NOTES ON COMMUTATIVE ALGEBRA

CHUNYI LI

CONTENTS

Key words and phrases. Ring, ideals, modules, integral closure, varieties, primary decomposition, valuations, dimension.

1. HILBERT BASES THEOREM AND NOETHERIAN RING

1.1. **Rings and subrings.** We collect some definitions/notations from previous modules.

Definition 1.1. A Ring $R = (R, +, \cdot)$ is a set R equipped with two operations (addition and multiplication) satisfying the following axioms:

(a) $(R, +)$ is an abelian group;
(b) $(R, \cdot)$ is associative and distributive with respect to addition;

ALL ring in this module will be commutative, i.e.,

(a) $\forall x, y \in R$, $xy = yx$;
(b) $\exists 1_R$ s.t. $\forall x \in R$, $1_R x = x$.

In this module, a **ring** is commutative with (multiplicative) identity, unless stated otherwise.

By the first axiom, the ring R has an 'additional identity' 0_R. By the second axiom, we have $0_R \cdot x = 0$ for any $x \in R$.

Example 1.2. Examples of rings:

(a) Zero ring: $R = (0)$ the only ring such that $0_R = 1_R$.
(b) $\mathbb{Z}$: ring of integers; $\mathbb{Q}$: rational numbers; $\mathbb{R}$: real numbers; $\mathbb{C}$: complex numbers.
(c) Polynomial Rings: Let R be a ring, we define the polynomial ring over R as

$$R[x] := \{a_0 + a_1 x + \cdots + a_n x^n | n \in \mathbb{N}, a_i \in R\}.$$

The set $R[x]$ has natural addition and multiplication operations.

Definition 1.3. A **subring** S (of R) is a subset of R when

(a) $(S, +_R, \cdot_R)$ is a ring (closed under operation);
(b) $1_S = 1_R \in S$.

Exercise 1.4. (a) $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$;
(b) $R \subset R[x]$;
(c) $\{0_R\}$ is a subset of the ring R. Though $\{0_R\}$ is a zero ring itself, it is NOT a subring of R when R is non-zero.

1.2. **Ideals and quotient rings.**

Definition 1.5. A **ring morphism** $\phi : R \to S$ is a map (from the set R to the set S) such that:

(a) Compatible with addition: $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$;
(b) Compatible with multiplication: $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$;
(c) $\phi(\mathrm{Id}_R) = \mathrm{Id}_S$.

Definition 1.6. Let R be a ring. An **ideal** $I \triangleleft R$ is a subset of R such that

(a) $(I, +)$ is a subgroup of $(R, +)$, i.e., $\forall x, y \in I$, we have $x - y \in I$;
(b) $\forall r \in R$ and $x \in I$, we have $rx \in I$.

Proper ideal: $I \neq R$.

Proposition and Definition 1.7. *Let I be an ideal in R, we define*

$$R/I := \{a_I | a \in R\}/\sim, \text{ where } a + I \sim a' + I \iff a - a' \in I.$$

We define two operations for elements in R/I as follows:

(1) $$(+_R) : (a + I) +_R (b + I) := (a + b) + I,$$

(2) $$(\cdot_R) : (a + I) \cdot_R (b + I) := (ab) + I.$$

Then $(R/I, +_R, \cdot_R)$ is a ring.

Example 1.8. Let R be a ring, then $\{0\}$ and R are always ideals in R.

Observation: $1_R \in I \implies \forall x \in R, I \ni 1_R x = x$. Hence $I = R$.

Definition 1.9. An element a is a **unit** if $\exists b \in R$ s.t. $ab = 1_R$.

The inverse of a unit r is unique, we denoted as r^{-1}.

Definition 1.10. A ring R is a **field** if

- it is not a zero ring;
- every non-zero element is a unit.

Lemma 1.11. *A field F has exactly two ideals, namely, (0) and F.*

Example 1.12. Fields: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$.

1.3. **PID.**

Definition 1.13. An element a is called a **zero-divisor** if $\exists 0 \neq b \in R$ s.t. $ab = 0$.
A ring R is called a **domain** if it has no non-zero divisor.

Example 1.14. A field is a domain. A finite domain is a field.
The ring of integers $\mathbb{Z}$ is a domain.
Let R be a domain, then $R[x]$ is a domain.
The ring $\mathbb{Z}/6\mathbb{Z} = \{\underline{0}, \underline{1}, \underline{2}, \underline{3}, \underline{4}, \underline{5}\}$ is not a domain.

Proposition and Definition 1.15. *Let A be a subset of R, we define the subset*

$$\langle A \rangle := \left\{ \sum_{f \in A} r_f f | r_f \in R, \text{ where only finitely many } r_f \text{ is non-zero} \right\}.$$

Then $\langle A \rangle$ is the minimum ideal that contains the subset A, in other words, if I is an ideal in R such that $I \supseteq A$, then $I \supseteq \langle A \rangle$.

An ideal is **principally generated** if $\exists f \in R$ such that $I = \langle f \rangle$.
An ideal is **finitely generated** if $\exists f_1, f_2, \ldots, f_m \in R$ such that $I = \langle f_1, f_2, \ldots, f_m \rangle$.

Example 1.16. Ideals in a field F: $\langle 0 \rangle$ and $\langle 1 \rangle = F$.

Definition 1.17. A ring R is a principal ideal domain (PID) if

- R is a domain;

- every ideal in R is principally generated.

Example 1.18.
(a) A field is a PID.
(b) The ring of integers $\mathbb{Z}$ is a PID.
(c) Let F be a field, then $F[x]$ is a PID.

We give a proof for the case of $F[x]$ with a 'trick' which will appear later.

Proof. Let I be an ideal in $F[x]$. If $I = \langle 0 \rangle$, then it is automatically principally generated by 0.

Let $f(x)$ be a non-zero element in I with the minimum degree. We write $f(x)$ term-wisely as

$$f(x) = a_n x^n + \dots,$$

for some $a_n \in F$ and $\deg f(x) = n$.

Suppose $I \neq \langle f(x) \rangle$, then we may let $g(x)$ be an element in $I \setminus \langle f(x) \rangle$ with the minimum degree. We write

$$g(x) = b_m x^m + \dots,$$

for some $b_m \in F$ and $\deg g(x) = m$.

Note that $g(x) \in I$, by the minimum assumption on $\deg f(x)$, we have $m \geq n$.

Let

$$\tilde{g}(x) := g(x) - a_n^{-1} b_m x^{m-n} f(x).$$

Here a_n^{-1} exists as F is a field. The element $a_n^{-1} b_m x^{m-n}$ is in $F[x]$.

Note that $f(x) \in I$ and $g(x) \in I \setminus \langle f(x) \rangle$, we have

$$\tilde{g}(x) \in I \setminus \langle f(x) \rangle.$$

Note that the leading terms in $g(x)$ and $a_n^{-1} b_m x^{m-n} f(x)$ cancel out, so we have

$$\deg \tilde{g}(x) < \deg g(x).$$

This contradicts to the minimum assumption on $\deg g(x)$ among all elements in $I \setminus \langle f(x) \rangle$.

Therefore, we must have $I = \langle f(x) \rangle$. □

1.4. Generators for ideals in $F[x, y]$.

Example 1.19. Let F be a field, consider the ring $F[x, y]$ and the ideal

$$I := \langle x, y \rangle = \{f(x, y) | f(0, 0) = 0\}.$$

We claim that I can NOT be generated by one element.

Proof. Suppose $I = \langle f(x, y) \rangle$, then we have $x = f(x, y)h(x, y)$ and $y = f(x, y)g(x, y)$. Note that $x = f(x, y)h(x, y)$ implies that $f(x, y)$ has no variable y. Therefore, $f(x, y)$ must be a constant function, $0 \neq f(x, y) \equiv f_0 \in F$. But then $I = F[x, y]$, which is a contradiction. □

Example 1.20. Let F be a field, consider the ring $F[x, y]$ and the ideal

$$I := \langle x^2, xy, y^2 \rangle = \{ \sum_{i+j \geq 2} a_{ij} x^i y^j | a_{ij} \in F \}.$$

We claim that I can NOT be generated by two elements.

Proof. Suppose $I = \langle f, g \rangle$ for some

$$f(x,y) = f_{20}x^2 + f_{11}xy + f_{02}y^2 + f_3(x,y),$$
$$g(x,y) = g_{20}x^2 + g_{11}xy + g_{02}y^2 + g_3(x,y),$$

where $f_{ij}, g_{ij} \in F$, the polynoimials $f_3(x,y)$ and $g_3(x,y)$ only have terms with degree ≥ 3.

Since $x^2, xy, y^2 \in I = \langle f, g \rangle$, we must have

$$\begin{cases} x^2 &= a_1(x,y)f(x,y) + b_1(x,y)g(x,y), \\ xy &= a_2(x,y)f(x,y) + b_2(x,y)g(x,y), \\ y^2 &= a_3(x,y)f(x,y) + b_3(x,y)g(x,y), \end{cases}$$

for some $a_i(x,y), b_i(x,y) \in F[x,y]$.

Compare the degree 2 terms on both hand sides of the equations, we have

$$\begin{cases} x^2 = a_1(0,0)(f_{20}x^2 + f_{11}xy + f_{02}y^2) + b_1(0,0)(g_{20}x^2 + g_{11}xy + g_{02}y^2), \\ xy = a_2(0,0)(f_{20}x^2 + f_{11}xy + f_{02}y^2) + b_2(0,0)(g_{20}x^2 + g_{11}xy + g_{02}y^2), \\ y^2 = a_3(0,0)(f_{20}x^2 + f_{11}xy + f_{02}y^2) + b_3(0,0)(g_{20}x^2 + g_{11}xy + g_{02}y^2), \end{cases}$$

Note that the coefficients for x^2, xy and y^2 must be the same on both hand sides, hence

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} a_1(0,0) & b_1(0,0) \\ a_2(0,0) & b_2(0,0) \\ a_3(0,0) & b_3(0,0) \end{pmatrix} \begin{pmatrix} f_{20} & f_{11} & f_{02} \\ g_{20} & g_{11} & g_{02} \end{pmatrix}$$

as a product of matrices with coefficients in F. Note that the matrices on the right hand side are 3×2 and 2×3, both of which has rank at most 2. Their product has rank at most 2. We get the contradiction as the the 3×3 identity matrix has rank 3. □

There is no bound for the number of generators for an arbitrary ideal in $F[x,y]$.

Example 1.21. Let F be a field, the ideal $I = \langle x^n, x^{n-1}y, \ldots, y^n \rangle$ in $F[x,y]$ can NOT be generated by n elements.

Theorem 1.22 (Hilbert Bases Theorem 'Toy Case')**.** *Let F be a field and I be an ideal in $F[x,y]$, then I is finitely generated.*

Convention: We think $F[x,y]$ as the polynomial ring $(F[x])[y]$ with variable y and coefficient in $F[x]$. For every element $f \in (F[x])[y]$, we can write

$$f(x,y) = f_n(x)y^n + f_{n-1}(x)y^{n-1} + \cdots + f_0(x)$$

for some $f_i(x) \in F[x]$ in a unique way, where $f_n(x) \neq 0$. We denote the y-degree of $f(x,y)$ as $\mathrm{Deg}_y f(x,y) = n$.

Proof. If $I = (0)$, then we are done.

Otherwise, let $F_1(x,y)$ be a non-zero element in I with the minimum degree Deg_y. We write

$$F_1(x,y) = f_1(x)y^{n_1} + \ldots,$$

where $\mathrm{Deg}_y F_1(x,y) = n_1$ and $f_1(x) \in F[x]$ is the leading coefficient.

If $I = \langle F_1(x,y)\rangle$, then we are done.

Otherwise, let $F_2(x,y)$ be a non-zero element in $I \setminus \langle F_1(x,y)\rangle$ with the minimum degree Deg_y. We write

$$F_2(x,y) = f_2(x)y^{n_2} + \dots,$$

where $\mathrm{Deg}_y F_2(x,y) = n_2$ and $f_2(x) \in F[x]$ is the leading coefficient.

By the minimum assumption on $\mathrm{Deg}_y F_1(x,y)$ among all non-zero elements in I, we have $n_2 \geq n_1$.

Suppose $f_2(x) \in \langle f_1(x)\rangle$ in $F[x]$, then we can write $f_2 = r_1(x)f_1(x)$ for some $r_1(x) \in F[x]$.

Let

$$\tilde{F}_2(x,y) := F_2(x,y) - r_1(x)y^{n_2-n_1}F_1(x,y),$$

, then by the same argument as that in Example 1.18, we have $\mathrm{Deg}_y \tilde{F}_2(x,y) < \mathrm{Deg}_y F_2(x,y)$ and $\tilde{F}_2(x,y) \in I \setminus \langle F_1(x,y)\rangle$. This contradicts the minimum assumption on $\mathrm{Deg}_y F_2(x,y)$ among all elements in $I \setminus \langle F_1(x,y)\rangle$. Therefore $f_2(x) \notin \langle f_1(x)\rangle$ in $F[x]$, in other words,

$$\langle f_1(x)\rangle \subsetneq \langle f_1(x), f_2(x)\rangle.$$

If $I = \langle F_1(x,y), F_2(x,y)\rangle$, then we are done.

Otherwise, let $F_3(x,y)$ be a non-zero element in $I \setminus \langle F_1(x,y), F_2(x,y)\rangle$ with the minimum degree Deg_y. We write

$$F_3(x,y) = f_3(x)y^{n_3} + \dots,$$

where $\mathrm{Deg}_y F_3(x,y) = n_3$ and $f_3(x) \in F[x]$ is the leading coefficient.

By the minimum assumption on $\mathrm{Deg}_y F_2(x,y)$ among all elements in $I \setminus \langle F_1(x,y)\rangle$, we have $n_3 \geq n_2$.

Suppose $f_3(x) \in \langle f_1(x), f_2(x)\rangle$ in $F[x]$, then we can write $f_2 = r_1(x)f_1(x) + r_2(x)f_2(x)$ for some $r_i(x) \in F[x]$.

Let

$$\tilde{F}_3(x,y) := F_3(x,y) - r_1(x)y^{n_3-n_1}F_1(x,y) - r_2(x)y^{n_3-n_2}F_2(x,y),$$

then by the same argument as that in Example 1.18, we have $\mathrm{Deg}_y \tilde{F}_3(x,y) < \mathrm{Deg}_y F_3(x,y)$ and $\tilde{F}_3(x,y) \in I \setminus \langle F_1(x,y), F_2(x,y)\rangle$. This contradicts the minimum assumption on $\mathrm{Deg}_y F_3(x,y)$ among all elements in $I \setminus \langle F_1(x,y), F_2(x,y)\rangle$.

Therefore $f_3(x) \notin \langle f_1(x), f_2(x)\rangle$ in $F[x]$, in other words,

$$\langle f_1(x), f_2(x)\rangle \subsetneq \langle f_1(x), f_2(x), f_3(x)\rangle.$$

Suppose the ideal I is not finitely generated, then we can continue this procedure to an ascending chain of ideals:

$$\langle F_1\rangle \subsetneq \langle F_1, F_2\rangle \subsetneq \langle F_1, F_2, F_3\rangle \subsetneq \dots \langle F_1, F_2, \dots, F_m\rangle \subsetneq \dots$$

such that $F_m(x,y)$ is with minimum Deg_y among all elements in $I \setminus \langle F_1, \dots, F_{m-1}\rangle$.

