Math494: Honors Algebra II

Yanzhi Li

February 26, 2026

Abstract

This is the note containning my personal thoughts as well as lecture notes. My course instructor is Prof. Mircea Immanuel Mustață.

Contents

Part I

Ring Theory

We've learnt about group theories which represents the symmetry for objects, which is kind of abstract. Rings are groups with extra structures, it is naturally more complicated, however it is closer to our intuition due to the same reason.

0.1 Ring and Ring Homomorphism

Definition 0.1.1 (**Ring**). A <u>Ring</u> is a tuple $(R, +, \cdot)$ being a set R endowed with 2 binary operations $(+)$ and $(\cdot)$, s.t.:

1. $(R, +)$ is an **abelian** group, with identity element 0_R or 0.

2. $(\cdot)$ is associative, and has an identity element 1_R or 1 (any element multiply with it will be itself).

3. It satisfy distributivity:

   - $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$, $\forall\, a, b, c \in R$.
   - $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$, $\forall\, a, b, c \in R$.

Notation.

1. Usually write ab for $a \cdot b$.

2. If we don't use parentheses, the order of operations is First $(\cdot)$ then $(+)$.

3. If $(+), (\cdot)$ are understood, simply denote the ring by R.

4. Write na for $a \in R$ and $n \in \mathbb{Z}$ for addition for multiple times.

5. Write a^n for $a \in R$ and $n \in \mathbb{Z}_{\geq 0}$ for multiplication for multiple times.

Remark 0.1.1.

1. As always, with identity elements $0_R, 1_R$ are unique.

2. For every $a \in R$, we have a unique inverse w.r.t $(+)$, denoted by $-a$.

3. In general, don't require $xy = yx \; \forall\, x, y \in R$, if this is the case, then R is a <u>commutative ring</u>.

4. Sometimes the definition of a ring does not require existence of 1_R, then when there is an identity it is called as <u>unitary ring</u>.

Example 0.1.1.

1. $\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}$ are rings w.r.t. $(+), (\cdot)$.

2. If $n \in \mathbb{Z}_{>0}$, then $\mathbb{Z} \,/\, n\mathbb{Z}$ carries two operations:

$$[a] + [b] := [a + b]$$
$$[a] \cdot [b] := [ab]$$

   where $[a] := a + n\mathbb{Z}$, this is well-defined since operations holds regardless of the choice of representatives This is a ring with $0_{\mathbb{Z}\,/\,n\mathbb{Z}} = [0]$ and $1_{\mathbb{Z}\,/\,n\mathbb{Z}} = [1]$.

3. Let R be any ring, then:

$$M_n(R) := \{A = (a_{ij})_{1 \leq i,j \leq n} \mid a_{ij} \in R \; \forall\, i, j\}$$

with "usual" addition and mult. for matrices:

$$(a_{ij}) + (b_{ij}) := (a_{ij} + b_{ij})$$

$$(a_{ij}) \cdot (b_{ij}) := (c_{ij}) \rightsquigarrow c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

then $(M_n(R), +, \cdot)$ is a ring with w.r.t. $1_{M_n(R)} = \begin{pmatrix} 1_R & & 0_R \\ & \ddots & \\ 0_R & & 1_R \end{pmatrix}$.

> **Note.** If $n \geq 2$, even if R is commutative, $M_n(R)$ is not commutative in general.

4. Given a family $(R_i)_{i \in I}$ of rings, where I may not be finite, define the following by **Cartesian Prod.**:

$$\prod_{i \in I} R_i := \{(a_i)_{i \in I} \mid a_i \in R_i \ \forall \ i\}$$

define the operations **componentwise**:

$$(a_i)_{i \in I} + (b_i)_{i \in I} := (a_i + b_i)_{i \in I}$$
$$(a_i)_{i \in I} \cdot (b_i)_{i \in I} := (a_i \cdot b_i)_{i \in I}$$

with $0 = (0_{R_i})_{i \in I}$ and $1 = (1_{R_i})_{i \in I}$. If $I = [n]$, simly write: $R_1 \times \cdots \times R_n$.

Proposition 0.1.1. If R is a ring and $a, b \in R$, then:

1. $a \cdot 0_R = 0_R = 0_R \cdot a$.

2. $-(ab) = (-a) \cdot b = a \cdot (-b)$.

The proof follows quickly from distributivity and the fact that $(R, +)$ is an abelian group.

> **Note.** If R is a set with 1 element $\star$, then we can make it into a ring in a unique way, namely:
>
> $$0_R = 1_R = \star$$
>
> If R is a ring, then the following are equiv.:
>
> 1. $\#R = 1$.
>
> 2. $R = \{0_R\}$.
>
> 3. $1_R = 0_R$.
>
> proof is also trivial.

Definition 0.1.2 (Ring Homomorphism). Let R, S be two rings, the ring homomorphism is a map $f : R \to S$, such that:

1. $f(a + b) = f(a) + f(b) \ \forall \ a, b \in R$.

2. $f(a \cdot b) = f(a) \cdot f(b) \ \forall \ a, b \in R$.

3. $f(1_R) = 1_S$.

Remark 0.1.2.

1. If $f : R \to S$ is a ring homo., then $f : (R, +) \to (S, +)$ is a group homomorphism, with $f(0_R) = 0_S$, $f(a - b) = f(a) - f(b) \ \forall \ a, b \in R$.

2. However, in def of ring hom. condition 3 **does not** implied by 1 and 2.

Example 0.1.2. If $R = \{0_R\}$, then the only map $f : R \to S$ that satisfies 1 and 2 in definition of ring homo. will satisfy:
$$f(0_R) = 0_S$$
however, this does not satisfy condition 3 if $S \neq \{0_S\}$.

Remark 0.1.3. In homework, we shall see if $f : R \to S$, $g : S \to T$ are ring homomorphisms, then $g \circ f : R \to T$ is again a ring homomorphisms. In particular we have a **category** <u>Rings</u>:

- Objects: rings.

- Morphisms: ring homomorphisms.

- composition: usual function composition.

Definition 0.1.3 (**Ring Isomorphism**). If R, S are rings, a <u>ring isomorphism $R \to S$</u> is a ring homomorphism $f : R \to S$, s.t. $\exists \ g : S \to R$ to be ring homomorphism, s.t. $g \circ f = \mathrm{Id}_R$, $f \circ g = \mathrm{Id}_S$.
Such is equivalent that $f : R \to S$ is an isomorphism in the category of <u>Rings</u>.
We say R and S are isomorphic, write $R \cong S$ if $\exists$ ring isomorphism $R \to S$.

Proposition 0.1.2. A ring isomorphism $f : R \to S$ is an isomorphism if and only if f is bijective.

Proof. The only if part is trivial, consider the if part. We know f is homomorphism and bijection, we need to see f^{-1} is still a ring homomorphism. We already have corresponding results for group isomoprhism for $(R, +)$:
$$f^{-1}(a + b) = f^{-1}(a) + f^{-1}(b)$$
Since $f(1_R) = 1_S \Rightarrow f^{-1}(1_S) = 1_R$. Remains to show: $f^{-1}(ab) = f^{-1}(a)f^{-1}(b) \ \forall \ a, b \in S$. Since f is injective, it is enough to show:
$$\underbrace{f(f^{-1}(ab))}_{=ab} = \underbrace{f\left(f^{-1}(a) \cdot f^{-1}(b)\right)}_{=f(f^{-1}(a)) \cdot f(f^{-1}(b)) = ab}$$
∎

Example 0.1.3 (**Chinese Remainder Theorem**). Suppose $m, n \in \mathbb{Z}_{>0}$ be relative primes:
$$f : \mathbb{Z}\big/ mn\mathbb{Z} \to \mathbb{Z}\big/ m\mathbb{Z} \times \mathbb{Z}\big/ n\mathbb{Z}$$
$$[a]_{mn} \to ([a]_m, [a]_n)$$

easily seen before that such is well-defined and being a ring homomorphism in homework. In particular, $\gcd(m, n) = 1 \Rightarrow \ker(f) = \{0\} \Rightarrow f$ is injective, thus $\#\text{LHS} = mn = \#\text{RHS}$ thus it is surjective. We thus obtain a ring **isomoprhism**.

0.2 Subrings and Ideals

We consider the subobjects of ring in this section. In particular, note that sometimes people define rings by unitary ring, in such case Ideals are exactly normal **ring**.

Definition 0.2.1 (**Subring**)**.** Let R be a ring. A $\underline{\text{Subring}}$ of R is a subset S, s.t. $(+), (\cdot)$ in R induce operations on S that make S a ring with unit 1_R.

Remark 0.2.1. Definition of subrings implies:

1. $\forall\, a, b \in S$, we have $a + b \in S$.

2. $\forall\, a, b \in S$, we have $a \cdot b \in S$.

3. With respect to these operations, S is a ring with unit 1_R.

Proposition 0.2.1. If R is a ring, a subset $S \subseteq R$ is a subring if and only if:

1. $a - b \in S$, $\forall\, a, b \in S$.

2. $ab \in S$, $\forall\, a, b \in S$.

3. $1_R \in S$.

Proof. Only left to proof if 1,2,3 holds, then S is a ring with unit 1_R w.r.t. the induced operations.

- S is a subgroup w.r.t. $(+)$: By 3, $S \neq \emptyset$, hence by 1, S is a subgroup. R is abelian thus S is also abelian.

- $1_R \in S$, this is the identity w.r.t. also in S.

- Associativity of $(\cdot)$ and distributivity also holds in S because they hold in R.

$\blacksquare$

Example 0.2.1.

1. $\mathbb{Z} \subseteq \mathbb{Q}, \mathbb{Q} \subseteq \mathbb{R}, \mathbb{R} \subseteq \mathbb{C}$ are all subrings.

2. $\{\text{even numbers}\} \subseteq \mathbb{Z}$ is not a subring since it doesn't contain 1.

Proposition 0.2.2. If $f : R \to S$ is ring homomorphism, then $\text{Im}(f) \subseteq S$ is a subring.

The proof is straightforward. With side note that $f(1_R) = 1_S \in \text{Im}(f)$.

Definition 0.2.2 (**Ideal**)**.** Suppose R be a ring and $I \subseteq R$ and $I \neq \emptyset$. Then

1. I is a $\underline{\text{left ideal}}$ (preseve multiplication on the **left**) if:

    - $a + b \in I \; \forall\, a, b \in I$.
    - $\forall\, a \in R, b \in I \Rightarrow ab \in I$.

2. I is a $\underline{\text{right ideal}}$ (preserve multiplication on the **right**) if:

    - $a + b \in I \; \forall\, a, b \in I$.
    - $\forall\, a \in I, b \in R \Rightarrow ab \in I$.

3. I is a $\underline{\text{two-sided ideal}}$ if it is both left and right ideal.

If R is **commutative**, then all the above definition coincide, so we simply say $\underline{\text{ideal}}$ in this case.

Remark 0.2.2.

1. Every (left/right) ideal is a **subgroup**.

   - $I \neq \emptyset \Rightarrow \exists\, a \in I \Rightarrow 0a = 0 \in I$.
   - $\forall\, a \in I \Rightarrow -a \in I,\ -a = (-1)a = a \cdot (-1)$.

2. If I is a left (or right) ideal and $1 \in I$, then $I = R$, since $\forall a \in R,\ a = a \cdot 1 \in I$.

   Hence the only subring that is a left or right ideal is R.

3. The addition axiom of ideal is w.r.t. **finite sum**, when there comes to infinite sum, things can be different. This is quite like the finite intersection axiom for the definition of general topology.

4. When one wants to approach to the idea that some ideal I equals to the whole ring R, try to deduce that $1_R \in I$, or say the ideal I contains a unit.

Example 0.2.2.

1. R and $\{0\}$ are always two-sided ideals in R.

2. Say R is **commutative** and $a \in R$, let (a) to be the subset of R which contain all multiples of a:

$$(a) := \{ab \mid b \in R\}$$

is an ideal in R, such ideal are called **Principal Ideals**.

   - $(a) \neq \emptyset$ since $a = a \cdot 1 \in (a)$.
   - $ab_1 + ab_2 = a(b_1 + b_2) \in (a)$.
   - $c \in R,\ (ab)c = a(bc) \in (a)$

Proposition 0.2.3. If $f : R \to S$ is a ring homomorphism, then $\ker(f) := \{a \in R \mid f(a) = 0\}$ is a two-sided ideal of R.

Proof. We know it is a subgroup of $(R, +)$, see that:

$$a \in \ker(f) \Rightarrow f(ba) = f(b) \cdot f(a) = f(b) \cdot 0 = 0 \Rightarrow ba \in \ker(f)$$

similarly, $ab \in \ker(f)\ \forall\, b \in R$. ∎

Also note, $f : R \to S$ be ring homomorphism, it is injective iff $\ker(f) = \{0\}$.

Proposition 0.2.4. Let R_1, R_2 be a commutative ring, and let $R = R_1 \times R_2$. Then the ideal of R will take form of:

$$I_1 \times I_2$$

where I_1 and I_2 be some ideal of R_1, R_2 respectively. Moreover, if P be prime ideal of R, then it will take form in:

   - $R_1 \times P_2$ for some P_2 be prime ideal in R_2.

   - $P_1 \times R_2$ for some P_1 be prime ideal in R_1.

Sketch. Consider the projection map π as the group homomorphism, and see that the **images** are the ideal. As for the prime ideal case, write out the definition and one should observe that there are only two case for a prime ideal to take form:

   - $P_1 \times P_2$, actually not a prime ideal, one can see by verify the definition.

   - $R_1 \times R_2$, not the prime ideal since it is the whole ring.

   - $R_1 \times P_2$, ok.

- $P_1 \times R_2$, ok.

∎

0.3 Quotient Rings

In this section we construct quotient rings. Main heuristics is to follow the construction of quotient groups while maintainning the compatibility with multiplication, in particular, with **ring homomorphism**.

Let $(R, +, \cdot)$ be a ring, if $I \subseteq R$ be subgroup, then I is automatically normal since $(R, +)$ is abelian. Thus we can construct $R \, / \, I$ as a group:

$$R\big/_I := R\big/_{\equiv \bmod I} \quad a \equiv b \bmod I \text{ if } a - b \in I$$

Write $a + I$ or simply $\overline{a}$ or $[a]$ for the image of $a \in R$ in $R \, / \, I$. The group structure is **defined** s.t.:

$$\pi : R \to R\big/_I$$
$$a \mapsto a + I$$

is **group homomorphism**. which is:

$$\overline{a} + \overline{b} = \overline{a + b}$$

We then want to see that $R \, / \, I$ to be not just a group, but make it a **ring**, which is: π to be a **ring homomorphism**.

Since $\ker(\pi) = I$, for the above to work, we need $I \subseteq R$ is a **2-sided ideal**. So let's just assume I is a 2-sided ideal.

Since we want π to be a ring homomorphism, we have to define multiplication on $R \, / \, I$, which is by the most obvious way:

$$\overline{a} \cdot \overline{b} = \overline{ab}$$

The **key point** here is then to show that it is **well-defined**. And we need: if $\overline{a} = \overline{a'}, \overline{b} = \overline{b'} \Rightarrow \overline{ab} = \overline{a'b'}$. We know that $a - a' \in I, b - b' \in I$ and we want $ab - a'b' \in I$, which is:

$$ab - a'b' = (ab - ab') + (ab' - a'b;)$$
$$= \underbrace{a\underbrace{(b - b')}_{\in I}}_{\in I \text{ since left ideal}} + \underbrace{\underbrace{(a - a')}_{\in I} b'}_{\in I \text{ since right ideal}} \in I$$

Once we know that multiplication is well-defined, need the following:

- multiplication is associative.

$$\underbrace{(\overline{a}\overline{b})\overline{c}}_{=\overline{abc}=\overline{(ab)c}} = \underbrace{\overline{a}(\overline{b}\overline{c})}_{=\overline{abc}=\overline{a(bc)}} \quad \forall \, \overline{a}, \overline{b}, \overline{c} \in R\big/_I$$
$$\underbrace{\phantom{(\overline{a}\overline{b})\overline{c} = \overline{a}(\overline{b}\overline{c})}}_{\text{by associativity in } R}$$

- distributivity holds by similar argument as above.

- identity element for multiplication.

$$\overline{1}\overline{a} = \overline{1a} = \overline{a}$$
$$\overline{a}\overline{1} = \overline{a1} = \overline{a}$$

- if R is commutative, then **so is** $R \, / \, I$.

The **upshot** is: $R \, / \, I$ is a ring and $\pi : R \to R \, / \, I$ is a ring homomorphism, note that $\pi(1_R) = 1_{R \, / \, I}$.

Proposition 0.3.1 (**Universal Property of Quotient Rings**)**.** Suppose R, I are as before, let $f : R \to S$ be a ring homomoprhism, s.t. $I \subseteq \ker(f)$. There is a **unique** ring homomophrism $\overline{f} : R / I \to S$, s.t. the following diagram is **commutative**:

$$
\begin{array}{ccc}
R & \xrightarrow{\ \pi\ } & R / I \\
{\scriptstyle f}\downarrow & \swarrow{\scriptstyle \overline{f}} & \\
S & &
\end{array}
$$

which is $f = \overline{f} \circ \pi$.

The main idea of the proof is to inherit from our idea for universal property of quotient groups and see that is compatible with ring multiplication.

Proof. The condition $f = \overline{f} \circ \pi \Leftrightarrow \overline{f}(\overline{a}) = f(a) \ \forall \ a \in R$, this implies uniqueness, since π is surjective, as it is explicitely defined for the whole domain R / I.

By the corresponding results for groups, there exists $\overline{f} : R / I \to S$ to be group homomorphism, s.t. $f = \overline{f} \circ \pi$. Hence, it is enough to show:

- $\overline{f}(u \cdot v) = \overline{f}(u)\overline{f}(v) \ \forall \ u, v \in R / I$.

- $\overline{f}(1_{R / I}) = 1_S$.

the second assertion follows directly:

$$
\overline{f}(1_{R / I}) = \overline{f}(\pi(1_R)) = f(1_R) = 1_S
$$

for the first assertion, write $u = \overline{a}, v = \overline{b}$ for some $a, b \in R$, then:

$$
\overline{f}(uv) = \overline{f}(\overline{ab}) = f(ab) = f(a) \cdot f(b) = \overline{f}(\overline{a})\overline{f}(\overline{b}) = \overline{f}(u)\overline{f}(v)
$$

$\blacksquare$

0.4 Isomorphism Theorem

Follow similarly with group, there is also corresponding isomorphism for rings. One should notice that the quotient ring is quite restricted since it requires I to be a **two-sided ideals**, not either left or right ideal.

Theorem 0.4.1 (**Fundemental Isomorphism Theorem**)**.** If $f : R \to S$ is a **surjective** ring homomorphism, and $I = \ker(f) \Rightarrow S \cong R / I$.

Note. Note that the theorem implies that $\text{Im}(f) \cong R / I$.

Remark 0.4.1. If f be arbitrary ring homomorphism, then $\text{Im}(f) \subseteq S$ is a subring.

Proof. Since $I = \ker(f) \Rightarrow I$ is a two-sided ideal. Apply the universal property of R / I, the following diagram is commutative:

$$
\begin{array}{ccc}
R & \xrightarrow{\ \pi\ } & R / I \\
{\scriptstyle f}\downarrow & \swarrow{\scriptstyle \overline{f}} & \\
S & &
\end{array}
$$

there exists a unique ring homomorphism $\overline{f} : R / I \to S$, s.t. $\overline{f} \circ \pi = f$. In the context of group, we've shown that $\overline{f}$ is a group isomorphism, so $\overline{f}$ is bijective, thus it is a ring isomorphism. $\blacksquare$

We then consider the analog of the third isomorphism for groups. We want to describe the left/right/two-sided ideals of R / I in terms of the ones for R, and in fact we have the following proposition.

Proposition 0.4.1. We have an order preserving bijection:

$$\left\{ \begin{array}{c} \text{left/right/2-sided} \\ \text{ideals in } R\,/\,I \end{array} \right\} \xrightarrow[\pi(I') \longleftarrow I' \supseteq I]{J \longrightarrow \pi^{-1}(J)} \left\{ \begin{array}{c} \text{left/right/2-sided} \\ \text{ideals of } R \text{ containing } I \end{array} \right\}$$

where

$$\pi : R \to {}^R\!/_I$$

Proof. We have already seen these two maps given **mutual inverses** for corresponding in groups, to conlcude, we only need to show:

- $J \subseteq R\,/\,I$ is a left/right/two-sided ideal, then so is $\pi^{-1}(J) \subseteq R$.

- $I' \subseteq R$ is a left/right/two-sided ideal, then so is $\pi(I')$.

