Math 516 Commutative Algebra
University Of Arizona Mathematics
Spring 2012

Lectured by Professor Yi Hu (yhu@math.arizona.edu)
Typeset by Alex Tao (taolapkei@math.arizona.edu)

Last Update: February 1, 2012

1 Rings and Ideals

Why rings?
Consider the curve

$$X = \{f(x, y) = 0\} \subset \mathbb{C}^2 \qquad \text{or some field } k$$

We want to understand the functions on this space, which are rings:
Topology: $C^0(X)$ ($C^0(U)$, $U^{\text{open}} \subset X$).
Differential Geometry: $C^\infty(C)$, ($C^\infty(U)$, $U \subset X$).
Complex Analysis: $C^{\text{an}}(U)$ (analytic functions) - holomorphic, meromorphic.
Algebraic Geometry: $k[X, Y]$ = {all polynomials}, rational functions.

Why ideals?

$$I = \{f(x, y)g \mid g \in k[X, Y]\} \subset k[X, Y]$$

These all vanish on X. i.e. they give zero function on X.
To get rid of this, we consider

$$k[X, Y]/I = \{g + I \mid g \in k[X, Y]\}$$

This also answers why we may need quotient rings.

Definition 1.1
A commutative ring A is a set with two binary operations $+, \cdot$ satisfying ...
We always assume that A has the identity 1, $0, 1 \in A$.
When $0 = 1$, we say $A = 0$, the zero ring.

Definition 1.2
Let A, B, be two rings. A ring homomorphism $f : A \to B$ is a map preserving $+, \cdot$, and $f(1_A) = 1_B$.

Example 1.3 (i) $f : \mathbb{Z} \to \mathbb{Z}$ by $n \mapsto 2n$ is not a ring homomorphism.

(ii) Does $f(1) = 1$ follow from $f(xy) = f(x)f(y)\ \forall x, y \in A$?
$f(x) = f(1)f(x), \forall x \in A$. Assume $f \not\equiv 0$, then

$$(f(1) - 1_B)f(x) = 0 \quad \forall x \in A$$

so they are both zero divisors.

(iii) A subring of a ring A is a subset B of A s.t. B is itself a ring under the binary operations of A, $1_A = 1_B \in B$ unless $B = 0$.

(iv) Ideal $\mathfrak{a} \subseteq A$ is a subring of A s.t. $\mathfrak{a}A \subseteq \mathfrak{a}$. It comes with a natural homomorphism:

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

Proposition 1.4

$$\begin{aligned} \{\text{ideals } \mathfrak{b} \supset \mathfrak{a} \subset A\} &\overset{1-1}{\leftrightarrow} \{\text{ideals } \overline{\mathfrak{b}} \in A/\mathfrak{a}\} \\ \phi^{-1}(\overline{\mathfrak{b}}) &\leftarrow \overline{\mathfrak{b}} \\ \mathfrak{b} &\to \overline{\mathfrak{b}} = \mathfrak{b} + \mathfrak{a} \in A/\mathfrak{a} \end{aligned}$$

Example 1.5
For any ring homomorphism $f : A \to B$,

(i) $f^{-1}(0) = \ker f$ and $\mathrm{Im} f$ are ideals.

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

(iii) An elemenet $x \in A$ is nilpotent if $x^n = 0$ for some $n > 0$. An element $x \in A$ is a unit if $\exists y \in A$ s.t. $xy = 1$.

(iv) $0 \neq x \in A$ is a zero divisor if $xy = 0$ for some $y \neq 0 \in A$.

(v) An integral domain is a ring without non-zero zero divisors.

(vi) A principal ideal of A is an ideal that has one generator, i.e. $a = (x) = xA$, for some $x \in A$.

(vii) x is a unit iff $(x) = (1) = A$.

Proposition 1.6
$A \neq 0$, TFAE:

(i) A is a field.

(ii) $0, (1)$ are the only ideals.

(iii) $\forall f : A \to B \neq 0$ is injective.

Proof
(iii) $\Longrightarrow$ (i):
Take a non-unit x in A, $(x) \neq A$. Then $\phi : A \to A/(x) \neq 0$ is injective.
$\ker \phi = (x) = 0$, hence $x = 0$, so A is a field. □

1.1 Prime Ideals and Maximal Ideals

Definition 1.7
An ideal $\mathfrak{m} \subset A$ is maximal if there is no ideal $\mathfrak{n}$ s.t. $\mathfrak{m} \subsetneq \mathfrak{n} \subsetneq A$.

Definition 1.8
An ideal $\mathfrak{p} \subset A$ is prime if $xy \in \mathfrak{p}$, then either $x \in$ *prideal* or $y \in \mathfrak{p}$.
e.g $p \in \mathbb{Z}$, $p \mid xy \implies p \mid x$ or $p \mid y$, $xy \in (p) \implies x \in (p)$ or $y \in (p)$.