Write $F_m(x,y) = f_m(x)y^{n_m} + \dots$.

By the 'Cancellation Technic', we get an ascending chain of ideals:

$$\langle f_1(x)\rangle \subsetneq \langle f_1(x), f_2(x)\rangle \subsetneq \langle f_1(x), f_2(x), f_3(x)\rangle \subsetneq \dots \langle f_1(x), f_2(x), \dots, f_m(x)\rangle \subsetneq \dots$$

in $F[x]$.

Note that $F[x]$ is a PID by Example 1.18, we have

$$\langle f_1, \dots, f_m \rangle = \langle h_m(x) \rangle$$

for some $h_m(x) \in F[x]$.

Note that $\langle h_{m-1}(x) \rangle \subsetneq \langle h_m(x) \rangle$, we have $h_{m-1}(x) = h_m(x) g_m(x)$ for non-unit polynomial $g_m(x)$. In particular, $\deg g_m(x) \geq 1$.

Therefore, we have the chain

$$\deg h_1 > \deg h_2 > \cdots > \deg h_m > \dots.$$

This is a contradiction as $\deg h_t \in \mathbb{Z}_{\geq 0}$ for every non-zero polynomial h_t. Hence I is finitely generated with at most $1 + \deg f_1(x)$ generators. $\square$

Example 1.23. Let $I = \{f(x,y) | f(0,0) = f(0,1) = f(1,0) = 0\}$. Find a set of generators for I according to the procedure as that in the proof.

Note that I is indeed an ideal: $\forall f, g \in I$ and $h \in F[x,y]$, we have

$$(f \pm g)(a,b) = f(a,b) \pm g(a,b) = 0;$$
$$(fh)(a,b) = f(a,b)g(a,b) = 0$$

for any $(a,b) = (0,0), (0,1)$ or $(1,0)$. Therefore, $f \pm g$, $fh \in I$.

To find generators for I, we first search element with $\text{Deg}_y = 0$. In particular, if $f(x) = 0$ for $x = 0$ and 1, then we have $x(x-1) | f(x)$. We may choose $F_1(x,y) = x(x-1)$ with $\text{Deg}_y = 0$ and leading coefficient $f_1(x) = x(x-1)$.

In the last paragraph, we have also shown that any element in $I \setminus \langle x(x-1) \rangle$ has $\text{Deg}_y \geq 1$. To search F_2, we may write it as $f_2(x)y + r(x)$. By the proof of Theorem 1.22, we may assume that $\deg f_2(x) \leq 1$ and $f_2(x) | f_1(x)$. This helps us to find $F_2(x,y) = xy$ 'quickly'.

By the proof of Theorem 1.22, there is at most one extra generator, and its leading coefficient has degree strictly smaller than 1. It is easy to figure out that $y + r(x) \notin I$ for any $r(x) \in F[x]$, therefore, the third generator has $\text{Deg}_y \geq 2$!

We may choose $F_3(x,y) = y^2 - y$, with $\text{Deg}_y F_3 = 2$ and leading coefficient 1. By the proof of Theorem 1.22, the ideal $I = \langle x(x-1), xy, y(y-1) \rangle$.

1.5. Noetherian Ring.

Definition 1.24. A ring R is called **Noetherian** if every ideal I in R can be finitely generated.

Definition 1.25. Let R be a ring. We say that (the set of ideals of) R has the **ascending chain condition (a.c.c.)** if every chain of ideals

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_m \subseteq \dots$$

eventually stops, in other words, there exists k such that $I_k = I_{k+1} = I_{k+2} = \dots$.

In other words, R has a.c.c. if it has no strictly ascending chain of ideals:

$$I_1 \subsetneq I_2 \subsetneq I_3 \cdots \subsetneq I_m \subsetneq \dots.$$

Proposition 1.26. *A ring R is Noetherian if and only if R has a.c.c..*

Proof. '$\Longleftarrow$': Let I be an ideal in R, suppose I is not finitely generated.

There exists $f_1 \in I$.

As I is not finitely generated, $I \neq \langle f_1 \rangle$. There exists $f_2 \in I \setminus \langle f_1 \rangle$, in other words, $\langle f_1 \rangle \subsetneq \langle f_1, f_2 \rangle$.

As I is not finitely generated, $I \neq \langle f_1, f_2 \rangle$. There exists $f_3 \in I \setminus \langle f_1, f_2 \rangle$, in other words, $\langle f_1 \rangle \subsetneq \langle f_1, f_2 \rangle \subsetneq \langle f_1, f_2, f_3 \rangle$.

We may carry on this procedure and get a strictly asceding chain of ideals:

$$\langle f_1 \rangle \subsetneq \langle f_1, f_2 \rangle \subsetneq \cdots \subsetneq \langle f_1, \ldots, f_m \rangle \subsetneq \ldots.$$

This contradicts to the a.c.c. on R.

'$\Longrightarrow$': Let

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_m \subseteq \ldots$$

be an ascending chain of ideals in R.

Take $J = \cup_{m=1}^{+\infty} I_m$, we claim that J is an ideal:

- $\forall x, y \in J$, we have $x, y \in I_k$ for some k large enough, therefore $x \pm y \in I_j \subseteq J$.
- $\forall r \in R$, we have $xr \in I_k \subseteq J$.

By the Noetherian assumption on R, the ideal J is finitely generated, namely,

$$J = \langle f_1, \ldots, f_t \rangle$$

for some $f_1, \ldots, f_t \in R$. Note that $f_i \in I_{m_i}$ for some $m_i \in \mathbb{Z}_{\geq 1}$, we may take $k := \max\{m_1, \ldots, m_t\}$, then $f_1, \ldots, f_t \in I_k$.

Therefore,

$$J = \langle f_1, \ldots, f_t \rangle \subseteq I_k \subseteq I_{k+1} \subseteq \cdots \subseteq J.$$

Hence, $I_k = I_{k+1} = \ldots$, in other words, R has a.c.c.. □

1.6. **Hilbert Bases Theorem.**

Theorem 1.27 (Hilbert Bases Theorem)**.** *Let R be a Noetherian ring, then $R[x]$ is Noetherian.*

Proof. Let I be an ideal in $R[x]$, suppose I is NOT finitely generated, we have an ascending chain of ideals in $R[x]$:

$$\langle F_1(x) \rangle \subsetneq \langle F_1(x), F_2(x) \rangle \subsetneq \cdots \subsetneq \langle F_1(x), \ldots, F_m(x) \rangle \subsetneq \ldots,$$

where $F_m(x)$ is with the minimum degree among all elements in $I \setminus \langle F_1(x), \ldots, F_{m-1}(x) \rangle$. We write

$$F_m(x) = f_m x^{n_m} + \ldots,$$

where $\mathrm{Deg} F_m = n_m$ and $f_m \in R$ is the leading coefficient of $F_m(x)$. By the minimum assumption on degree of F_i's, we have

$$n_1 \leq n_2 \leq \cdots \leq n_m \leq \ldots.$$

Suppose $f_m \in \langle f_1, \ldots, f_{m-1} \rangle$, then we have

$$f_m = r_1 f_1 + \cdots + r_{m-1} f_{m-1}$$

for some $r_1, \ldots, r_{m-1} \in R$. We may consider

$$\tilde{F}_m(x) := F(x) - r_1 x^{n_m - n_1} F_1(x) - \cdots - r_{m-1} x^{n_m - n_{m-1}} F_{m-1}(x).$$

By a formal check, we have

- $\deg \tilde{F}_m(x) < \deg F_m(x)$;
- $\tilde{F}_m(x) \in I \setminus \langle F_1(x), \ldots, F_{m-1}(x) \rangle$.

This contradicts the minimum assumption on $\deg F_m(x)$ among all elements in $I \setminus \langle F_1(x), \ldots, F_{m-1}(x) \rangle$.

Therefore, $f_m \notin \langle f_1, \ldots, f_{m-1} \rangle$. We have a strictly ascending chain of ideals

$$\langle f_1 \rangle \subsetneq \langle f_1, f_2 \rangle \subsetneq \cdots \subsetneq \langle f_1, \ldots, f_m \rangle \subsetneq \ldots.$$

This contradicts to the fact that R has a.c.c.(by Proposition 1.26). □

Proposition 1.28. *Let R be a Noetherian ring and I be an ideal in R. Then R/I is Noetherian.*

Proof. Let J be an ideal in R/I. We may consider the ideal (check!)

$$\tilde{J} := \{r \in R | r + I \in J\}.$$

Since R is Noetherian, the ideal $\tilde{J} = \langle f_1, \ldots, f_m \rangle$ for some $f_1, \ldots, f_m \in R$.

For any $r + I \in J$, since $r \in \tilde{J}$, we have $r = \sum r_i f_i$ for some $r_i \in R$. Therefore,

$$r + I = \sum (r_i + I)(f_i + I),$$

. The ideal J is finitely generated. □

Example 1.29. Let R be field or PID, then $R[x_1, \ldots, x_n]/I$ is Noetherian for any ideal I in $R[x_1, \ldots, x_n]$.

If R is Noetherian, then the formal power series ring

$$R[[x]] := a_0 + a_1 x + a_2 x^2 + \ldots a_n x^n + \ldots | a_i \in R$$

is Noetherian.

Example 1.30. The following rings are not Noetherian:

(a) Polynomial ring with infinitely many variables $F[x_1, \ldots, x_n, \ldots]$.
(b) $F[x, xy, xy^2, \ldots, xy^n, \ldots]$.
(c) $R = \{$real-valued continuous function from $\mathbb{R} \to \mathbb{R}\}$.

2. Ideals and Primary Decomposition

2.1. Prime ideals.

There are two equivalent definitions for a prime number in the ring of integers:

Definition 2.1. Let R be a domain, an element p is called **irreducible**, if

- it is not a unit nor zero;
- if $p = xy$, then x or y is a unit.

Definition 2.2. Let R be a ring, an element p is called **prime**, if

- it is not a unit nor zero;
- if $p|xy$, then $p|x$ or $p|y$.

These two definitions are the same when the ring is a so-called UFD.

Definition 2.3. A domain R is called a **unique factorization domain** (UFD), if for every non-zero, non-unit element $r \in R$, r can be written as a product of irreducible elements, uniquely up to order and units.

In other words, if $r = p_1p_2\dots,p_s = q_1\dots q_t$ for some p_i, q_j irreducible, then $t = s$ and there exists a bijective map $\sigma : \{1,\dots,s\} \longleftrightarrow \{1,\dots,t\}$ such that $p_i = q_{\sigma(i)}u_i$ for some units u_i.

Example 2.4. Here are some examples of UFD:

- The ring of integers $\mathbb{Z}$ is a UFD.
- A PID is a UFD.
- Let R be a UFD, then $R[x]$ is also a UFD.

Lemma 2.5. *A prime element in a domain is irreducible. An irreducible element in a UFD is prime.*

Proof. Let p be a prime element in a domain. Suppose $p = xy$, then $p|x$ or $p|y$.

WLOG, $p|x \implies x = pa \implies p = pay \implies p(1 - ay) = 0$. Since there is no non-zero divisor in a domain, we have $ay = 1$. Therefore, y is a unit.

Let p be an irreducible element in a UFD. Suppose $p|xy$, then $rp = xy$ for some $r \in R$. We may consider the prime decomposition for r, x and y:

$$r = q_1\dots,q_m; x = p_1\dots p_t; y = s_1\dots s_l.$$

Since $rp = xy$, the collection $q_1,\dots,q_m,p$ is the same as $p_1,\dots,p_t,s_1\dots,s_l$ up to orders and units. Hence, $p|x$ or $p|y$. □

In general, the condition in the first definition is strictly 'weaker' than that in the second definition.

Example 2.6. Consider the number 3 in the ring $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5}|a,b \in \mathbb{Z}\}$, then 3 is irreducible but NOT prime.

Instead of thinking about prime decomposition for elements in a ring, a more meaningful task is to considering decomposition for ideals.

Definition 2.7. An ideal $P \subset R$ is called **prime**, if

- $P \neq R$;

- if $xy \in P$, then $x \in P$ or $y \in P$.

We denote the set of all prime ideals of R by **Spec**R, and call it the spectrum of R.

Example 2.8. Spec$\mathbb{Z} = \{(0), \langle p \rangle | p$ is a prime number$\}$.
Let F be a field, then Spec$F = \{(0)\}$.

Proposition 2.9. *An ideal P is prime $\iff$ R/P is a domain.*

Proof.

$$\begin{aligned} & \text{An ideal } P \text{ is prime} \\ \iff & \text{for any } a, b \notin P,\ ab \notin P \\ \iff & \text{for any } a, b \notin P,\ (a+P)(b+P) \neq P \\ \iff & \text{for any } a+P, b+P \neq 0+P \text{ in } R/P,\ (a+P)(b+P) \neq 0+P \text{ in } R/P \\ \iff & \ R/P \text{ is a domain.} \end{aligned}$$

□

Example 2.10. The ideal $\langle 3 \rangle$ is NOT prime in the ring $\mathbb{Z}[\sqrt{-5}]$.
The ideal $\langle 3, 1+\sqrt{-5} \rangle$ contains all elements of the form $3a+b+b\sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$. Therefore, $\mathbb{Z}[\sqrt{-5}]/\langle 3, 1+\sqrt{-5} \rangle \simeq \{\underline{0}, \underline{1}, \underline{2}\} \simeq \mathbb{Z}/3\mathbb{Z}$. By Proposition 2.9, $\langle 3, 1+\sqrt{-5} \rangle$ is prime.

Definition 2.11. Let I and J be two ideals in R, we define their product as:

$$IJ := \langle xy | x \in I, y \in J \rangle$$

Exercise 2.12. Check: $\langle 3 \rangle = \langle 3, 1+\sqrt{-5} \rangle \langle 3, 1-\sqrt{-5} \rangle$.

2.2. **Maximal ideals.**

Definition 2.13. An ideal $I \subset R$ is called **maximal**, if

(a) $I \neq R$;
(b) there is no proper ideal J s.t $I \subsetneq J \subsetneq R$.

We denote the set of all maximal ideals of R by **max-Spec**R.

Example 2.14. A field F has a unique maximum ideal (0).

Proposition 2.15. *Let I be an ideal of R,*
then I is maximal $\iff$ R/I is a field.

Lemma 2.16. *Let I be an ideal in R. Denote the natural quotient ring homomorphism by $\pi : R \to R/I$. There is a one-to-one correspondence:*

$$\psi : \{\text{ideal in } R/I\} \longleftrightarrow \{\text{ideal of } R \text{ containing } I\} : \psi^{-1}.$$

Here for every ideal J in R/I the map ψ is defined as $\psi(J) := \pi^{-1}(J)$. For every ideal $\tilde{J}$ of R containing I, the map ψ^{-1} is defined as $\psi^{-1}(\tilde{J}) := \pi(\tilde{J})$.

Proof of Proposition 2.15. The ideal I is maximal.

$\iff$ The set $\{$ideal of R containing $I\}$ has exactly two elements, namely, I and R.

$\iff$ The ring R/I has exactly two ideals.

$\iff$ The ring R/I is a field. □

Corollary 2.17. *A maximal ideal is prime.*

Proof. $I \triangleleft R$ is maximal $\implies$ R/I is a field $\implies$ R/I is a domain $\implies$ I is prime. □

The existence of a maximal ideal is equivalent to the Zorn's Lemma.