It will be proved in homework. ∎

Notation. if $I' \subseteq I$ be ideal, we denote $\pi(I')$ by $I'\,/\,I$.

Theorem 0.4.2 (**Third Isomoprhism Theorem**)**.** If R is a ring and $I \subseteq I'$ are two-sided ideals, then:

$$\left.{}^R\!/_I\middle/{}^{I'}\!/_I\right. \cong {}^R\!/_{I'}$$

Note that quotient rings doesn't make sense when I' is left ideal or right ideal.

Proof. By the universal property of $R\,/\,I$ for $R \xrightarrow{p} R\,/\,I'$, there exists a unique $\overline{p} : R\,/\,I \to R\,/\,I'$, s.t. $p(a+I) = a + I' \; \forall \, a \in R$.
Easy to see that $\overline{p}$ is surjective and $\ker(\overline{p}) = I'\,/\,I$ as we've concluded in context of groups, then by the fundemental isomorphism theorem, yields the result. ∎

Example 0.4.1. Let $n \in \mathbb{Z}_{>0}$, in $\mathbb{Z}$, we have ideal:

$$(n) := \{nk \mid k \in \mathbb{Z}\}$$

then $\mathbb{Z}\,/\,(n)$ is exactly $\mathbb{Z}\,/\,n\mathbb{Z}$. $d \in \mathbb{Z}_{>0}$, $(d) \supseteq (n) \Leftrightarrow d\,|\,n$. We have an ideal:

$$(\overline{d}) := \{\overline{d}a \mid a \in {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}\} = {}^{(d)}\!/_{(n)}$$

and the theorem implies:

$$\left({}^{\mathbb{Z}}\!/_{n\mathbb{Z}}\right)\!\Big/_{(\overline{d})} \cong {}^{\mathbb{Z}}\!/_{d\mathbb{Z}}$$

0.5 Polynomial Ring and Formal Power Series Ring

In this section we define two important examples of commutative ring derived from a given commutative ring, namely the polynomial rings and formal power series ring. They are recursively define so one shall first define them for one variable.

Definition 0.5.1. Fix R to be a **commutative ring**, define:

$$R[x] := \{a_0 + a_1 x + \cdots + a_n x^n \mid n \in \mathbb{Z}_{\geq 0}, \; a_0, \ldots, a_n \in R\}$$

note that x which is the variable here is to help track how ring multiplication is defined.

Define the operations as:

1. $\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i := \sum_{i=0}^{n} (a_i + b_i) x^i$.

2. $\left(\sum_{i=0}^{n} a_i x^i\right) \cdot \left(\sum_{j=0}^{m} b_j x^j\right) := \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j\right) x^k$.

See that $(R[x], +, \cdot)$ is a **commutative ring**, with

- zero element: 0, all coefficients being 0.

- unit element: 1, all coefficients of x^i, $i \geq 1$ are 0.

One shall see that we have a **injective** ring homomorphism:

$$R \xrightarrow{i} R[x]$$
$$a \mapsto a$$

which yields the universal property of $R[x]$.

Theorem 0.5.1 (**Universal Property of R[x]**)**.** For every ring homomorphism $\varphi : R \to S$ with R, S commutative and for every $\mathbf{a} \in \mathbf{S}$, there is a **unique** ring homomorphism $\psi : R[x] \to S$, s.t.

1. The following diagram is commutative:

$$
\begin{array}{ccc}
R & \xrightarrow{\varphi} & S \\
{\scriptstyle i}\downarrow & \nearrow{\scriptstyle \psi} & \\
R[X] & &
\end{array}
$$

   i.e. $\psi(b) = \varphi(b) \; \forall \, b \in R$.

2. $\psi(x) = a$.

Proof. Suppose we have such $\psi : \psi(x^i) = a^i \; \forall i > 0$, then $\psi \circ i = \varphi \Rightarrow$ if $P = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n \Rightarrow$

$$\psi(P) = \underbrace{\varphi(\alpha_0) + \varphi(\alpha_1) a + \cdots + \varphi(\alpha_n) a^n}_{\text{denoted by } P(a)}$$

this is explicitly defined, yields uniqueness.

For existence, we use this formula to define $\psi : R[x] \to S$ explicitly, thus property 1 and 2 is clear, only left to check that ψ is actually a ring homomorphism:

- $\psi(P + Q) = \psi(P) + \psi(Q)$ is straightforward.

- $\psi(1) = 1$ is also straightforward.

- $\psi(PQ) = \psi(P)\psi(Q)\ \forall P, Q$. Suppose that $P = \sum_{i=0}^{n} \alpha_i x^i$, $Q = \sum_{j=0}^{m} \beta_j x^j$, then:

$$PQ = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} \alpha_i \beta_j \right) x^k$$

$$\Rightarrow \psi(PQ) = \sum_{k=0}^{m+n} \varphi\left(\sum_{i+j=k} \alpha_i \beta_j \right) a^k$$

$$= \sum_{k=0}^{m+n} \left(\sum_{i+j=k} \varphi(\alpha_i) \cdot \varphi(\beta_j) \right) a^k \quad (\varphi \text{ is a ring homomorphism})$$

And $\quad \psi(P)\psi(Q) = \left(\sum_{i=0}^{n} \varphi(\alpha_i) a^i \right) \cdot \left(\sum_{j=0}^{m} \varphi(\beta_j) a^j \right)$

$$= \sum_{i=0}^{n} \sum_{j=0}^{m} \varphi(\alpha_i)\varphi(\beta_j) a^j$$

$$= \sum_{k \geq 0} \left(\sum_{i+j=k} \varphi(\alpha_i)\varphi(\beta_j) \right) a^{i+j=k} \quad (R \text{ is commutative})$$

$$= \psi(PQ)$$

■

One can iterate this since $R[x]$ is still a commutative ring, and thus get multi-variable polynomial ring over R, which is defined recursively by:

$$R[x_1, \ldots, x_n] := (R[x_1, \ldots, x_{n-1}])[x_n]$$

This is again a commutative ring.

Theorem 0.5.2 (**Universal Property of $R[x_1, \ldots, x_n]$**). $\forall$ ring homomorphism $\varphi : R \to S$, R, S commutative, and $\forall\, a_1, \ldots, a_n \in S$, there exists a **unique** ring homomorphism $\psi : R[x_1, \ldots, x_n] \to S$, s.t.

1. the following diagram is commutative:

$$R \longrightarrow R[x_1] \longrightarrow R[x_1, x_2] \longrightarrow \ldots \longrightarrow R[x_1, \ldots, x_n]$$

with φ and ψ to S

2. $\psi(x_i) = a_i\ \forall i \in [\![1, n]\!]$.

Example 0.5.1. $x_1^2 + x_1 x_3 + x_2^4 \in R[x_1, x_2, x_3]$

The proof is straightforward by using induction on n with the previous universal property of $R[x]$.

Example 0.5.2. If $\sigma \in S_n \Rightarrow \exists!$ ring homomoprhism, s.t. the following diagram is commutative:

$$R \longrightarrow R[x_1, \ldots, x_n]$$

with f_σ to $R[x_1, \ldots, x_n]$

and $f_\sigma(x_i) = x_{\sigma(i)}$ $\forall i$. In fact this is a ring isomoprhism, thus be a automorphism, with inverse being $f_{\sigma^{-1}}$. In particular it shows that the process of constructing $R[x_1, \ldots, x_n]$ is just labelling anmd **doesn't matter with order** of $x_1, \ldots, x_n$.

Notation. Every element of $R[x_1, \ldots, x_n]$ can be written as

$$f = \sum_{u=(u_1,\ldots,u_n)\in\mathbb{Z}_{\geq 0}^n} a_u x^u$$

where $x^u = x_1^{u_1} \cdots x_n^{u_n}$ with $a_u \in R$ which is a <u>monomial</u>.

Example 0.5.3.
$$f(x,y) = 3x^2 y + 5xy^2 + 7$$

We then define the ring for formal power series, basically it allows infinite sum in this case.

Definition 0.5.2 (**Ring of Formal Power Series**)**.** Suppose R a commutative ring, define the ring of <u>formal power series</u> as:
$$R[[x]] := \{\sum_{i\geq 0} a_i x^i \mid a_i \in R, \ \forall\, i \geq 0\}$$

with the operations defined:

- addition: $\sum_{i\geq 0} a_i x^i + \sum_{i\geq 0} b_i x^i := \sum_{i\geq 0}(a_i + b_i)x^i$.

- multiplication:

$$\left(\sum_{i\geq 0} a_i x^i\right) \cdot \left(\sum_{j\geq 0} b_j x^j\right) := \sum_{k\geq 0} c_k x^k$$
$$\text{where} \quad c_k = \sum_{i+j=k} a_i b_j \in R$$

See that $(R[[x]], +, \cdot)$ is again a **commutative ring**, s.t. we have $R[x] \subseteq R[[x]]$ being a subring.

0.5.1 R-Algebra

Definition 0.5.3 (**R-Algebra**)**.** Suppose that R is a commutative ring, an <u>R-Algebra</u> is a ring S together with a ring homomorphism $R \xrightarrow{\varphi} S$, s.t. $\varphi(a)b = b\varphi(a)$ $\forall\, a \in R, b \in S$.

Example 0.5.4.

1. $R[x], R[[x]]$ have natural structures of R-Algebras $R[x_1, \ldots, x_n]$.

2. here is a non-commutative ring example: $M_n(R)$ with the ring homomorphism defined as:

$$R \to M_n(R)$$
$$a \mapsto \begin{pmatrix} a & & 0 \\ & \ddots & \\ 0 & & a \end{pmatrix}$$

See that we can derive a category of R-Algebras, with objects being the R-algebras and the morphisms

are given by the ring homomorphism that makes the following diagram commutative:

$$R \longrightarrow S_1$$
$$\downarrow u_1$$
$$S_2$$

such category is w.r.t. the usual function composition.

0.6 Fields and Integral Domain

It will be better to think fields and integral domain as very special ring, as they are already endowed with relatively complex structure, thus they are more closer to our intuition sometimes, and easier to construct examples from $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

Definition 0.6.1 (**Invertible — Unit**). Fix a ring R, $a \in R$ is <u>invertible</u> if there exists $b \in R$, s.t. $ab = 1_R = ba$.
  b is the inverse of a and denoted as a^{-1}. An element $a \in R$ is called a <u>unit</u> if it is invertible.

Definition 0.6.2 (**Field**). A ring R is a field if;

1. R is commutative.

2. $1_R \neq 0_R$, namely it is not a 0 ring.

3. **Every** $a \in R\backslash\{0\}$ is invertible.

Remark 0.6.1.

- Note that for I being an ideal of R, $I = R$ if and only if I contains an unit of R.

- This directly shows that $\mathbb{K}$ being a field if and only if it attains no non-trivial ideal. In particular, see that the ideal structure of a field is trivial.

- One result from this is that given any non-zero ring homomorphism $\varphi : \mathbb{K} \to R$, such ring homomorphism is always **injective** as $\ker(f)$ being a ideal of $\mathbb{K}$ and thus can only be $\{0\}$ for a non-zero map.

Example 0.6.1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields, $\mathbb{Z}$ is not a field.

Definition 0.6.3 (**Zero-Divisor**). If R is a commutative ring, $a \in R$ is a <u>zero-divisor</u> if $\exists\, b \neq 0$ in R, s.t. $ab = 0$. Otherwise, we say a is a non-zero-divisor.

Definition 0.6.4 (**Integral Domain**). A ring R is an <u>integral domain</u> or simply a <u>domain</u> if:

1. R is commutative.

2. $1_R \neq 0_R$.

3. Every $a \neq 0$ is a non-zero-divisor. Or it is equivalent to say:

$$\forall\, a, b \in R, \ ab = 0 \Rightarrow a = 0 \text{ or } b = 0$$

Remark 0.6.2. If R is a domain, then we have **cancellation rule w.r.t. multiplication**. Namely if $ab = bc$, $a.b.c \in R$, $a \neq 0 \Rightarrow b = c$.

Proof. $a(b - c) = 0 \Rightarrow b - c = 0$. ∎

Example 0.6.2. If $n > 0$, then $\mathbb{Z}/n\mathbb{Z}$ is a domain if and only if n is **prime number**.

Proof. Suppose $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$, with $\bar{a}, \bar{b} \neq 0 \Leftrightarrow a \nmid a, n \nmid b$, and $\overline{ab} = 0 \Leftrightarrow n \mid ab$. Now if n is prime number, then $n \nmid a, n \nmid b \Rightarrow n \nmid ab$, hence $\mathbb{Z}/n\mathbb{Z}$ is a domain.

Now if n is not a prime, then $n = n_1 \cdot n_2$ for some $n_1, n_2 > 1$, which means $\overline{n_1}, \overline{n_2} \neq 0$, but $\overline{n_1} \cdot \overline{n_2} = 0$ in $\mathbb{Z}/n\mathbb{Z}$. ∎

Proposition 0.6.1. If $\mathbb{K}$ is a field, then $\mathbb{K}$ is an integral domain.

Proof. $\mathbb{K}$ is commutative with $1_{\mathbb{K}} \neq 0_{\mathbb{K}}$. Suppose that $a, b \in \mathbb{K}$, $ab = 0$, $a \neq 0$ means that it will attain an inverse by field property, denote it as a^{-1}. Thus we have:

$$b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$$
$$\Rightarrow b = 0$$

∎

Proposition 0.6.2. If R is a finite domain, then R is a field.

Proof. R being a domain means that R is commutative and $1_R \neq 0_R$.

Now fix $a \in R$, $a \neq 0$, and consider the map given by:

$$f : R \to R$$
$$f(b) = ab$$

By cancellation w.r.t. multiplication, since $a \neq 0$, this function is thus injective. But R is finite, meaning f is also surjective, and thus bijective. So there exists $b \in R$, s.t. $ab = 1 \Rightarrow a$ is invertible, thus being a field. ∎

Example 0.6.3. If $n \in \mathbb{Z}_{>0}$, then $\mathbb{Z}/n\mathbb{Z}$ is field if and only if n is prime.

Remark 0.6.3. If R is a domain, then **every subring** of R is a domain. In particular, every subring of a **field** is a domain.

Our goal then now switch to focus on R being a domain implies that $R[x]$ is also a domain, for formal power series, the proof is almost the same.

Definition 0.6.5 (Degree of R[x]). Fix R to be a commutative ring. If $f \in R[x]$, $f \neq 0$, write:

$$f = a_0 + a_1 x + \cdots + a_n x^n$$

s.t. $a_n \neq 0$, then the degree of f is $\deg(f) = n$. And we follow the convention that $\deg(0) = -\infty$.

Remark 0.6.4. $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$

Proposition 0.6.3. If R is a domain, and $f, g \in R[x]$ are non-zero, we have:

$$\deg(f \cdot g) = \deg(f) + \deg(g)$$

In particular, $f \cdot g \neq 0$ thus $R[x]$ being a domain by contraposition. Note that if it is not a domain, it is not generally true as one can cancel out the highest degree coeffecient by product on **zero divisor** on the coeffecient on the highest degree term.

Proof. Suppose that:

$$f = a_0 + a_1x + \cdots + a_mx^m \quad a_m \neq 0 \quad \deg(f) = m$$
$$g = b_0 + b_1x + \cdots + b_nx^n \quad b_n \neq 0 \quad \deg(g) = n$$

then:

$$fg = \sum_{k \geq 0} \left(\sum_{i+j=l} a_i b_j \right) x^k$$
$$= \underbrace{a_m b_n}_{\neq 0} x^{m+n} + \text{ lower degree monomials}$$

Since R is a domain, then $a_m b_n \neq 0 \Rightarrow \deg(f \cdot g) = m + n$. ∎

Corollary 0.6.1. If $n \geq 1$, then R is a domain if and only if $R[x_1, \ldots, x_n]$ is a domain.

Proof. Arguing by induction on n, and it is enough to treat $n = 1$. R being a domain implies that $R[x]$ also be a domain. And if $R[x]$ being a domain, we have a injective ring homomorphism $R \hookrightarrow R[x]$, thus it is a subring of a domain, thus be a domain. ∎

0.7 Ring Fraction

In this section, we want to construt the ring fraction. Our goal is to show that starting with a domain, we want to have fraction field. More generally, we don't require R to be a domain, and start with arbitrary "set of denominators", just like from $\mathbb{Z}$ to get $\mathbb{Q}$.

Definition 0.7.1 (Multiplicative System). Fix R be commutative ring, $S \subseteq R$ be a multiplicative system if:

1. $1 \in S$.

2. If $s_1, s_2 \in S \Rightarrow s_1 \cdot s_2 \in S$.

We can make an attempt to construct ring fraction:
Consider pairs (a, s) where $a \in R, s \in S$, up to equivalence relation, we want to see:

$$(a_1, s_1) \sim (a_2, s_2) \Leftrightarrow s_2 a_1 = s_1 a_2$$
$$\text{denoted as} \quad \frac{a_1}{s_1} = \frac{a_2}{s_2}$$

The issue is that in general this is not an equivalence relation, as it will fail **transitivity**: Let

$$(a, s) \sim (a', s') \quad (a', s') \sim (a'', s'')$$
$$\Leftrightarrow s'a = sa' \quad s''a' = s'a''$$

We want to see that $(a, s) \sim (a'', s'') \Leftrightarrow s''a = sa''$. And see that:

$$s's''a = s''sa' = ss'a'' = s'sa''$$

And it is not clear that the blue one is equal to the red one by definition. Thus we make some modification to the definition.

Definition 0.7.2. Let R be a commutative ring and $S \subseteq R$ be a multiplication system. Consider pairs a, s where $a \in R. s \in S$, write $(a, s) \sim (a', s')$ if there exists $t \in S$, s.t. $t(s'a - sa') = 0$.

Note that 0 is not necessarily in S, and usually we don't care about the situation where a **zero divisor** in S. When there is no zero-divisor in S, the following canonical homomorphism is injective.

And when there is a zero-divisor in S it is not.

$$R \to S^{-1}R$$

$$a \mapsto \frac{a}{1}$$

Claim. Above definition is a **equiavlence relation**.

Notation. Write $\frac{a}{s}$ denote the equivalence class of (a, s).

Proof of Claim.

- Reflexive and symmetric is straightforward.

- Consider Transitivity:

$$(a, s) \sim (a', s') \quad (a', s') \sim (a'', s'')$$
$$\Rightarrow t_1(s'a - sa') = 0 \quad t_2(s''a' - s'a'') = 0 \quad \text{for some } t_1, t_2 \in S$$

We now interest in:

$$t_1 t_2 s'(s''a - sa'') = t_2 s'' \underbrace{t_1(s'a - sa')}_{=0} + \underbrace{t_2 t_1 s'' sa' - t_1 t_2 s' sa''}_{=t_1 s \underbrace{t_2(s''a' - s'a'')}_{=0}}$$

$$= 0$$
$$\Rightarrow (a, s) \sim (a'', s'')$$

note that $t_1 t_2 s' \in S$ since $s', t_1, t_2 \in S$ and S being a multiplication system.

∎

And thus we denote:

$$S^{-1}R := \{(a, s) \mid a \in R, \ s \in S\}$$

or say:

$$S^{-1}R := \{\frac{a}{s} \mid a \in R, s \in S\}$$

We want to then define the $(+)$ and $(\cdot)$ operations on it to make it a ring.
Define:

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} := \frac{s_2 a_1 + s_1 a_2}{s_1 s_1}$$
$$\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} := \frac{a_1 a_2}{s_1 s_2}$$

See that it is well-defined: suppose $\frac{a_1}{s_1} = \frac{b_1}{t_1}$ and $\frac{a_2}{t_2} = \frac{b_2}{t_2}$, we want to see:

$$\frac{s_2 a_1 + s_1 a_2}{s_1 s_2} = \frac{t_2 b_1 + t_1 b_2}{t_1 t_2} \tag{1}$$

$$\frac{a_1 a_2}{s_1 s_2} = \frac{b_1 b_2}{t_1 t_2} \tag{2}$$

Proof of Equation 1. By our hypothesis, there exists $u, v \in S$, s.t.:

$$u(t_1 a_1 - s_1 b_1) = 0$$
$$v(t_2 a_2 - s_2 b_2) = 0$$

Consider:

$$t_1 t_2(s_2 a_1 + s_1 a_2) - s_1 s_2(t_2 b_1 + t_1 b_2) = t_2 s_2(t_1 a_1 - s_1 b_1) + t_1 s_1(t_2 a_2 - s_2 b_2)$$

If we multiply with $uv \in S$, we get 0, which shows that they are in the same equivalence class thus equal. ∎

Proof of Equation 2. Similarly:

$$t_1 t_2 a_1 a_2 - s_1 s_2 b_1 b_2 = t_2 a_2(t_1 a_1 - s_1 b_1) + s_1 b_1(t_2 a_2 - s_2 b_2)$$

Multiply $uv \in S$, we get 0. ∎

Example 0.7.1. When there is a zero divisor in S, consider the case $R = \mathbb{Z}/6\mathbb{Z}$ with $S = \{\overline{1}, \overline{2}, \overline{4}\} \subseteq R$, there is a ring isomorphism:

$$S^{-1}R \cong \mathbb{Z}\big/3\mathbb{Z}$$

which, as one can see, there could never be injective homomorphism from R to $S^{-1}R$ as $|R| = 6$ and $|S^{-1}R| = 3$. But the point is, even though there is zero-divisor in S, we can still define $S^{-1}R$, which behaves in a somewhat peculiar way.