Proposition 1.9

(i) $\mathfrak{p}$ is prime $\iff A/\mathfrak{p}$ is an ID.

(ii) $\mathfrak{m}$ is maximal $\iff A/\mathfrak{m}$ is a field.

Corollary 1.10
Every maximal ideal is a prime ideal.

Example 1.11
$A = \mathbb{Z}[x]$, $\mathfrak{p} = (x)$, $A/\mathfrak{p} = \mathbb{Z}$, $(x) \subset (x)+(2) \subseteq \mathbb{Z}[x]$. $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$, an ID and $\mathbb{Z}[x]/(x,2) \cong \mathbb{Z}/2\mathbb{Z}$, a field.

Example 1.12
$f : A \to B$, $\mathfrak{q}$ prime of B, then $f^{-1}(\mathfrak{q})$ is prime:

$$A/f^{-1}(\mathfrak{q}) \hookrightarrow B/\mathfrak{q}$$
$$x + f^{-1}(\mathfrak{q}) \to f(x) + \mathfrak{q} = \mathfrak{q}$$

RHS is an ID and the map is injective.

Example 1.13
Is $f^{-1}(\mathfrak{m})$ a maximal ideal for some maximal $\mathfrak{m}$ in B?
No. Consider $f : \mathbb{Z} \hookrightarrow \mathbb{Q}$, then $f^{-1}((0)) = (0)$.

Theorem 1.14
Every ring $A \neq 0$ has a maximal ideal.

Proof
Let $\Sigma = \{\text{proper ideals in } A\} \neq \emptyset$ (0 is always in there). Σ is partially ordered by inclusion.
Claim: Every chain (a_α) has an upper bound. $\forall \alpha, \beta$, either $a_\alpha \subset a_\beta$ or $a_\beta \subset a_\alpha$.
Consider $\bigcup_\alpha a_\alpha$, it is a proper ideal and is an upperbound. By Zorn's lemma, Σ has maximal element, which is a maximal ideal of A. □

Corollary 1.15
$\forall \mathfrak{a} \subset A$ proper, $\exists$ a maximal ideal $\mathfrak{m}$ containing $\mathfrak{a}$. $\mathfrak{a} \subset \mathfrak{m} \subsetneq A$.

Example 1.16

(i) $\mathbb{Z}[X]$. $(x, 2), (x, 3), (x, 5) \ldots$ are all maximal.

(ii) $k[X]$, k = field. $(x), (x-1), (x-a)$ are all maximal for all $a \in k$.

(iii) Find one example of A with a unique maximal ideal.
$0 \in \mathbb{C}$.
$A = \{$germs of holomorphic functions at $0\}$ is a ring.
$\mathfrak{m} = \{$germs of holomorphic functions vanishing at $0\}$ is a proper maximal ideal. $\mathfrak{m} \subset \mathfrak{m}' \subsetneq A$, $f \in \mathfrak{m}' \setminus \mathfrak{m}$, $f(0) \neq 0$, f is a unit.
$\implies$ $\mathfrak{m}$ is a maximal element.
Note: This works with any space and any ring!!

Definition 1.17
A ring is <u>local</u> if A has a unique maximal ideal $\mathfrak{m}$. $A/\mathfrak{m}$ is called the <u>residue field of A</u>.
A ring is <u>semi-local</u> if it has finitely many maximal ideals.

Proposition 1.18
Let $\mathfrak{m}$ be a proper ideal of A.

(i) If every $x \in A \setminus \mathfrak{m}$ is a unit, then A is a local ring and $\mathfrak{m}$ is the unique maximal ideal.

(ii) Assume $\mathfrak{m}$ is a maximal. If every $1 + x \in 1 + \mathfrak{m}$ is a unit of A, then A is a local ring.

Proof

(i) Take any ideal $(1) \neq \mathfrak{a} \subset A$.
<u>Claim</u>: $\mathfrak{a} \subseteq \mathfrak{m} \subsetneq A$.
Suppose $\mathfrak{a} \nsubseteq \mathfrak{m}$, then $\exists x \in \mathfrak{a} \setminus \mathfrak{m} \subset A \setminus \mathfrak{m}$. Then x is a unit. $\implies$ $\mathfrak{a} = (1)$. Contradiction.
So, A is a local ring with $\mathfrak{m}$ its unique maximal ideal.

(ii) Use (i). $\forall x \in A \setminus \mathfrak{m}$, $(\mathfrak{m}, x) = (1)$.
$1 = t + xy$ for some $t \in \mathfrak{m}$, $y \in A$.
$xy = 1 - t \in 1 + \mathfrak{m}$ is a unit by hypothesis, so x is a unit.
By (i), A is local.

□

Example 1.19 Primes and Maximal ideals (i) $k[x, y]$. If f is irreducible, then (f) is prime.
$(x - a, x - b)$ is maximal.
$(xy - 1)$ is prime.
$xy - 1 = xy - x + x - 1 = x(y-1) + (x-1) \subseteq (y-1, x-1)$.