Axiom:(Zorn's Lemma) Let $\mathcal{S}$ be a non-emplty, partially ordered **set** with the property that

"Any chain $U_1 < U_2 < \cdots < U_n < \ldots$ has at least one maximal element in $\mathcal{S}$."

Then $\mathcal{S}$ has at least one maximal element.

Proposition 2.18. *Let $I \triangleleft R$ be a proper ideal of R, then there exists a maximal ideal $\mathfrak{m}$ containing I.*

Proof. Let $\mathcal{S}$ be the set

$$\{\text{proper ideals of } R \text{ which contains } I\}.$$

with inclusion as partially order. As $I \in \mathcal{S}$, $\mathcal{S}$ is not empty.

For any chain of elements in $\mathcal{S}$:

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \ldots.$$

Let $\tilde{I} = \cup I_j$, then $\tilde{I}$ is an ideal containing I. Since $1 \notin I_j$ for any j, $1 \notin \tilde{I}$ as well. $\tilde{I}$ is a proper ideal of R, therefore an element in $\mathcal{S}$.

By Zorn's lemma, S has a maximal element, which is a maximal ideal containing I. □

Remark 2.19. The Zorn's Lemma is equivalent to several other logical statements, including: Axiom of Choice and Well-Ordering Principal. It also has some highly anti-intuitive implications, such as Banach-Tarski Paradox. A reference for more details is the blog: https://plato.stanford.edu/entries/axiom-choice/

Example 2.20. $\operatorname{maxSpec}(\mathbb{Z}) = \{\langle p\rangle | p \text{ is a prime number}\}$.

By Example 2.10, $\langle 3, 1+\sqrt{-5}\rangle$ is a maximal ideal in $\mathbb{Z}[\sqrt{-5}]$.

Most important example: let F be a field and $a_1, \ldots, a_n \in F$, then

$$\langle x_1 - a_1, \ldots, x_n - a_n\rangle$$

is a maximal ideal in $F[x_1, \ldots, x_n]$.

Theorem (First Ring Isomorphism Theorem)**.** Let $\phi : R \to S$ be a ring homomorphism, then $\ker \phi$ is an ideal in R. Moreover, the homomorphism ϕ induces a ring isomorphism:

$$\tilde{\phi} : R/\ker \phi \cong \operatorname{im} \phi.$$

Proof. For any element $x, y \in \ker \phi$ and $r \in R$, we have $\phi(x \pm y) = \phi(x) \pm \phi(y) = 0$ and $\phi(xr) = \phi(x)\phi(r) = 0$. Hence $\ker \phi$ is an ideal.

We define the map $\tilde{\phi}$ as $\tilde{\phi}(r+\ker\phi) := \phi(r)$. The map $\tilde{\phi}$ is well-defined: for any pair $r+\ker\phi \sim r'+\ker\phi$, we have $\phi(r) = \phi(r) - \phi(r-r')) = \phi(r')$. It is straitforward to check $\tilde{\phi}$ is a ring homomorphism.

The map $\tilde{\phi}$ is injective: $\phi(r) = 0 \implies r + \ker\phi \sim 0 + \ker\phi$.

The map $\tilde{\phi}$ is surjective onto $\operatorname{im}\phi$ by definition. □

To show that $\langle x_1 - a_1, \dots, x_n - a_n\rangle$ is a maximal ideal in $F[x_1, \dots, x_n]$, we may consider the following map:

$$\phi_{a_1,\dots,a_n} : F[x_1, \dots, x_n] \to F : f(x_1, \dots, x_n) \mapsto f(a_1, \dots, a_n).$$

The map $\phi_{a_1,\dots,a_n}$ is a ring homomorphism with kernel generated by $x_1 - a_1, \dots, x_n - a_n$. By Proposition 2.15 and RIT, the ideal $\langle x_1 - a_1, \dots, x_n - a_n\rangle$ is maximal.

2.3. **Primary ideal.**

Naively, we would like to express every ideal I in R as:

$$I = P_1^{e_1} \dots P_m^{e_m}$$

for some prime ideals P_i in R and powers $e_m \in \mathbb{Z}_{\geq 0}$.

Consider the example $I = \langle x^2, y\rangle$ in the ring $F[x, y]$. Suppose I admits such a decomposition, then for every prime factor P_i, we have

$$I \subseteq P_i.$$

Since $x^2 \in P_i$ and P_i is prime, $x \in P_i$. Therefore, $\langle x, y \subseteq P_i$. We must have $P_i = \langle x, y\rangle$.

However, it is not hard to check that

$$\langle x, y\rangle \supsetneq \langle x^2, y\rangle \supsetneq \langle x^2, xy, y^2\rangle = \langle x, y\rangle^2.$$

It is therefore impossible to have a naive prime decomposition theorem for every ideal in the ring. We should include more ideals as 'prime' factors.

Definition 2.21. Let R be a ring. An ideal Q of R is called **primary** if:

- $Q \neq R$;
- $fg \in Q \implies f \in Q$ or $g^m \in Q$ for some $m \in \mathbb{Z}_{\geq 1}$.

Definition 2.22. Let I be an ideal in a ring R, the **radical** of I is

$$\sqrt{I} := \{f \in R | f^m \in I \text{ for some } m \in \mathbb{N}\}.$$

Note that the radical of an ideal is an ideal.

For $\forall f, g \in \sqrt{I}$ and $x \in R$, suppose $f^m, g^n \in I$ for some $m, n > 0$. Then

$$(f-g)^{m+n} \in I; (xf)^m \in I.$$

Lemma 2.23. *If Q is primary, then $\sqrt{Q}$ is a prime ideal.*

Proof. Suppose $fg \in \sqrt{Q}$, then $(fg)^m \in Q$ for some $m > 0$. Then f^m or $g^m \in \sqrt{Q}$. So f^{mn} or $g^{mn} \in Q$. Hence, f or $g \in Q$. □

Example 2.24. The ideal $Q = \langle 27 \rangle$ is a primary in $\mathbb{Z}$.

If $27|nm$, then $27|n$ or $3|m \implies 27|m^3$.

The ideal $\langle 3 \rangle$ is NOT primary in $\mathbb{Z}[\sqrt{-5}]$.

The ideal $\langle 2 \rangle$ is primary in $\mathbb{Z}[\sqrt{-5}]$!

The deal $I = \langle xy, y^2 \rangle$ in $F[x, y]$ has radical $\sqrt{I} = \langle y \rangle$. But it is NOT primary.

Lemma 2.25. *Let R be a Noetherian ring and I be a proper ideal. Suppose I is NOT primary, then*

$$I = J_1 \cap J_2$$

for some $J_1, J_2 \neq I$.

Proof. By Lemma 2.16 and Proposition 1.28, we may assume that $I = (0)$!

Let f and g be two elements such that $fg = 0$, $f \neq 0$ and $g^m \neq 0$ for any m.

Consider the chain of ideals:

$$J_k := \{r \in R | rg^k = 0\}.$$

Note that $J_k \subseteq J_{k+1}$ is an ascending chain of ideals. Since R is Noetherian, $\exists k_0$ such that $J_k = J_{k_1}$ for all $k > k_0$.

Claim: $(0) = \langle f \rangle \cap \langle g^{k_0} \rangle$.

Let r be an element in both ideals, then

$$r = fr_1 = g^{k_0} r_2$$

for some $r_1, r_2 \in R$. Timing g on the equality, we have

$$gr = gfr_1 = 0 = g^{k_0+1} r_2.$$

Therefore, $r_2 \in J_{k_0+1} = J_{k_0}$. We have $r = g^{k_0} r_2 = 0$. □

Definition 2.26. Let I be a proper ideal in a ring R. A **primary decomposition** of I is an expression

$$I = Q_1 \cap \cdots \cap Q_r$$

with each Q_i primary.

The decomposition is called **irredundant** if $I \neq \cap_{i \neq j} Q_j$ for any j, and is called **minimal** if r is as small as possible.

Theorem 2.27. *Let $I \triangleleft R$ be a proper ideal in a Noetherian ring. Then I admits a primary decomposition.*

Proof. Suppose there is an ideal I that does NOT admits a primary decomposition, then I is not primary itself and by Lemma 2.25,

$$I = J_1 \cap J_2$$

for some $I \subsetneq J_1, J_2$. At least one of these two factors does NOT admits a primary decomposition, since otherwise I admits a primary decomposition. WLOG, we may assume J_1 does not admits a primary decomposition and denote it by I_2.

Repeat this procedure for I_2 and so on, we get a strictly ascending chain of proper ideals that does NOT admits a primary decomposition. This contradicts the Noetherian assumption on R. □

Remark 2.28. The Noetherian assumption is essential here. Consider the example of ring $R = \{\text{real-valued continuous functions on } \mathbb{R}\}$. Then the ideal $\langle \sin x \rangle$ does NOT have a primary decomposition.

A prime ideal P is NOT decomposible: suppose $P = I \cap J$ for some $I \neq P$, $J \neq P$, then we may choose $x \in I \setminus J$ and $y \in J \setminus I$. The product xy will violates the primality of P.

Example 2.29. Let $I = \langle xy, x - yz \rangle$ be an ideal in $\mathbb{C}[x, y, z]$. Find the primary decomposition of I.

Solution. Note that $xy \in I$, we claim that $x \notin I$ and $y^m \notin I$ for any $m \geq 1$.

If $x \in I$, then

$$x = xyF_1(x, y, z) + (x - yz)F_2(x, y, z)$$

for some $F_1, F_2 \in \mathbb{C}[x, y, z]$. We may substitute $x = yz$, then we have

$$yz = y^2 z F_1 + 0,$$

which is impossible. Therefore, $x \notin I$.

If $f(y) \in I$, then

$$f(y) = xyF_1(x, y, z) + (x - yz)F_2(x, y, z)$$

for some $F_1, F_2 \in \mathbb{C}[x, y, z]$. We may substitute $x = z = 0$, then we have

$$f(y) = 0, \tag{3}$$

which is impossible. Therefore, $f(y) \notin I$ for any $0 \neq f(y) \in \mathbb{C}[x, y, z]$.

Following the argument in Lemma 2.25, we let

$$J_m := \{F(x, y, z) | y^m F(x, y, z) \in I\}.$$

It is easy to see that $I \subset J_1$ and $x \in J_1$, therefore, $J_1 \supset \langle I, x \rangle = \langle x, yz \rangle$.

Note that $J_2 = \{F | yF \in J_1\}$, we have $z \in J_2$. Hence $J_2 \supset \langle J_1, z \rangle \supset \langle x, z \rangle$. We claim:

$$J_m = \langle x, z \rangle.$$

Let $F(x, y, z)$ be an element in J_m for some $m \geq 2$. Then we may write

$$F = xG_1(x, y, z) + zG_2(x, y, z) + f(y)$$

for some $G_1, G_2 \in \mathbb{C}[x, y, z]$ and $f(y) \in \mathbb{C}[y]$. Since $J_m \supset \langle x, z \rangle$, we have $f(y) \in J_m$. In particular, we have

$$y^m f(y) \in I.$$

By (3), $f(y) = 0$.

By the argument as that in Lemma 2.25, we have

$$I = \langle xy, x - yz, x \rangle \cap \langle xy, x - yz, y^2 \rangle = \langle x, yz \rangle \cap \langle y^2, x - yz \rangle.$$

The first factor has an ‘obvious’ primary decomposition as $\langle x, y \rangle \cap \langle x, z \rangle$.

We claim that the second factor $\langle y^2, x - yz \rangle$ is primary.

Lemma 2.30. *Let $\phi : R \to S$ be a ring homomorphism and Q be a primary ideal in S. Then $\phi^{-1}(Q)$ is primary in R.*

Proof. Easy exercise. □

Consider the ring homomorphism

$$\begin{aligned}\phi : \mathbb{C}[x, y, z] &\to \mathbb{C}[y, z]\\ x &\mapsto yz\\ y &\mapsto y\\ z &\mapsto z\end{aligned}$$

Then $\phi^{-1}(\langle y^2\rangle) = \langle y^2, x - yz\rangle$. Note that $\mathbb{C}[y, z]$ is a UFD, the ideal $\langle y^2\rangle$ is primary. By Lemma 2.30, $\langle y^2, x - yz\rangle$ is primary.

Note that $\langle y^2, x - yz\rangle \subset \langle x, y\rangle$, the ideal I have a primary decomposition:

$$I = \langle x, z\rangle \cap \langle y^2, x - yz\rangle.$$

□

3. Modules and Integral extensions

3.1. Modules.

Definition 3.1. Let R be a ring, an **R-module** M is an abelian group $(M, +)$ with a multiplication map

$$R \times M \to M : (r, m) \mapsto rm,$$

such that $\forall m, n \in M$ and $r, r' \in R$

(a) $r(m \pm n) = rm \pm rn$
(b) $(r + r')m = rm + r'm$
(c) $(rr')m = r(r'm)$
(d) $1_R m = m$

Example 3.2. For a field k, the definition of a module is the same as a vector space over the field. In particular, if M is of finite dimension, then $M \simeq k^{\oplus n}$.

An ideal I is an R-module by definition.

Definition 3.3. A subset $N \subseteq M$ of an R-module is an **R-submodule** if $(N, +)$ is an abelian subgroup of M and $\forall r \in R, n \in N$, one has $rn \in N$.

The **quotient module** M/N is constructed as equivalence classes of elements $m \in M$ modulo N. In other words, the coset

$$M/N = \{m + N | m \in M\}/\sim,$$

where $m_1 + N \sim m_2 + N \iff m_1 - m_2 \in N$, has a well-defined R-module structure:

$$R \times M/N \to M/N : f(m + N) := fm + N.$$

Example 3.4. Let I be an ideal of R, then both I and R/I are R-modules.

Definition 3.5. A map $\phi : M \to N$ is an **R-module homomorphism** if $\forall f, g \in R, m, n \in M$:

$$\phi(fm + gn) = f\phi(m) + g\phi(n).$$

Proposition 3.6. *Let $\phi : M \to N$ be an R-module homomorphism, then*

(a) $\ker \phi$ *and* $\operatorname{im} \phi$ *are both R-modules;*
(b) $M/\ker \phi \simeq \operatorname{im} \phi$.

Definition 3.7. Let M and N be two R-module. Their **direct sum** $M \oplus N$ is defined as

$$M \oplus N := \{(m, n) | m \in M, n \in N\}$$
$$R \times (M \oplus N) \to M \oplus N$$
$$r(m, n) \mapsto (rm, rn).$$

Notation: $M^{\oplus r} = M \oplus \cdots \oplus M$ for r times.

Definition 3.8. Let M be an R-module, and let $A = \{m_a\}$ be a subset of M. The set A **generates a submodule** $\langle A \rangle_M$ in M:

$$\{m \in M | m = \sum_{m_a \in A} r_a m_a \text{ for some } r_a \in R, \text{ only finitely many } r_a \neq 0\}.$$

In other words, the module $\langle A\rangle_M$ is the minimum R-submodule in M containing A.

We say that A **generates** M **as an** R**-module** if $\langle A\rangle_M = M$. The module M is called **finitely generated** if there is a finite generating set for M.