Proposition 0.7.1. With $(+)$ and $(\cdot)$, $S^{-1}R$ is a **commutative ring**. This is the ring of fraction of "R with denominator in S" or the "localization of R w.r.t. S".

Sketch of Proof. It's easy to see that both $(+)$ and $(\cdot)$ are commutative.
The 0 element is given by $\frac{0}{1}$, see that:

$$\frac{0}{1} + \frac{a}{s} = \frac{0 \cdot s + 1 \cdot a}{1 \cdot s} = \frac{a}{s}$$

and the inverse of $\frac{a}{s}$ is $-\frac{a}{s}$.
The 1 element is given by $\frac{1}{1}$.
Associativity of $(+)$:

$$\begin{aligned}
\left(\frac{a_1}{s_1} + \frac{a_2}{s_2}\right) + \frac{a_3}{s_3} &= \frac{s_2 a_1 + a_2 s_1}{s_1 s_2} + \frac{a_3}{s_3} \\
&= \frac{s_3 s_2 a_1 + s_3 a_2 s_1 + a_3 s_1 s_2}{s_1 s_2 s_3} \\
&= \frac{a_1}{s_1} + \left(\frac{a_2}{s_2} + \frac{a_3}{s_3}\right) \qquad \text{by symmetry}
\end{aligned}$$

Associativity of $(\cdot)$ is clear, and distributivity is similar manner. ∎

Remark 0.7.1. If R is an integral domain and $S = R\backslash\{0\}$, then $S^{-1}R$ is a field.

Remark 0.7.2. $S^{-1}R$ has a canonical structure of R-Algebra with the following canonical ring homomorphism:

$$\varphi : R \to S^{-1}R$$
$$\varphi(r) = \frac{r}{1}$$

Note that it is not injective in general, we care whether it is injective because we want not to lose information.

Remark 0.7.3.

1. $a \in \ker(\varphi) \Leftrightarrow \frac{a}{1} = \frac{0}{1} \Leftrightarrow \exists\, s \in S$, s.t. $sa = 0$. Hence: φ is not injective if and only if $\exists\, s \in S$, which is a **zero divisor**.

2. $S^{-1}R = \{0\}$ iff $0 \in S$, it tells us in general we don't care about the case where $0 \in S$.

Example 0.7.2 (**Construction of Fraction Field**)**.** Let R be a integral domain (no zero-divisor in R), and $S = R\backslash\{0\}$, then $\varphi : R \to S^{-1}R$ is injective, see that $S^{-1}R$ in this case is a field: it is not 0, it is commutative, and if $\frac{a}{s} \neq 0(\Leftrightarrow a \neq 0) \Rightarrow$ this has the multiplicative inverse $\frac{s}{a}$ since:

$$\frac{a}{s} \cdot \frac{s}{a} = \frac{as}{as} = \frac{1}{1}$$

We then give some example on how things are constructed:

1. If $R = \mathbb{Z} \rightsquigarrow \mathbb{Q}$.

2. If F be a field, and $R = F[x_1, \ldots, x_n] \rightsquigarrow$ field of rational function $F(x_1, \ldots, x_n)$ which is quotients of polynomials.

Note. In this case, by property of intergal domain and property of S that $0 \notin S$, $\frac{a_1}{s_1} = \frac{a_2}{s_2}$ if and only if $s_2 a_1 - s_1 a_2 = 0$.

Example 0.7.3.

- Let $f \in R$ and $S = \{1, f, f^2, \ldots\} = \{f^n \mid n \in \mathbb{Z}_{>0}\}$ be a multiplicative system, then $S^{-1}R$ is denoted by R_f.

- There is a **universal property** of $S^{-1}R$: Suppose $S \subseteq R$ is a multiplicative system and $\varphi : R \to S^{-1}R$ is the canonical ring homomorphism, then:

  1. $\forall s \in S$, $\varphi(s)$ is invertible.

  2. $S^{-1}R$ is universal with the following property: if $R \xrightarrow{\psi} T$ is commute R-Algebra, s.t. $\psi(s)$ is invertible $\forall\, s \in S$, then there exists a **unique** R-Algbera homomorphism $S^{-1}R \xrightarrow{f} T$, s.t. the following diagram is commutative;

$$R \xrightarrow{\varphi} S^{-1}R$$
$$\psi \searrow \quad \downarrow f$$
$$T$$

Note. Proof manner is very similar to what we do for those universal property: We first suppose that it exists, try to prove uniqueness, in such process we may be able to write out the explicit formula of such morphism, so we can then proof the well-definedness and so on to see the existence.

Proof.

- $\varphi(s) = \frac{s}{1}$ with inverse $\frac{1}{s}$.
- First uniqueness then existence:
    * **Uniqueness**: Suppose $f : S^{-1}R \to T$ is a morphism of R-Algebra, s.t. $f(\frac{a}{1}) = \psi(a) \; \forall \, a \in R$. Given any $\frac{a}{s} \in S^{-1}R$, we have $\frac{a}{s} \cdot \frac{s}{1} = \frac{a}{1}$, see that since f is a ring homomorphism:

    $$f(\frac{a}{s}) \cdot \underbrace{f(\frac{s}{1})}_{\psi(s)} = \underbrace{f(\frac{a}{1})}_{\psi(a)}$$

    $$\Rightarrow f(\frac{a}{s}) = \psi(a)\psi(s)^{-1} \qquad (\psi(s) \text{ is invertible by hypothesis.})$$

    Hence f is unique, as we have it a formula, and clearly it is unique.
    * **Existence**: Define $f : S^{-1}R \to T$ by $f(\frac{a}{s}) = \psi(a)\psi(s)^{-1}$, need to check the following:
      1. f is well-defined: Suppose $\frac{a}{s} = \frac{b}{t}$ then there exists $u \in S$, s.t. $u(ta - sb) = 0$. Apply ψ to both sides we get:

      $$\psi(u)(\psi(t)\psi(a) - \psi(s)\psi(b)) = 0$$

      Multiply by $\psi(u)^{-1}\psi(s)^{-1}\psi(t)^{-1}$ on both sides:

      $$\psi(a)\psi(s)^{-1} - \psi(b)\psi(t)^{-1} = 0$$

      Thus definition is unique.
      2. $f \circ \varphi = \psi$: $f(\frac{a}{1}) = \psi(a)\psi(1)^{-1} = \psi(a)$.
      3. f is a ring homomorphism:

      $$\begin{aligned} f(\frac{a}{s} + \frac{b}{t}) &= f(\frac{ta + sb}{st}) \\ &= \psi(ta + sb)\psi(st)^{-1} \\ &= (\psi(t)\psi(a) + \psi(s)\psi(b))\psi(s)^{-1}\psi(t)^{-1} \\ &= \psi(a)\psi(s)^{-1} + \psi(b)\psi(t)^{-1} \\ &= f(\frac{a}{s}) + f(\frac{b}{t}) \end{aligned}$$

      and

      $$\begin{aligned} f(\frac{a}{s}\frac{b}{t}) &= f(\frac{ab}{st}) \\ &= \psi(ab)\psi(st)^{-1} \\ &= \psi(a)\psi(s)^{-1}\psi(b)\psi(t)^{-1} \\ &= f(\frac{a}{s}) \cdot f(\frac{b}{t}) \end{aligned}$$

      and

      $$f(1) = 1$$

    ∎

Remark 0.7.4. The essence of localizing R into $S^{-1}R$ is to find a **smallest ring**, such that the element of S in the ring will become **invertible** in the sense of canonical ring homomorphism. Thus such construction is unique up to the ring, and thus we have the above universal property.

0.8   Prime Ideals and Maximal Ideals

In this section we shall discuss prime ideals and maximal ideals _____ | leave some overview!

0.8.1   Prime Ideals

Definition 0.8.1 (**Prime Ideal**)**.** Let R be a commutative ring, an ideal $P \subseteq R$ is a prime ideal if:

1. $P \neq R$.

2. If $x, y \in R$ are s.t. $xy \in P \Rightarrow x \in P$ or $y \in P$.

Parenthesis. If P is a prime ideal, then $S = R - P$ is a **multiplicative system**, in this case $S^{-1}R$ is denoted as R_p, which is called local ring.

Proposition 0.8.1. An ideal $P \subseteq R$ is prime ideal if and only if $R\,/\,P$ is an integral domain.

Proof. See that $R\,/\,P$ is always commutative. $R\,/\,P \neq \{0\} \Leftrightarrow P \neq R$.
    (Let $\overline{x}, \overline{y} \neq 0 \in R\,/\,P \Rightarrow \overline{x} \cdot \overline{y} \neq 0) \Leftrightarrow (\forall\, x, y \in R,\ x, y \notin P \Rightarrow xy \notin P$), which, LHS is definition of integral domain, and RHS is deifnition of prime ideal. ∎

Example 0.8.1. If $R = \mathbb{Z}$, then

1. $\{0\}$ is a prime ideal ($\mathbb{Z}$ itself is an intergal domain).

2. If $n \in \mathbb{Z}_{>0}$, then (n) is a prime ideal if and only if $\mathbb{Z}\,/\,n\mathbb{Z}$ is an integral domain if and only if n is prime number. Namely $n\mathbb{Z}$ is prime ideal if and only if n is prime number.

Note. If I is an ideal in R, then all ideals in $R\,/\,I$ are of the form $P\,/\,I$ where $I \subseteq P$ is an ideal. See that by isomorphism theorem:

$$\left. ^{R}/_{I} \middle/ ^{P}/_{I} \right. \cong \left. ^{R}/_{P} \right.$$

Hence $P\,/\,I$ is prime ideal if and only if P is prime ideal.

Example 0.8.2. The following are equivalent:

- R is a domain.

- $(x) := \{xf \mid f \in R[x]\}$ inside $R[x]$ is a prime ideal.

Proof. This follows if we show the following, which gives the result be **Proposition** 0.8.1:

$$R[x]/_{(x)} \cong R$$

Consider the R-algebra homomorphism:

$$R[x] \xrightarrow{\varphi} R$$
$$\varphi(x) = 0$$
$$a_0 + a_1x + \cdots + a_nx^n \to a_0$$

This is a surjective homomorphism, with kernel being:

$$\ker(\varphi) = (x)$$

Then by isomomorphism theorem 0.4.1, yields the result. ∎

Question 0.8.1. What about now consider $(x - a) \subseteq R[x]$?

Note. There exists a R-Algebra isomorphism:

$$f : R[x] \to R[x]$$
$$f(x) = x - a$$

So see that (x) is prime ideal if and only if $(x - a)$ is prime ideal, if and only if R is a domain, thus if and only if $(x - a)$ is also a prime ideal.

By the universal property of $R[x]$: there exists a unique such morphism f of R-Algebra, and exists a unique morphism of R-Algebra $R[X] \xrightarrow{g} R[X]$, $x \mapsto x + a$, thus $g = f^{-1}$, and we can use the universal property to show that the composition $f \circ g$ and $g \circ f$ are identity, which yields isomorphism property.

Definition 0.8.2 (**Comaximal Ideal**). Given R to be a commutative ring, let I_1, I_2 be two ideal s.t. $I_1 \neq I_2$, these two ideals are <u>comaximal</u> if:

$$I_1 + I_2 = R$$

Proposition 0.8.2. When $I_1 + I_2 = R$, namely when they are comaximal, we have:

$$I_1 \cap I_2 = I_1 I_2$$

Proof. The ideal $I_1 I_2$ always contained in $I_1 \cap I_2$. Since there exists $1 = x + y$ for some $x \in I_1, y \in I_2$ since $I_1 + I_2 = R$. Thus for $c \in I_1 \cap I_2$ we have $c = c1 = cx + cy \in I_1 I_2$ thus $I_1 \cap I_2 \subseteq I_1 I_2$. ∎

Theorem 0.8.1 (**Generalized Chinese Remainder Theorem**). Let $I_1, \ldots, I_n$ be ideals in R such that $I_i + I_j = R$ for all $i \neq j$. Then:

$$R/_{I_1 \cap \cdots \cap I_n} \cong \prod_{i=1}^{n} R/_{I_i}$$

with the ring homomorphism defined by:

$$R \to R/_{I_1} \times \cdots \times R/_{I_n}$$
$$r \mapsto (r + I_1, \ldots, r + I_n)$$

with kernel being $I_1 \cap I_2 \cap \cdots \cap I_n$.

Sketch. One should first prove the case that when $I_1 + I_2 = R$, then:

$$R\big/_{I_1 \cap I_2} \cong R\big/_{I_1} \times R\big/_{I_2}$$

by first isomorphism theorem. Then show that:

$$I_1 + (I_2 \cap I_3) = R$$

by noticing that one can have such decomposition:

$$
\begin{aligned}
1 &= (x+y) \cdot (u+v) \\
&= xu + yu + xv + yv \\
&\quad \text{where } x, u \in I_1, y \in I_2, v \in I_3 \\
&\Rightarrow xu \in I_1, yu \in I_1 \cap I_2, xv \in I_1 \cap I_3, yv \in I_2 \cap I_3 \\
&\quad \text{with } xu + yu + xv \in I_1, yv \in I_2 \cap I_3
\end{aligned}
$$

and proceed on induction on n. ∎

0.8.2 Maximal Ideals

Definition 0.8.3 (**Maximal Ideal**). An ideal $M \subseteq R$ is a <u>maximal ideal</u> if:

1. $M \neq R$.

2. If $M \subseteq I \subseteq R$ and I be an ideal, then $I = M$ or $I = R$.

Notably, it is not necessarily for a ring to poccess a maximal ideal unless $1_R \neq 0_R$. One can make such ring by taking abelian groups that pocess no maixmal subgroup, for example $\mathbb{Q}$, and just set the multiplication into the trivial case $ab = 0 \ \forall \ a, b$. **Theorem** 0.8.2 state that when $1_R \neq 0_R$ there's always maximal ideal. Hence any result related to maximal ideal forces the ring to be non-zero ring.

Lemma 0.8.1. If R is a commutative ring, then R is a field if and only if $\{0\}$ is a maximal ideal.

Proof.

- Suppose that R is a field, then $R \neq \{0\}$. If $I \subseteq R$ is an ideal, and $I \neq \{0\}$. Let $a \in I \backslash \{0\}$, since R is a field, see that a is **invertible**. Then:

$$\forall \ b \in R, \quad b = (ba^{-1})a \in I \Rightarrow I = R$$

- If $\{0\}$ is a maximal ideal, then $R \neq \{0\}$. $\forall \ a \in R$ with $a \neq 0$, then $a \in (a) \neq \{0\} \Rightarrow (a) = R \Rightarrow \exists \ b \in R$, s.t. $ab = 1 \Rightarrow a$ is invertible.

∎

Corollary 0.8.1. An ideal $M \subseteq R$ is maximal if and only if R/M is a field.

Proof. By correspondance between ideals of R/M and ideals in R **containing** M, this follows from **Lemma** 0.8.1. ∎

In particular this corollary basically tells us how to construct some fields, we later shall use it to construct all kinds of finite fields, by taking quotients on the ring $\mathbb{Z}[x]$. To see whether an ideal is maximal, either try to find some ideal strictly bigger than it or try to prove the ring quotient it out becomes a field.

Example 0.8.3.

- Let R be the ring of all functions from $[0,1] \to \mathbb{R}$, see that for each $a \in [0,1]$ define:

$$M_a = \{f \in R \mid f(a) = 0\}$$

and since evaluation is a surjective ring homomoprhism from $R \to \mathbb{R}$, thus:

$$R\big/ M_a \cong \mathbb{R}$$

and thus M_a being a maximal ideal.

- $(x) \in \mathbb{Z}[x]$ is not a maixmal ideal. One can see that from either $(x) \subsetneq (2,x) \subseteq \mathbb{Z}[x]$ or $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ with $\mathbb{Z}$ not being a field.

Corollary 0.8.2. Every maximal ideal is prime ideal.

Proof. This follows since **every field is a domain**. And by **Corollary** 0.8.1 and **Proposition** 0.8.1. ∎

Example 0.8.4. The following are ideals that are prime but not maximal:

1. $\{0\} \subseteq \mathbb{Z}$ is a prime ideal, but not maximal ideal, same ideal as the proof below.

2. $(x) \subseteq \mathbb{Z}[x]$ is a prime ideal, but not maximal ideal. Since

$$\mathbb{Z}[x]\big/(x) \cong \mathbb{Z}$$

with $\mathbb{Z}$ being an integral domain not a field, thus (x) is prime ideal but not maximal ideal.

Theorem 0.8.2. If $I \subsetneq R$ is a proper ideal in a commutative ring R, then there exists M being a maximal ideal, s.t. $I \subseteq M$.

To prove it we'll need the famous **Zorn's Lemma**.

Lemma 0.8.2 (Zorn's Lemma). If $(A, \leq)$ is a non-empty partially ordered set, s.t. every totally ordered subset $B \subseteq A$ has an upper bound in A ($\exists\, a \in A$, s.t. $b \leq a \,\forall\, b \in B$), then A has at least a maximal element. ($\exists\, a \in A$, s.t. if $a \leq a' \in A \Rightarrow a = a'$)

Proof uses Zorn's Lemma 0.8.2. Fix I be in the theorem, and let $\mathcal{J} = \{J \subseteq R \text{ is ideal} \mid I \subseteq J\}$. See that it is ordered by inclusion: $J \leq J' \Leftrightarrow J \subseteq J'$. Note that $\mathcal{J} \neq \emptyset$ since $I \in \mathcal{J}$.

So our basic task is to check it satisfies the hypothesis in **Zorn's Lemma** 0.8.2.

Let $\mathcal{J}' \subseteq \mathcal{J}$ be a totally ordered subset: namely if $J_1, J_2 \in \mathcal{J}' \Rightarrow (J_1 \subseteq J_2) \vee (J_2 \subseteq J_1)$. Now let:

$$J := \bigcup_{J' \in \mathcal{J}'} J'$$

The **key point** is that J is an ideal. Suppose $a, b \in J$, let $J', J'' \in \mathcal{J}'$ are s.t. $a \in J'$, $b \in J''$. If $J' \subseteq J'' \Rightarrow a \in J'' \Rightarrow a + b \in J'' \Rightarrow a + b \in J$. Similarly for $J'' \subseteq J'$.

If $x \in J$ and $\lambda \in R$, then there exists $J' \in \mathcal{J}'$, s.t. $x \in J' \Rightarrow \lambda x \in J' \subseteq J$.

See that $J \neq \emptyset$ since $0 \in J$. So the **conclusion** is J is an ideal. And it is clear that $I \subseteq J$.

See that $J \neq R$, otherwise $1 \in J \Rightarrow 1 \in J'$ for some $J' \in \mathcal{J}'$, contradict to the fact that $J' \neq R$.

It is clear that $J' \leq J \,\forall\, J' \in \mathcal{J}' \Rightarrow J$ is the upperbound for $\mathcal{J}'$. The Apply **Zorn's Lemma** 0.8.2: there exists $M \in \mathcal{J}$ to be the maximal element, and this is a maximal ideal that containing I. ∎

Similar technique can be used to prove the following proposition, which takes the minimal prime ideal to be:

$$\mathfrak{p}_1 = \bigcap_{\mathfrak{p}' \in \mathfrak{P}} \mathfrak{p}'$$

where in the following, $\mathfrak{p}_0$ is a fixed prime ideal in R. Notably, $\mathfrak{p}_1$ is a prime ideal, only when $\mathfrak{P} \subseteq \mathfrak{p}$ is

arbitrary totally ordered set w.r.t. reverse set inclusion.

$$\mathfrak{p} = \{\mathfrak{q} \subseteq \mathfrak{p}_0 \mid \mathfrak{q} \text{ is a prime ideal in } R\}$$

> **Proposition 0.8.3.** Let R be a commutative ring, every prime ideal $\mathfrak{p}$ in R contains a minimal prime ideal, that is, a prime ideal $\mathfrak{q}$ such that there is no prime ideal $\mathfrak{q}'$, with $\mathfrak{q}' \subsetneq \mathfrak{q}$.