(ii) $A = \mathbb{Z}$, (p) is prime and maximal.

(iii) $A = \mathbb{C}[X]$, $(x - a)$.

Definition 1.20
A <u>principal ideal domain</u> A is an integral domain s.t. every ideal is of the form (x) for some

$x \in A$, such ideals are called principal ideals.
Non-example: $k[x, y]$ is not a PID.

Proposition 1.21
In a PID, {non-zero prime ideals}={non-zero maximal ideals}

Proof
For any $\mathfrak{p} = (x)$ prime, suppose $(x) \subsetneq (y) \subset A$, i.e. $x = yz$ for some $z \in A$.
$yx \in (x)$ = prime.
$y \notin (x)$, $z \in (x)$. $z = xt, t \in A$.
$x = ytx$, integral domain $\implies yt = 1$. □

1.2 Nilradical and Jacobson Radical

Definition 1.22
A = ring, $1 \in A$.
The nilradical of A is

$$\begin{aligned}\mathfrak{n} &= \{\text{all nillpotent elements}\} \\ &= \{f \in A \mid f^n = 0 \text{ for some } n > 0\}\end{aligned}$$

.

Proposition 1.23 (i) $\mathfrak{n}$ is an ideal.

(ii) $A/\mathfrak{n}$ has no nilpotent element $\neq 0$.

Proof
(i) $A \cdot \mathfrak{n} \subset$, obvious.
Want: $\forall x, y \in \mathfrak{n}, x + y \in \mathfrak{n}$. $x^n = 0, y^m = 0$ for some $n > 0, m > 0$.

$$(x + y)^N = \cdots + c_{ij} x^i y^j + \cdots = 0$$

$i + j = N$, $\begin{matrix} i < n & i \leq n-1 \\ j < m & j \leq m-1 \end{matrix}$, $i + j < n + m - 1$.
Take $N \geq n + m - 1$.

(ii) Suppose $\overline{x} \in A/\mathfrak{n}$, $x \in A$ s.t. $\overline{x}^n = \overline{0}$ for some $n > 0$.
$x^n \in \mathfrak{n} \implies (x^n)^m = 0$ for some $m > 0 \implies x \in \mathfrak{n} \implies \overline{x} = 0$. □

Proposition 1.24
$\mathfrak{n} = \bigcap$ prime ideals.

Proof
$\mathfrak{n}' = \bigcap_{\mathfrak{p} \text{ prime}} \mathfrak{p}$.
Claim: $\mathfrak{n}' = \mathfrak{n}$.

$\mathfrak{n} \subseteq \mathfrak{n}'$: Take any $f \in R$, let $\mathfrak{p}$ be any prime ideal.
$f^k = 0$ for some k, $0 \in \mathfrak{p} \implies f \in \mathfrak{p}$.

$\mathfrak{n}' \subseteq \mathfrak{n}$: $\iff \forall f \notin \mathfrak{n}$, then $f \notin \mathfrak{n}'$.

$$0 \in \Sigma = \{\mathfrak{a} \mid f^n \notin \mathfrak{a}\ \forall n\}$$

Σ is ordered by inclusion.
Any chain in Σ has an upper bound.
Hence, Σ has a *maximal element* $\mathfrak{p} \in \Sigma$.
Claim: $\mathfrak{p}$ is prime.
Let $x, y \in A$, $xy \in \mathfrak{p}$. Suppose $x, y \notin \mathfrak{p}$.
$\mathfrak{p} \subsetneq \mathfrak{p} + (x)$, $\mathfrak{p} + (y) \notin \Sigma$.
$f^n \in \mathfrak{p} + (x)$, $f^m \in \mathfrak{p} + (y)$.
$f^{nm} \in \mathfrak{p} + (xy) = \mathfrak{p} \notin \Sigma$.
So $\mathfrak{p}$ is prime, $f \notin \mathfrak{n}$. □

Definition 1.25
Jacobson ideal $\mathfrak{R} = \bigcap_{\mathfrak{m} \text{ maximal}} \mathfrak{m}$.

Proposition 1.26
$x \in \mathfrak{R} \iff 1 - xy$ is a unit for any $y \in A$.

Proof
$\Rightarrow$:
Suppose $1 - xy$ is not a unit.
$1 - xy \in \mathfrak{m}$ for some maximal $\mathfrak{m}$, so $1 \in \mathfrak{m}$. Contradiction.
$\Leftarrow$:
Suppose $x \notin \mathfrak{m}$ for some maximal $\mathfrak{m}$.
$\mathfrak{m} + (x) = 1$, $1 = u + xy$, $u \in \mathfrak{m}$, $y \in A$.
$u = 1 - xy$ is a unit, and in $\mathfrak{m}$. Contradiction. □

1.3 Operation on Ideals.

A ring, $\mathfrak{a}, \mathfrak{b}, \{\mathfrak{a}_i\}_{i \in I}$ ideals.