Definition 3.9. Let M be an R-module, a subset $A \subset M$ is called a basis if

(a) A generates M as an R-module;
(b) A is linear independent, i.e., $\forall \mathbf{e}_1, \ldots, \mathbf{e}_n \in A$,

$$r_1\mathbf{e}_1 + \ldots r_n\mathbf{e}_n = 0 \iff r_1 = \cdots = r_n = 0.$$

An R-module is called **free** if it has a basis. The cardinality of a basis (independent of the choice of basis) is called the **rank** of the module.

Example 3.10. Let M be a free R-module of rank n, then

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

as an R-module.

In particular, if $I = \langle f\rangle$ is a principally generated ideal in a domain R, then $\{f\}$ is a basis for I as an R-module, and

$$I \cong R$$

as an R-module.

When R is a field, then every R-module/vector space has a basis.

When R is not a field, let I be a non-zero, non-proper ideal of R, then R/I is an R-module generated by $1 + I$. But it is NOT free.

Theorem 3.11. *Let R be a PID, M be a finitely generated R-module, then*

$$M \cong R^{\oplus n} \oplus R/P_1^{n_1} \oplus \cdots \oplus R/P_s^{n_s}$$

for some maximal ideals P_i and positive integers n_i, n.

Example 3.12. The ideal $\langle x, y\rangle$ in $F[x, y]$ is NOT a free $F[x, y]$-module.

Let $M = \mathbb{Z}[\frac{1}{2}] := \{\frac{n}{2^m} | m, n \in \mathbb{Z}\}$ be a $\mathbb{Z}$-module, then M is NOT finitely generated. M does NOT have a basis.

3.2. **Cayley-Hamilton Theorem.** Cayley-Hamilton for vector spaces over a field:

Let A be a $n \times n$ matrix with coefficients in k, its characteristic polynomial is:

$$p_A(x) = \det(x\,\mathrm{Id}_n - A).$$

Then $p_A(A) = 0$.

Example 3.13. Let $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, then $p_A(x) = (x-1)(x-4) - 2 \times 3 = x^2 - 5x - 2$.

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^2 - 5\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} - 2\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix} - \begin{pmatrix} 5 & 10 \\ 15 & 20 \end{pmatrix} - \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = 0$$

Definition 3.14. Let M be a $n \times n$ matrix

$$\begin{bmatrix} m_{11} & m_{12} & \dots & m_{1n} \\ \dots & \dots & \dots & \dots \\ m_{n1} & m_{n2} & \dots & m_{nn} \end{bmatrix}$$

with coefficients in R, then the determinant of M is

$$\det M := \sum_{\sigma \in S_n} (-1)^{sgn(\sigma)} \prod_{i=1}^{n} m_{i\sigma(i)} \in R$$

The characteristic polynomial $p_A(x)$ is

$$x^n - trace(A)x^{n-1} + \cdots + (-1)^n \det A.$$

Theorem 3.15. *Let R be a ring, A be a $n \times n$ matrix with coefficients in R, its characteristic polynomial is:*

$$p_A(x) = \det(x \operatorname{Id}_n - A).$$

Then $p_A(A) = 0$.

Remark 3.16. Recall how did one prove the following statement in linear algebra:

Let B be a $n \times n$ matrix with coefficient in k, suppose $\exists v \neq 0$, s.t. $Bv = 0$. Then $\det B = 0$.

Proof. Let C be the adjoint of B: $C = [C_{ij}]$ such that

$$C_{ij} = (-1)^{i+j} \det \hat{B}_{ji}.$$

Here $\hat{B}_{ij}$ is the $(n-1) \times (n-1)$ matrix by taking off the ith-column and jth-row from B. We have $BC = CB = \det BI_n$.

Hence $0 = CBv = \det Bv$ for a non-zero v, and therefore $\det B = 0$. □

Proof. Note that $R[A]$ is a commutative ring. Consider the $n \times n$ matrix B with coefficient in $R[A]$:

$$B = \begin{pmatrix} A - a_{11}I_n & -a_{21}I_n & \dots & -a_{n1}I_n \\ -a_{12}I_n & A - a_{22}I_n & \dots & -a_{n2}I_n \\ \dots & \dots & \dots & \dots \\ -a_{1n}I_n & -a_{2n}I_n & \dots & A - a_{nn}I_n \end{pmatrix}$$

The statement is to show $\det B = 0$. Consider the adjoint of B: $C = [C_{ij}]$ such that

$$C_{ij} = (-1)^{i+j} \det \hat{B}_{ji}.$$

Here $\hat{B}_{ij}$ is the $(n-1) \times (n-1)$ matrix by taking off ith-column and jth-row from B. We have $BC = CB = \det BI_n$. Let $\mathbf{e}_i = (0, \dots, 1, \dots, 0)^T$ with 1 at the i-th position. Then for

$\forall a \leq i \leq n$,

$$\begin{aligned} &A\mathbf{e}_i = a_{1i}\mathbf{e}_1 + \cdots + a_{ni}\mathbf{e}_n \\ \Longrightarrow\ &(A - a_{ii})\mathbf{e}_i - a_{1i}\mathbf{e}_1 - \cdots - a_{ni}\mathbf{e}_n = 0 \\ \Longrightarrow\ &B_{ii}\mathbf{e}_i + B_{i1}\mathbf{e}_1 + \cdots + B_{in}\mathbf{e}_n = 0 \\ \Longrightarrow\ &\sum_{j=1}^{n} B_{ij}\mathbf{e}_j = 0 \end{aligned}$$

Let $v = (\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n)^T$, then $Bv = 0$. Therefore $CBv = 0$ and $(CB)v = 0$ (Here the product of B on v is not the product of matrix with vector, but composing the action of A on $\mathbf{e}_i$).

We may conclude that for $\forall 1 \leq i \leq n$: $\det B\mathbf{e}_i = 0$. Therefore, $\det B = 0$. □

Theorem 3.17. *Let M be a finitely generated R-module with n generators, $\phi : M \to M$ be an endomorphism. Suppose $\phi(M) \subseteq IM$ for some ideal of R, then ϕ satisfies a relation:*

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

for some $a_m \in I^m$ for $1 \leq m \leq n$.

Proof. Let $(\mathbf{e}_1, \ldots, \mathbf{e}_n)$ be a set of generators, then

$$\phi(\mathbf{e}_j) = r_{1j}\mathbf{e}_1 + r_{2j}\mathbf{e}_2 + \cdots + r_{nj}\mathbf{e}_n$$

for some $r_{ij} \in I$.

Let A be the $n \times n$ matrix (r_{ij}), and $p_A(x) = x^n + a_1x^{n-1} + \cdots + a_n$, then the coefficient $a_j \in I^j$.

By Theorem 3.15,

$$A^n + a_1A^{n-1} + \cdots + a_n = 0.$$

Hence true for ϕ. □

Here few more explanations for the last sentence in the proof:

For any element $m \in M$, m can be written as

$$m = b_1\mathbf{e}_1 + \cdots + b_n\mathbf{e}_n.$$

Note that these b_j's are not unique, but this is the only difference between a finitely generated module and a free module. Let

$$\begin{bmatrix} c_1 \\ c_2 \\ \cdots \\ c_n \end{bmatrix} = A \begin{bmatrix} b_1 \\ b_2 \\ \cdots \\ b_n \end{bmatrix}$$

then $\phi(m) = c_1\mathbf{e}_1 + \cdots + c_n\mathbf{e}_n = \begin{bmatrix} \mathbf{e}_1 & \mathbf{e}_2 & \ldots & \mathbf{e}_n \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ \cdots \\ c_n \end{bmatrix} = \begin{bmatrix} \mathbf{e}_1 & \mathbf{e}_2 & \ldots & \mathbf{e}_n \end{bmatrix} A \begin{bmatrix} b_1 \\ b_2 \\ \cdots \\ b_n \end{bmatrix}.$

$$
\begin{aligned}
&(\phi^n + a_1\phi_{n-1} + \cdots + a_n)m \\
&= \begin{bmatrix}\mathbf{e}_1 & \mathbf{e}_2 & \ldots & \mathbf{e}_n\end{bmatrix} (A^n + a_1A^{n-1} + \cdots + a_n Id) \begin{bmatrix} b_1 \\ b_2 \\ \ldots \\ b_n \end{bmatrix} = 0.
\end{aligned}
$$

3.3. **Integral and Finite Extensions.** An algebraic number is a complex number which is a root of a non-zero polynomial in $\mathbb{Z}[x]$. The set of all algebraic numbers is denoted as $\overline{\mathbb{Q}}$ in this notes.

'Well-known facts': $\overline{\mathbb{Q}}$ is a field. For an algebraic number $\alpha \in \overline{\mathbb{Q}}$, there exists a minimal polynomial $f(x) \in \mathbb{Z}[x]$ of α such that:

if $g(\alpha) = 0$ and $g(x) \in \mathbb{Z}[x]$, then $g(x) = f(x)h(x)$ for some $h(x) \in \mathbb{Z}[x]$.

As for an integer n, its minimal polynomial is just $x - n$. As for a rational number $\frac{m}{n}$, where $\gcd(m, n) = 1$, its minimal polynomial is $nx - m$. For a rational number q, it is not hard to figure out that q is an integer if and only if it is a root of monic polynomial in $\mathbb{Z}[x]$, i.e., its minimal polynomial is monic.

The concept of being an integral element can be generalized to all algebraic numbers.

Definition 3.18. A number $\alpha \in \overline{\mathbb{Q}}$ is called an algebraic integer, if $f(\alpha) = 0$ for some monic polynomial $f(x) \in \mathbb{Z}[x]$.

Example 3.19. All integers are algebraic integers. Given positive integers m and n, the number $\sqrt[n]{m}$ is an algebraic integer.

Without a general theory for integral elements, it is usually very hard to tell whether a given number is an algebraic integer or not, say, $\sqrt{2} + \sqrt[3]{3}$. In this section, we apply the Cayley-Hamilton theorem to set up some basic theories of integral and finite algebra. This will allow us to describe several properties of algebraic integers that are not trivial at a first glance.

Definition 3.20. Let R be a ring. A ring S is called an R-algebra if there is a ring homomorphism $\phi : R \to S$.

Note that this makes S into an R-module.

In practice, we may always assume that R is a subring of S.

Definition 3.21. Let R be a ring and S be an R-algebra. An element $s \in S$ is **integral over** R if there is a monic polynomial

$$f(y) = y^n + a_1y^{n-1} + \cdots + a_n \in R[y]$$

such that $f(s) = 0$.

If all elements of S are integral over R, then S is said to be integral over R.

Example 3.22.
(a) Let $R = \mathbb{C}$ and $S = \mathbb{C}[x]$, then an element in S is integral over R if and only if it is a constant function.
(b) Let $R = \mathbb{Z}$ and $S = \mathbb{C}$, a number if integral over $\mathbb{Z}$ if and only if it is an algebraic integer.
(c) Let $R = \mathbb{C}[x^2]$ and $S = \mathbb{C}[x]$, then x is integral over R.

Definition 3.23. Let S be an R algebra, we say that S is a finite R-algebra(or finite over R) if it is finitely generated as an R-module.

Example 3.24.
(a) $\mathbb{C}[x]$ is NOT finite over $\mathbb{C}$.
(b) $\mathbb{C}[x]$ is finite over $\mathbb{C}[x^2]$.

Proposition 3.25. *Let S be a finite R algebra, then S is integral over R.*

Proof. For any element $s \in S$, we may consider

$$\phi_s : S \to S : m \mapsto sm.$$

Apply Cayley-Hamilton Theorem 3.17 for R, S, ϕ_s and $I = R$. Then there exists $a_1, \dots, a_n \in R$ such that

$$\phi_s^n + a_1\phi_s^{n-1} + \cdots + a_n = 0.$$

In particular, the homomorphism on the left hand side maps 1 to 0. That is

$$s^n + a_1 s^{n-1} + \dots a_n = 0.$$

Hence s is integral over R. Since this holds for any $s \in S$, S is integral over R. □

Example 3.26.
(a) $t^5 + t^3 + 1$ satisfy the equation $x^4 + f_1(t^4)x^3 + f_2(t^4)x^2 + f_3(t^4)x + f_r(t^4) = 0$ for some $f_i(t) \in \mathbb{C}[t]$.
(b) $1 + \sqrt[3]{2} + \sqrt[3]{4}$ is an algebraic integer.

Definition 3.27. Let S be a ring and $R \subseteq S$ be a subring. Let $s_1, \dots, s_m$ be elements of S, then we write $R[s_1, s_2 \dots, s_m]$ for the smallest subring of S containing R and $s_1, s_2 \dots, s_m$.

We say that S is finitely generated over R if $\exists\, s_1, \dots, s_m$ such that $R[s_1, s_2, \dots, s_m] = S$.

In particular, every element of $R[s_1, s_2 \dots, s_m]$ can be written as a polynomial in $s_1, s_2 \dots, s_m$ with coefficients in R.

$$R[s_1, \dots, s_m] = \{f(s_1, \dots, s_m | f(x_1, \dots, x_m) \in R[x_1, \dots, x_m]\}.$$

By the definition,

$$R[s_1, \dots, s_{m-1}][s_m] = R[s_1, \dots, s_{m-1}, s_m].$$

Proposition 3.28. *Let S be an R-algebra with $R \subseteq S$. Let $s \in S$. The followings statements are equivelant.*

(a) The element s is integral over R.
(b) Then the subring $R[s]$ is finite over R.
(c) There exists an R-subalgebra $\tilde{R} \subset S$ such that $\tilde{R}$ is finite over R and $R[s] \subset \tilde{R}$

Proof. 'a $\implies$ b': Since the element s is integral over R, there exists a monic polynomial $f(x)$ such that

$$f(s) = s^n + a_1 x^{n-1} + \cdots + a_{n-1}s + a_n = 0.$$

Claim: $R[s]$ as an R-module is generated by $s^{n-1}, \dots, s, 1$.

For any element $g(s) \in R[s]$, since $f(x)$ is a monic polynomial,

$$g(x) = f(x)h(x) + r(x)$$

for some $\deg r(x) < \deg f(x)$. Therefore, $g(s) = r(s)$ which is $r_1 s^{n-1} + \dots r_{n-1}s + r_n$.

'b $\implies$ c': Let $\tilde{R} = R[s]$.
'c $\implies$ a': Corollary 3.25. ☐

3.4. Tower Laws.

Lemma 3.29. *Let $R \subseteq S \subseteq S'$ be rings, such that S' is finite over S and S is finite over R. Then S' finite over R.*

Proof. Let S' be generated by $a_1, \dots, a_n$ as an S-module; S be generated by $b_1, \dots, b_m$ as an R-module.