> **Corollary 0.8.3.** If $R \neq \{0\}$ is a commutative ring, then there exists a maximal ideals in R, in particular, there exists a prime ideal.
>
> **Proof.** Apply the theorem with $I = \{0\}$ shows the existence of maximal ideal. ∎

> **Proposition 0.8.4.** Let R be a commutative ring, and $\mathfrak{p}_1, \mathfrak{p}_2$ be two distinct maximal ideal, then:
>
> $$\mathfrak{p}_1 + \mathfrak{p}_2 = R$$
>
> **Sketch.** It is straightforward once realized that $\mathfrak{p}_1 + \mathfrak{p}_2$ is actually an ideal by definition. ∎

Notably for $\mathbb{Z}$ there is no difference between the notion of maximal ideal and prime ideal except for $\{0\}$ being a prime ideal but not a maximal ideal, (p) is always maixmal. Consider (p_1, p_2) by Bezout's Theorem one shall notice that $1 \in (p_1, a)$ and they must be coprime if distinct and thus directly be $\mathbb{Z}$.

0.9   Local Ring

In this section we shall discuss local rings. ⟶ leave some overview!

> **Definition 0.9.1** (**Local Ring**). A commutative ring R is a local ring if R has a **unique** maximal ideal.

> **Proposition 0.9.1.** For a commutative ring R, the following are equivalent:
>
> 1. R is a local ring. (with maximal ideal $M = \{a \in R \mid a \text{ is not invertible}\}$)
>
> 2. $R \neq \{0\}$ and for all $a, b \in R$, s.t. $a + b = 1$, either a or b is invertible.
>
> **Proof.** Suppose that R is a local ring with maximal ideal M, then $M \subseteq \{a \in R \mid a \text{ is not invertible}\}$ since $M \neq R$. If $a \in R$ is not invertible, then $(a) \neq R$, by **Theorem** 0.8.2, it is contained in a maximal ideal $\Rightarrow (a) \subseteq M \Rightarrow a \in M$.
>
> In this case, $R \neq \{0\}$ since $M \neq R$. If $a + b = 1$, since $1 \notin M$ and M being a subgroup, then either $a \notin M$ or $b \notin M \Rightarrow a$ is invertible or b is invertible.
>
> Define $M = \{a \in R \mid a \neq \text{ invertible.}\}$. We claim that M is an ideal:
>
> - $0 \in M$ since $R \neq \{0\}$.
>
> - If $a \in M, \lambda \in R \Rightarrow \lambda a \in M$, otherwise $\exists \mu \in R$, s.t. $(\mu\lambda)a = 1 \Rightarrow a$ is invertible, leading to contradiction ⨍.
>
> - If $a, b \in M \Rightarrow c := a + b \in M$, otherwise, If c is invertible, then:
>
> $$(a + b)c^{-1} = ac^{-1} + bc^{-1} = 1$$
>
>   then this implies that ac^{-1} or bc^{-1} is invertible, then $a = (ac^{-1})c$ is also invertible, similar for b is invertible, leading to contradiction ⨍.
>
> So we see that M is an ideal, remains to check that it is the only maximal ideal.
>
> - $1 \notin M \Rightarrow M \neq R$.

- If $I \neq R$ is an ideal, then $I \subseteq M$: $I \neq R \Rightarrow 1 \notin I$, thus $\forall\, a \in I$, see that a is not invertible, since $(a) \subseteq I \neq R \Rightarrow 1 \notin (a) \Rightarrow a \in M$.

Since we know R has an maximal ideal by **Corollary** 0.8.3, then M is a maximal ideal, and in fact the unique one. See that any maximal ideal $M' \subseteq M \Rightarrow M' = M$. ∎

Example 0.9.1.

1. $\mathbb{K}$ is a field $\Rightarrow \mathbb{K}$ is a local ring.

2. Let R be a commutative ring, $P \subseteq R$ be a prime ideal, define $S = R - P$, and thus be a multiplicative system. Define $R_p := S^{-1}R$. By HW #3:

$$\{\text{Prime ideal in } S^{-1}R\} \xleftarrow{\text{order preserving bij.}} \{\text{Prime ideal } q \text{ in } R \text{ with } S \cap q = \emptyset \Leftrightarrow q \subseteq P\}$$

where order preserving means the bijection is compatible with inclusion. This implies that $S^{-1}R$ is a local ring with maximal ideal:

$$S^{-1}P = \{\frac{a}{s} \in R_p \mid a \in P\}$$

since P is the largest prime ideal for $S^{-1}R$ with $S = R - P$, s.t. $S \cap P = \emptyset$.

> **Example 0.9.2.** If $p \in \mathbb{Z}_{>0}$ is a prime integer, then:
>
> $$\mathbb{Z}_{(p)} = \{\frac{a}{b} \mid a, b \in \mathbb{Z},\ (p \nmid b) \Leftrightarrow (S = \mathbb{Z} - (p))\}$$
>
> with the maximal ideal being:
>
> $$\{\frac{pa}{b} \mid a, b \in \mathbb{Z},\ p \nmid b\} \quad \text{by } pa \in (p)$$

The point is that if we want to study the property of the ring, we can sometimes go to the local ring and use their properties.

0.10 Radical Ideals

In this section we shall discuss radical rings.

leave some overview!

Definition 0.10.1 (Radical Ideal). Let R be commutative ring, and $I \subseteq R$ be an ideal. I is a radical ideal if $\forall\, a \in R$, s.t. $a^n \in I$ for some $n \geq 1 \Rightarrow a \in I$.

Definition 0.10.2 (Reduced Ring). Let R commutative ring, R is called a reduced ring if $\{0\}$ is a radical ideal.

Theorem 0.10.1. Let R be commutative ring, and $I \subseteq R$ be an ideal. I is a radical ideal if and only if R/I is a reduced ring.

The proof is straightforward by just formally write out the definition.

Example 0.10.1.

1. I is a prime ideal $\Rightarrow I$ is a radical ideal. As one can consider $a^n \in I \Rightarrow (a^{n-1})a \in I \Rightarrow$ either $a^{n-1} \in I$ or $a \in I$ and doing this repeatedly eventually leads to $a \in I$.

2. If $n \in \mathbb{Z}_{>0}$, then (n) is radical ideal if and only if n is square free, namely if $n = p_1^{a_1} \cdots p_r^{a_r}$ to be

the prime decomposition, then $a_i = 1 \ \forall \ i$.

Sketch of Proof. One can consider the prime factorization of n as:

$$n = p_{i_1}^{a_{i_1}} \cdots p_{i_r}^{a_{i_r}}$$

and consider arbitrary element $a \in \mathbb{Z}$ such that $a^k \in (n)$, the prime factorization of a^k given by:

$$a^k = p_{j_1}^{b_{j_1}} \cdots p_{j_l}^{b_{j_l}} = cn \qquad \text{for some } c \in \mathbb{Z}$$

and since c is integer it means that LHS should cancel out all the prime factors of n, in particular, this means that:

$$\{i_1, \ldots, i_r\} \subseteq \{j_1, \ldots, j_l\}$$

and cancel things out one can still write $a = dn$ for some $d \in \mathbb{Z}$. ∎

Remark 0.10.1.

1. We showed in HW#2, that:

$$\text{rad}(I) = \{a \in R \mid a^n \in I \text{ for some } n \geq 1\}$$

is an ideal in R. See that $I \subseteq \text{rad}(I)$, with equality if and only if I is a **radical ideal**.

Sketch of Proof. Its straightforward to see that $I \subseteq \text{rad}(I)$. When I is a radical ideal, this means that $a^n \in I \Rightarrow a \in I \Rightarrow \text{rad}(I) \subseteq I \Rightarrow I = \text{rad}(I)$. When $I = \text{rad}(I)$, then $\text{rad}(I) \subseteq I \Rightarrow a^n \in I \Rightarrow a \in I$. ∎

2. $\text{rad}(I)$ is a radical ideal. Just check above proof.

3. $\text{rad}(I)$ is the **smallest** radical ideal containing I.

4.

Parenthesis. If $(I_\alpha)_\alpha$ is a family of left/right/two-sided ideals in **any ring** R, then:

$$\bigcap_\alpha I_\alpha \text{ has the same property.}$$

5. If each I_α is a radical ideal, then $\bigcap_\alpha I_\alpha$ is also a radical ideal. The proof is quite straightforward.

Note. This is **false** for prime ideals, see that in $\mathbb{Z}$, $(2) \cap (3) = (6)$, where (6) is not a prime ideal.

However, if the family is a **totally ordered set characterized by reverse set inclusion**, then this statement is true. See homework related to Zorn's Lemma, this also gives us the statement that **every prime ideals have a minimal prime ideal**.

Proposition 0.10.1. For every ideal $I \subseteq R$, see that:

$$\text{rad}(I) = \bigcap_{P \supseteq I, P \text{ prime ideal.}} P$$

Proof. First note that:

$$I \subseteq \underbrace{\bigcap_{I \subseteq P, P \text{ prime ideal}} P}_{\text{radical, since prime is radical and intersection of radical is radical}} \qquad \Rightarrow \text{rad}(I) \subseteq \bigcap_{I \subseteq P, P \text{ prime ideal}} P$$

since $\text{rad}(I)$ is the smallest radical ideal that contains I.

Suppose $f \in \bigcap_{I \subseteq P, P \text{ prime ideal}} P$, we want to see that $f^n \in I$ for some $n \geq 1$.

The general ideal here is to replace (R, I, f) by $(R/I, \{0\}, \overline{f})$, as one can see that:

$$\overline{f}^n = 0 \Leftrightarrow f^n \in I$$

big picture is that the property $f^n \in I$ is **carried** by ring homomorphism, and one will make it easier to consider in quotient ring, and further to fraction it out using the multiplicative system $S = \{1, f, f^2, \dots\}$.

May assume $I = \{0\}$, thus $f \in P$ for all prime ideal P. The **tricks** here is to consider $R_f = S^{-1}R$ where S is defined as above. The prime ideals in R_f is the same as the prime ideals P in R, s.t. $S \cap P = \emptyset \Leftrightarrow f \notin P$. And see that there are no such prime ideals in R, and so there will be no such prime ideal in $S^{-1}R$, but we've seen in **Theorem** 0.8.2 that every commutative ring who have a proper ideal should have a maximal ideal, and maximal ideal is prime ideal, and itself is an ideal, it follows that $R_f = \{0\}$. So:

$$R_f = \{0\} \Rightarrow \frac{0}{1} = \frac{1}{1} \Leftrightarrow \exists\, n, \text{ s.t. } f^n = 0$$

$\blacksquare$

Corollary 0.10.1. An ideal is a radical ideal if and only if it is the intersection of all prime ideals who contains it.

Proof. As prime ideals are radical ideal, the forward direction trivially holds. The reverse direction directly yields combining the proposition and the fact that I is radical if and only if $I = \text{rad}(I)$. $\blacksquare$

Corollary 0.10.2. In a commutative ring R, since all prime ideal contains 0, and thus contain (0), we have:

$$\bigcap_{\mathfrak{p} \in \text{Spec } R} \mathfrak{p} = \text{rad}((0)) = \{x \in R \mid \exists\, n \in \mathbb{Z}_{>0},\ x^n = 0\} =: \sqrt{(0)}$$

In particular, A ring R is reduced if and only if

$$\bigcap_{\mathfrak{p} \in \text{Spec } R} \mathfrak{p} = \{0\}$$

0.11 Operations with Ideals

In this section we will see several operators to help us construct more and more ideals from existing ideals.

0.11.1 Sum of Ideals

Let R be any ring, then we've seen that the intersection of ideals are ideals, we now define the <u>sum of ideals</u> for $(I_\alpha)_{\alpha \in \Lambda}$.

Let I_α be left/right/2-sided ideal in R, define the sum of them as:

$$\sum_{\alpha \in \Lambda} I_\alpha := \bigcap_{I \text{ be \underline{such} ideal } I_\alpha \subseteq I\, \forall\, \alpha} I$$

This is the unique **smallest** ideal containing all I_α. Note that we consider **finite sum** here, if it is infinite sum, then we put finitely of them that are non-zero.

such here means corresponding left/right/2-sided

Proposition 0.11.1 (**Equivalence def. of Sum of Ideals**).

$$\sum_{\alpha \in \Lambda} I_\alpha = \{\sum_{\alpha \in \Lambda} a_\alpha \mid a_\alpha \in I_\alpha \ \forall \ \alpha, \text{ only finitely many } a_\alpha \text{ are } \neq 0\}$$

Example 0.11.1.
$$I_1 + I_2 = \{a + b \mid a \in I_1, \ b \in I_2\}$$

Sketch of Proof. It is straightforward to verify that the RHS is an ideal, and it contains all I_α, thus "$\subseteq$" part directly yields.

On the other hand, if I is an ideal, s.t. $I_\alpha \subseteq I \ \forall \ \alpha$, then RHS $\subseteq I$, which then yields "$\supseteq$" part. ∎

More generally, given any subset $A \subseteq R$, may consider the smallest left/right/2-sided ideal **generated** by A:

$$\bigcap_{I \text{ be } \underline{\text{such}} \text{ ideal } A \subseteq I} I$$

If R is commutative, write (A) for this ideal.

Example 0.11.2. If $A = \{a\}$, then the left ideal generated by A is:

$$Ra = \{\lambda a \mid \lambda \in R\}$$

One can also write the following for the corresponding ideal, the definition is easy to understand by the notation:
$$RA := \{r_1 a_1 + \cdots + r_n a_n \mid n \in \mathbb{Z}_{>0}, a_i \in A, r_i \in R \ \forall \ i \in [\![1, n]\!]\}$$

On one hand, since R contains the identity elements, thus we have $A \subseteq RA$, one the other hand, any left ideal containing A should contain all the finite sums of the element in the form ra with $r \in R, a \in A$, thus RA is **precisely** the left ideal generated by A. Similarly, things happen for AR and RAR which corresp. to the right/2-sided ideal generated by A. Note that when R is not commutative, the set $\{ras \mid r, s \in R\}$ is not necessarily the two-sided ideal generated by **a** as it is not closed under addition.

Remark 0.11.1.

1. For any A, we have left/right ideal generated by A is:

$$\sum_{a \in A} Ra \quad (\text{resp. } \sum_{a \in A} aR)$$

2. If $A = \{a_1, \ldots, a_n\}$ and R be a commutative ring, then the ideal generated by A is denoted as $(a_1, \ldots, a_n)$, which is:

$$(a_1, \ldots, a_n) := \{\lambda_1 a_1 + \cdots + \lambda_n a_n \mid \lambda_1, \ldots, \lambda_n \in R\}$$

3. We say A is a **system of generators** of I, where I being a left/right/2-sided ideal, if I is $\underline{\text{such}}$ ideal generated by A.

4. If A is a infinite set, then the ideal generated by A is the set of all the **finite sum of elements** in A.

Example 0.11.3. If R is commutative, a principal ideal in R is an ideal generated by 1 element: (a), $a \in R$.

Proposition 0.11.2. Given $a, b \in R$, see that the following are equivalent:

- $b \in (a)$.

- $(b) \subseteq (a)$.

The proof is quite straightforward, one thing to note is that the containment relations between ideals, in particular between principal ideals, is seen to capture some of the arithmetic of general commutative rings. Notably, the construction of (a) is quite like what we did in group theory to contruct cyclic subgroup from an element, which shows the usage of single or multiple generators.

0.11.2 Product of Ideals

Let R be commutative ring, $I_1, \ldots, I_n \subseteq R$ be ideals, then define:

$$I_1 \cdots I_n = \text{ideal genearted by } \{a_1 a_2 \cdots a_n \mid a_j \in I_j \ \forall j\}$$

This means that it can be written as:

$$I_1 \cdots I_n := \{\sum_{k=1}^{d} a_{k_1} a_{k_2} \cdots a_{k_n} \mid d \in \mathbb{Z}_{>0}, \ a_{k_j} \in I_j \ \forall j\}$$

> **Example 0.11.4.**
>
> 1. For example:
> $$I_1 \cdot I_2 = \{\sum_{i=1}^{d} a_i b_i \mid d \in \mathbb{Z}_{>0}, a_i \in I_1, b_i \in I_2\}$$
>   Note that the sum here runs over all finite sum.
>
> 2. Let $f, g \in R$, then:
> $$(f) \cdot (g) = (fg)$$

> **Note.** It should be stated clear that
> $$I_1 \cdot I_2 \neq \{ab \mid a \in I_1, b \in I_2\}$$
> RHS is in general not closed under addition, thus **not** being an **ideal**.

Suppose that $f : R \to S$ be a ring homomorphism of commutative rings. If $I \subseteq R$ be an ideal, what can we say about $f(I)$?

- $f(I) \subseteq S$ is a subgroup.

- $f(I)$ is not necessarily an ideal, and it is if and only if f is **surjective**.

Thus we can look into the ideal generated by $f(I)$, which is denoted by IS or $I \cdot S$:

$$IS := \{\sum_{j=1}^{n} a_j f(b_j) \mid n \in \mathbb{Z}_{>0}, \ a_j \in S, \ b_j \in I\} \tag{3}$$

> **Example 0.11.5.** Suppose that $S = T^{-1}R$ where $T \subseteq R$ be a multiplicative system. Let $I \subseteq R$ be an ideal. See that:
> $$IS = T^{-1}I = \{\frac{a}{s} \mid a \in I, \ s \in T\}$$

0.12 Spectrum of a Commutative Ring

This connects closely on topology. Basically it allow us to glue several ring to get some geometric shape.

Definition 0.12.1. Given a commutative ring R, define:

$$\operatorname{Spec} R := \{\mathfrak{p} \subset R \mid \mathfrak{p} \text{ is prime ideal.}\}$$

For every ideal (not necessarily prime) $I \subset R$, let

$$V(I) := \{\mathfrak{p} \in \operatorname{Spec} R \mid I \subseteq \mathfrak{p}\}$$

Note that we consider it as some sort of topology with closed set being $V(I)$ for some $I \subset R$ being ideal.

Proposition 0.12.1. We have a topology on $\operatorname{Spec} R$, s.t. the **closed sets** are the $V(I)$ for $I \subseteq R$.

Proof. To verify topology property we basically need to check:

1. $\operatorname{Spec} R = V(I)$ for some I.

   This follows by taking $I = \{0\}$.

2. $\emptyset = V(I)$ for some I.

   This follows by taking $I = R$.

3. $\forall (I_\alpha)$ be ideals in R, we have

$$\bigcap_{\alpha \in \Lambda} V(I_\alpha) = V(J) \quad \text{for some } J$$

   Consider let $P \in \bigcap_\alpha V(I_\alpha) \Leftrightarrow P \supseteq I_\alpha \ \forall \alpha \Leftrightarrow P \subseteq \sum_{\alpha \in \Lambda} I_\alpha$. So this follows by taking $J = \sum_\alpha I_\alpha$.

4. $\forall$ ideals $I_1, I_2 \subseteq R$, we have:

$$V(I_1) \cup V(I_2) = V(J) \quad \text{for some } J$$

   We try to show that $V(I_1) \cup V(I_2) = V(I_1 \cap I_2)$, the "$\subseteq$" part is clear simply by the fact that $I_1 \cap I_2 \subseteq I_1$ and $I_1 \cap I_2 \subseteq I_2$. Now suppose that $P \in V(I_1 \cap I_2)$, then see that $I_1 \cap I_2 \subseteq P$. If $I_1 \not\subseteq P, I_2 \not\subseteq P \Rightarrow \exists x_1 \in I_1 - P, \ x_2 \in I_2 - P$, s.t. $x_1 x_2 \in I_1 \cap I_2$ (follows by ideal property) but $x_1 x_2 \notin P$ since P is prime ideal, and reason by contraposition. This leads to contradiction $\notlightning$. Hence by contradiction, either $P \supseteq I_1$ or $P \supseteq I_2$, thus $P \in V(I_1) \cup V(I_2)$.

   Note. Note that the formula only holds for ideal $I_1, I_2 \subseteq R$:

$$V(I_1) \cup V(I_2) = V(I_1 \cap I_2)$$

∎

Example 0.12.1. Let $R = \mathbb{Z} \Rightarrow$ the prime ideals are **precisely** $\{\{0\}, p\mathbb{Z} \text{ for } p \text{ prime}\}$. Then:

- $\{p\mathbb{Z}\}$ are closed.

- $\overline{\{(0)\}} = \overline{\{0\}} = \operatorname{Spec}(\mathbb{Z})$.