(i) $a + b$, $\sum_{i \in I} \mathfrak{a}_i$ finite sum, still an ideal and is the smallest ideal contining all of $\mathfrak{a}_i$

(ii) $\mathfrak{ab} = \{\sum x_i y_i \mid x_i \in \mathfrak{a}, y_i \in \mathfrak{b}\}$ is an ideal. If $|I| < \infty$, then $\prod_{i \in I} \mathfrak{a}_i = \mathfrak{a}_1(\mathfrak{a}_2 \cdots \mathfrak{a}_n)$.
$\mathfrak{a}^n =< x_1 \cdots x_n \mid x_i \in \mathfrak{a} >$, $a^0 = (1)$.

Example 1.27
$A = \mathbb{Z}$, $\mathfrak{a} = (m)$, $\mathfrak{b} = (n)$, $\mathfrak{a} + \mathfrak{b} = (\gcd(m, n))$.

(i) If m, n are coprime, then $\mathfrak{a} + \mathfrak{b} = \mathbb{Z}$.

(ii) $\mathfrak{a} \cap \mathfrak{b} = (\operatorname{lcm}(m, n))$.

(iii) $\mathfrak{a}\mathfrak{b} = (mn)$, $\mathfrak{a} \cap \mathfrak{b} \supsetneq \mathfrak{a} \cdot \mathfrak{b}$.
$\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a} \cdot \mathfrak{b} \iff (m, n) = 1$.

Definition 1.28
Two ideals $\mathfrak{a}, \mathfrak{b}$ are coprime if $\mathfrak{a} + \mathfrak{b} = (1)$.

In general,

(i) $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$.

(ii) $\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) \supseteq \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}$, with equality if $\mathfrak{a} \geq \mathfrak{b}$ or $\mathfrak{a} \geq \mathfrak{c}$.

(iii) $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b}$, with equlity if $\mathfrak{a} + \mathfrak{b} = 1$.

Definition 1.29
The direct product of the rings $A_1, \ldots, A_n$ is

$$A = \prod_{i=1}^{n} A_i$$

$1_A = (1_{A_1}, \ldots, 1_{A_n})$.
Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals in A, we have a natural map

$$\phi : A \to \prod_{i=1}^{n} A/\mathfrak{a}_i$$

Proposition 1.30 (i) If $\mathfrak{a}_i + \mathfrak{a} = (1)$, $i \neq j$, tten $\prod_{i=1}^{n} \mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{a}_i$.

(ii) $\phi :\to \prod_{i=1}^{n} A/\mathfrak{a}_i$ is surjective $\iff$ $\mathfrak{a}_i + \mathfrak{a}_j = (1)$, $i \neq j$.

(iii) ϕ is injective $\iff$ $\bigcap \mathfrak{a}_i = 0$.

Proof

(i) Prove by induction. True for $n = 1$.
Assume true for $\mathfrak{a}_1, \ldots, \mathfrak{a}_{n-1}$.

$$\mathfrak{b} = \prod_{i=1}^{n-1} \mathfrak{a}_i = \bigcap_{i=1}^{n-1}$$

Compare $\mathfrak{b}$ and $\mathfrak{a}_n$.
$\mathfrak{a}_i + \mathfrak{a}n = (1)$ for all $i \neq n$, so $\underbrace{x_i}_{\in \mathfrak{a}_i} + \underbrace{y_i}_{\in \mathfrak{a}_n} = 1$.

$$\prod_{+}^{n-1} i = 1 = \prod_{i=1}^{n-1}(1 - y_i) \equiv 1 \bmod \mathfrak{a}_n$$

$$\equiv 0 \bmod \mathfrak{a}_i, i \neq n$$

Claim: $\mathfrak{b}\mathfrak{a}_n = \mathfrak{b} \cap \mathfrak{a}_n$.
This follows from $\mathfrak{a}_n + \mathfrak{b} = (1)$. (Check $n = 2$ case.)

(ii) $\Rightarrow$, $\forall i \neq j$, want $\mathfrak{a}_i + \mathfrak{a}_j = 1$, $x + y = 1$.
For simplicity, $i = 1$, $j = 2$,

$$\phi : x \mapsto (1, 0, \ldots, 0), \quad y \mapsto (0, 1, 0, \ldots, 0)$$

$1 = \underbrace{x}_{\in \mathfrak{a}_2} + \underbrace{(1 - x)}_{\mathfrak{a}_1}$.
Can also try

$$\begin{aligned} x &\mapsto (0, 1, \ldots, 1) \\ x &\equiv 0 \bmod \mathfrak{a}_1 \\ x &\equiv 1 \bmod \mathfrak{a}_i, i \neq 1 \end{aligned}$$

