$$

Proposition 3.5. *Let*

$$0 \to M_0 \to M_1 \to \cdots \to M_n \to 0$$

be an exact sequence of A-modules with all the modules M_i and kernels of all the homomorphisms belong to C. Then if λ is a additive function on C, we have

$$\sum_{i=0}^{n} (-1)^i \lambda(M_i) = 0.$$

Proof. Using the method we described at the start of this section, we splite the long exact sequence into short exact sequences

$$0 \to N_i \to M_i \to N_{i+1} \to 0$$

with $N_i = \ker(f_{i+1}) = \mathrm{Im}(f_i)$. Since λ is additive function, we obtain

$$\lambda(M_i) = \lambda(N_i) + \lambda(N_{i+1}).$$

Hence,

$$\begin{aligned}\sum_{i=0}^{n} (-1)^i \lambda(M_i) &= \lambda(N_0) + \lambda(N_1) - (\lambda(N_1) + \lambda(N_2)) + \cdots + (-1)^n (\lambda(N_n) + \lambda(N_{n+1})) \\ &= 0.\end{aligned}$$

Note that $N_0 = N_{n+1} = 0$. □

4 Tensor product of Modules

Let M, N, P be three A-modules. A map

$$f : M \times N \to P$$

is bilinear if for $x \in M$ the mapping

$$\begin{aligned} g : N &\to P \\ y &\mapsto f(x, y) \end{aligned}$$

is A-linear and also for each $y \in N$ the mapping

$$\begin{aligned} g' : M &\to P \\ x &\mapsto f(x, y) \end{aligned}$$

Constructing the tensor product of two A-modules M and N by using the universal property of tensor product i.e.,

Proposition 4.1. *Let M, N be A-modules. Then there exists a pair (T, g) with T being an A-module and g an A-bilinear mapping*

$$g : M \times N \to T,$$

such that if P is an A-module, then given any A-module homomorphism, there exists a unique A-linear map f' such that the following diagram communtes

$$\begin{tikzcd}
M \times N \arrow[rr, "f"] \arrow[dr, "\phi"'] & & P \\
& T \arrow[ur, "\exists! \overline{f}"] &
\end{tikzcd} ,$$

Moreover, if (T, g) and (T', g') are two pairs with the same univerisal property, then there exists a unqiue $j : T \to T'$ such that $j \circ g = g'$.

Proof. The uniqueness part of the proof is rather clear with P replaced with T' and vice versa. It is important however to forcus on the construction of the tensor product. Define the free module

$$C = \bigoplus_{i \in M \times N} A_i,$$

where $A_i = A\text{-}\operatorname{span}\{(m_i, n_j)\}$ where $m_i \in M$ and $n_j \in N$. So C consisting of formal linear combinations of elements of $M \times N$ with coefficients in A i.e., if $c \in C$, then

$$c = \sum_{i \in I, j \in J} a_i \cdot (x_i, y_j) \quad \text{where } a_i \in A, x_i \in M, y_j \in N.$$

Let D be the submodule of C generated by the following elements

$$\begin{gathered} (x + x', y) - (x, y) - (x', y) \\ (x, y + y') - (x, y) - (x, y) \\ (ax, y) - a \cdot (x, y) \\ (x, ay) - a \cdot (x, y) \end{gathered}$$

□

5 Affine algebraic varieties

Let K be an algebraically closed field of any charactreistic. Define

$$A = A_n = K[t_1, \dots, t_n],$$

where $t_1, \dots, t_n$ are independent indetrminates over K. The elements of A are polynomials in the t_i with coefficients in K. Define the **affine space** to be

$$K^n = K \times \dots K.$$

If $f \in A$ and $x = (x_1, \dots, x_n) \in K^n$, then

$$f(x) = f(x_1, \dots, x_n) \in K.$$

In particular, define

$$t_i(x) = x_i, \text{ so that } t_i \text{ is the i-th coordinate function on } K^n.$$

Let $S \subseteq A$. An **algebraic set** of S in K^n is

$$V(S) = \{x \in K^n \mid f(x) = 0 \text{ for all } f \in S\},$$

in english: $V(S)$ is the set of all points in K^n for which all the polynoimals in S vanish.
We list the properties of V in the following proposition

Proposition 5.1. *Let S, S_1, S_2, S_i be subsets of A. Then*

1. *$V(S_1) \cup V(S_2) = V(S_1 S_2)$, where $S_1 S_2$ is the set of products of $f_1 f_2$ with $f_1 \in S_1$ and $f_2 \in S_2$.*
2. *$\bigcap_{i \in J} V(S_i) = V(\bigcup_{i \in J} S_i)$ for any index set J.*
3. *$V(A) = \emptyset, \quad V(\emptyset) = K^n$.*
4. *$S_1 \subseteq S_2 \implies V(S_1) \subseteq V(S_2)$.*
5. *Let $\mathfrak{a}$ be the ideal in A generated by S. Then $V(S) = V(\mathfrak{a})$*

Now we list the set of axioms that characterize closed sets. Let $\mathcal{P}$ be a set of closed set of a topological space X. Then

1. If $I = \{P_1, \dots, P_n, \dots\} \subseteq \mathcal{P}$, then $\bigcap_{i \in I} P_i \in \mathcal{P}$.
2. If $\{P_1, \dots, P_n\} \subseteq \mathcal{P}$ is a finite subset, then $\bigcup_{i=1}^n P_i \in \mathcal{P}$.