In fact, we can define Spec as **functor** as follows:

$$\text{CommutativeRings} \longrightarrow \underline{\text{Top}}^\circ$$

where LHS is the category of commutative rings, and the RHS is the dual of the category of topological spaces.

First recall the definition of a functor:

Definition 0.12.2 (Functor). If $\mathcal{C}$ and $\mathcal{D}$ are categories, then a functor:

$$F : \mathcal{C} \to \mathcal{D}$$

is given by:

1. For every $X \in \mathrm{Ob}(\mathcal{C})$, we have $F(X) \in \mathrm{Ob}(\mathcal{D})$.

2. For all $X, Y \in \mathrm{Ob}(\mathcal{C})$, we have a map

$$\mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{D}}(F(X), F(Y))$$

s.t.

(a) $F(1_X) = 1_{F(X)} \quad \forall X \in \mathrm{Ob}(\mathcal{C})$.

(b) $\forall\ u \in \mathrm{Hom}_{\mathcal{C}}(X, Y), v \in \mathrm{Hom}_{\mathcal{C}}(Y, Z)$, preserving the composition structures of the morphisms.
$$F(u \circ v) = F(v) \circ F(u)$$

If $f : R \to S \supseteq P$ to be a ring homomorphism between commutative rings, one can define:

$$f^{\#} : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$$
$$f^{\#}(P) = f^{-1}(P)$$

We know that $f^{-1}(P) \subseteq R$ is an ideal, it's "inverse" is "surjective", notably to see that it is actually a **prime ideal**:

If $xy \in f^{-1}(P) \Rightarrow f(xy) = f(x)f(y) \in P \Rightarrow f(x) \in P$ or $f(y) \in P \Rightarrow x \in f^{-1}(P)$ or $y \in f^{-1}(P)$

Claim. $f^{\#}$ is **continuous**.

Proof. It is enough to show that $(f^{\#})^{-1}(\text{closed set})$ is also closed.
    Fix $I \subseteq R$ be an ideal, then:

$$(f^{\#})^{-1}(V(I)) = \{P \subseteq S \mid P \text{ prime. } f^{\#}(P) \supseteq I \Leftrightarrow f^{-1}(P) \supseteq I \Leftrightarrow P \supseteq f(I) \Leftrightarrow P \supseteq IS\ \ 3\}$$

Thus we can conclude: $(f^{\#})^{-1}(V(I)) = V(IS)$ which is closed. ∎

To check that it is a functor, need:

1. $(\mathrm{Id}_R)^{\#} = \mathrm{Id}_{\mathrm{Spec}\,R}$, which is clear.

2. The following is true since $(g \circ f)^{-1}(P) = f^{-1}(g^{-1}(P))$:

$$R \xrightarrow{f} S \xrightarrow{g} T$$
$$(g \circ f)^{\#} = f^{\#} \circ g^{\#}$$

We can actually also do similar things for maximal ideal!

Remark 0.12.1. May consider:

$$\mathrm{MaxSpec}(R) := \{P \subset R \mid P \text{ maximal ideal.}\} \subseteq \mathrm{Spec}(R) \text{ w.r.t. subspace topology.}$$

- It **doesn't** give a functor in general.

- It indeed **well-behaved** and useful in geometry if R is a quotient of a polynomial ring, namely: $\frac{\mathbb{K}[x_1,\dots,x_n]}{I}$ where $\mathbb{K}$ be a field, and in this case, it indeed **gives a functor**.

0.13 Noetherian Rings

In this section we focus on the context of R being any ring instead of being commutative ring.

Definition 0.13.1 (**Noetherian Rings and Artinian Rings**)**.** Let R be any ring. Then R is left/right Noetherian ring if there exists **no** strictly increasing sequence:

$$I_1 \subsetneq I_2 \subsetneq \cdots \text{ of left/right ideals.}$$

R is left/right Artinian ring if there exists **no** strictly decreasing sequence

$$I_1 \supsetneq I_2 \supsetneq \cdots \text{ of left/right ideals.}$$

Note. Aritinian ring is a stronger property, most of the rings doesn't satisfy the property of artinian ring.

Example 0.13.1.

1. A field is both Noetherian and Artinian.

2. Every finite ring is both Noetherian and ArtiNian.

3. $\mathbb{Z}$ is not a Artinian ring, because there exists the following strictly decreasing ideal sequence:

$$2\mathbb{Z} \supsetneq 2^2\mathbb{Z} \supsetneq 2^3\mathbb{Z} \supsetneq \cdots$$

4. $\mathbb{Z}$ is a Noetherian ring. One can directly use 1 to finitely generate it. Notably, one may use the following as construction for counterexample:

$$(2) \subseteq (2,3) \subseteq (2,3,5) \subseteq (2,3,5,7) \subseteq \cdots$$

But actually by **Bezout's theorem**, $2x + 3y = 1$ and thus see that $1 \in (2,3) \Rightarrow (2,3) = \mathbb{Z}$.

Proposition 0.13.1. For a ring R, **TFAE**:

1. R is left/right Noetherian ring.

2. Every non-empty family $\mathcal{I}$ of left/right ideals of R contains a maximal element. The maximal element namely is:
$$\exists\, I \in \mathcal{I} \text{ s.t. if } I \subseteq J,\ J \in \mathcal{I} \Rightarrow I = J$$

3. Every left/right ideal of R is finitely generated. Namely:

$$\exists\, a_1, \ldots, a_n \in R,\ \text{ s.t. } I = \sum_{i=1}^{n} Ra_i \quad \left(I = \sum_{i=1}^{n} a_i R \right)$$

Proof.

- $(2) \Rightarrow (1)$: This is clear as one cannot find family of ideals that form a strictly increasing sequence family given the condition of existence of maximal element.

- $(1) \Rightarrow (2)$: One can reason by contraposition, non-existing maximal element means we can always find ideal that is strictly bigger than the current one, and thus construct a infinite increasing sequence, fail the property of Noetherian ring.

- $(1) \Rightarrow (3)$: Given a left ideal I that is not finitely generated. We can construct inductively

$a_1, a_2, \ldots \in i$, s.t.:

$$a_{n+1} \notin \sum_{i=1}^{n} R a_i \ \forall \ n$$

This implies that the sequence of ideals $\left(\sum_{i=1}^{n} R a_i \right)$ is strictly increasing and infinite, thus fail the property of Noetherian ring.

- $(3) \Rightarrow (1)$: Suppose we have $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ is a sequence of left ideals. Let:

$$I := \bigcup_{n \geq 1} I_n$$

we've seen before in the proof of **Theorem** 0.8.2, I is also a left ideal given that $\{I_\alpha\}$ is a total ordered set. Now **by (3)**, I is finitely generated, so we can write:

$$I = \sum_{i=1}^{n} R a_i \text{ for some } a_1, \ldots, a_n \in R$$

Suppose that $a_i \in I_{r_i}$ for $1 \leq i \leq n$, let $r = \max\{r_i\}$, this implies that:

$$\sum_{i=1}^{n} R a_i \subseteq I_r \subseteq I = \sum_{i=1}^{n} R a_i \quad \forall \ s \geq r$$

thus $I_s = I_r \ \forall \ s \geq r$. So we see that the sequence **stablize to some ideal**, leading to the property of Noetherian ring.

∎

The following theorem gives us a basic idea that in fact a lot of rings a actually Noetherian, because the property can inherit from some other ring. So we can build up Noetherian ring from the existing one.

> **Theorem 0.13.1** (**Hilbert's Basis Theorem**). If R is a **Noetherian commutative ring**, then $R[x]$ is also a Noetherian ring.

In fact this proof is quite influentiall and this is actually the first result in Commutative Algebra. Commutative property here basically only help us construct the polynomial ring.

Proof. We will show basically every ideal $I \subseteq R[x]$ is finitely generated, and yield that $R[x]$ is Noetherian by **Proposition** 0.13.1.

Suppose I is not finitely generated. Then we can inductively construct a sequence of element as follow, each time of iteration, the condition on the degree of such element is a little bit stronger than before.

$$I \neq \{0\} \Rightarrow \text{chose } f_1 \in I \backslash \{0\} \text{ of minimal degree } d_1$$
$$I \neq (f_1) \Rightarrow \text{chose } f_2 \in I \backslash (f_1) \text{ of minimal degree } d_2$$

We repeat this to construct $f_1, f_2, \ldots$, s.t.:

$$\forall n \geq 0, \ f_{n+1} \in I \backslash (f_1, f_2, \ldots, f_n)$$

and $\deg(f_{n+1} = d_{n+1})$ is minimal among such f_{n+1}. The reason why we can construct f_i in this way is that I is not finitely generated, so there is always some element between $(f_1, \ldots, f_n) \subset I$.

> **Note.** By constuction and **minimality** of d_n, we have:
>
> $$d_1 \leq d_2 \leq \cdots$$

We then want to make contradiction to this minimality. For every $n \geq 1$, let's write:

$$f_n = a_n x^{d_n} + \text{ lower degree monomials}$$

Let $J \subseteq R$ be the ideal generated by $\{a_n \mid n \geq 1\}$. Since R is a Noetherian ring, J is then **finitely generated**. So we can write:

$$J = (b_1, \ldots, b_k)$$

We can write each b_i as an linear combination of a_j's, by the fact that J be the ideal generated by the whole sequence $\{a_n \mid n \geq 1\}$. Namely:

$$b_i = \sum_{j=1}^{m_i} \lambda_{ij} a_j \quad \lambda_{ij} \in R$$

Now if we let $m = \max\{m_i\}$, then $(a_1, \ldots, a_m) \supseteq (b_1, \ldots, b_k) = (a_1, a_2, \ldots)$, and it is clear that $(a_1, \ldots, a_m) \subseteq (b_1, \ldots, b_k)$. Thus we conclude.

> **Conclusion 0.13.1.** $J = (a_1, \ldots, a_m)$.

Thus see that $a_{m+1} \in (a_1, \ldots, a_m) \Rightarrow$ we can write $a_{m+1} = \lambda_1 a_1 + \cdots + \lambda_m a_m$. One can then define:

$$g = \underbrace{f_{m+1}}_{=a_{m+1}x^{d_{m+1}} + \text{l.d.m.}} - \sum_{i=1}^{m} \lambda_i x^{\overbrace{d_{m+1} - d_i}^{\text{by non-dec.}}} \underbrace{f_i}_{}$$

$$\underbrace{\phantom{\sum_{i=1}^{m} \lambda_i x^{d_{m+1} - d_i} f_i}}_{\lambda_i a_i x^{d_{m+1}} + \text{ l.d.m.}}$$

$$g = f_{m+1} - \sum_{i=1}^{m} \lambda_i x^{d_{m+1} - d_i} f_i$$

> l.d.m. stands for lower degree monomials.

> **Note.**
>
> 1. $\deg(g) < d_{m+1}$ $(\star)$.
>
> 2. $g \in I$ and $g \notin (f_1, \ldots, f_n)$, otherwise, see that:
>
> $$f_{m+1} = g + \sum_{i=1}^{m} \lambda_i x^{d_{m+1} - d_i} f_i \in (f_1, \ldots, f_m)$$
>
>   which is **not** ok.
>
> Thus see that $(\star)$ implies a contradiction with minimality of d_{m+1}. ∎

> **Corollary 0.13.1.** If $\mathbb{K}$ is a field, then $\mathbb{K}[x_1, \ldots, x_n]$ is Noetherian ring for all $n \geq 1$.

> **Proof.** Basically use **Theorem** 0.13.1 and induction on n and the fact that $\mathbb{K}$ is a Noetherian ring. ∎

> **Remark 0.13.1.** Let R be a ring.
>
> 1. If I is a two-sided ideal in R and R is left (right) Noetherian, then R / I is left (right) Noetherian.
>
> 2. If R is commutative and Noetherian, then for every multiplicative system $S \subseteq R$, the ring fractions $S^{-1}R$ is Noetherian.

0.14 PIDs and Euclidean Domains

> **Definition 0.14.1** (**PID**). Let R be a domain, then R is a Principal ideal domain (PID) if every ideal in R is principal: namely it is of the form (a) for some $a \in R$.

Example 0.14.1 (**Non-PID Example**).

1. $(2, x) \subseteq \mathbb{Z}[x]$ is not a principal ideal, and thus $\mathbb{Z}[x] \neq$ PID.

   > **Proof.** Suppose that $(2, x) = (f)$ for some $f \in \mathbb{Z}[x]$, then $2 \in (f) \Rightarrow 2 = fg$ for some $g \in \mathbb{Z}[x] \Rightarrow \deg(f) = 0$. Thus see that $f = n \in \mathbb{Z} \backslash \{0\}$, and see that $x = ng \Rightarrow n = \pm 1$ by considering the fact that the coefficient of x is 1, and in the domain $\mathbb{Z}$, the only way to get 1 is by multiplying ± 1.
   >
   > Hence $(2, x) = \mathbb{Z}[x]$ by the fact that ± 1 is in the ideal. Then it means that there exists $P, Q \in \mathbb{Z}[x]$, s.t. $1 = 2P + xQ$.
   >
   > $$P = a_0 + a_1 x + \cdot$$
   > $$Q = b_0 + b_1 x + \cdots$$
   >
   > $\Rightarrow 1 = 2a_0$, but it cannot happen since $a_0 \in \mathbb{Z}$. ∎

2. If $\mathbb{K}$ is a field, then $(x, y) \subseteq \mathbb{K}[x, y]$ is not finitely generated. ⟶ exer!

Definition 0.14.2 (**Euclidean Domain**). A domain R is an <u>Euclidean Domain</u> if there eixsts $N : R\backslash\{0\} \to \mathbb{Z}_{\geq 0}$ being **arbitrary** functions, such that, $\forall\, a, b \in R$ with $b \neq 0$, there exists $q, r \in R$ (**not necessarily unique**), such that:

- $a = bq + r$.

- Either $r = 0$ or ($r \neq 0$ and $N(r) < N(b)$). (the norm of r should be smaller than the norm of b)

Proposition 0.14.1. Every Euclidean Domain R is a PID.

In particular it tells us that every ideal in an Euclidean domain is principal. Thus it is a good theorem to tell that some integral domains are not Euclidean domains (with repsect to any norm N).

Proof. Let $I \subseteq R$ be an ideal, If $I = \{0\}$, clearly that I is principl. If $I \neq \{0\}$ and N is as in the definition of Euclidean domain. Let $b \in I\backslash\{0\}$ be s.t. $N(b)$ is minimal.

> **Claim.** We claim that $I = (b)$.

"$\supseteq$" part is clear as $b \in I$. For "$\subseteq$" part, Suppose that $a \in I$, with $b \neq 0$, then $\exists\, q, r \in R$, s.t. $a = bq + r$ and:

- $r = 0 \Rightarrow a \in (b)$ which is ok.

- $r \neq 0$ and $N(r) < N(b)$, thus $r = a - bq \in I$ by the ideal property, which contradict to the minimality assumption of $N(b)$ ↯. So this case cannot happen.

∎

Proposition 0.14.2. Every nonzero prime ideal in a PID is a maximal ideal.

Proof. Let (p) be a nonzero prime ideal in the PID R and let $I = (m)$ be any ideal containing (p), we want to see that $I = (p)$ or $I = R$. Now $p \in (m)$ thus $p = rm$ for some $r \in R$. Since (p) is a prime ideal and $rm \in (p)$, either $r \in (p)$ or $m \in (p)$. If $m \in (p)$ then $(p) = (m) = I$. If $r \in (p)$, write $r = ps$ for some $s \in R$. Then:

$$p = rm = psm \Rightarrow sm = 1 \quad (R \text{ is a domain.})$$

thus m is a unit so $I = R$. ∎

Corollary 0.14.1. If R be any commutative ring such that $R[x]$ is a PID, then R is a field.

Proof. (x) is maximal ideal, and see that:

$$R[x]\big/_{(x)} \cong R$$

∎

Example 0.14.2.

1. $\mathbb{Z}$ is an Euclidean domain, with:
$$N : \mathbb{Z}\backslash\{0\} \to \mathbb{Z}_{\geq 0}$$
$$N(a) = |a|$$

   Proof. Suppose $b \in \mathbb{Z}\backslash\{0\}$, then there are two cases:

   - $b > 0$: we know $a = qb + r$, $0 \leq r < b = N(b)$ for some $q, r \in \mathbb{Z}$ with the usual division algorithm.
   - $b < 0$: do the same for $-a, -b$. Have $-a = (-b)q + r \Leftrightarrow a = bq - r$ for $0 \leq r < -b$, with $N(r)|-r| = r < -b = |b| = N(b)$.

   ∎

2. $\mathbb{Z}[i]$ is a Euclidean domain, with:

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$$
$$N(a + bi) = a^2 + b^2$$

   Proof. Let $a + bi, c + di \neq 0 \in \mathbb{Z}[i]$, in $\mathbb{Q}[i]$, have:

$$\frac{a + bi}{c + di} = p + qi \quad p, q \in \mathbb{Q}$$
$$= (\alpha + \beta i) + (\gamma + \delta i)$$
   where $\alpha, \beta \in \mathbb{Z}$, $\gamma, \delta \in \mathbb{Q}$, $|\gamma|, |\delta| \leq \dfrac{1}{2}$.

   This implies that:
$$\underbrace{a + bi}_{\in \mathbb{Z}[i]} = \underbrace{(c + di)}_{\in \mathbb{Z}[i]} \cdot \underbrace{(\alpha + \beta i)}_{\in \mathbb{Z}[i]} + r$$
   $$\text{where } r = (c + di)(\gamma + \delta i)$$
   $$\Rightarrow r \in \mathbb{Z}[i]$$

   thus:
$$N(r) = N(c + di) \cdot \underbrace{N(\gamma + \delta_i)}_{=\gamma^2 + \delta^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}} \quad \text{by } (\star\star)$$

   thus either $r = 0$ or $N(r) < N(c + di)$ since $N(c + di) \neq 0$. ∎

3. If $\mathbb{K}$ is a field, then $\mathbb{K}[x]$ is an Euclidean domain, with:

$$N : \mathbb{K}[x]\backslash\{0\} \to \mathbb{Z}_{\geq 0}$$
$$N(f) = \deg(f)$$

   We verify the condition by showing the following proposition.

Proposition 0.14.3. Let R be any commutative ring, $f, g \in R[x]$ and $g \neq 0$. Let

$$g = a_n x^n + \cdots + a_1 x + a_0$$

s.t. a_n is **invertible**, then there exists **unique** $q, r \in R[x]$, s.t. $f = gq + r$ and either $r = 0$ or $r \neq 0$ and $\deg(r) < n = \deg(g)$.

Proof of Existence is Enough. Proceed the proof by contradiction. If for given g, there are f's that don't satisfy this condition. Let's choose such f of minimal degree, clearly we have $m := \deg(f) \geq n \Rightarrow f = b_m x^m +$ lower order term. Consider

$$f' = f - b_m a_n^{-1} x^{m-n} g$$

see that $\deg(f') < \deg(f) \Rightarrow \exists \, q', r'$, s.t. $f' = q'g + r' \Rightarrow f = \left(b_m a_n^{-1} x^{m-n} + q'\right)g + r'$, which leads to contradiction $\sharp$, as we see that since f is minimal case that don't satisfy the condition, meaning we have either $r' = 0$ or $r' \neq 0$ and $\deg(r) < n = \deg(g)$. $\blacksquare$

Note. To show the <u>uniqueness</u>, show that $\deg(gh) = \deg(g) + \deg(h) \; \forall \, h$. We've proceed this for the case of <u>domain</u>, and it is crucial that a_n is invertible here.

Example 0.14.3. Consider $S = \frac{\mathbb{Z}/3\mathbb{Z}[x]}{(2x^3+x+1)}$, see that $\#S = 27 = 3^2$, which is determined by how many choices for r.

Remark 0.14.1. It is very hard to say a domain is not an euclidean domain, because it's very hard to tell that N doesn't exists for sure.

0.15 The Rings $\mathbb{Z}[\sqrt{d}]$ and $\mathbb{Q}[\sqrt{d}]$

Definition 0.15.1. Fix $\mathbf{d} \in \mathbb{Z}$, with $|d|$ not a <u>square</u>: namely $\nexists \, n \in \mathbb{Z}$, s.t. $n^2 = d$. This implies that $\sqrt{|d|} \notin \mathbb{Q}$. We write $\sqrt{|d|} = \sqrt{-d}$ if $d < 0$. Thus define:

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$$
$$\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$$

Remark 0.15.1.

1. Since $\sqrt{d} \notin \mathbb{Q}$, thus if $a + b\sqrt{d} = a' + b'\sqrt{d}$ for some $a, a', b, b' \in \mathbb{Q} \Rightarrow a = a', b = b'$.