($\Leftarrow$), we have $\forall i \neq j$, $\mathfrak{a}_i + \mathfrak{a}_j = 1$, $x + y = 1$.(*)
It suffices to show that $\exists x_i \mapsto (0, \ldots, 0, 1, 0, \ldots, 0)$ in the ith position. That means

$$\begin{aligned} x &\equiv 1 \bmod \mathfrak{a}_i \\ &\equiv 0 \bmod \mathfrak{a}_j, j \neq i \end{aligned}$$

by (*) $x_i + y_j = 1, x_i \in \mathfrak{a}_i, y_j \in \mathfrak{a}_j, i \neq j$.
$x = \prod_{j \neq i} y_i = \prod_{j \neq i} (1 - x_i) \mapsto (0, \ldots, 0, 1, 0, \ldots, 0)$.

(iii) $\ker \phi = \bigcap_{i=1}^n \mathfrak{a}_i$.

□

Proposition 1.31
Suppose $\{\mathfrak{p}_i\}_{i=1}^n$ are prime.

(i) If an ideal $\mathfrak{a} \subset \bigcup_{i=1}^n \mathfrak{p}_i$, then $\mathfrak{a} \subset \mathfrak{p}_i$ for some i.

(ii) If $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are ideals, $\mathfrak{p}$ is prime s.t. $\mathfrak{p} \supset \bigcap_{i=1}^n \mathfrak{a}_i$, then $\mathfrak{p} \supset \mathfrak{a}$ for some i. In particular, if $\mathfrak{p} = \bigcap_{i=1}^n \mathfrak{a}_i$, $\mathfrak{p} = \mathfrak{a}_i$ for some i.

Proof

(i) Induction on n.
If $\mathfrak{a} \nsubseteq \mathfrak{p}_i$ for all i, then $\mathfrak{a} \nsubseteq \bigcup_{i=1}^n \mathfrak{p}_i$.
True for $n = 1$.
Suppose true for $n - 1$. $\mathfrak{a} \nsubseteq \bigcup_{j \neq i} \mathfrak{p}_j$ for any i.
For each i, $\exists x_i \in \mathfrak{a}$ s.t. $x_i \notin \mathfrak{p}_j$, $\forall j \neq i$.
If there is i_0 s.t. $x_{i_0} \notin \mathfrak{p}_{i_0}$, done.
Otherwise $\forall i$, $x_i \in \mathfrak{p}_i$ ($x_i \in \mathfrak{p}_j, i \neq j$).
$x_1, \ldots, x_n \in \mathfrak{a}$, $x_i \in \mathfrak{p}_i \setminus \bigcup_{j \neq i} \mathfrak{p}j$.

$$\sum_{i=1}^n x_1 \cdots \widehat{x_i} \cdots x_n \in \mathfrak{a}_j \notin \mathfrak{p}_{i_0} \qquad \forall i_0$$

$$\underbrace{x_1 \cdots \widehat{x_i} \cdots x_n}_{\notin \mathfrak{p}_{i_0}} + \underbrace{\text{rest}}_{\ni x_{i_0}, \in \mathfrak{p}_{i_0}}$$

(ii) Suppose $\mathfrak{p} \not\supset \mathfrak{a}_i$ for all i.
$\exists x_i \in \mathfrak{a}_i, \notin \mathfrak{p}, \forall 1 \leq i \leq n$.
$\prod_{i=1}^{n} x_i \in \mathfrak{a}_i \setminus \mathfrak{p}$, because $\mathfrak{p}$ is pirme, $\forall i$.
Finally, if $\mathfrak{p} = \bigcup \mathfrak{a}_j \subseteq \mathfrak{a}_i$, $\mathfrak{p} \supset \mathfrak{a}_i \implies \mathfrak{p} = \mathfrak{a}_i$.

□

1.4 Quotients of Ideals, Extensions and Contractions

Definition 1.32
$\forall \mathfrak{a}, \mathfrak{b} \subset A$ two ideals, the ideal quotient

$$(\mathfrak{a} : \mathfrak{b}) = \{x \in A \mid x\mathfrak{b} \subseteq \mathfrak{a}\}$$
$$\text{Ann}(\mathfrak{b}) = (0 : \mathfrak{b}) = \{x \in A \mid x\mathfrak{b} = 0\} = \text{Annihilator of } \mathfrak{b}$$

Example 1.33
$A = \mathbb{Z}$, $\mathfrak{a} = (m)$, $\mathfrak{b} = (n)$. $(\mathfrak{a} : \mathfrak{b}) = \{x \in \mathbb{Z} \mid x(n) \subset (m)\} = (\frac{m}{(m,n)})$.

Definition 1.34
If $\mathfrak{a}$ is an ideal of A, the radical of $\mathfrak{a}$ is

$$r(\mathfrak{a}) = \{x \in A \mid x^n \in \mathfrak{a} \text{ for some } n > 0\} \supseteq \mathfrak{a}$$

Proposition 1.35 (i) $r(\mathfrak{a})$ is an ideal.