3. $\emptyset \in P$

4. $X \in P$.

Since the sets $V(S)$ with $S \subseteq A$ satisfy the axioms for the closed sets, we can induce a topology on K^n formed by the closed sets $V(S)$.

Definition. The open sets of Zariski topology are

$$O = \{K^n \backslash V(S) \mid S \subseteq K[x_1, \ldots, x_n]\}$$

Example 5.1. *The non-empty open sets are very large. Let $n = 1$ and take $K = \mathbb{C}$. Then we are looking at an affine line. The open sets are the complements of finite subsets of $\mathbb{C}$. In particuar any two non-empty open sets in the affine line always intersect.*

Note that in proposition 4.1 (5), the operation V take ideal in A sent to subsets of K^n. Now we think about how to send subsets of K^n to ideals in A. Let $E \subset K^n$ and define

$$I(E) = \{f \in A \mid f(x) = 0, \text{ for all } x \in E\}.$$

It is clear that $I(E) \subseteq A$ is an ideal of A. Therefore, the operation I takes subsets of K^n to ideals in A. Now we need to check that

Lemma 5.2. *If $E \subseteq K^n$, then*

$$V(I(E)) = \overline{E}.$$

Proof. □

Now we recall the strong version of Hilbert Nullstellensatz

Theorem 5.3 (Hilbert Nulstellensatz)**.** *Let k be an algebraically closed field, let A denote the polynomial ring $k[t_1, \ldots, t_n]$ and let $\mathfrak{a}$ be an ideal in A. Define*

$$V(\mathfrak{a}) = \{x = (x_1, \cdots, x_n) \in k^n \mid f(x) = 0 \text{ for all } f \in \mathfrak{a}\}.$$

Then

$$I(V(\mathfrak{a})) = r(\mathfrak{a}),$$

where $r(\mathfrak{a})$ is the radical of $\mathfrak{a}$.

Proof. □

Now there are several correspondence, firstly the operator I sends algebraic set to ideal and V sends ideal to algebraic set

$$\begin{gathered}\big\{\text{algebraic sets}\big\} \iff \big\{\text{ideals of } k^n\big\}\\ S \mapsto I(S)\\ V(\mathfrak{a}) \mapsfrom \mathfrak{a}\end{gathered}$$

Now by Hilbert Nulstellensatz, there is a bijection(order reversing) between the following

$$\begin{gathered}\big\{\text{algebraic sets}\big\} \iff \big\{\text{radical ideals}\big\}\\ S \mapsto I(S)\\ V(\mathfrak{a}) \mapsfrom \mathfrak{a}\end{gathered}$$

Some other important properties about the operator V and I, we will list them below

Proposition 5.4. *1. If $T_1 \subseteq T_2$ are subsets of A, then $V(T_2) \subseteq V(T_1)$.*

2. If $Y_1 \subseteq Y_2$ are subsets of A^n, then $I(Y_2) \subseteq I(Y_1)$.

3. Let Y_1, Y_2 be subsets of A^n, then

$$I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2)$$

Let X be a topological space, and let Y be a nonempty subset of X. Then Y is **irreducible** if it cannot be expressed as the union

$$Y = Y_1 \cup Y_2$$

of two proper subsets, where Y_1, Y_2 are closed in Y. Empty set is not irreducible.

Example 5.2. *Let A^1 be the affine line. Then A^1 is irreducible and the closed subsets of A^1 are finite(??????????????). But A^1 is infinite, because every algebraically closed field is infinite. Indeed, if k is a finite algebraically closed set with $a_1, \ldots, a_n$, then the polynoimal*

$$1 + \prod_{i=1}^{n}(x - a_i) = 0,$$

has no roots in k. Hence, contradiction, the result follows. Since union of two finite set is still finite. The affine line A^1 is irreducible.

Example 5.3 (Open subsets of irreducible space are big)**.** *Any nonempty open subset of an irreducible space is irreducible and dense.(THIS CAN BE PROVED)*

Example 5.4. *If Y is an irreducible subset of X, then its closure $\overline{Y}$ in X is irreducible.*

Definition (affine algebraic variety)**.** Let X be a subset of A^n. Then X is an affine algebraic variety if

$$X \text{ is } \begin{cases} \textbf{closed in } A^n, \\ \textbf{irreducible}, \end{cases}$$

where the topology on A^n is the Zariski topology. An open subset of an affine variety is called **quasi-affine variety**. In here, the word affine means we are looking at the subsets of the affine space A^n.