2. $\mathbb{Z}[\sqrt{d}]$ and $\mathbb{Q}[\sqrt{d}]$ are subring of $\mathbb{C}$, thus they are **domains**.

3. $\mathbb{Q}[\sqrt{d}]$ is a field, as one can multiply by its conjugate. If $u = a + b\sqrt{d} \Rightarrow u \cdot (a - b\sqrt{d}) = a^2 - b^2 d \in \mathbb{Q}\backslash\{0\}$, thus:
$$u^{-1} = \frac{a}{a^2 - db^2} - \frac{b}{a^2 - db^2}\sqrt{d}$$

4. Since $\mathbb{Z}[\sqrt{d}] \subseteq \mathbb{Q}[\sqrt{d}]$, by the universal property of fraction field $\mathbb{K}$ of $\mathbb{Z}[\sqrt{d}]$ gives us: $f : \mathbb{K} \to \mathbb{Q}[\sqrt{d}]$ as a ring homomorphism.

   - This is injective since $\mathbb{K}$ is a field, since clearly the map is induced by $\mathbb{Z}[\sqrt{d}] \subseteq \mathbb{Q}[\sqrt{d}]$ so it is not a zero map. The field has no non-trivial ideals and $\ker(f)$, thus the only case would be $\ker(f) = \{0\}$, yields injectivity.

- This is surjective as for $a + b\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, one can always write:

$$a + b\sqrt{d} = \frac{p_1 q_2 + p_2 q_1 \sqrt{d}}{q_1 q_2} \text{ with } p_1 q_2 + p_2 q_1 \sqrt{d} \text{ and } q_1 q_2 \in \mathbb{Z}[\sqrt{d}]$$

Thus yields to be **isomorphism**. Note here the multiplicative system yields to be $\mathbb{Z}[\sqrt{d}]\backslash\{0\}$ which is the only case can be constructed as field for $\mathbb{K}$.

In particular this tells us **up to isomorphism**, the fraction field of $\mathbb{Z}[\sqrt{d}]$ is $\mathbb{Q}[\sqrt{d}]$, thus every element in $\mathbb{Z}[\sqrt{d}]$ is invertible in $\mathbb{Q}[\sqrt{d}]$.

5. Define:

$$\mathbb{Z}[\sqrt{d}] \xrightarrow{\varphi} \mathbb{Z}[\sqrt{d}]$$
$$\varphi(a + b\sqrt{d}) = a - b\sqrt{d}$$

when d is negative, this is exactly the conjugation for complex number. See that φ is actually a **ring homomorphism** and in particular $\varphi \circ \varphi = \text{Id} \Rightarrow \varphi$ is actually a ring isomorphism.

6. Define:

$$N : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}]$$
$$N(u) = u \cdot \varphi(u)$$
$$N(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 \in \mathbb{Z}$$

> **Note.**
> $$N(uv) = N(u)N(v) \quad \forall\, u, v \quad\quad (\star\star)$$
>
> since $\varphi(uv) = \varphi(u)\varphi(v)$. But similar result doesn't holds for addition. Thus it is not a ring homomorphism.

7. One can view $\mathbb{Z}[\sqrt{d}]$ as being the the quotient ring $\mathbb{Z}[x]/(x^2 - d)$. Since $\mathbb{Z}$ is a Noetherian ring, by **Hilbert Basis Theorem** 0.13.1, $\mathbb{Z}[x]$ is also a Noetherian ring, and thus $\mathbb{Z}[\sqrt{d}]$ is a **Noetherian ring**. Alternatively, one can see that $\mathbb{Z}[\sqrt{d}] = (1, \sqrt{d})$, so it's finitely generated, and being a Noetherian ring.

Example 0.15.1. $u = a + b\sqrt{d}$ is invertible in $\mathbb{Z}[\sqrt{d}]$ if and only if $N(u) = \pm 1$.

Proof. If u is invertible, then $uv = 1$ for some $v \in \mathbb{Z}[\sqrt{d}]$, thus:

$$N(u)N(v) = N(uv) = N(1) = 1$$

Since $N(u), N(v)$ are integers, this implies that $N(u) = \pm 1$. Conversely, if $u \cdot \varphi(u) = N(u) = \pm 1 \Rightarrow u^{-1} = \pm\varphi(u)$. ∎

Example 0.15.2 (**Gauss Integers:** $d = -1$). The $\underline{\text{Gauss Integers}}$ is given as:

$$\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$$

and $N(a + bi) = a^2 + b^2$. We see $a + bi$ is a $\underline{\text{unit}}$ (invertible elments in a ring) if and only if $a^2 + b^2 = 1 \Rightarrow$ the units are exactly $\pm 1, \pm i$.

0.16 R-subalgebras and R-algebra of Finite Type

Definition 0.16.1 (R-**subalgebra**). Let R be a commutative ring, together with $R \xrightarrow{\varphi} S$ forms a R-

algebra, the <u>R-subalgebra of S</u> is given by a subring $S' \subseteq S$, s.t. $\varphi(R) \subseteq S'$. In this case, we have a R-algebra struture on S', s.t. $S' \hookrightarrow S$ is an R-algebra homomorphism.

Proposition 0.16.1. If $(S_i)_{i \in I}$ is family of R-subalgebra of S then $\bigcap_{i \in I} S_i \subseteq S$ is an R-algebra.

Definition 0.16.2. If $A \subseteq S$ is any subset, the <u>R-subalgebra of S generated by A</u> is

$$R[A] := \bigcap_{S' \subseteq S \text{ be } R\text{-subalgebra}, A \subseteq S'} S'$$

Definition 0.16.3 (R-**algebra of Finite Type**)**.** S is an R-algebra of <u>finite type</u> if $\exists \, A \subseteq S$ be finite, s.t. $R[A] = S$.

Example 0.16.1 (**Special Case**)**.** Let S be commutative and $A = \{a_1, \ldots, a_n\}$. By the universal property of polynomial rings, we have an R-algebra homomorphism

$$R[x_1, \ldots, x_n] \xrightarrow{f} S$$
$$f(x_i) = a_i$$

Claim. $R[a_1, \ldots, a_n] = \operatorname{Im}(f)$

Proof. It's clear that $A \subseteq \operatorname{Im}(f) \subseteq S$ is an R-subalgebra, thus $R[a_1, \ldots, a_n] \subseteq \in (f)$. On the other hand, since $a_i \in R[a_1, \ldots, a_n] \; \forall \, i$, if $P \in R[x_1, \ldots, x_n] \Rightarrow P(a_1, \ldots, a_n) \in R[a_1, \ldots, a_n] \Rightarrow \operatorname{Im}(f) \subseteq R[a_1, \ldots, a_n]$. ∎

Example 0.16.2. $\mathbb{Z}[\sqrt{d}] \subseteq \mathbb{C}$ is the $\mathbb{Z}$-subalgebra generated by $\sqrt{d}$.

Proof. It's clear that the subalgebra generated by $\sqrt{d} \subseteq \mathbb{Z}[\sqrt{d}]$ and conversely $a + b\sqrt{d} \in$ subalgebra generated by $\sqrt{d} \; \forall \, a, b \in \mathbb{Z}$. ∎

Remark 0.16.1. If R is a Noetherian ring and S is a commutative R-algebra of finite type, then S is a Noetherian ring.

Proof. Since S will be a quotient ring of some $R[x_1, \ldots, x_n]$ and by Hilbert Basis Theorem 0.13.1 this will be Noetherian, and the quotient of a Noetherian ring will still be Noetherian. ∎

0.17 Divisibility

In this section we restrict our view basically on R being a domain.

Definition 0.17.1.

1. If $a, b \in R$ with $b \neq 0$, say b <u>divides</u> a, or $b \mid a$ if $\exists \, c \in R$, s.t. $a = bc$ ($\Leftrightarrow (a) \subseteq (b)$).

2. If $a, b \in R \backslash \{0\}$, say a and b are <u>associated</u> ($a \sim b$) if $a \mid b$ and $b \mid a$ ($\Leftrightarrow (a) = (b)$).

> **Note.** This is a **equivalence relation**, see that $a \sim b \Leftrightarrow a = ub$ with u being a unit.
>
>> **Proof.** $\Leftarrow$ is clear, and for $\Rightarrow$ part, see that $ac = b, bd = a$ for some $c, d \in R \Rightarrow acd = bd = a$, and since R being a domain, this means $cd = 1$, thus d is invertible and being a unit. $\blacksquare$

Proposition 0.17.1 (**Easy Property w/o Proof**).

1. If $a \mid b$ and $b \mid c \Rightarrow a \mid c$.

2. If $a \mid b$ and $a \mid c \Rightarrow a \mid \alpha b + \beta c \ \forall \ \alpha, \beta \in R$.

Definition 0.17.2 (**Greatest Common Divisor (gcd)**). If $a, b \in R$ are not both 0, then a greatest common divisor (gcd) denoted as (a, b) or $\gcd(a, b)$ is $d \in R$, s.t.:

1. $d \neq 0$.

2. $d \mid a$ and $d \mid b$.

3. $\forall d'$, s.t. $d' \mid a, d' \mid b \Rightarrow d' \mid d$.

Note.

1. Such a gcd might not exists!

2. If d is a gcd for $a, b \Rightarrow d'$ is also a gcd of a, b if and only if $d \sim d'$.

Proposition 0.17.2. If a, b not both zero and $(a, b) = (d) \Rightarrow d = \gcd(a, b)$. In particular, in a PID, any 2 element that are not both zero **have a gcd**.

Proof. Let $a, b \in (d) \Rightarrow d \mid a$ and $d \mid b$. $d \in (a, b) \Rightarrow \exists \ \alpha, \beta \in R$, s.t. $d = a\alpha + b\beta$. If $d' \mid a, d' \mid b \Rightarrow d' \mid d$. Hence d is a a gcd of a, b. $\blacksquare$

Definition 0.17.3 (**Prime**). If $a \in R$ is **non-zero**, then a is prime if (a) is a prime ideal, namely:

1. $a \neq$ unit.

2. whenever $b, c \in R$ are s.t. $a \mid bc \Rightarrow a \mid b$ or $a \mid c$.

Definition 0.17.4 (**Irreducible**). Let $a \in R$ be **non-zero**, it is irreducible if

1. $a \neq$ unit.

2. whenever $a = bc$ for some $b, c \in R$, either b or c is a unit.

Proposition 0.17.3. If $a \in R$ is prime, then a is irreducible.

Proof. It's clear that $a \neq$ unit. If $a = bc$ for some $b, c \in R \Rightarrow a \mid bc \Rightarrow a \mid b$ or $a \mid c$. Say $a \mid b \Rightarrow b = au$ for some $u \in R$. Thus $a = auc \Rightarrow uc = 1 \Rightarrow c$ is a unit. $\blacksquare$

Remark 0.17.1. The converse is false in general.

Definition 0.17.5 (**Unique Factorization Domain (UFD)**). A domain R is a unique factorization domain

(UFD) if:

- $\forall\, a \in R, a \neq 0$, a is not a unit. We can write $a = p_1 \cdots p_r$ where $p_1, \ldots, p_r$ are **irreducible elements**.

- This decomposition is essentially **unique**: If $a = q_1 \cdots q_s$ is another such decomposition, then:
    - $r = s$.
    - after reordering the q_i, we have $p_i \sim q_i\ \forall\, i$.

> **Note.** The decomposition in a UFD is **finite**.

Conclusion 0.17.1. fields $\subset$ Euclidean Domains $\subset$ PIDs $\subset$ UFDs $\subset$ integral domains.

Proposition 0.17.4. If R is a UFD, then every irreducible element is prime.

Proof. Let a be irreducible, then $a \neq 0$ and $a \neq$ unit. Suppose that $a \mid bc \Rightarrow bc = ad$ for some $d \in R$. We write b, c, d as product of irreducible elements. By condition **2** in definition of UFD, a is associated with one of the irreducible factors of $b(\Rightarrow a \mid b)$ or $c(\Rightarrow a \mid c)$. $\blacksquare$

Proposition 0.17.5. If every irreducible elements in R is prime, then we have essential uniqueness of irreducible decomposition in R.

Proof. We want to show that if $p_1 \cdots p_r \sim q_1 \cdots q_s$, with p_i, q_j being irreducible, then $r = s$ and after reordering the q_j we have $p_i \sim q_i\ \forall i$
  We proceed induction on $\min\{r, s\}$:

- Base case: if $\min\{r, s\} = 0$, trivially holds.

- Inductive step: Let $r > 0$, if p_1 is irreducible, it is then prime by the hypothesis. Then $p_1 \mid q_1 \cdots q_s \Rightarrow$ after reordering the q_j, may assume $p_1 \mid q_1$. Then $q_1 = p_1 u$ for some $u \in R$. Then q_1 is irreducible $+\ p_1 \neq$ unit $\Rightarrow u$ is a unit $\Rightarrow p_1 \sim q_1$.

$\blacksquare$

Example 0.17.1 (Non-UFD Example). Take $R = \mathbb{Z}[\sqrt{5}i]$, write

$$2 \cdot 3 = 6 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$$

We have the following claim:

> **Claim.** 2 is irreducible.

> **Claim.** $2 \nmid 1 + \sqrt{5}i \Rightarrow 2$ is not prime.

  Combining the above two **Claim** we have $R \neq$ UFD. Recall that:

$$N(a + b\sqrt{5}i) = a^2 + 5b^2$$

We saw, $u \in R$ is a unit iff $N(u) = \pm 1$ in 0.15.1.

> **Proof of Claim 1.** Suppose that $2 = \alpha\beta$ for some $\alpha, \beta \in R$ that are not units, then $N(\alpha), N(\beta) \neq 1$. Then $N(2) = 4 = N(\alpha)N(\beta) \Rightarrow$ they are 2. However there is no $a + \sqrt{5}i$, s.t. $a^2 + 5b^2 = 2(\Rightarrow b = 0, \sqrt{2} \notin \mathbb{Z})$. Hence 2 is irrecucible. $\blacksquare$

> **Proof of Claim 2.** If $2 \mid 1 + \sqrt{5}i \Rightarrow 2(a + b\sqrt{5}i)$ for some $a, b \in \mathbb{Z} \Rightarrow 2a = 1$, leading to contradiction $\frac{\mem}{}$. ∎
>
> The fact is that in the modern study, currently when $b > 0$ things are still being open problem. For $b < 0$, things are already well-studied.

> **Proposition 0.17.6.** If R is Noetherian, then every $a \in R, a \neq 0$, not being a unit is a product of finitely many irreducible elements.
>
> **Proof.** Suppose that there exists $a \in R$ as above, which can't be written like this. By Noetherian, we may choose a such that (a) is maximal w.r.t. $\subseteq$ among all ideals. In particular, $a \neq$ irreducible, thus we can write $a = bc$ with $b, c \in R$ not units. See that:
>
> - $(a) \subset (b) \neq R$: with equality cannot be taken, otherwise making b a unit and $c \neq$ unit.
>
> - $(a) \subset (c) \neq R$: similar reason.
>
> Hence by maximality in the choice of a, b and c are product of irreducible elments, then so is a, leading to a contradiction $\frac{\mem}{}$. ∎

> **Proposition 0.17.7.** Every PID is a UFD.
>
> **Proof.** By **Proposition** 0.17.6, condition 1 in the definition of UFD are satisfied, since PIDs are Noetherian ring. Moreover, by **Proposition** 0.17.5 tells us: to check condition 2 in the definition of UFD, it is enough to show: if $a \in R$ is irreducible, then a is prime.
>
> - a irreducible $\Rightarrow a \neq$ unit.
>
> - We want: if $a \mid bc \Rightarrow a \mid b$ or $a \mid c$. Let d be s.t. $(a, b) = (d)$, then $a \in (d) \Rightarrow a = dd'$ for some $d' \in R$. a being irreducible leads to two cases:
>
>   1. d' is a unit, then $a \sim d$. Since $b \in (d) \Rightarrow d \mid b \Rightarrow a \mid b$.
>   2. d is a unit, write $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$. Then $c \sim dc = \underbrace{\lambda ca}_{a \text{ divide this}} + \underbrace{\mu(bc)}_{a \text{ divide this}} \Rightarrow$
>
> $a \mid c$. ∎

> **Corollary 0.17.1.** $\mathbb{Z}$, $\mathbb{K}[x]$ with $\mathbb{K}$ being a field, $\mathbb{Z}[i]$ are UFDs.

So for, we've seen:
$$\{\text{Euclidean Domain}\} \subseteq \{\text{PIDs}\} \subseteq \{\text{UFDs}\}$$

- The first inclusion is strict since $\mathbb{Z}[\frac{1+\sqrt{19}i}{2}]$ is PID but not Euclidean domain.

- The second inclusion is strict, for example, $\mathbb{Z}[x]$ is a UFD but not a PID.

0.18 Parenthesis about Roots of Polynomial

General setup: suppose S be any commmutative ring, and $a \in S$. If $f \in S[x]$, say a is a <u>root of f</u> if $f(a) = 0$. And we can define the root of f in T where $S \to T = S$-algebra.

> **Note.** since $x - a$ has coefficient of x invertible. We know $\exists!$ q, r, s.t.
>
> $$f = (x - a)q + r \text{ where } r \in S$$
>
> and clearly $f(a) = r$. Hence a is a root of f if and only if $\exists$ q, s.t. $(x - a)q = f$.

Proposition 0.18.1. If S is a domain and $\deg(f) = n \Rightarrow f$ has at most n distinct roots in S.

Proof. We proceed induction on $n \geq 0$.

- It is ok if $n = 0$.

- Suppose $a_1, \ldots, a_d$ are distinct roots of f. We saw:

$$f = (x - a_1)g \text{ for some } g \in S[x]$$

then

  - $\deg(g) = n - 1$.
  - $f(a_i) = 0 = \underbrace{(a_i - a_1)}_{\neq 0} g(a_i) \Rightarrow a_1, \ldots, a_d$ are distinct roots of $g \Rightarrow d - 1 \leq n - 1$.

■

Theorem 0.18.1. Let R be a field, then $\frac{R[x]}{(p(x))}$ is a field $\Leftrightarrow p(x)$ is irreducible.

Proof. ■

finish the proof here after homework proof.

0.19 Divisibility Cont.

Remark 0.19.1. If R is a PID, see that (0) is always a prime ideal:

- It is the unique one iff R is a field.

- Otherwise we have prime ideals (π) with π being some prime elements. These are all maximal ideals, then:
$$(\pi) \subsetneq (a) \subsetneq R \Rightarrow \pi = ab$$
where a, b are not unit, which contradicts to the fact that π is irreducible $\notz$.

Remark 0.19.2. Suppose now $R = \mathbb{K}[x]$ where $\mathbb{K}$ being a field. We have the following facts:

- It has units: $\mathbb{K} \backslash \{0\}$.

- $f \in \mathbb{K}[x]$ being non-zero is irreducible if and only if:

  - It has $\deg > 0$.
  - It cannot be written as a product of two polynomials with positive degree, namely $\deg \geq 1$, which are not units.

Note.

1. If $f \neq 0$, $f \in \mathbb{K}[x]$ is irreducible $\Rightarrow$ it has no roots.

2. The converse of the statements holds if $0 < \deg(f) \leq 3$.

Proposition 0.19.1. If $f \in \mathbb{K}[x]$ has $\deg(f) > 0$, then there exists a ring homomorphism $\mathbb{K} \xrightarrow{i} \mathbb{L}$ (automatically injective), with $\mathbb{L}$ being a field, and $a \in \mathbb{L}$, s.t. $f(a) = 0$.

Proof. Let $(f) \neq \mathbb{K}[x] \Rightarrow \exists$ maximal ideal $M \supseteq (f)$. Then take:

$$i : \mathbb{K} \to \frac{\mathbb{K}[x]}{M}, \quad a = x + M \in \mathbb{L} \Rightarrow f(a) = 0$$

∎

Definition 0.19.1 (**Algebraic Closed**)**.** A field $\mathbb{K}$ is <u>algebraic closed</u> if every non-constant polynomial $f \in \mathbb{K}[x]$ has a root in $\mathbb{K}$.

Theorem 0.19.1 (**Foundemental Theorem of Algebra**)**.** The field $\mathbb{C}$ is algebraic closed.

Proposition 0.19.2. If $f \in \mathbb{K}[x] \backslash \{0\}$ and $\mathbb{K}$ is algebraic closed, then f can be written as a product of linear factors, i.e. there exists $a_1, a_2, \ldots, a_n \in \mathbb{K}$ such that:

$$f = c \cdot (x - a_1) \cdots (x - a_n)$$

where $n = \deg(f)$ and $c \in \mathbb{K} \backslash \{0\}$.