Then for any $m \in S'$:

$$\begin{aligned} m &= s_1 a_1 + \dots s_n a_n && \text{for some } s_1 \dots, s_n \in S \\ &= (r_{11}b_1 + \dots + r_{1m}b_m)a_1 + \dots + (r_{n1}b_1 + \dots + r_{nm}b_m)a_n && \text{for some } a_{ij} \in R \\ &= \sum r_{ij}a_i b_j. \end{aligned}$$

Therefore, S' is generated by $\{a_i b_j\}$ as an R-module. ☐

Corollary 3.30. *Let $R \subseteq S$ be rings, $s_1, \dots, s_m \in S$ be integral over R. Then $R[s_1, \dots, s_m]$ is finite over R.*

Proof. Consider the extension of rings:

$$R \subseteq R[s_1] \subseteq R[s_1, s_2] \subseteq \cdots \subseteq R[s_1, s_2, \dots, s_m].$$

For each extension, as s_l is integral over $S[s_1, \dots, s_{l-1}]$, by Proposition 3.28, $R[s_1, \dots, s_l]$ is finite over $R[s_1, \dots, s_{l-1}]$. By Lemma 3.29, $R[s_1, s_2, \dots, s_m]$ is finite over R. ☐

Definition 3.31. Let $R \subseteq S$ be rings, the **integral closure** of R in S is

$$\overline{R} = \{s \in S | s \text{ is integral over } R\}$$

Corollary 3.32. *Let $R \subseteq S$ be rings, then $\overline{R}$ is a subring of S.*

Proof. For any $s_1, s_2 \in S$, the ring $R[s_1, s_2]$ is integral over R. In particular, $s_1 \pm s_2$ and $s_1 s_2$ are integral over R, therefore they are both in $\overline{R}$. ☐

Proposition 3.33. *Let $R \subseteq S \subseteq S'$ be rings such that S' integral over S and S integral over R. Then S' is integral over R.*

Proof. $\forall b \in S'$, since b is integral over S, there exist $a_1, \dots, a_n \in S$ such that

$$b^n + a_1 b^{n-1} + \dots + a_n = 0.$$

This implies b is integral over $R[a_1, \dots, a_n]$.

By Proposition 3.28, $R[a_1, \dots, a_n][b]$ is finite over $R[a_1, \dots, a_n]$.

Since $a_1, \dots, a_n$ are all integral over R, by Corollary 3.30, $R[a_1, \dots, a_n]$ is finite over R.

We may consider the tower

$$R \subseteq R[a_1, \dots, a_n] \subseteq R[a_1, \dots, a_n][b],$$

by Lemma 3.29, $R[a_1, \dots, a_n][b]$ is finite over R, by Corollary 3.25, $R[a_1, \dots, a_n][b]$ is integral over R, therefore b is integral over R and S' is integral over R. ☐

Example 3.34. The number $\sqrt[5]{\frac{\sqrt{17}+\sqrt{5}}{2}} + \sqrt[7]{6}$ is an algebraic integer.

The golden ration number $\frac{\sqrt{5}-1}{2}$ satisfies the equation $x^2 + x - 1 = 0$. The number $\frac{\sqrt{17}-1}{2}$ satisfies the equation $x^2 + x - 4 = 0$. Both numbers are algebraic integers.

As $\mathbb{Z} \subset \mathbb{Z}[\frac{\sqrt{17}-1}{2}, \frac{\sqrt{5}-1}{2}, \sqrt[7]{6}] \subset \mathbb{Z}[\frac{\sqrt{17}-1}{2}, \frac{\sqrt{5}-1}{2}, \sqrt[7]{6}, \sqrt[5]{\frac{\sqrt{17}+\sqrt{5}}{2}}]$ is a chain of integral extensions, therefore $\sqrt[5]{\frac{\sqrt{17}+\sqrt{5}}{2}} + \sqrt[7]{6}$ is integral over $\mathbb{Z}$, in other words, an algebraic integer.

Corollary 3.35. *Let $R \subseteq S \subseteq T$ be rings such that S is integral over R. Then $\overline{R} = \overline{S}$ in T. In particular, $\overline{R} = \overline{(\overline{R})}$ in T.*

Proof. Consider $R \subseteq S \subseteq \overline{S}$, by Proposition 3.33, $\overline{S}$ is integral over R, therefore, $\overline{S} \supseteq \overline{R}$. □

Definition 3.36. Let S be an R-algebra. We say that R is **integrally closed** in S if $R = \overline{R}$ in S.

Proposition 3.37. *Let S be an integral domain. Suppose S is integral over R, then*

$$R \textit{ is a field} \iff S \textit{ is a field.}$$

Proof. ‘ $\implies$ ’: For $\forall 0 \neq x \in S$,

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

for some $a_i \in R$. We may assume that $a_n \neq 0$ since otherwise we may cancel x as S is a domain.

Since R is a field,

$$x(-a_n^{-1}(x^{n-1} + a_1 x^{n-2} + \ldots a_{n-1})) = 1.$$

Therefore, x is invertible and S is a field.

‘$\Longleftarrow$’: For $\forall 0 \neq x \in R$, $x^{-1} \in S$ and is integral over R, we have

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

for some $a_i \in R$. Therefore,

$$x^{-1} = a_1 + a_2 x + \cdots + a_n x^{n-1} \in R.$$

And R is a field. □

4. The Nullstellensatz

4.1. Ideals and Varieties.

Definition 4.1. Let k be a field. Let I be an ideal in $k[x_1, \dots, x_n]$. The **variety** of I is the set

$$V(I) := \{(a_1, \dots, a_n) \in k^n | f(a_1, \dots, a_n) = 0 \text{ for any } f \in I\}.$$

Let k be a field. Let I be an ideal in $k[x_1, \dots, x_n]$. By Hilbert Bases Theorem: Theorem 1.27, $I = \langle f_1, \dots, f_m \rangle$ for some $f_i \in k[x_1, \dots, x_n]$.

Lemma 4.2. *Adopt the notation as above, we have* $V(I) = \{(a_1, \dots, a_n) \in k^n | f_i(a_1, \dots, a_n) = 0$ *for all* f_i*'s*$\}$.

Proof. The '$\subseteq$' direction is by definition.

As for the '$\supseteq$' direction: For every $f \in I$, $f = h_1 f_1 + \dots h_m f_m$ for some $h_i \in k[x_1, \dots, x_n]$. If $f_i(a_1, \dots, a_n) = 0$ for all f_i's, then

$$f(a_1, \dots, a_n) = h_1(a_1, \dots, a_n) f_1(a_1, \dots, a_n) + \dots h_m(a_1, \dots, a_n) f_m(a_1, \dots, a_n) = 0.$$

Therefore, the point $(a_1, \dots, a_n) \in V(I)$. □

Example 4.3.
(a) Let $I = (0)$, then $V(I) = k^n$.
(b) Let $I = k[x_1, x_2, \dots, x_n]$, then $V(I) = \phi$.
(c) Let $I = \langle xy, x - yz \rangle$ in $k[x, y, z]$, then $V(I) = \{(x, y, z) | x = y = 0 \text{ or } x = z = 0\}$.
This implies that $f(y)$ is not in the ideal I.
(d) Let $I = \langle x^2 + x - 2 \rangle$, then $V(I) = \{-2, 1\}$.
Therefore, $x^{24} - 1$ is not in the ideal I.

Definition 4.4. Let $X \subseteq k^n$ be a subset, the **ideal** of X is

$$I(X) := \{f \in k[x_1, \dots, x_n] | f(x) = 0, \forall x \in X\}.$$

Lemma 4.5.
(a) $I(X)$ *is a radical ideal in* $k[x_1, \dots, x_n]$*, in other words,* $I(X) = \sqrt{I(X)}$.
(b) Let I *be an ideal in* $k[x_1, \dots, x_n]$*, then*

$$V(I) = V(\sqrt{I}).$$

Proof. a): For any elements $f, g \in I(X)$, $h \in k[x_1, \dots, x_n]$ and $x \in X$, we have

$$(f \pm g)(x) = f(x) \pm g(x) = 0; (fh)(x) = f(x)h(x) = 0.$$

Therefore, $I(X)$ is an ideal.

It is obvious that $I(X) \subset \sqrt{I(X)}$.

Let $f \in k[x_1, \dots, x_n]$ such that $f^m \in I(X)$ for some $m \in \mathbb{N}$. Then for any $x \in X$,

$$f^m(x) = 0 \implies f(x) = 0.$$

Therefore, $\sqrt{I(X)} = I(X)$.

b): Let $f \in \sqrt{I}$, then $f^m \in I$ for some $m \in \mathbb{N}$. For any $x \in V(I)$,

$$f^m(x) = 0 \implies f(x) = 0.$$

Therefore, $x \in V(\sqrt{I})$ and $V(I) = V(\sqrt{I})$. □

Example 4.6. (a) Let $I = \langle x^2 \rangle$ in $k[x]$, then $V(I) = \{0\}$ and $I(V(I)) = \langle x \rangle$.

(b) Let $I = \langle xy, x - yz \rangle$ in $k[x, y, z]$, then $V(I) = \{(x, y, z) | x = y = 0 \text{ or } x = z = 0\}$ and $I(V(I)) = \langle x, yz \rangle$.

(c) $I(\phi) = k[x_1, \ldots, x_n]$; $I(k^n) = (0)$.

4.2. **Weak Nullstellensatz.**

Theorem 4.7. *Let $k \subset K$ be fields with $K = k[s_1, \ldots, s_n]$ for some $s_1 \ldots, s_n \in K$. Then the field K is finite/integral/algebraic over k.*

Remark 4.8. An element s is algebraic over a field F if and only if it is integral over F.

By Corollary 3.25 and 3.30, the statements that 'K is finite/integral/algebraic over k' are all equivalent.

Proof of Theorem 4.7. We prove by induction on the number of generators n.

When $n = 1$, since $k[s_1] = K$ is a field, the generator s_1 has an inverse

$$\frac{1}{s_1} = a_n s_1^n + \cdots + a_0$$

for some $a_i \in k$. Therefore, the element s_1 is algebraic/integral over k. By Proposition 3.28, $k[s_1]$ is finite over k.

Assume the statement holds for $n-1$ generators case, we consider the case when $K = k[s_1, \ldots, s_n]$.

CASE I: The generator s_n is algebraic/integral over k.

By Proposition 3.28, the ring $k[s_n]$ is integral over k. By Proposition 3.37, the ring $k[s_n]$ is a field. Consider the tower of fields extensions:

$$k \subset k[s_n] \subset (k[s_n])[s_1, \ldots, s_{n-1}] = K.$$

By induction, $K = (k[s_n])[s_1, \ldots, s_{n-1}]$ is finite over $k[s_n]$. By the argument for the one generator case, $k[s_n]$ is finite over k. By Tower Law Lemma 3.29, K is finite over k.

CASE II: The generator s_n is NOT algebraic over k. We will show that this would finally lead to a contradiction!

Step 1: The smallest subfield in K containing $k[s_n]$ is

$$F = \{f(s_n)(g(s_n))^{-1} | f(x), g(x) \in F[x]\}.$$

Since s_n is assumed to be non-algebraic, one may check that F is isomorphic to the rational function field with coefficient in k.

Step 2: Note that $K = F[s_1, \ldots, s_{n-1}]$, by induction, K is integral over F.

Since each s_i is integral over F, there exists $A_{ij} \in F$ such that

$$s_i^{n_i} + A_{i1} s_i^{n_i - 1} + \cdots + A_{in_i} = 0.$$

By Step 1, each $A_{ij} = \frac{P_{ij}(s_n)}{Q_{ij}(s_n)}$ for some $P_{ij}(x), Q_{ij}(x) \in k[x]$. Let $Q(x) := \prod_{1 \leq i \leq n} \prod_{1 \leq j \leq n_i} Q_{ij}(x)$. Then $s_1, \ldots, s_{n-1}$ are also integral over $k[s_{n-1}, (Q(s_n))^{-1}]$. By Proposition 3.37, $k[s_{n-1}, (Q(s_n))^{-1}]$ must be a field.

Step 3: We show that there exists an element in $k[s_n]$ that does not have an inverse in $k[s_n, (Q(s_n))^{-1}]$.

When $Q(x)$ is a constant function, then $k[s_n, (Q(s_n))^{-1}] = k[s_n] \simeq k[x]$ is NOT a field.

When $Q(x)$ is not a constant function, then inverse of $Q(s_n)+1$ is in $k[s_n, (Q(s_n))^{-1}]$, hence of the form $\frac{f(s_n)}{(Q(s_n))^m}$ for some $f(x) \in k[x]$ and $m \in \mathbb{Z}_{\geq 0}$. Therefore, $(Q(s_n))^m = (Q(s_n)+1)f(s_n)$. Since s_n is not algebraic over F, we must have

$$(Q(x))^m = (Q(x)+1)f(x).$$

This is NOT possible since $\gcd(Q(x), Q(x)+1) = 1$.

We get the contradiction for Case II. Hence the generator s_n must be algebraic over k. □

4.3. **Maximal Ideals in $\mathbb{C}[x_1, \ldots, x_n]$.** Let k be a field, recall from Example 2.20 that for any $a_1, \ldots, a_n \in k$, the ideal

$$\mathfrak{m}_{a_1,\ldots,a_n} := \langle x_1 - a_1, \ldots, x_n - a_n \rangle$$

is a maximal ideal in $k[x_1, \ldots, x_n]$. When the field F is algebraically closed, we proved that every maximal ideal in $k[x_1, \ldots, x_n]$ is of this form.

Theorem 4.9. *Let k be an algebraically closed field, then every maximal ideal $\mathfrak{m} =$ in $k[x_1, \ldots, x_n]$ is of the form*

$$\langle x_1 - a_1, \ldots, x_n - a_n \rangle,$$

for some $a_1, \ldots, a_n \in k$.

Remark 4.10. A field F is algebraically closed, if and only if for every field extension $F \subset K$ and every element s algebraic over F, we have $s \in F$.

For example, the complex number field is algebraic closed

Proof of Theorem. By Proposition 2.15, $k[x_1, \ldots, x_n]/\mathfrak{m}$ is a field. Consider the field extension

$$k \subset k[x_1 + \mathfrak{m}, \ldots, x_n + \mathfrak{m}].$$

By Theorem 4.7, $k[x_1 + \mathfrak{m}, \ldots, x_n + \mathfrak{m}]$ is algebraic over k. Since k is algebraically closed, $k = k[x_1 + \mathfrak{m}, \ldots, x_n + \mathfrak{m}]$. Therefore, for each $x_i + \mathfrak{m}$, we have

$$x_i + \mathfrak{m} = a_i + \mathfrak{m}$$

for some $a_i \in k$. Therefore, $\mathfrak{m} \supseteq \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ which is already a maximal ideal. They must be the same. □

Theorem 4.11. *Let k be an algebraically closed field. Let I be an ideal in $k[x_1, \ldots, x_n]$ such that $V(I) = \phi$, then $I = k[x_1, \ldots, x_n]$.*

Proof. Suppose I is a proper ideal, by Proposition 2.18, $I \subset \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. By Theorem 4.9, $V = (\mathfrak{m}) = (a_1, \ldots, a_n)$ for some $a_1, \ldots, a_n \in k$. By Lemma 4.20, $V(I) \supset V(\mathfrak{m})$ and is not empty.

We get the contradiction. The ideal is therefore not proper. □

Remark 4.12. Both results fail without the algebraically closed assumption.

Example 4.13. What is the ideal $I = \langle xy, x^4 + y^5, x^2 + y^2 + 1 \rangle$ in $\mathbb{R}[x, y]$?