Now we will use Hilbert's Nullstellensatz, to conclude that there is an order reversing correspondence between irreducible algebraic set and prime ideals.

Theorem 5.5. *There is an one to one* ***inclusion reversing*** *correspondence given by*

$$\big\{\textit{Irreducible algebraic set}\big\} \iff \big\{\textit{prime ideals}\big\}$$
$$S \mapsto I(S)$$
$$V(\mathfrak{p}) \mapsfrom \mathfrak{p}$$

Example 5.5. *It is now easy to show that A^n is irreducible. Using the above inclusion reversing correspondence, the affine space A^n correspondence to the ideal $I(A^n) = (0)$, which is an prime ideal. Hence, A^n is irreducible.*

Example 5.6. *Let f be an irreducible polynomial in $A = k[x, y]$. Since A is a unique factorization domain, f generates a prime ideal in A. Using the correspondence between the irreducible algebraic sets and the prime ideals, we see that*

$$Y = V(f) \quad \textit{is irreducible.}$$

The irreducible set Y is called the ***affine curve*** *defined by the equation $f(x, y) = 0$. If f has degree d, then we say that Y is a curve of degree d.*

Example 5.7. *In a more general setting, let f be an irreducible polynomial in $A = k[x_1, \ldots, x_n]$, then the set*

$$Y = V(f) \text{ is an affine variety}$$

and we call it a ***surface*** *if $n = 3$, or a* ***hypersurface*** *if $n \geq 3$.*

The next lemma which is quite important I think(which is the example 1.4.5 in Hartshorne's book).

Lemma 5.6. *A maximal ideal $\mathfrak{m}$ of $A = k[x_1, \ldots, x_n]$ is given by*

$$\mathfrak{m} = (x - a_1, \ldots, x_n - a_n) \quad \text{for some } a_1, \ldots, a_n \in k.$$

Proof. Notice that the smallest irreducible closed subset of A^n is just a point $P = (a_1, \ldots, a_n)$. Now the vanishing set

$$V(\mathfrak{m}) = \{(a_1, \ldots, a_n)\},$$

this means that the polynomials in the maximal ideal $\mathfrak{m}$ must contain linear factors $x_1 - a_1, \ldots, x_n - a_n$. Hence,

$$\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n) \quad \text{for some} a_1, \ldots, a_n \in k.$$

□

Definition. If $Y \subseteq A^n$ is an affine algebraic set, then define the **affine coordinate ring** to be

$$A[Y] := K[x_1, \ldots, x_n]/I(Y),$$

where $I(Y)$ is the operator I applied on the set Y.

Example 5.8. *Now if Y is an affine variety, then Y is closed and irreducible. So $I(Y)$ is a prime ideal. Therefore,*

$$A[Y] \text{ is an integral domain and is a finitely generated } K\text{-algebra.}$$

Conversely, any finitely generated K-algebra B which is a domain is the affine coordinate ring of some affine variety. Let B be a finitely generated K-algebra. Then B cane be written as a quotient

$$B \cong K[x_1, \ldots, x_n]/\mathfrak{a}, \text{ by some prime ideal} \mathfrak{a}.$$

Then $Y = Z(\mathfrak{a})$ is an irreducible closed set.

6 Noetherian rings and Dedekind ring

Firstly, let us consider the Noetherian modules

Theorem 6.1. *Let A be a ring and M be a A-module. The following are equivalent.*

1. *Every submodules is finitely generated.*
2. *Every nonempty collection of submodules of M has a maximal element.*
3. *Every ascending chain of submodules of M is stationary.*

Definition. An A-module M is called **Noetherian** if it satisfies the equivalent conditions.

Example 6.1. *Let R be a principal ideal domain. Then R is a module over R. So the modules of R are just left ideals and since every ideal is generated by one element, every module is finitely generated. So R is Noetherian.*

Definition. A ring A is called **Noetherian** if considered as A-module it is a Noetherian A-module.

Lemma 6.2. *Let E, E', E'' be A-modules and*

$$0 \to E \to E' \to E'' \to 0$$

is a short exact sequence. Then E' is Noetherian if and only if E'' and E are Noetherian.