Proof. Proceed the proof by induction on $n = \deg(f)$.

- Case $n = 0, 1$ is clear.

- Inductive step: $n \geq 2$, we know that $\exists\, a_1 \in \mathbb{K}$, s.t. $f(a_1) = 0$ since $\mathbb{K}$ is algebraic closed. Then can write $f = (x - a_1)g$ where $g \in \mathbb{K} \backslash \{0\}$. Since g is a domain, then $\deg(g) = n - 1$, then apply induction on g yields the result.

∎

Corollary 0.19.1. If $\mathbb{K}$ is algebraic closed, and $f \in \mathbb{K}[x]$. Then f is irreducible if and only if $\deg(f) = 1$.

We now take a closer look on what would happen if $\mathbb{K} = \mathbb{R}$ which is not algebraic closed. Let $f \in \mathbb{R}[x] \backslash \mathbb{R}$, and we know that there exists $a \in \mathbb{C}$, s.t. $f(a) = 0$. There will be two cases:

- Case 1: $a \in \mathbb{R} \Rightarrow f = (x - a)g$ for some $g \in \mathbb{R}[x]$.

- Case 2: $a \in \mathbb{C} \backslash \mathbb{R} \Rightarrow f(\bar{a}) = 0$, where $\bar{a}$ is the conjugate of a.

  Note. We have such ring automorphism:

  $$\sigma : \mathbb{C} \to \mathbb{C}$$
  $$\sigma(z) = \bar{z}$$

  and notice that $f = c_n x^n + \cdots + c_1 x + c_0 \Rightarrow \overline{c_n a^n + \cdots c_1 a + c_0} = 0$. Since the coefficient being real numbers, then:
  $$c_n \bar{a}^n + \cdots + c_1 \bar{a} + c_0 = 0$$

  Since $a \neq \bar{a}$ by the fact that $a \in \mathbb{C} \backslash \mathbb{R}$, thus:

  $$f = \underbrace{(x - a)(x - \bar{a})}_{= x^2 - 2\,\mathrm{Re}(a)x + |a|^2 \in \mathbb{R}[x]} g$$

  then one can apply the division algorithm to g and repeat the process until we get the factorization of f into linear and quadratic factors.

Conclusion 0.19.1. The irreducible polynomials over $\mathbb{R}$ are (up to association) of the form:

- $x - a \quad a \in R$.

- $(x - a)(x - \bar{a})$ where $a \in \mathbb{C}\backslash\mathbb{R}$.

We then want to prove the theorem of Gauss, which states the following:

Theorem 0.19.2 (**Gauss's Theorem**). If R is a UFD, then $R[x]$ is also a UFD.

And one shall have following straightfoward results:

Corollary 0.19.2.

1. If $\mathbb{K}$ is a field, then $\mathbb{K}[x_1, \ldots, x_n]$ is a UFD.

2. $\mathbb{Z}[x_1, \ldots, x_n]$ is a UFD.

Proof. Use the Guass theorem + induction on $n \geq 0$ + the fact that $\mathbb{Z}$ and $\mathbb{K}$ are UFDs yields the corollary. ∎

Remark 0.19.3. We saw $\mathbb{Z}[i]$ is not a PID, but it is a UFD.

Exercise. Show that $\mathbb{K}[x_1, x_2]$ is not a PID, hint is to use (x_1, x_2).

To proof the theorem, one may need to prove a sequence of lemma first, we introduce the setup first: Let R be a UFD, and $\mathbb{K}$ is the corresponding fraction field. Which is:

$$\mathbb{K} = S^{-1}R \quad \text{where} \quad S = R\backslash\{0\}$$

Definition 0.19.2. If $a_1, \ldots, a_n \in R$ are not all 0. A <u>greatest common divisor</u> of $a_1, \ldots, a_n$ is an element $d \in R\backslash\{0\}$ such that:

1. $d \mid a_i \ \forall i$.

2. If $d' \mid a_i \ \forall i \Rightarrow d' \mid d$.

Lemma 0.19.1. If R is a UFD, then any such $a_1, \ldots, a_n$ have a gcd.

Note. Note that here n can goes to **infinity**.

Proof. Ignoring those a_i that are 0. May assume $a_i \neq 0 \ \forall i$. R is UFD means that there exists prime elements $p_1, \ldots, p_r$, s.t.

$$a_i = (\text{unit}) \prod_j p_j^{n_{ij}}$$

now let

$$d := \prod_j p_j^{\min_i n_{ij}}$$

may check:

- $d \mid a_i \ \forall i$ is clear.

- If $d' \mid a_i \ \forall i$, consider the irreducible decomposition of d' and of all $\frac{a_i}{d'}$, by uniqueness, this shows that $d' \mid d$.

■

Remark 0.19.4.

- The proof basically implies that if $a_1, \ldots, a_n$ are as above, and $b \in R \backslash \{0\}$, then $b \cdot \gcd(a_1, \ldots, a_n)$ is a $\gcd(ba_1, \ldots, ba_n)$.

- If the n_{ij} above are all 0, then the gcd becomes a **unit**.

Definition 0.19.3 (**Primitive Polynomial**)**.** A non-zero polynomial $f = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ is <u>primitive</u> if $\gcd(a_n, \ldots, a_0) = 1 \Leftrightarrow \nexists$ prime element p, s.t. $p \mid a_i \; \forall \; i$.

Lemma 0.19.2. If $f, g \in R[x]$ are primitive, then $f \cdot g$ is primitive.

Proof. We need to show: $\forall \; p \in R$ being prime element, we can't have $p \mid$ all coefficients of fg, i.e. $\overline{fg} = \overline{f}\overline{g} \in \overline{R}[x]$ where $\overline{R} = R / (p)$ is non-zero. This is ok since $\overline{f}, \overline{g}$ are non-zero by hypothesis and $\overline{R}$ is a domain since (p) is a prime idea is a prime ideal. ■

Lemma 0.19.3.

1. Given any $f \in \mathbb{K}[x]$ non-zero, there exists $c(f) \in \mathbb{K} \backslash \{0\}$ and $g \in R[x]$ primitive, s.t. $f = c(f)g$.

2. Moreover, $c(f)'$ have the same property if and only if $c(f) = c(f)' \cdot u$ where $u \in R$ being a unit.

Proof.

1. Choose a, s.t. $af \in R[x]$. For example take $a = $ product of denominators of coefficients of f. Then take $d = \gcd$ (coefficients of af), this implies that $\frac{a}{d}f$ is primitive polynomial in $R[x]$ bt the remark after **Lemma** 0.19.1. Then we can take $g = \frac{a}{d}f$ and $c(f) = \frac{d}{a}$.

2. Suppose we write:
$$f = c(f)g = c(f)'h$$
where g, h are primitive polynomials in $R[x]$. Then can write:
$$g = \underbrace{\frac{c(f)'}{c(f)}}_{= \frac{a}{b}} h \Rightarrow bg = ah$$

Take the gcd of coefficients of bg and ah respectively, and using the fact that g, h are primitive, see that $b = a \cdot$unit, thus $\frac{c(f)'}{c(f)}$ is a unit in R.

■

Remark 0.19.5.

1. Given $f_1, f_2 \in \mathbb{K}[x]$ being nonzero, write
$$f_1 = c(f_1)g_1$$
$$f_2 = c(f_2)g_2$$
where $g_1, g_2 \in R[x]$ are primitive, then:
$$f_1 f_2 = c(f_1)c(f_2) \underbrace{g_1 g_2}_{\text{primitive by lemma } 0.19.2}$$

47

thus:
$$c(f_1 f_2) = c(f_1) \cdot c(f_2) \text{ up to units}$$

2. If $f \in R[x] \Rightarrow c(f) = $ gcd of coefficients of f.

Let's fix R being a UFD, and $\mathbb{K} = \text{Frac}(R)$ being the fraction field of R.

Proposition 0.19.3. $f \in R[x]$ nonzero polynomial being irreducible if and only if:

- **Case 1**: $f \in R[x]$ is irreducible in R.

- **Case 2**: $\deg(f) \geq 1$, f is primitive, and irreducible in $\mathbb{K}[x]$.

Note. Invertible elements in $R[x]$ is exactly the invertible elements in R (i.e. units in R).

Proof.

- Suppose that $0 \neq f \in R[x]$ being invertible, then:

  1. **Case 1**: $f \in R$. It is not a unit in R since it is not a unit in $R[x]$. Now suppose that $f = gh$ with $f \in R$ and clear that $g, h \in R \Rightarrow g, h$ being unit in $R[x]$ since f is irreducible in $R[x]$ and $g, h \in R[x]$ in the canonical sense, which means they are also unit in R, thus f is irreducible as elements in R.

  2. **Case 2**: Suppose $\deg(f) \geq 1$, with $f \in \mathbb{K}[x]$ being non-zero in the canonical sense. By **Lemma** 0.19.3, can write:
  $$f = \underbrace{c(f)}_{\in R} \underbrace{g}_{\text{primitive in } R[x]}$$

  thus either $c(f)$ is unit in $R[x]$ and hence being unit in R or g is unit in $R[x]$, by the irredcuible property of f, with the latter case cannot happen, the former case holds. Hence $c(f)$ being a unit in R, hence f is primitive up to units, as g is primitive. We then want to show that f is irreducible in $\mathbb{K}[x]$. It is clear that it is not a unit in $\mathbb{K}[x]$. Suppose that for some $g, h \in \mathbb{K}[x]$, have

  $$\begin{aligned} f &= g \cdot h \\ &= c(g)g'c(h)h' \quad \text{where } g', h' \in R[x] \text{ are primitive} \\ &= \underbrace{c(g)c(h)}_{\text{unit in } R} \underbrace{g'h'}_{\text{primitive by lemma } 0.19.2} \end{aligned}$$

  since f is irreducible in $R[x] \Rightarrow g', h'$ are invertble in $R[x] \Rightarrow g, h$ are invertible in $\mathbb{K}[x]$ and thus f is also irreducible in $\mathbb{K}[x]$.

- Conversely, check in the two cases, f is indeed irreducible in $R[x]$.

  1. **Case 1**: Say $f \in R$ is irreducible, we want to see that f is irreducible in $R[x]$.
     - It is not uit in $R[x]$ as it is not unit in R.
     - If $f = gh$ with $g, h \in R[x] \Rightarrow g, h \in R$ by analyzing the degree by the fact that R being a domain. Then either g or h is a unit in R, hence unit in $R[x]$.

  2. **Case 2**: Let $f \in R[x] \backslash \{0\}$, $\deg(f) \geq 1$ being primitive, and is irreducible in $\mathbb{K}[x]$, we want to see that f is irreducible in $R[x]$.
     - It is not a unit in $R[x]$ since $\deg(f) > 0$.
     - Say $f = gh$ where $g, h \in R[x]$. Since f is irreducible in $\mathbb{K}[x]$, then g or h have degree 0 (unit in $\mathbb{K}[x]$) and since $g, h \in R[x]$, may assume $g \in R$. Since f is primitive, and that g will be a gcd of the coefficients of f, this means that g will be a unit in R, hence unit in $R[x]$.

■

We are now fully equipped to prove the Guass Theorem, this theorem is important as it allows us to reduce the irreducibility of polynomials in $R[x]$ to the irreducibility of R.

> **Theorem 0.19.3** (**Gauss Theorem**). R is a UFD $\Rightarrow$ $R[x]$ is a UFD.
>
> **Proof.**
>
> - Existence of irreducible decomposition: Let $f \in R[x]$ with $f \neq 0$ and $f \neq$ unit, view it as polynomial in $\mathbb{K}[x]$ and one can write $f = c(f)f'$ with $c(f) \in R$ and f' primitive in $R[x]$. Since $\mathbb{K}[x]$ is a UFD, then if $\deg(f) > 0$ can write:
>
> $$f' = g_1 \cdots g_r \quad \text{where } g_i \in \mathbb{K}[x] \text{ are irreducible}$$
> $$= c_1(g_1)g_1' \cdots c_r(g_r)g_r' \quad \text{where } g_i' \in R[x] \text{ are primitive and irreducible in } \mathbb{K}[x] \text{ since } g_i' \text{ is}$$
> $$\Rightarrow \text{ By Proposition } 0.19.3, g_i' \text{ is irreducible in } R[x]$$
> $$= \underbrace{c_1(g_1) \cdots c_r(g_r)}_{\text{a unit } \in R \text{ since } f' \text{ primitive}} \underbrace{g_1' \cdots g_r'}_{\text{primitive in } R[x]}$$
>
> If $c(f) \neq$ unit, since R is a UFD, then we can factor it out as:
>
> $$c(f) = \pi_1 \cdots \pi_s \quad \text{where } \pi_i \in R \text{ are irreducible, hence irreducible in } R[x] \text{ by Proposition } 0.19.3$$
>
> thus:
> $$f = \text{unit} \cdot \pi_1 \cdots \pi_s \cdot g_1' \cdots g_r'$$
>
> being the irreducible decomposition of f.
>
> - Uniqueness of irreducible decomposition: We saw that it is enough to show that f is irreducible in $R[x] \Rightarrow f$ is prime in $R[x]$ as in the proof of **Proposition** 0.17.4.
>
>   - **Case 1**: Let $f \in R$ be irreducible in R and R being a UFD, this means f is prime element in R. Consider the map:
>
> $$R \to R/(f) \quad \text{domain}$$
> $$\text{gives } R[x] \to R/(f)[x] \quad \text{surj. ring homo.}$$
> $$x \mapsto x$$
>
>   where $R/(f)[x]$ is a domain since $R/(f)$ is a domain. Now what is the kernel of this ring homomorphism? being $R[x]f$, see that $R[x]f$ is prime ideal since $R[x]/R[x]f$ is a domain, thus f is prime element in $R[x]$.
>
>   - **Case 2**: Let $\deg(f) \geq 1$ with f primitive and irreducible in $\mathbb{K}[x]$. $\mathbb{K}[x]$ is a UFD, then f is prime in $\mathbb{K}[x]$ since f is irreducible in it. We want to see f is prime in $R[x]$. Suppose $f \mid gh$ where $g, h \in R[x]$, the fact that f is prime in $\mathbb{K}[x]$ allows us to assume $f \mid g$ in $\mathbb{K}[x]$. Then one can write $g = fp$ for some $p \in \mathbb{K}[x]$. Since f is primitive, can write:
>
> $$c(g) = c(p) \cdot \text{unit}$$
>
>   with $c(g) \in R \Rightarrow c(p) \in R \Rightarrow p \in R[x]$ as
>
> $$p = c(p) \cdot p' \text{ where } p' \in R[x] \text{ is primitive in } R[x]$$
>
>   thus $f \mid g$ in $R[x]$.
>
> ■

0.20   Introduction to Algebraic Sets

In this section we shall give an introduction on algebraic geometry, basically try to build the bridge between algebra and geometry by showing the famous Hilbert's Nullstellensatz.

Let's fix a algebraic closed field k (e.g. $\mathbb{C}$) and define $\mathbb{A}_k^n = k^n$. Define:

$$R = k[x_1, \ldots, x_n]$$

Now given fixed $a = (a_1, \ldots, a_n) \in \mathbb{A}^n$, we look into the surjective ring homomprhism:

$$\varphi : R \longrightarrow k$$
$$f \longmapsto f(a_1, \ldots, a_n) = f(a)$$

The map is simply given by the polynomial evaluation at the point a. We can easily check that φ is a ring homomorphism and it is surjective since k is algebraically closed. Now we want to understand the kernel of φ.

Claim. $\ker(\varphi) = (x_1 - a_1, \ldots, x_n - a_n)$

Proof. For every $f \in R$, apply the division algorithm for f w.r.t. $x_1 - a_1, \ldots, x_n - a_n$, then for $f \in R$ we can write:
$$f = (x_1 - a_1)g_1 + \cdots + (x_n - a_n)g_n + b \quad b \in k$$
which implies $b = f(a)$. Hence $f(a) = 0 \Rightarrow f \in (x_1 - a_1, \ldots, x_n - a_n)$. This shows that $(x_1 - a_1, \ldots, x_n - a_n)$ is a maximal ideal since k being a field and implied by first isomorphism theorem. ∎

Our goal then is to show that every maximal ideal is **of this form**. We shall define several useful notions first.

Definition 0.20.1. For any ideal $I \subseteq R$ be ideal, define

$$V(I) := \{a \in \mathbb{A}^n \mid f(a) = 0 \ \forall f \in I\}$$

Namely those Nullstellen that shares among all the polynomials in the ideal.

Remark 0.20.1.

1. If $I = (f_1, \ldots, f_r) \Rightarrow V(I) = \{a \mid f_i(a) = 0 \ \forall 1 \le i \le r\}$.

   Proof. By $f = \sum f_i g_i$ and $f_i(a) = 0 \ \forall i \Rightarrow f(a) = 0$. ∎

2. Since R is Noetherian, then every $V(I)$ can be defined by finitely many equations. R is Noetherian is by the fact that k is Noetherian, as it only has two ideal, which follows definition of Noetherian. And that by the first remark, finitely generated ideal I will have $V(I)$ being expressed by finitely many equations.

See that it shall have the following **Properties**.

Remark 0.20.2.

1. $I \subseteq J \Rightarrow V(J) \subseteq V(I)$. As clearly more polynomial adding in will decrease the number of common Nullstellen.

2. $V(R) = \emptyset$. As one can clearly find polynomial that don't have any Nullstellens.

3. $V(\{0\}) = \mathbb{A}^n$. As the zero polynomial attains Nullstellen to be the whole space.

4. If (I_α) is a family of ideals, shall have:

$$V\left(\sum_\alpha I_\alpha\right) = \bigcap_\alpha V(I_\alpha)$$

Since the polynomial summing together will attains their Nullstellens being the intersections of the Nullstellen of the individual polynomial.

5. If I, J are ideals, then:

$$V(I) \cup V(J) = V(I \cap J) = V(IJ)$$

Proof. One shall clearly see that

$$IJ \subseteq I \cap J$$
$$I \cap J \subseteq I$$
$$I \cap J \subseteq J$$
$$\Rightarrow V(I) \cup V(J) \subseteq V(I \cap J) \subseteq V(IJ)$$

we want to see that:

$$V(IJ) \subseteq V(I) \cup V(J)$$

If this is not the case, there exists $a \in V(IJ)$, s.t. $a \notin V(I), a \notin V(J)$. It means that there exists $f \in I, g \in J$, s.t.

$$f(a) \neq 0 \quad g(a) \neq 0 \Rightarrow fg \in IJ \text{ but } fg(a) = f(a)g(a) \neq 0 \text{ as we are in a domain.}$$

But this leads to contradiction as a is taken as the nullstellen of polys in $IJ \notin$, the proof directly finish the whole inclusion chain. ∎

Definition 0.20.2 (Algebraic Subsets of $\mathbb{A}^n$). The sets of the form $V(I)$ are the algebraic subsets of $\mathbb{A}^n$.

Definition 0.20.3 (Zariski Topology). Properties 2, 3, 4, 5 in the above remark shows that $V(I)$ forms the closed sets for a topology **on** $\mathbb{A}^n$, which is the Zariski Topology.

One can also going the opposite direction by giving a sets of "Nullstellens" $Z \subseteq \mathbb{A}^n$ and ask the ideal who contains polynomials who have exactly those Nullstellens.

Definition 0.20.4. Given $Z \subseteq \mathbb{A}^n$, can define:

$$I(Z) = \{f \in R \mid f(a) = 0 \ \forall a \in Z\}$$

This is an ideal in R, and in fact it is a **radical ideal**.

The following easy properteis are straightforward to check:

Remark 0.20.3.

1. If $Z_1 \subseteq Z_2 \subseteq \mathbb{A}^n \Rightarrow I(Z_2) \subseteq I(Z_1)$. Which is straightforward as more Nullstellens results in smaller sets of corresponding polynomials who have such Nullstellens.

2. $I(Z_1 \cup Z_2) = I(Z_1) \cap I(Z_2)$. This is also straightforwards as those polys that have both of the sets as nullstallens will be exactly the intersection of $I(Z_1)$ and $I(Z_2)$.

Proposition 0.20.1. For every $Z \subseteq \mathbb{A}^n$, we have:

$$V(I(Z)) = \overline{Z}$$

where the closure is w.r.t. Zariski topology.

Proof. Recall that by definition of closure, have:

$$\overline{Z} = \bigcap_{Z \subseteq V(J)} V(J)$$

Then:

- $Z \subseteq V(I(Z)) \Rightarrow \overline{Z} \subseteq V(I(Z))$ as $V(I(Z))$ is closed set and $\overline{Z}$ is the smallest closed set containing Z.