Consider the ideal $J = \langle xy, x^4 + y^5, x^2 + y^2 + 1\rangle$ in $\mathbb{C}[x, y]$. Its variety is

$V(\langle xy, x^4+y^5, x^2+y^2+1\rangle) = \{xy = x^4+y^5 = 0 = x^2+y^2+1\} = \{x = y = 0 = x^2+y^2+1\} = \phi.$

By Theorem 4.11, $J = \mathbb{C}[x, y]$, in particular, $1 \in J$. In other words,

$$1 = xyf(x, y) + (x^4 + y^5)g(x, y) + (x^2 + y^2 + 1)h(x, y)$$

for some $f, g, h \in \mathbb{C}[x, y]$. By taking the conjugates on both sides, we have

$$1 = xy\overline{f}(x, y) + (x^4 + y^5)\overline{g}(x, y) + (x^2 + y^2 + 1)\overline{h}(x, y).$$

Therefore,

$$1 = xy\left(\frac{f + \overline{f}}{2}\right)(x, y) + (x^4 + y^5)\left(\frac{g + \overline{g}}{2}\right)(x, y) + (x^2 + y^2 + 1)\left(\frac{h + \overline{h}}{2}\right)(x, y).$$

Here the polynomials $\left(\frac{f+\overline{f}}{2}\right)(x, y)$ (g, h respectively) are all with real coefficients. Therefore they are all in $\mathbb{R}[x, y]$. Hence $1 \in I$. We have $I = \mathbb{R}[x, y]$.

4.4. **Nullstellensatz.**

Theorem 4.14. *Let k be an algebraically closed field, I an ideal in $k[x_1, \dots, x_n]$. Let $f \in k[x_1, \dots, x_n]$ such that $f(V(I)) = 0$. Then $f^t \in I$ for some $t \in \mathbb{Z}_{\geq 1}$.*

Proof. By Hilbert bases theorem, the ideal $I = \langle f_1, \dots, f_m\rangle$ for some $f_i \in k[x_1, \dots, x_n]$. We consider the ideal

$$J := \langle f_1, \dots, f_m, yf - 1\rangle$$

in the ring $k[x_1, \dots, x_n, y]$.

The variety of J is

$$\begin{aligned} V(J) &= \{(a_1, \dots, a_n, b) \in k^{n+1} | f_i(a_1, \dots, a_n) = 0 \text{ for every } i; f(a_1, \dots, a_n)b = 1\} \\ &= \{(a_1, \dots, a_n, b) \in k^{n+1} | (a_1, \dots, a_n) \in V(I); f(a_1, \dots, a_n)b = 1\} \\ &= \{(a_1, \dots, a_n, b) \in k^{n+1} | (a_1, \dots, a_n) \in V(I); 0b = 1\} = \phi. \end{aligned}$$

By Theorem 4.11, $J = k[x_1, \dots, x_n, y]$. In particular, $1 \in J$:

$$1 = h_1f_1 + \cdots + h_mf_m + g(yf - 1),$$

for some $h_1, \dots, h_m, g \in k[x_1, \dots, x_n, y]$.

Substitute $y = \frac{1}{f}$, we have

$$1 = h_1(x_1, \dots, x_n, \frac{1}{f})f_1(x_1, \dots, x_n) + \cdots + h_m(x_1, \dots, x_n, \frac{1}{f})f_m(x_1, \dots, x_n),$$

which is an equality of elements in $k(x_1, \dots, x_n)$, the rational function field of $k[x_1, \dots, x_n]$.

Note that there exists an t large enough such that

$$h_i(x_1, \dots, x_n, \frac{1}{f}) = \frac{H_i(x_1, \dots, x_n)}{f^t}$$

for every i and some $H_i(x_1,\dots,x_n) \in k[x_1,\dots,x_n]$. Therefore,

$$f^t = H_1(x_1,\dots,x_n)f_1(x_1,\dots,x_n) + \cdots + H_m(x_1,\dots,x_n)f_m(x_1,\dots,x_n) \in I.$$

□

Corollary 4.15. *Let k be an algebraically closed field, J be an ideal in $k[x_1,\dots,x_n]$. Then $I(V(J)) = \sqrt{J}$.*

Proof.

$$f \in \sqrt{J} \iff f^t \in J \text{ for some } t \iff f(V(J)) = 0 \iff f \in I(V(J)).$$

□

Example 4.16. Let $I = \langle x^2y^3, (x^2+y^2)^3 - 4x^2y^2\rangle$ in $\mathbb{C}[x,y]$, then I is primary.

Solution. We first compute the radical of I. The variety of I is

$$V(I) = \{(x,y) | x^2y^3 = (x^2+y^2)^3 - 4x^2y^2 = 0\}.$$

Note that $x^2y^3 = 0$ implies $x = 0$ or $y = 0$. If $x = 0$, then by the second equation, we have $y = 0$. If $y = 0$, then by the second equation, we have $x = 0$. Therefore, $V(I) = \{(0,0)\}$.

The ideal $I(\{(0,0)\}) = \{f(x,y) | f(0,0) = 0\} = \langle x, y\rangle$. By Corollary 4.15, the radical $\sqrt{I} = I(V(I)) = \langle x, y\rangle$, which is a maximal ideal. The I is primary by the following lemma. □

Lemma 4.17. *Let I be an ideal in R such that $\sqrt{I}$ is maximal, then I is primary.*

Proof. Since $I \subseteq \sqrt{I}$ which is proper, the ideal I is also proper.

Let $fg \in I$, if $g \notin \sqrt{I}$, then since $R/\sqrt{I}$ is field, the element $g + \sqrt{I}$ is a unit in $R/\sqrt{I}$. In particular, $m + gr = 1$ for some $m \in \sqrt{I}$ and $r \in R$.

Suppose $m^n \in I$, as $1 = (m+gr)^n = m^n + sg$ for some s, we have $f = fm^n + sfg \in I$. Therefore, the ideal I is primary. □

Example 4.18. Let $I = \langle x^2y^3, (x^2+y^2)^2 - x^3 + 3xy^2\rangle$ in $\mathbb{C}[x,y]$, what is the radical of I? Is I primary?

Solution. The variety of I is $\{(0,0)\} \cup \{(1,0)\}$.

The ideal $I(\{(0,0)\} \cup \{(1,0)\})$ contains y and $x(x-1)$. We claim that $I(V(I))$ is generated by these two elements.

Note that for every $f(x,y) \in \mathbb{C}[x,y]$, we have $f(x,y) = yg(x,y) + h(x)$ for some $g(x,y) \in \mathbb{C}[x,y]$ and $h(x) \in \mathbb{C}[x]$. If $f \in I(\{(0,0)\} \cup \{(1,0)\})$, then $h(0) = h(1) = 0$. Hence, $x(x-1) | h(x)$. In particular, $f \in \langle x(x-1), y\rangle$. Therefore,

$$\sqrt{I} = I(V(I)) = \langle x(x-1), y\rangle.$$

This is not a prime ideal: $x(x-1) \in \sqrt{I}$ but $x, x-1 \notin \sqrt{I}$. Therefore, I is not primary. □

4.5. **Varieties in $\mathbb{C}^n$.**

Proposition 4.19. *There is a one-to-one correspondence:*

$$V : \{\textit{radical ideals in } \mathbb{C}[x_1, \ldots, x_n]\} \longleftrightarrow \{\textit{varieties in } \mathbb{C}^n\}.$$

Proof. Let J be a radical ideal in $\mathbb{C}[x_1, \ldots, x_n]$, by 0-satz, $I(V(J)) = \sqrt{J} = J$.

Let $X = V(J)$ be a variety, by Lemma 4.5 b), $X = V(\sqrt{J})$. By 0-satz, $V(I(X)) = V(I(V(J))) = V(\sqrt{J}) = X$. □

Lemma 4.20. *Let X and Y be subspaces in k^n, A and B be subsets in $k[x_1, \ldots, x_n]$, and I, J be ideals in $k[x_1, \ldots, x_n]$. Then*

(a) If $X \subset Y \subset k^n$, then $I(X) \supset I(Y)$.
If $A \subset B \subset k[x_1, \ldots, x_n]$, then $V(A) \supset V(B)$.

(b) $I(X \cup Y) = I(X) \cap I(Y)$;
$V(I \cap J) = V(IJ) = V(I) \cup V(J)$;
$V(I + J) = V(I) \cap V(J)$.

Proof. a): For $\forall f \in I(Y)$, $f(x) = 0$ for any $x \in Y$ therefore any $x \in X$. Hence, $f \in I(X)$.

b): By a), $I(X \cup Y) \subset I(X) \cap I(Y)$. For any $f \in I(X) \cap I(Y)$ and any $x \in X \cup Y$, since x is either on X or Y, $f(x)$ is always 0.

Let $x \in V(I_1 \cap I_2)$, suppose $x \notin V(I_1) \cup V(I_2)$, then $\exists f_1 \in I_1$ and $f_2 \in I_2$ such that $f_1(x), f_2(x) \neq 0$. In particular, $(f_1 f_2)(x) \neq 0$. But $f_1 f_2 \in I_1 \cap I_2$, and we get the contradiction.

The rest one is easy. □

In particular, the intersection and union of varieties are varieties.

More relations (NOT examinable):

$\sqrt{I}$ is a prime ideal $\iff$	$V(I)$ is **irreducible**;
$\sqrt{I}$ is a maximum ideal $\iff$	$V(I)$ is a point;
$\dim \mathbb{C}[x_1, \ldots, x_n]/I =$	Dimension of $V(I)$;
A maximum ideal $\mathfrak{m}$ containing $I \longleftrightarrow$	A point $P_{\mathfrak{m}}$ on $V(I)$;
$\mathfrak{m}/\mathfrak{m}^2 =$	Cotangent space at $P_{\mathfrak{m}}$.

4.6. **Irreducible Varieties.**

Definition 4.21. An variety X is called **irreducible** if it is non-empty and is NOT the union of two proper varieties, i.e.,

if $X = X_1 \cup X_2$ for some varieties X_1 and X_2, then either X_1 or X_2 is X.

Proposition 4.22. *Let X be a variety in $\mathbb{C}^n$, then*

$$X \textit{ is irreducible} \iff I(X) \textit{ is prime.}$$

Proof. '$\implies$': For $\forall fg \in I(X)$,

$$X = V(I(X)) \subseteq V(fg) = V(f) \cup V(g)$$

$$\implies X = V(I(X)) = (V(I(X)) \cap V(f)) \cup (V(I(X)) \cap V(g)) = V(I + \langle f \rangle) \cup V(I + \langle g \rangle)$$

As X is irreducible, either $V(I(X)) \cap V(f))$ or $(V(I(X)) \cap V(g)$ is X. Therefore, either X is contained in either $V(f)$ or $V(g)$. Hence, f or $g \in I(X)$.

'$\Longleftarrow$': Let $X = X_1 \cup X_2 = V(J_1) \cup V(J_2)$ for some $J_i = \sqrt{J_i}$. Then $I(X) = J_1 \cap J_2$. Since $I(X)$ is prime, either J_1 or $J_2 = I$. □

Example 4.23. Let the whole space be $\mathbb{C}^2$:

(a) $X = \{(0,0)\}$ is irreducible;
(b) $X = \{(0,0)\} \cup \{(1,0)\}$ is not irreducible;
(c) $X = \{x = 0\} \cup \{y = 0\}$ is not irreducible;
(d) $X = \mathbb{C}^2$;
(e) $X = \{(t^2, t^3) | t \in \mathbb{C}\}$;

Corollary 4.24. *Let X be an irreducible variety in $\mathbb{C}^n$. If $X \subseteq X_1 \cup \cdots \cup X_n$ for some varieties $X_1, \ldots, X_n$, then $X \subseteq X_i$ for some i.*

Proof. Note that $X = (X \cap X_1) \cup (X \cap X_2) \cup \cdots \cup (X \cap X_n)$. By Lemma 4.20, the set $X \cap X_1$ and $(X \cap X_2) \cup \cdots \cup (X \cap X_n)$ are both varieties in $\mathbb{C}^n$. Since X is irreducible, $X = X \cap X_1$ or $X = (X \cap X_2) \cup \cdots \cup (X \cap X_n)$. By induction on the numbers of varieties, $X = X \cap X_i$ for some i. □

Proposition 4.25. *Let X be a variety in $\mathbb{C}^n$, then X has a decomposition*

$$X = X_1 \cup \cdots \cup X_m$$

with each X_i an irreducible variety.

By omitting some terms if necessary, one can arrange the expression such that $X_i \not\subseteq X_j$ for any $i \neq j$. Then this expression is unique up to renumbering the components.

Each X_i is called an irreducible component of X.

Proof. By Theorem 2.27, the ideal $I(X)$ admits a primary decomposition in $\mathbb{C}[x_1, \ldots, x_n]$. We may write

$$I(X) = Q_1 \cap \cdots \cap Q_n$$

with each Q_i primary.

By taking V on both sides, Proposition 4.19, and Lemma 4.20, we have

$$\begin{aligned} X &= V(I(X)) = V(Q_1 \cap \cdots \cap Q_m) \\ &= V(Q_1) \cup \cdots \cup V(Q_m) \\ &= V(\sqrt{Q_1}) \cup \cdots \cup V(\sqrt{Q_m}) = X_1 \cup \cdots \cup X_m \end{aligned}$$

By Lemma 2.23, each ideal $\sqrt{Q_i}$ is prime. By Proposition 4.22, each variety X_i is irreducible.

As for the uniqueness, let

$$X = X_1 \cup \cdots \cup X_m = Y_1 \cup \ldots Y_t$$

be two irredundant irreducible decompositions, in other words, all X_i, Y_j's are irreducible varieties, $X_i \not\subseteq X_j$, and $Y_i \not\subseteq Y_j$ for any $i \neq j$.

Then for every i, we have $X_i \subseteq Y_1 \cup \dots Y_t$. By Corollary 4.24, $X_i \subseteq Y_j$ for some j. Since $Y_j \subseteq X_1 \cup \dots \cup X_m$, by Corollary 4.24, $Y_j \subseteq X_k$ for some k. Hence, $X_i \subseteq Y_j \subseteq X_k$. As $X_i \not\subseteq X_k$ for any $i \neq k$, we must have $i = k$ and $X_i = Y_j$.

Therefore, $\{X_1, \dots, X_m\} = \{Y_1, \dots, Y_t\}$. □

Example 4.26. Let $f(x, y)$ and $g(x, y)$ be two polynomials with coefficient in $\mathbb{C}$ such that $\gcd(f, g) = 1$. Then the equation $f(x, y) = g(x, y) = 0$ has only finitely many solutions.

Proof. By Lemma 4.2 and Proposition 4.25,

$$\begin{aligned} &\{(a, b) \in \mathbb{C}^2 | f(a, b) = g(a, b) = 0\} \\ =&V(\langle f(x, y), g(x, y)\rangle) \\ =&X_1 \cup X_2 \cup \dots \cup X_m \end{aligned}$$

for some irreducible varieties $X_1, \dots, X_m$.

$$\begin{aligned} & V(\langle f, g\rangle) \supseteq X_i \\ \Longrightarrow\ & f(x) = g(x) = 0 \text{ for every point } x \in X_i. \\ \Longrightarrow\ & f, g \in I(X_i)\ (I(X_i) \text{ is a prime ideal}). \end{aligned}$$

Suppose $I(X_i) = \langle h\rangle$ for some $h \neq 0$, then $\gcd(f, g) \neq 1$. Therefore, each prime ideal $I(X_i)$ is NOT principally generated.