(ii) $r(\mathfrak{a}) = \bigcap_{\substack{\mathfrak{p} \text{ prime}_{\mathfrak{p}} \\ \mathfrak{p} \supseteq \mathfrak{a}}}$.
$\phi : A \to A/\mathfrak{a}$

Proof

(i) $r(\mathfrak{a}) = \phi^{-1}(\mathfrak{n}_{A/\mathfrak{a}})$ is an ideal.

(ii) Follows from (i)

□

Definition 1.36
$f : A \to B$ ring homomorhpism. $\mathfrak{a} \in A$, $\mathfrak{b} \in B$ ideals. $f^{-1}(\mathfrak{b}) = \mathfrak{b}^C$ is called the contraction of $\mathfrak{b}$.
$f(\mathfrak{a})$ need not be an ideal in $\mathfrak{b}$. (e.g. $\mathbb{Z} \hookrightarrow \mathbb{Q}$, $0 \neq (n)$).

$$\begin{aligned} \mathfrak{a}^e &= \text{ ideal generated by } f(\mathfrak{a}) \\ &= \{\sum f(x_i)y_i \mid x_i \in \mathfrak{a}, y_i \in B\} \end{aligned}$$

is the extension of $\mathfrak{a}$.

Pullbacks of prime ideals are prime, but if $\mathfrak{a}$ is a prime, $\mathfrak{a}^e$ may not be prime. e.g.

$$\begin{array}{ll} \mathbb{Z} \hookrightarrow \mathbb{Q} & \\ (3) \hookrightarrow (3), & (3)^e = (3)\mathbb{Q} = \mathbb{Q} \end{array}$$

Example 1.37
Consider $\mathbb{Z} \hookrightarrow \mathbb{Z}[\sqrt{-1}]$.

(i) $(2)^e = ((1+i)^2), 2\sqrt{-1} = (1+i)^2$.

(ii) $(5)^e = ((2+i)(2-i)), 5 = (2+i)(2-i)$

Proposition 1.38

(i) $\mathfrak{a} \subset \mathfrak{a}^{ec}$, $\mathfrak{b} \supseteq \mathfrak{b}^{ce}$.

(ii) $\mathfrak{b}^c = \mathfrak{b}^{cec}$, $\mathfrak{a}^e = \mathfrak{a}^{ece}$.

(iii) C = contracted ideals in A.
Then $E = \{\mathfrak{b} \text{ ideal} \mid \mathfrak{b}^{ce} = \mathfrak{b}\}$, $\begin{array}{l} C \to E \\ \mathfrak{a} \mapsto \mathfrak{a}^e \end{array}$, $\begin{array}{l} E \to C \\ \mathfrak{b} \mapsto \mathfrak{b}^c \end{array}$ are inverses to each other.

Proof

(i) Obvious.

(ii) $\mathfrak{b}^c \subseteq (\mathfrak{b}^c)^{ec} = \mathfrak{b}^{cec}$, $\mathfrak{b} \supseteq \mathfrak{b}^{ce}$, $\mathfrak{b}^c \supseteq B^{cec}$.

(iii) $C \longrightarrow E \longrightarrow C$

$\mathfrak{a} \longrightarrow \mathfrak{a}^e \longrightarrow \mathfrak{a}^{ec} = \mathfrak{a}$

□

2 Modules

k a field. A vector space V over k is a group where k acts linearly $k \times V \to V$ is a linear action. Let A be a ring, an A-module M is a group where A acts linearly $A \times M \to M$, i.e. for all $u, v \in A$, $x, y \in M$,

$$\begin{aligned} u(x+y) &= ux + uy \\ (u+v)x &= ux + vx \\ x(vx) &= (uv)x \end{aligned}$$

Example 2.1 (i) A vector space is a k-module for some field k.

(ii) A $\mathbb{Z}$-module is an abelian group.

(iii) If $\mathfrak{a}$ is an ideal of A, then $\mathfrak{a}$ is an A-modules. In particular, A is an A-module.

(iv) M, N are A-modules, then $f : M \to N$ is a homomorphism of A-modules is a group homomorphism and is A-linear

$$f(ux + vy) = uf(x) + vf(y)$$

(v) $\mathrm{Hom}_A(M, N) = \{f : M \to N\}$ is an A-module.

2.1 Submodules

$N \hookrightarrow M$ is an A-submodule of M if it is a subgroup and is closed under A-multiplication.
If $\mathbb{N} \hookrightarrow M$ is a submodule, then M/N has a structure of A-module.

$$\{\text{submodules } M \supset N \text{ in } M\} = \{\text{submodules of } M/N\}$$

Let $f : M \to N$ be a homomorphism of A-modules.
$\ker f = \{x \in M \mid f(x) = 0\}$ is an A-module in M.
$\mathrm{Im}(f) = f(M)$ is an A-module in N.
The <u>cokernel</u> of f is $N/\mathrm{Im}(f)$.