Lemma 6.3. *If E_i for $i \in \{1, \ldots, n\}$ are Noetherian A-modules, then $E_1 \times \cdots \times E_n$ is a Noetherian A-module.*

Proof. Assume E_i for $i \in \{1, \ldots, n\}$ are Noetherian A-modules.
To show: $E_1 \times \cdots \times E_n$ are Noetherian A-modules.
To show: If E_1, E_2 are Noetherian, then $E_1 \times E_2$ are Noetherian.
Assume E_1, E_2 are Noetherain.
To show $E_1 \times E_2$ are Noetherain.
Since E_1, E_2 are Noetherain and

$$0 \to E_1 \to E_1 \times E_2 \to E_2 \to 0$$

is a short exact sequence, $E_1 \times E_2$ is Noetherian. □

The following theorem is an important one for algebraic geometry

Theorem 6.4 (Hilbert's basis Theorem)**.** *If A is Noetherian, then the polynomial ring $A[x]$ is Noetherian.*

Proof. FILL In the proof!! □

By induction, we can simply extend this into n-varaible cases.

Corollary 6.5. *If A is Noetherian so is $A[x_1, \dots, x_n]$.*

The above thereom tells us that if A is Noetherian, then $A[x_1, \dots, x_n]$ the polynoimal ring is also Noetherian. Now we notice that if A is a field(algebraically closed or not), then $A[x_1, \dots, x_n]$ is Notherian.

Theorem 6.6. *Let A be a Notherian ring, and E be a finitely generated A-module. Then E is Notherian.*

Proof. Assume: A is Notherian and E is finitely generated.
To show: E is Notherian.
Since E is finitely generated, there exists a surjective homomorphism

$$\varphi : A^n \to E.$$

Hence,

$$0 \to \ker(\varphi) \to A^n \to E \to 0$$

is a short exact sequence.
To show: E is Noetherian.
Since A is Noetherian and by lemma 11.3, A^n is Noetherian.
Since A^n is Noetherian and by lemma 11.2, E is Noetherian and $\ker(\varphi)$ is Noetherian. □

Let A be a integral domain, and let K be field of fractions of A. Then K is a A-module.

7 Noetherian topological space

Now we introduce the ideal of a topological space being Noetherian

Definition. Let X be a topolgical space. Then X is called **Noetherian** if it satisfies the **decending chain condition** i.e., for any sequence

$$Y_1 \supseteq Y_2 \supseteq \cdots$$

of closed subsets, then there is an integer r such that $Y_r = Y_{r+1} = \cdots$

Example 7.1. *For some reason, there are always nice examples in this subject. The affine space A^n is Noetherian topological space. If*

$$Y_1 \supseteq Y_2 \supseteq \cdots$$

is a decending chain of closed subsets. Then

$$I(Y_1) \subseteq I(Y_2) \subseteq \cdots$$

is an ascending chain of ideals in $A = K[x_1, \ldots, x_n]$. By Hilbert's basis theorem, we know that $A = K[x_1, \ldots, x_n]$ is a Noetherian ring. Hence, this chain is stational. But for each i, $Y_i = Z(I(Y_i))$ because Y_i is closed. So the chain Y_i is also stationary.

Proposition 7.1. *Let X be a Noetherian topological space and let Y be a subset of X. Then Y can be expressed as*

$$Y = Y_1 \cup \cdots \cup Y_r$$

*where Y_i are **irreducible closed** subsets of X. If we require that $Y_i \not\subseteq Y_j$ for $i \neq j$, then Y_i are uniquely determined.*

Corollary 7.2. *Every algebraic set in A^n can be expressed uniquely as a union of varieties.*

Proof. Since A^n is a Noetherian topological space and by proposition 6.1, every subset of A^n can be expressed as a union of irreducible closed sets uniquely. So the result follows. □

Now there is a further lemma that is important

Lemma 7.3. *Let X be a topological space. Then*

X is Noetherian $\iff$ its coordinate ring $K[x_1, \ldots, x_n]/I(X)$ is Noetherian ring

Proof. Where is the proof??????? □

Next we are going to define the Krull dimension of $K[x_1, \ldots, x_n]$.

Definition (Krull dimension)**.** Let X be a topological space. Define the **dimension** of X to be the

sup{length of a chian $Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_n$ of distinct irreducible closed subsets of X}.

Let X be a affine or quasi affine variety. Define

$$\dim(X) = \text{Krull dimension of } X.$$

Now we define the height of a prime ideal in the ring and the dimension of a ring A.

Definition. Let A be a ring. Then the **height** of a prime ideal $\mathfrak{p}$ is the supremum of all integers n such that there exists a chain

$$\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_n = \mathfrak{p},$$

i.e., the length of the longest chain that start with some prime ideal $\mathfrak{p}_0$ and end at the prime ideal $\mathfrak{p}$. The hegith of a prime ideal is denoted by $\mathrm{ht}(\mathfrak{p})$.

Definition. Let A be a ring. Define the dimension(Krull dimension) of A to be

$$\dim(A) = \sup_{\mathfrak{p} \in \mathrm{Spec}(A)} \{\mathrm{ht}(\mathfrak{p})\}$$