Lemma 4.27. *Let P be a prime ideal in $\mathbb{C}[x, y]$. Suppose $P \neq \langle h(x, y)\rangle$ for any $h(x, y)$, then P is a maximal ideal.*

Proof. Let $F_1(x, y)$ be a non-zero element in P with the minimum degree Deg_y. As P is a prime ideal, we may assume $F_1(x, y)$ is irreducible. We write

$$F_1(x, y) = f_1(x)y^{n_1} + \dots,$$

where $\mathrm{Deg}_y F_1(x, y) = n_1$ and $f_1(x) \in F[x]$ is the leading coefficient.

Let $F_2(x, y)$ be with the minimum degree Deg_y among all elements in $P \setminus \langle F_1(x, y)\rangle$, which is non-empty by the condition in the lemma. We write

$$F_2(x, y) = f_2(x)y^{n_2} + \dots,$$

where $\mathrm{Deg}_y F_2(x, y) = n_2$ and $f_2(x) \in F[x]$ is the leading coefficient.

Let

$$\tilde{F}_2(x, y) := f_1(x)F_2(x, y) - f_2(x)y^{n_2 - n_1}F_1(x, y),$$

, then

- $\mathrm{Deg}_y \tilde{F}_2 < \mathrm{Deg} F_2$;
- $\tilde{F}_2 \in P$.

By the minimum assumption on $\mathrm{Deg}_y F_2(x, y)$ among all elements in $P \setminus \langle F_1(x, y)\rangle$, we must have

$$\tilde{F}_2 \in \langle F_1\rangle \implies f_1(x)F_2 \in \langle F_1\rangle \implies f_1(x)F_2(x, y) = H(x, y)F_1(x, y)$$

for some $H(x, y) \in \mathbb{C}[x, y]$. Since $F_1(x, y)$ is irreducible and can divide $f_1(x)$, it must be $x - a$ for some $a \in \mathbb{C}$. Therefore, $P \ni x - a$.

Repeat the same argument for $(\mathbb{C}[y])[x]$ by viewing x as the main variable, we have $P \ni y - b$ for some $b \in \mathbb{C}$. Therefore, $P = \langle x - a, y - b \rangle$. □

Back to the proof of the example, by the lemma, we have

$$V(\langle f, g \rangle) = \{(a_1, b_1)\} \cup \dots \{(a_m, b_m)\}.$$

□

Example 4.28. Let f_1, f_2, f_3 be different irreducible polynomials in $\mathbb{C}[x, y, z]$ such that $f_i \notin \langle f_j, f_k \rangle$. Then $V(\langle f, f_2, f_3 \rangle)$ needs NOT to be finite. For example, $xz - y^2$, $yz - x^3$ and $z^2 - x^2y$.

5. Primary Decomposition

5.1. Associated primes.

Definition 5.1. Let M be an R-module, and $m \in M$. The **annihilator** of m is the set:

$$ann(m) := \{r \in R | rm = 0\}.$$

Definition 5.2. Let M be an R-module. An ideal $P \triangleleft R$ is called an **associated prime** of M if P is a prime ideal and $P = ann(m)$ for some $m \in M \setminus \{0\}$.

The **assassin** $\text{ass}(M)$ is the set of associated primes of an R-module M.

Remark 5.3. The annihilator $\text{ann}(m)$ is always an ideal, but it needs not to be prime.

The annihilator $\text{ann}(r)$ is the whole ring if and only if $r = 0$.

Example 5.4.
(a) Let $R = F$ be a field and M be a finite dimensional vector space. Then $\text{ann}(v) = (0)$ for every non-zero vector v. In particular, $\text{ass}(M)$ is $\{(0)\}$.
(b) Let R be an integral domain, and $M = I$ be an ideal as an R-module then $\text{ann}(r) = (0)$ for every non-zero r. In particular, $\text{ass}(M)$ is $\{(0)\}$.
(c) $R = \mathbb{Z}$ and $M = \mathbb{Z}/6\mathbb{Z}$, then $\text{ass}(M)$ is $\{\langle 2\rangle, \langle 3\rangle\}$.

Let X be a variety in $\mathbb{C}^n$ with an irreducible decomposition

$$X = X_1 \cup \cdots \cup X_m$$

such that $X_i \not\subseteq X_j$ for any $i \neq j$.

Let $R = \mathbb{C}[x_1, \ldots, x_n]$ and $M = R/I(X)$ be an R-module. We claim that $\text{Ass}(R/I) \supseteq \{I(X_1), \ldots, I(X_m)\}$. We only need to prove the $I(X_1)$ case for example.

Since the decomposition is irredundant, by Corollary 4.24,

$$X \supsetneq X_2 \cup X_3 \cdots \cup X_m.$$

By Proposition 4.19, there exists

$$f \in I(X_2 \cup X_3 \cdots \cup X_m) \setminus I(X) \neq \phi.$$

We compute the annihilator of $f + I(X)$:

$$\begin{aligned}
\text{ann}(f + I(X)) &= \{g | g(f + I(X)) = 0 + I(X)\} \\
&= \{g | gf \in I(X)\} = \{g | gf(x) = 0, \forall x \in X\} \\
&= \{g | gf(x) = 0, \forall x \in I(X_1)\} \\
&= \{g | (gf)^m \in I(X_1)\} = \{g | gf \in I(X_1)\} = I(X_1).
\end{aligned}$$

Therefore, $I(X_1) \in \text{Ass}(R/I(X))$.

Lemma 5.5. *Let M be a non-zero module over a Noetherian ring R, then $ass(M) \neq \phi$.*

Proof. Let $\mathcal{S} := \{ann(m) | m \in M \setminus \{0\}\}$. Then S is non-empty since M is non-zero.

Every ideal in S is proper as $1 \notin ann(m)$. Since R is Noetherian, S has a maximal element $ann(m)$.

Claim: $\text{ann}(m)$ is a prime ideal.

Proof for the claim: Let $fg \in$ann(m), then $fgm = 0$. If $f \notin$ann(m) which is iff $fm \neq 0$, then we may consider ann$(fm) \in \mathcal{S}$. Note that

- ann$(fm) \supset$ann(m);
- $g \in$ann(fm).

By the maximum assumption on I, we must have ann(m) =ann(fm). Therefore, $g \in$ann(fm) =ann(m). The ideal ann(m) is by definition prime. □

In particular, ass(M) is non-empty. □

Proposition 5.6. *Let Q be a primary ideal in a Noetherian ring R, then*

$$\text{ass}(R/Q) = \{\sqrt{Q}\}.$$

Proof. Let $r \in R \setminus Q$. If $s(r+Q) = 0 + Q$ for some $s \in R$, then $rs \in Q$. Since $r \notin Q$ and Q primary, the element s must be in $\sqrt{Q}$. Therefore,

$$Q \subseteq ann(r) \subseteq \sqrt{Q}.$$

As the radical of a prime ideal is itself, if ann(r) is prime, it can only be $\sqrt{Q}$. Hence, ass$(R/Q) \subset \{\sqrt{Q}\}$. By Lemma 5.5, ass$(R/Q) = \{\sqrt{Q}\}$. □

Lemma 5.7. *Let $\phi : M \to N$ be an injective R-mod homomorphism, then $ann(m) = ann(\phi(m))$. In particular,*

$$ass(M) \subseteq ass(N).$$

Proof. $a \in ann(m) \iff am = 0 \iff \phi(am) = 0 \iff a\phi(m) = 0 \iff a \in ann(\phi(m))$. □

Lemma 5.8. *Let $M_1, \dots, M_s$ be R-modules, then*

$$ass(\oplus_{i=1}^s M_i) = \cup_{i=1}^s ass(M_i).$$

Proof. Since M_i is a submodule of $\oplus_{i=1}^s M_i$, '$\supseteq$' holds.

Suppose a prime $P = ann((m_1, \dots, m_s))$ is not in any ass(M_i).

Then $P \subsetneq ann(m_i)$ and $P = \cap_{i=1}^s ann(m_i)$. Contradict the fact that P is irreducible. □

Definition 5.9. An ideal Q is called **P-primary** if Q is primary and $\sqrt{Q} = P$.

Lemma 5.10. *Let Q_1 and Q_2 be two primary ideals such that $\sqrt{Q_1} = \sqrt{Q_2}$, then $Q_1 \cap Q_2$ is primary.*

Proof. Let $fg \in Q_1 \cap Q_2$, then either $g \in \sqrt{Q_1} = \sqrt{Q_2}$, or $f \in Q_1 \cap Q_2$. □

Corollary 5.11. *Let R be a Noetherian ring and $I = Q_1 \cap \dots \cap Q_r$ be a minimum primary decomposition. Then $\sqrt{Q_i} \neq \sqrt{Q_j}$ when $i \neq j$.*

Theorem 5.12. *Let R be a Noetherian ring and $I = Q_1 \cap Q_2 \cap \dots \cap Q_r$ be a primary decomposition. Then*

$$ass(R/I) \subseteq \{\sqrt{Q_1}, \dots, \sqrt{Q_r}\}.$$

If the decomposition is irredundant, then the above is an equality. In particular, an irredundant decomposition with $\sqrt{Q_i} \neq \sqrt{Q_j}$ for $i \neq j$ is minimal.

Proof. Consider the module $M := \oplus_{i=1}^r R/Q_i$, by Proposition 5.6 and Lemma 5.8,

$$ass(M) = \{\sqrt{Q_1}, \dots, \sqrt{Q_r}\}.$$

Consider the R-mod homomorphism:

$$\phi : R \to M$$
$$r \mapsto (r + Q_1, \dots, r + Q_r).$$

The ideal I is the kernel. Therefore, ϕ induces an injective morphism from R/I to M. By Lemma 5.7, $\text{ass}(R/I) \subseteq \{\sqrt{Q_1}, \dots, \sqrt{Q_r}\}$.

If the decomposition is irredundant, then $I \subsetneqq \bigcap_{i \neq j} Q_i = J_i$ for any $1 \leq j \leq r$.

The image $\phi(J_i/I)$ is not 0 in M. By Lemma 5.5, $\text{ass}(\phi(J_i/I))$ is non-empty. Note that the image $\phi(J_i/I)$ is contained in the component R/Q_i, by Lemma 5.7 and Proposition 5.6, $\text{ass}(J_i/I) = \{\sqrt{Q_i}\}$.

By Lemma 5.7 again,

$$\{\sqrt{Q_1}, \dots, \sqrt{Q_r}\} = \cup_i ass(J_i/I) \subseteq ass(R/I) \subseteq \{\sqrt{Q_1}, \dots, \sqrt{Q_r}\}.$$

□

Theorem 5.13. *Let I be a proper ideal in a Noetherian ring R. Let P be a minimal prime ideal in Ass(R/I), in other words, $P \not\supseteq P'$ for any other $P' \in \text{Ass}(R/I)$. Then for any minimal primary decomposition of $I = Q_1 \cap \cdots \cap Q_m$, the factor Q_i with $\sqrt{Q_i} = P$ is given as*

$$\{r \in R | rf \in I \textit{ for some } f \notin P\}.$$

In particular, the factor Q_i does not rely on the decomposition.

Proof. '$\supseteq$': If $rf \in I \subset Q_i$ for some $f \notin P$, then since Q_i is primary and $f \notin \sqrt{Q_i} = P$, we must have $r \in Q_i$.

'$\subseteq$': By the condition in the statement, $P \not\supseteq \sqrt{Q_j}$ for any $j \neq i$. As the prime ideal P is radical, $P \not\supseteq Q_j$ for any $j \neq i$.

There exists $f_j \in Q_j \setminus P$ for every $j \neq i$.

As P is a prime ideal, $f := f_1 \dots f_{i-1} f_{i+1} \dots f_m \notin P$. For every $r \in Q_i$, we have $rf \in Q_1 \cap \cdots \cap Q_{i-1} \cap Q_{i+1} \cap \cdots \cap Q_m \cap Q_i = I$. Hence, the '$\subseteq$' part holds. □

Remark 5.14. In some examples that of I that $\text{Ass}(R/I)$ has non-minimal prime ideals, there could be more than one minimal primary decompositions for I. For example, let $I = \langle xy, y^2 \rangle$ in $\mathbb{C}[x, y]$, then I has the following different minimal primary decompositions:

$$I = \langle y \rangle \cap \langle x^2, xy, y^2 \rangle = \langle y \rangle \cap \langle x^3, xy, y^2 \rangle = \langle y \rangle \cap \langle x^m, xy, y^2 \rangle.$$

The non-minimal factor $\langle x, y \rangle$ in $\text{Ass}\mathbb{C}[x, y]/I$ may appear in infinitely many different forms.

Example 5.15. Find a minimal primary decomposition for $I = \langle 20, x^2 + 1 \rangle$ in $\mathbb{Z}[x]$

Note that the number 20 has an obvious factorization as 4×5, we may expect $I = I_4 \cap I_5$, where $I_4 = \langle 4, x^2+1 \rangle$ and $I_5 = \langle 5, x^2+1 \rangle$. This is indeed that case since

$$I = \{(x^2+1)f(x) + 20ax + 20b | f(x) \in \mathbb{Z}[x], a, b \in \mathbb{Z}\};$$
$$I_4 = \{(x^2+1)f(x) + 4ax + 4b | f(x) \in \mathbb{Z}[x], a, b \in \mathbb{Z}\};$$
$$I_5 = \{(x^2+1)f(x) + 5ax + 5b | f(x) \in \mathbb{Z}[x], a, b \in \mathbb{Z}\}.$$

Moreover, the injective map $\mathbb{Z}[x]/I \to \mathbb{Z}[x]/I_4 \oplus \mathbb{Z}[x]/I_5$ must be also surjective since the number of elements in the modules are both 400. By Lemma 5.8,

$$\text{Ass}(\mathbb{Z}[x]/I) = \text{Ass}(\mathbb{Z}[x]/I_4) \cup \text{Ass}(\mathbb{Z}[x]/I_5).$$

We first show that I_4 is primary:

$$4 \in I_4 \implies 2 \in \sqrt{I_4}.$$

In particular, $2x \in \sqrt{I_4}$. Since $(x+1)^2 - 2x \in \sqrt{I_4}$, we have $x+1 \in \sqrt{I_4}$.

The ideal $\langle 2, x+1 \rangle$ is maximal since $\mathbb{Z}[x]/\langle 2, x+1 \rangle \simeq \mathbb{F}_2$, which is a field. Therefore, I_4 is primary.

As for $I_5 = \langle 5, x^2+1 \rangle$, note that $x^2+1 \equiv (x+2)(x-2) (\text{mod} 5)$, we have the following isomorphisms as $\mathbb{Z}[x]$-modules:

$$\mathbb{Z}[x]/I_5 \simeq \mathbb{F}_5[x]/\langle x^2+\underline{1} \rangle \simeq \mathbb{F}_5[x]/\langle x+2 \rangle \oplus \mathbb{F}_5[x]/\langle x-2 \rangle \simeq \mathbb{Z}[x]/\langle 5, x+2 \rangle \oplus \mathbb{Z}[x]/\langle 5, x-2 \rangle.$$

Note that $\mathbb{Z}[x]/\langle 5, x+2 \rangle \simeq \mathbb{Z}[x]/\langle 5, x-2 \rangle \simeq \mathbb{F}_5$, which is a field. The ideals $\langle 5, x \pm 2 \rangle$ are all maximal. Therefore, $\text{Ass}(\mathbb{Z}[x]/I_5) = \{\langle 5, x-2 \rangle, \langle 5, x+2 \rangle\}$.