Theorem 2.2
$M/\ker f \cong \mathrm{Im} f$ as A-modules.

Let $\{M_i\}$ be a set of submodules of M. Then

$$\sum_{i \in I} M = \{\sum_{\text{finite}} x_i \mid x_i \in M_i\} \bigcap M_i \qquad \subset M$$

are submodules of M.

Proposition 2.3 (i) $N \subset M \subset L$ are A-modules.

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

(ii) $M_1, M_2 \hookrightarrow M$, then

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

Proof

(i) $f : \begin{matrix} L/N \twoheadrightarrow L/M \\ x + N \mapsto x + M \end{matrix}$ for all $x \in L$.

$$\begin{aligned} \ker f &= \{x + N \mid x + M = M\} \\ &= \{x + N \mid x \in M\} \\ &= M/N \end{aligned}$$

(ii) $M_2 \hookrightarrow M_1 + M_2 \overset{g}{\twoheadrightarrow} (M_1 + M_2)/M_1$
$\ker(g) = M_1 \cap M_2$, hence result.

□

If $\mathfrak{a}$ if an ideal of A, then $aM = \{\sum_{\text{finite}} a_i x_i \mid a_i \in \mathfrak{a}, x_i \in M\}$ is a submodule of M.
N, P are submodules of M, then the quotient ideal of N by P is:
$(N : P) = \{a \in A \mid aP \subset N\}$ is an ideal of A.
$(0 : M) = \{a \in A \mid aM = 0\} = \text{Ann}(M)$.

Example 2.4
$A = k[x]$, $M = k[x]/(x)$ is a A-module, then $Ann(M) = (x) \subset A$

If $\mathfrak{a} \subset \text{Ann}(M)$ is an ideal of A, then M is an $A/\mathfrak{a}$-module.

$$(u + a)x = ux \qquad \forall a \in A, x \in M$$

Definition 2.5
If $\text{Ann}(M) = 0$, then M is said to be a A-faithful.
Thus, any A-module M is $A/\text{Ann}(M)$-faithful.

Definition 2.6
Let $\{M_i\}_{i \in I}$ be A-modules. The direct sum and direct product if defined to be

$$\bigoplus_{i \in I} M_i = \{(x_i)_{i \in I} \mid x_i \in M_i, \text{only finitely many } x_i \text{ are non-zero}\}$$
$$\prod_{i \in I} M_i = \{(x_i)_{i \in I} \mid x_i \in M_i\}$$

A a ring. A is an A-module which is generated by 1 (the trivial A-module),
$\underbrace{A \oplus \cdots \oplus A}_{n} = A^{\oplus n} = A^n$.

Definition 2.7
M is a free A-module of rank n if $M = \bigoplus_{i=1}^{n} M_i$ such that $M_i \cong A$.

Definition 2.8
M is finitely generated if $\exists x_1, \ldots, x_n \in M$ such that

$$M = \{\sum_{i=1}^{n} a_i x_i \mid a_i \in A\}$$

x_i's generated M but is not a basis as the representation of an element may not be unique, this does not happen in a vector space.

Example 2.9
$(x) \subset A = k[x]$, (x) is an A-module generated by x, $(x) \ncong A = k[x]$.

Proposition 2.10
Any finitely generated module M is a quotient of some free module.

Definition 2.11
A free module of rank 1 is an A-module $M \cong A$ as modules.
A free module of rank n is an A-module M s.t. $M \cong \bigoplus_{i=1}^{n} M_i$ and $M_i \cong A$. i.e. $M_i =< e_i >=< 0, \ldots, 0, 1, 0, \ldots, 0 >$ and each representation of an element is unique, $M = \{\sum a_i e_i \mid a_i \in A\}$.

Example 2.12
k a field, $A = k[x]$, (x) is an ideal, an A-modules, and also a submodule of A.
Is (x) a free A-module? i.e. $(x) \cong A$? If so, we need an A-module isomorphism beteen (x) and A.

$$\begin{aligned} \varphi : (x) &\to A \\ xf(x) &\leftrightarrow f(x) \\ x &\leftrightarrow 1 \end{aligned}$$

So it is indeed free.
Note that as A-modules, $(x) \cong A$, $k[x] \cong A$ but $(x) \subsetneq k[x]$.

Example 2.13
$M = k[x]/(x)$ is an A-module. Is M a free A-module? Is $M \cong A$?
Consider annihilators of M and A:

$$\begin{aligned} \mathrm{Ann}(M) &= \{u \in A \mid uM = 0\} = (x) \\ \mathrm{Ann}(A) &= \{u \in A \mid uA = 0\} = 0 \end{aligned}$$

So they are not isomorphic.

2.2 Finitely Generated Modules

Definition 2.14
M is finitely generated if $\exists x_1, \ldots, x_n$ s.t. $M = \{\sum_{i=1}^{n} a_i x_i \mid a_i \in A\}$, (but representation may not be unique).