Combine the discussion on I_4 and I_5 together, we have

$$\text{Ass}(\mathbb{Z}[x]/I) = \{\langle 5, x-2 \rangle, \langle 5, x+2 \rangle, \langle 2, x+1 \rangle\}.$$

The unique minimal primary decomposition of I is $I = \langle 5, x-2 \rangle \cap \langle 5, x+2 \rangle \cap \langle 4, x^2+1 \rangle$.

6. Localisation and Normalisation

6.1. **Ring of fractions.**

Definition 6.1. Let R be a ring. A set U in R is called a **multiplicatively closed set** (**m.c.s**) if:

(a) $1 \in U$;
(b) $f, g \in U \implies fg \in U$.

Example 6.2. (a) Let $f \in R$, then $U = \{1, f, f^2, \dots\}$ is an m.c.s.
(b) Let $P \triangleleft R$ be a prime ideal, then $R \setminus P$ is an m.c.s.
(c) Let R be an integral domain, then $R \setminus (0)$ is an m.c.s.

Definition 6.3. Let R be a ring and $U \subseteq R$ be an m.c.s., the **ring of fractions** of R with respect to U is:

$$U^{-1}R := \{\frac{r}{u} | r \in R, u \in U\}/\sim,$$

where '$\sim$' is the equivalence relation defined by:

$$\frac{r}{u} \sim \frac{r'}{u'} \iff \exists v \in U \text{ such that } v(ru' - r'u) = 0.$$

The arithmetic operations on $U^{-1}R$ are:

$$\frac{r_1}{u_1} \pm \frac{r_2}{u_2} = \frac{r_1u_2 \pm r_2u_1}{u_1u_2}; \frac{r_1}{u_1} \cdot \frac{r_2}{u_2} = \frac{r_1r_2}{u_1u_2}.$$

Lemma 6.4. *Adopt the notation as above:*

(a) '$\sim$' is an equivalence relation;
(b) The operations on $U^{-1}R$ are well-defined and $(U^{-1}R, +, \cdot)$ is a ring;
(c) The map $\phi : R \to U^{-1}R$: $r \mapsto \frac{r}{1}$ is a ring homomorphism.

Proof. We only check the equivalence relation:

- Reflexive: $1(ru - ru) = 0$, therefore, $\frac{r}{u} \sim \frac{r}{u}$.
- Symmetric: suppose $\frac{r}{u} \sim \frac{r'}{u'}$, then $\exists v$ s.t. $v(ru' - r'u) = 0$, which means $v(r'u - ru') = 0$ and $\frac{r'}{u'} \sim \frac{r}{u}$.
- Transitivity, suppose $\frac{r}{u} \sim \frac{r'}{u'} \sim \frac{r''}{u''}$, then $\exists v, v'$ s.t. $v(ru' - r'u) = v'(r'u'' - r''u') = 0$.
$$v'u''(v(ru' - r'u)) + uv(v'(r'u'' - r''u')) = 0.$$
Since U is m.c., $vv'u' \in U$, we have $\frac{r}{u} \sim \frac{r''}{u''}$.

□

We make notations for some important ring of fractions.

Definition 6.5. Let R be a ring.

- Let $f \in R$ and $U_f := \{1, f, f^2, \dots, f^m, \dots\}$. We denote $R_f := R[\frac{1}{f}] = (U_f)^{-1}R$.
- Let P be a prime ideal. We denote
$$R_P := (R \setminus P)^{-1}R$$
and call it the **localisation** of R at P.

- Let R be an integral domain. We denote
$$\text{Frac}(R) := (R \setminus (0))^{-1}R$$
and call it the **field of fractions** of R.

Here are some more concrete examples of ring of fractions:

Example 6.6. (a) Let $R = \mathbb{Z}$, then $\text{Frac}(\mathbb{Z}) = \mathbb{Q}$.
The localisation of $\mathbb{Z}$ at $\langle 2 \rangle$ is
$$\mathbb{Z}_{\langle 2 \rangle} = \{\frac{a}{b} | a, b \in \mathbb{Z}, 2 \nmid b\} \subset \mathbb{Q}.$$
The ring of fractions $\mathbb{Z}_2$ is $\mathbb{Z}_2 = \mathbb{Z}[\frac{1}{2}] = \{\frac{a}{2^m} | a \in \mathbb{Z}, m \in \mathbb{Z}_{\geq 0}\} \subset \mathbb{Q}$.
(b) Let $R = \mathbb{Z}/6\mathbb{Z}$, we consider the ring of fractions: $(\mathbb{Z}/6\mathbb{Z})_{\underline{2}}$. The set $\{\frac{a}{b} | a \in \mathbb{Z}/6\mathbb{Z}, b \in \{\underline{1}, \underline{2}, \underline{4}\}\}$ has 18 elements. By definition of '$\sim$', $\frac{a}{b} \sim \frac{0}{1}$ if and only if $a = \underline{0}$ or $\underline{3}$. $\frac{a}{b} \sim \frac{1}{1}$ if and only if $a - b = \underline{0}$ or $\underline{3}$. $\frac{a}{b} \sim \frac{2}{1}$ if and only if $a - 2b = \underline{0}$ or $\underline{3}$. Therefore, $(\mathbb{Z}/6\mathbb{Z})_{\underline{2}} \simeq \mathbb{Z}/3\mathbb{Z}$.

6.2. **Localisation and local rings.**

Definition 6.7. A ring is called **local** if it has a unique maximal ideal.

Example 6.8. (a) A field k is a local ring;
(b) $k[x]/\langle x^m \rangle$ is a local ring, but it is not an integral domain;
(c) $\mathbb{Z}$, $k[x]$ are not local rings.

Lemma 6.9. *Let I be a proper ideal of R, then*
The ideal I is the unique maximal ideal of R $\iff$ every element in $R \setminus I$ is a unit.

Proof. '$\implies$': For $\forall r \in R \setminus I$, if $\langle r \rangle$ is not the whole ring, by Proposition 2.18, $\exists$ a maximal ideal $J \supset \langle r \rangle \nsubseteq I$. This invalidates the uniqueness of I. Therefore, $\langle r \rangle = R$ and $1 \in \langle r \rangle$, r is a unit.
'$\impliedby$': For $\forall J \lhd R$ s.t. $J \nsubseteq I$, $\exists x \in J \setminus I$. x is a unit by assumption, therefore $J = R$. □

Proposition 6.10. *Let P be a prime ideal of R, then $PR_P := P_P := \{\frac{r}{u} | r \in P, u \notin p\}$ is the unique maximal ideal in R_P.*

Proof. For any elements $\frac{r}{u}, \frac{r'}{u'} \in PR_P$, and $\frac{a}{b} \in R_P$: $\frac{r}{u} + \frac{r'}{u'} = \frac{ur' + u'r}{uu'} \in PR_P$; $\frac{r}{u}\frac{a}{b} = \frac{ra}{ub} \in PR_P$.
If $1 \sim \frac{r}{u}$, then $\exists v \notin P$ such that $v(r - u) = 0 \implies vr = vu \notin P$ as P is prime. Therefore, $r \notin P$ and $1 \notin PR_P$.
We have shown that PR_P is a proper ideal in R_P.
$\forall \frac{r}{u} \in R_P \setminus PR_P \implies r \notin P \implies \frac{u}{r} \in R_P \implies \frac{r}{u}$ is a unit in R_P. By Lemma 6.9, PR_P is the unique maximal ideal in R_P. □

Example 6.11. (a) The ring $\mathbb{Z}_{\langle 3 \rangle}$ is a local ring with unique maximal ideal generated by $\frac{3}{1}$.
(b) The ring $\mathbb{C}[x]_{\langle x \rangle}$ is a local ring consisting of all rational functions on C with no pole at the origin. The ring has unique maximal ideal consisting of rational functions vanishing at the origin.
(c) The ring $\mathbb{C}[x, y]_{\langle x,y \rangle}$ is a local ring. It has infinitely many prime ideals: $\langle ax + by \rangle$.

6.3. **Nakayama Lemma.**

Lemma 6.12. *Let R be a ring, I be an ideal, and M be a finitely generated R-module. If $IM = M$, then $\exists r \in R$ with*

$$r \equiv 1 (\mathrm{mod}\, I)$$

such that $rM = 0$.

Picture from Google: middle of the mountain in Japan
Cayley+Hamilton → Nakayama (中山正)

Proof. Consider $\phi : M \to M$, where ϕ is the identity morphism, then $\phi(M) \subseteq IM$. Apply Cayley-Hamilton for ϕ and I, then

$$\mathrm{id} + a_1 + a_2 + \cdots + a_n = 0$$

for some $a_j \in I^j$, where n is the number of generators of M. Denote $a = a_1 + a_2 + \cdots + a_n \in I$, then $(\mathrm{id} + a)m = 0$ for any m, in other words, $(1 + a)m = 0$. □

Lemma 6.13. *Let R be a local ring with maximal ideal $\mathfrak{m}$, and M a finitely generated R-module. If $M = \mathfrak{m}M$, then $M = 0$.*

Proof. By Lemma 6.12, $\exists r \notin \mathfrak{m}$ s.t. $rM = 0$. By Lemma 6.9, r is a unit. Therefore $M = 0$. □

Lemma 6.14. *Let R be a local ring with maximal ideal $\mathfrak{m}$, and M a finitely generated R-module. Let $a_1, \dots, a_t$ be elements in M such that $a_1 + \mathfrak{m}M, \dots, a_t + \mathfrak{m}M$ spans $M/\mathfrak{m}M$ as a vector space over $R/\mathfrak{m}$.*

Then $a_1, \dots, a_t$ generate M.

Proof. Let N be the submodule of M generated by $a_1, \dots, a_t$. Since $a_i + \mathfrak{m}M$ spans $M/\mathfrak{m}M$, for any element $m \in M$,

$$m + \mathfrak{m}M = r_1(a_1 + \mathfrak{m}M) + \cdots + r_t(a_t + \mathfrak{m}M)$$

for some $r_i \in R$. Therefore, $m = r_1a_1 + \cdots + r_ta_t + \tilde{m}$ for some $m \in \mathfrak{m}M$. By the definition of N, $m + N = \tilde{m} + N$. Therefore,

$$M/N = \mathfrak{m}M/N.$$

By Lemma 6.13, $M/N = 0$. □

Example 6.15. Consider the localization of $\mathbb{C}[x, y]$ at $\langle x, y\rangle$, the unique maximal ideal is $\mathfrak{m} = \langle x, y\rangle$.

$$\text{Claim:}\mathfrak{m} = \langle x + y^4, y + xy + x^4y^3\rangle = I.$$

The quotient field $\mathbb{C}[x, y]_{\langle x,y\rangle}/\mathfrak{m}$ is isomorphic to $\mathbb{C}$. Consider the module $M = \mathfrak{m}$, then

$$M/\mathfrak{m}M = \mathfrak{m}/\mathfrak{m}^2 = \langle x, y\rangle/\langle x^2, xy, y^2\rangle$$

is a $\mathbb{C}$-vector space spanned by $x + \mathfrak{m}M$ and $y + \mathfrak{m}M$ as well as spanned by $x + y^4 + \mathfrak{m}M$ and $y + xy + x^4y^3 + \mathfrak{m}M$.

By Lemma 6.14, $x + y^4, y + xy + x^4y^3$ spans the whole module M.

6.4. **Normalisation.**

Definition 6.16. Let $R \subseteq S$ be rings. We say R is integrally closed in S if every element in S that is integral over R is contained in R.

Definition 6.17. Let R be a domain, then we say R is an **integrally closed domain** or **normal** if it is integrally closed in its field of fractions $\mathrm{Frac}R$. The integral closure of R in $\mathrm{Frac}(R)$ is called the **normalization** of R.

Remark 6.18. Let R be an integral domain, then the normalisation of R is a normal ring.

Example 6.19. (a) A field F is normal: $\mathrm{Frac}F = F$.

(b) The ring of integers $\mathbb{Z}$ is normal.

Note that $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$, $\forall q \in \mathbb{Q}$, we may write $q = \gcd(a, b) = 1$ for some $a, b \in \mathbb{Z}$. Suppose $\frac{a}{b}$ is integral over $\mathbb{Z}$, then

$$\left(\frac{a}{b}\right)^n + \cdots + a_{n-1}\frac{a}{b} + a_n = 0,$$

for some $a_1, \dots, a_n \in \mathbb{Z}$. We have

$$a^n + a_1a^{n-1}b + \cdots + a_nb^n = 0.$$

Note that a^n is the only term that cannot be divided by b, therefore, $b = \pm 1$. And $\frac{a}{b} \in \mathbb{Z}$.

(c) By the same argument, a unique factorization domain (UFD) is normal.

(d) $\mathbb{Z}[\sqrt{5}]$ is not normal.

As $\frac{\sqrt{5}+1}{2}$ $\in$Frac$(\mathbb{Z}[\sqrt{5}]) = \mathbb{Q}(\sqrt{5})$, but it satisfies the equation $\phi^2 - \phi - 1 = 0$ hence is integral over $\mathbb{Z}$.

The normalisation of $\mathbb{Z}[\sqrt{5}]$ is $\mathbb{Z}\left[\frac{\sqrt{5}+1}{2}\right]$.

(e) $R = \mathbb{C}[t^2, t^3]$ is NOT normal: its normalization is $\mathbb{C}[t]$.

Note that $\mathrm{Frac}(\mathbb{C}[t^2, t^3]) = \mathrm{Frac}(\mathbb{C}[t]) = \mathbb{C}(t)$. The element $t = \frac{t^3}{t^2} \in \mathrm{Frac}(\mathbb{C}[t^2, t^3])$ satisfies the equation $x^2 - t^2 = 0$, but is not in $\mathbb{C}[t^2, t^3]$. By definition $\mathbb{C}[t^2, t^3]$ is not normal.

Moreover, since $t \in \overline{R}$, we have $\mathbb{C}[t] \subseteq \overline{R}$. On the other hand, $R \subset \mathbb{C}[t] \implies \overline{R} \subseteq \overline{\mathbb{C}[t]}$ in $\mathbb{C}(t)$. Since $\mathbb{C}[t]$ is normal by c), $\overline{\mathbb{C}[t]} = \mathbb{C}[t]$. Hence, $\overline{R} = \mathbb{C}[t]$.

Lemma 6.20. *Let R be a normal ring, S be an m.c.s. not containg 0, then $S^{-1}R$ is normal.*

Proof. Note that $\mathrm{Frac}R \subseteq \mathrm{Frac}(S^{-1}R) \subseteq \mathrm{Frac}(\mathrm{Frac}R) = \mathrm{Frac}R$, we have $\mathrm{Frac}R = \mathrm{Frac}(S^{-1}R)$.

Let $t \in \mathrm{Frac}R$ be integral over $S^{-1}R$, then

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

for some $a_i = \frac{b_i}{c_i} \in S^{-1}R$, where $b_i \in R$ and $c_i \in S$. Let $c := c_1 c_2 \ldots c_n \in S$, then ct is integral over R. Therefore, $t = \frac{tc}{c} \in S^{-1}R$. By definition, $S^{-1}R$ is normal. □

C. L.:, B1.32: MATHEMATICS INSTITUTE, UNIVERSITY OF WARWICK
Email address: C.Li.25@warwick.ac.uk
URL: https://sites.google.com/site/chunyili0401/