Example 2.15

(i) Free modules of finite rank are finitely generated.

(ii) Is $k[x]/(x)$ finitely generated? Consider $c + (x) = c(1 + (x))$, $c + (x) = (c + xf(x))(1 + (x))$.

Proposition 2.16
Any f.g. module M is a quotient of a free module.

Proof
Suppose M is generated by $x_1, \ldots, x_n$.

$$\varphi : \text{free module} A^n \twoheadrightarrow M =< x_1, \ldots, x_n >$$
$$\sum a_i e_i \mapsto \sum a_i x_i$$

It is easy to check surjectivity, so $M \cong A^n / \ker \varphi$. □

Proposition 2.17
M f.g. A-module.
$\varphi : M \to M$ homom s.t. $\varphi(M) \subset \mathfrak{a}M$ for some ideal $\mathfrak{a}$ in A. Then φ satisfies

$$\varphi^n + a_1\varphi^{n-1} + \cdots + a_{n-1}\varphi + a_n = 0$$

for some $a_i \in \mathfrak{a}$.

Proof
$M =< x_1, \ldots, x_n >$, $\varphi(x_i) = \sum a_{ij} x_j$, $a_{ij} \in \mathfrak{a}$.
$\varphi \sim (a_{ij})$. $\det(\lambda I - (a_{ij})) = \lambda^n + a_1\lambda^{n-1} + \cdots + a_n$.
$\sum_{i=1}^n (\delta_{ij}\varphi - a_{ij}I)x_j = 0$, δ_{ij} = Kronecker delta.
Multiplying by the adjoint matrix $\implies$ determinant of $(\delta_{ij}\varphi - a_{ij})$ annihilates all x_j.
Let the determinant be $\varphi^n + a_1\varphi^{n-1} + \cdots + a_{n-1}\varphi + a_n = 0 : M \to M$. □

Corollary 2.18
M f.g., $\mathfrak{a} \in A$ ideal.
Suppose $\mathfrak{a}M = M$, then $\exists x \equiv 1 \bmod \mathfrak{a}$ s.t. $xM = 0$.

Proof
$\phi = \mathrm{Id} : M \to M$, $\phi(M) = M = \mathfrak{a}M \subset M$.
$\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0 : M \to M$, $v \mapsto 0$.
$x = 1 + \underbrace{a_1 + \cdots + a_n}_{\in \mathfrak{a}} : v \mapsto 0$.
$x \equiv 1 \bmod \mathfrak{a}$, $xM = 0$, $xv = 0$? □

Lemma 2.19 Nakayama
M f.g. A-module. $\mathfrak{a} \subset \mathcal{R} \subset A$. If $\mathfrak{a}M = M$, then $M = 0$.

Proof
$\exists x \equiv 1 \bmod \mathfrak{a}$ s.t. $xM = 0$.
$x = 1 + u$, $u \in \mathfrak{a} \subset \mathcal{R}$, so x is a unit $\implies$ $x^{-1}xM = M = 0$. □

Corollary 2.20
M f.g., $N \subset M$, $\mathfrak{a} \subseteq \mathcal{R}$. If $M = \mathfrak{a}M + N$, then $M = N$.

Proof
Suffices to show $M/N = 0$.

Need to check: $\mathfrak{a}(M/N) = M/N$, $M = \mathfrak{a}M + N$.

$$\begin{aligned} m + N &= \mathfrak{a}m' + n + N \\ &= \mathfrak{a}(m' + N) = \mathfrak{a}(M/N). \end{aligned}$$

□

A = local ring. $\mathfrak{m}$ = unique maximal ideal. $k = A/\mathfrak{m}$ = residue field.
Let M be a f.g. A-module, $\mathfrak{m}M$ = f.g. module.
$M/\mathfrak{m}M$ is an A-module and also an $A/\mathfrak{m}A$-module.
Since $A/\mathfrak{m}A$ is a field, $M/\mathfrak{m}M$ is an $A/\mathfrak{m}\mathfrak{m}A$-vector space of finite dimension.
(In general, if $\mathfrak{a} \subset \mathrm{Ann}(M)$, then M is an $A/\mathfrak{a}A$-module.)

Proposition 2.21
Let $x_1, \ldots, x_n \in M$ s.t. their images in $M/\mathfrak{m}M$ form a basis, then $x_1, \ldots, x_n$ are generators of M.

Proof
Let $N =< x_1, \ldots, x_n > \subset M$. Need to check that $\mathfrak{m}M + N = M$. ($\subset$ is clear).

$$N \longrightarrow M \xrightarrow{\varphi} M/\mathfrak{m}M \to 0$$

$\mathfrak{m}' + \mathfrak{m}M = n + \mathfrak{m}M$, $N + \mathfrak{m}M = M \implies N = M$. □