- To show that $V(I(Z)) \subseteq \overline{Z}$, need to show that if $Z \subseteq V(J)$, then $V(I(Z)) \subseteq V(J)$. See that $Z \subseteq V(J) \Rightarrow J \subseteq I(Z) \Rightarrow J \subseteq I(Z) \Rightarrow V(J) \supseteq V(I(Z))$.

∎

Theorem 0.20.1 (**Hilbert's Nullstellensatz**)**.** If $J \subseteq R = k[x_1, \ldots, x_n] \Rightarrow I(V(J)) = \mathrm{rad}(J)$.

Remark 0.20.4.

1. $J \subseteq \underbrace{I(V(J))}_{\text{radical ideal}}$ is clear and thus $\mathrm{rad}(J) \subseteq I(V(J))$, one direction is quickly yielded, the interesting statement is the converse.

2. **Proposition** 0.20.1 + **Hilbert's Nullstellansatz** 0.20.1 reveals the following **mutual order reversing biijections**, which bridge the geometry and algebra and being the most openning and important theorem in Algebraic Geometry.

$$
\begin{matrix}
\text{Geometry} & & \text{Algebra} \\
\left\{ \begin{matrix} \text{Alg subsets} \\ \text{of } \mathbb{A}^n \end{matrix} \right\} & \begin{matrix} \xrightarrow{\ I(-)\ } \\ \xleftarrow[\ V(-)\ ]{} \end{matrix} & \left\{ \begin{matrix} \text{Radical ideals} \\ \text{in } R \end{matrix} \right\}
\end{matrix}
$$

Theorem 0.20.2 (**Weak Nullstellensatz**)**.** Every maximal ideal M in R is of the form $(x_1 - a_1, \ldots, x_n - a_n)$ for some $(a_1, \ldots, a_n) \in k^n$.

Proof. We'll only work with the proof in special case, namely when k is **uncountable**, which is the case for $\mathbb{C}$.

We will show: Given M being maximal ideal of R, there exists $a_1, \ldots, a_n$, s.t. $x_i - a_i \in M \ \forall \ i \Rightarrow \underbrace{(x_1 - a_1, \ldots, x_n - a_n)}_{\text{maximal ideal}} \subseteq M \Rightarrow M = (x_1 - a_1, \ldots, x_n - a_n)$. First notice we have the following morphism:

$$k \hookrightarrow R \longrightarrow {}^R\!/_M =: L \text{ being a field}$$

See that L is a vector space over k: L is generated by

$$\overline{\{x_1^{a_1} \cdots x_n^{a_n} \mid a_1, \ldots, a_n \in \mathbb{Z}_{\geq 0}\}}$$

the generation is quite clear if one revisit how R and thus R/M are constructed. Basically being the linear combination of the monomials in the form of $x_1^{a_1} \cdots x_n^{a_n}$. This implies that $\dim_k L$ is at most countable.

52

Now consider the k-algebra homomorphism:

$$k[y] \xrightarrow{\varphi} L$$
$$y \to \overline{x_i}$$

where $k[y]$ is a domain (not a field!). Now consider the situation of the kernel of φ:

- If $\ker(\varphi) = 0 \Rightarrow$ thus have the injection $\mathrm{Frac}(k[y]) \hookrightarrow L$. (It being a field, containing a domain, and thus must contain its fraction field).

  Note. $\{\frac{1}{y-\lambda} \mid \lambda \in k\}$ being a independent set over k. Thus it is uncountable as we assume $k = \mathbb{C}$, which leads to contradiction with previous reasoning that $\dim_k L$ at most countable $\natural$.

  Proof. Why is it independent set? Consider

  $$\sum_{i=1}^{r} c_i \frac{1}{y - \lambda_i} = 0$$
  $$\Rightarrow \sum_{i=1}^{r} c_i \prod_{j \neq i} (y - \lambda_j) = 0$$

  If we make $y = \lambda_k$, then

  $$\Rightarrow c_k \underbrace{\prod_{j \neq k} (\lambda_k - \lambda_j)}_{\neq 0} = 0 \underbrace{\Rightarrow}_{\text{by domain}} c_k = 0$$

  ∎

  Note. The injection here is important as it basically preserve the relation of dimensionality, which is the key to yield the contradiction. Besides that, the proof is quite like Lagrange interpolations, which is quite intuitive and straightforward.

  Thus there will be no case that $\ker(\varphi) = \{0\}$.

- If $\ker(\varphi) \neq \{0\} \Rightarrow \exists f \in k[y]$, s.t. $f(\overline{x_i}) = 0$ where the equality holds in target field L. Since k is algebraically closed, can factor f as $c(y - \lambda_1) \cdots (y - \lambda_m)$ where $c, \lambda_1, \ldots, \lambda_m \in k$. Thus

  $$c(\overline{x_i} - \lambda_1) \cdots (\overline{x_i} - \lambda_m) = 0 \Rightarrow \overline{x_i} = \lambda_j \in k \text{ for some } j \text{ as } L \text{ is a field}$$

  thus $\overline{x_i} \in k \Rightarrow \exists a_i \in k$, s.t. $\overline{x_i} = \overline{a_i} \Rightarrow x_i - a_i \in M$. Doing mapping repeatedly for all x_i will yield the desired result as we stated at the beginning of the proof.

  ∎

Proof of Hilbert's Nullstellensatz 0.20.1 (via Rabinowitsch's Trick). Suppose $f \in I(V(J))$, and we want to see that $\exists d > 0$, s.t. $f^d \in J$. Let's take $S = R[y] \supseteq J'$ being the ideal generated by J and g where

$$g = 1 - fy$$

Claim. $V(J') = \emptyset$.

If $a' = (a, \lambda) \in V(J')$ where $a \in k^n$ and $\lambda \in k \Rightarrow a \in V(J) \Rightarrow f(a) = 0$. Thus

$$g(a') = 1 - f(a)\lambda = 1 \neq 0$$

leading to contradiction $\lightning$ as a' is taken as the Nullstellen of g and thus $V(J') = \emptyset$.

If $J' \neq S$, then $J' \subseteq M$ where M be some maximal ideal. Then by **Weak Nullstellensatz** 0.20.2, have $V(M) \neq \emptyset \Rightarrow V(J') \neq \emptyset \lightning$. Hence $J' = S \Rightarrow$

$$\exists f_1, \ldots, f_m \in J$$
$$\exists g_1, \ldots, g_m; h \in S$$
$$\text{s.t. } 1 = f_1 g_1 + \cdots f_m g_m + h(1 - fy)$$

Let $T = \{f^p \mid p \geq 0\}$ and take advantadge of the following ring homomorphism:

$$R[y] \to R_f = T^{-1}R$$
$$y \mapsto \frac{1}{f}$$

In R_f, have:

$$1 = \sum_{i=1}^{m} f_i g_i(x_1, \ldots, x_n, \frac{1}{f}) \quad y \text{ here was localized into } \frac{1}{f}$$

If $d \gg 0$, then $f^d = f^d \cdot$ RHS $\in J$. Note that $f^d \cdot$ RHS is to erase all the f who is on the denominator, and thus $f^d \cdot$ RHS is a polynomial in R and it is in J by the ideal property. $\blacksquare$

Hilbert's Nullstellensatz is the beginning of Alegbraic Geometry, which allow us to use algerba to explain the property of geometry and vice versa.

0.21 Modules of Rings

In this section we look into modules of rings. Basically special structures of rings endowed on a abelian group. Note that a vector space is a module of a field. So we can build more intuition on modules based on what we learnt in vector spaces. It is also somewhat like the extension of group actions.

> **Definition 0.21.1** (R-**Module**). Fix a ring R. A <u>left R-module</u> M is an **abelian group** $(M, +)$ together with an operation $R \times M \to M$, written as $(a, u) \mapsto au$, such that
>
> 1. $1_R u = u \; \forall \, u \in M$.
>
> 2. $a(bu) = (ab)u \; \forall \, a, b \in R, u \in M$.
>
> 3. $a(u_1 + u_2) = au_1 + au_2 \; \forall \, a \in R, u_1 u_2 \in M$.
>
> 4. $(a_1 + a_2)u = a_1 u + a_2 u \; \forall \, a_1, a_2 \in R, u \in M$.
>
> A <u>right R-module</u> is defined similarly, with the operation $M \times R \to M$ written as $(u, a) \mapsto ua$, with the similar conditions, with the difference on the second one that:
>
> $$(ua)b = u(ab) \; \forall \, a, b \in R, u \in M$$

One may observe the duality between the left and right modules, and a direct question to ask is: How can we relate the notions of left module and right module?

Basically fix R, we can defined another ring R^{op} as the same abelian group of R, with the same addition, but the multiplication is defined as:
$$a \star b := ba$$

It is immediately clear that R^{op} with these operations is a ring, with $1_R = 1_{R^{\text{op}}}$ and see that $(R^{\text{op}})^{\text{op}} = R$.

> **Notation.**
>
> 1. R^M: M is a left R-module.
>
> 2. M_R: M is a right R-module.

Remark 0.21.1.

1. Left R-modules $\Leftrightarrow$ Right R^{op}-modules.

2. Right R-modules $\Leftrightarrow$ Left R^{op}-modules.

To check this, First fix M as a left modules of R, for $M_{R^{\text{op}}}$, define the scalar multiplication of modules as

$$ua := au \ \forall \ u \in M, a \in R$$

One then want to check the difference between the second condition, thus have:

$$(ba)u = b(au) = \underbrace{(ua)b}_{\text{switch to } M_{R^{\text{op}}}} \overset{?}{=} u(a \star b) = (a \star b)u = (ba)u$$

thus the quality with the question mark holds, which is what we intended.

Remark 0.21.2. R is commutative ring $\Leftrightarrow R^{\text{op}} = R$ ($R^{\text{op}} \cong R$). In this case, we simply say $\underline{R\text{-module}}$.

Example 0.21.1.

1. R has $\underline{\text{natural structures}}$ of both left and right R-modules given by the usual ring multiplication:

$$R \times R \to R$$
$$(a, b) \mapsto ab$$

with condition 2 holds because of the associativity of the ring multiplication.

2. If R is a field, an R-module is usually called a **vector space over** R.

3. If R is commutative, and $f : R \to S$ is an R-algebra, then one can view S has natural structure of both left and right R-modules, and they actually coincide by definition of R-algebra, the image of f commutes in S:

$$a \in R, u \in S \Rightarrow \begin{cases} au := f(a)u \\ ua := uf(a) \end{cases} \Rightarrow au = ua$$

Definition 0.21.2 (**Morphism of R-module**). If M, N are left R-modules, a $\underline{\text{morphism}}$ of left R-module $f : M \to N$ is an R-linear map, namely

1. f is a group homomprhism.

2. $f(au) = af(u) \ \forall \ a \in R, u \in M$.

Remark 0.21.3.

1. Id_M is a morphism of R-modules.

2. If $M_1 \overset{f}{\to} M_2 \overset{g}{\to} M_3$ are morphisms of left R-modules, then $g \circ f : M_1 \to M_3$ is also a morphism of left R-modules. Thus we get a Catgeory R-$\underline{\text{mod}}$ of left R-modules. And similarly, have a category $\underline{\text{mod}}$-R of right R-modules.

Note. A morphism of left R-modules $\Leftrightarrow$ A morphism of right R^{op}-modules.

Definition 0.21.3 (**Isomorphism**). An $\underline{\text{isomorphism}}$ of left R-modules is a morphism of left R-modules

55

55

8

$f : M \to M'$, s.t. there exists $g : M' \to M$ be morphism of left R-modules, s.t.

$$g \circ f = \mathrm{Id}_M; \quad f \circ g = \mathrm{Id}_{M'}$$

There are some easy properties for the scalar multiplication of a modules, quite similar from what we have done for vector spaces.

Remark 0.21.4.

1. $0_R u = 0_M \ \forall \ u \in M$.

   Proof. $0_R u = (0_R + 0_R)u = 0_R u + 0_R u$ and by cancellation of the abelian group M, done. ∎

2. $a0_M = 0_M \ \forall \ a \in R$.

   Proof. $a0_M + a0_M = a(0_M + 0_M) = a0_M$ and by cancellation of the abelian group M, done. ∎

3. $(-a)u = -(au) = a(-u)$.

   Proof.
   $$(-a)u + au = ((-a) + a)u = 0u = 0 \text{ by } 1 \Rightarrow \text{first equality}$$
   $$au + a(-u) = a(u + (-u)) = a_0 = 0 \text{ by } 2 \Rightarrow \text{second equality}$$
   ∎

Definition 0.21.4 (Submodule). If M is a left R-module, a <u>submodule</u> of M is a subset $N \subseteq M$ which is a subgroup and is closed under the scalar multiplication of M: $a \in R, u \in N \Rightarrow au \in N$. In this case, the operations on M induce operation on N that make N a left R-module, s.t.

$$i : N \to N$$
$$i(u) = u$$

is a morphism of left R-modules.

Example 0.21.2.

1. If we consider R as a left/right R-module, it's submodules are left/right ideals of R.

2. If $f : M \to M'$ is a morphism of left R-modules, the kernel is a submodule of M:

   $$\ker(f) := \{u \in M \mid f(u) = 0\}$$

   since $f(u) = 0 \Rightarrow f(au) = af(u) = a0 = 0$. Besides, the image is also a submodule of M', $\mathrm{Im}(f) \subseteq M'$, since $af(u) = f(au)$.

3. Trivial examples, Let R be ring:

   - 0_R-module: $\{0\}$.
   - M be any left R-module, have:
     $$\{0\} \subseteq M$$
     $$M \subseteq M$$
     be obvious submodule of M.

Remark 0.21.5. A morphism of R-module $f : M \to N$ of left R-modules is injective $\Leftrightarrow \ker(f) = 0$.

Remark 0.21.6. Suppose $R = \mathbb{Z}$, if M is a $\mathbb{Z}$-module, have

$$
n \cdot u = \begin{cases} \underbrace{u + u + \cdots + u}_{n \text{ times}} & n \geq 0 \\ \underbrace{-(u + u + \cdots + u)}_{-n \text{ times}} & n < 0 \end{cases}
$$

since $1u = u +$ distributivity. Conversely, if M is an abelian group, we put nu just the usual notations in abelian groups $\Rightarrow M$ is a $\mathbb{Z}$-module.

> **Conclusion 0.21.1.**
>
> - $\mathbb{Z}$-module $\Leftrightarrow$ abelian group.
>
> - morphism of $\mathbb{Z}$-modules $\Leftrightarrow$ morphism of abelian groups.

0.22 Direct Product of R-modules

> **Definition 0.22.1** (**Direct Product of R-modules**)**.** Fix R ring and a family $\{M_i\}_{i \in I}$ of left R-submodules. The <u>direct product</u> $\prod_{i \in I} M_i$ is the group direct product, i.e. on Cartesian product
>
> $$
> \prod_{i \in I} M_i \rightsquigarrow (a_i)_i + (b_i)_i = (a + b)_i
> $$
>
> with component-wise scalar multiplication:
>
> $$
> \lambda \cdot (a_i)_i = (\lambda a_i)_i \quad \forall \lambda \in R
> $$
>
> It is easy to check that $\prod_{i \in I} M_i$ is indeed a left R-module.

> **Remark 0.22.1.**
>
> 1. $(a_i)_i \in \prod_{i \in I} M_i$ is an element in the direct product, can imagine it as a big vector with the i-th entry is $a_i \in M_i$.
>
> 2. We have the following projection as the morphism of R-modules.
>
> $$
> \pi_j : \prod_{i \in I} M_i \to M_j
> $$
> $$
> (x_i)_i \mapsto x_j
> $$

> **Proposition 0.22.1** (**Universal Property of Direct Product of R-modules**)**.** Given any left R-module M and morphism of R-modules $f_i : M \to M_i$ for $i \in I$, there exists a unique morphism of R-module $f : M \to \prod_{i \in I} M_i$, s.t.
> $$
> \pi_j \circ f = f_j \quad \forall j \tag{4}
> $$
>
> **Proof.** Basically Formula 4 says that
> $$
> f(u) = (f_i(u))_i
> $$
>
> which gives a explicit formula and thus uniqueness is clear. For existence, we need to show that the above definition f is actually a morphism of R-modules. It is clear
>
> $$
> a(f_i(u))_i = af(u) \stackrel{?}{=} f(au) = (f_i(au))_i = (af_i(u))_i
> $$
>
> and the sum is basically the same thing. The morphism is basically inherit from the fact that f_i is a

morphism of R-modules. ■

0.23 Direct Sum of R-modules

Definition 0.23.1 (**Direct Sum of R-modules**)**.** Given a family of left R-modules $(M_i)_{i\in I}$, the <u>direct sum</u>

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

is a submodule of $\prod_{i\in I} M_i$, such that it is defined as:

$$\bigoplus_{i\in I} M_i = \{(a_i)_{i\in I} \mid a_i = 0 \text{ for all but } \textcolor{red}{\text{finitely}} \text{ many } i\}$$

One can check that this is indeed a submodule.

Remark 0.23.1. For each $j \in I$, we can define the dual notion of projection

$$\alpha_j : M_j \to \bigoplus_{i\in I} M_i$$

$$\alpha_j(u) = (u_i)_i$$

$$\text{where } u_i = \begin{cases} u, & \text{if } i = j \\ 0, & \text{otherwise} \end{cases}$$

Note that direct sum is actually a dual notion of direct product

Proposition 0.23.1 (**Universal Property of Direct Sum**)**.** Given any left R-module and family of R-module morphisms $f_j : M_j \to N$, there exists a unique morphism of R-module

$$f : \bigoplus_{i\in I} M_i \to N$$

s.t.

$$f \circ \alpha_j = f_j \quad \forall j \in I \tag{5}$$

Proof. The key point is that given any $u = (u_i)_{i\in I} \in \bigoplus_{i\in I} M_i$, have

$$u = \sum_{i\in I} \alpha_i(u_i)$$

which makes sense because of finite sum since only $\textcolor{blue}{\text{finitely}}$ many u_i are non-zero. If f satisfies formula 5, then

$$f(u) = \sum_{i\in I} f_i(u_i) \quad \forall \, u = (u_i)_i \in \bigoplus_{i\in I} M_i$$

this gives us a explicit formula and thus yield uniqueness. For existence, we define f by this formula and then it is clear that

$$f \circ \alpha_j = f_j \quad \forall j \in I$$

It remains to show that f is a $\textcolor{blue}{\text{morphism}}$ of R-modules, which is similar as what we done above for universal property of direct product. ■

Note. If I is finite, then

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

0.24 Quotient R-modules

Let M be a left R-modules and $N \subseteq M$ an R-submodule, in particular: N is a subgroup of M and as M is abelian, it is then automatically normal. Hence we have a quotient group M/N which is also an abelian group, with morphism of abelian groups

$$\pi : M \to {}^{M}\!/_{N}$$
$$\pi(u) = u + N$$

> **Claim.** We can make M/N a left R-module, s.t. π is morphism of R-modules.

Define:

$$R \times {}^{M}\!/_{N} \to {}^{M}\!/_{N}$$
$$(\lambda, u + N) \to \lambda u + N$$

To check that it is indeed well-defined, see that

$$\underbrace{u + N = u' + N}_{\Leftrightarrow u - u' \in N} \Rightarrow \underbrace{\lambda u + N = \lambda u' + N}_{\Leftrightarrow \lambda u - \lambda u' = \lambda(u - u') \in N}$$

which is ok since N is submodule and thus it is well-defined.

One can easily check that with this scalar multiplication, M/N becomes an R-module and π is a morphism of R-module.

> **Proposition 0.24.1** (**Universal Property of** M/N)**.** If $f : M \to M'$ is a morphism of left R-module, s.t. $N \subseteq \ker(f)$, then there exists a unique morphism of R-modules $\overline{f} : M/N \to M'$, s.t. the following diagram is commutative
>
> $$\begin{array}{ccc} M & \xrightarrow{\;f\;} & M' \\ {\scriptstyle \pi}\downarrow & \nearrow_{\overline{f}} & \\ M/N & & \end{array}$$
>
> namely
>
> $$\overline{f} \circ \pi = f$$
>
> .

> **Proof.** We already know this at the level of abelian groups:
>
> $$\overline{f} : {}^{M}\!/_{N} \to M', \quad u + N \mapsto f(u)$$
>
> It is only left to show it is indeed morphism of R-modules:
>
> $$\overline{f}(a \cdot (u + N)) \stackrel{?}{=} a \cdot \overline{f}(u + N) \quad \forall\, a \in R, u \in M$$
>
> and see that:
>
> $$\text{LHS} = \overline{f}(au + N) = f(au)$$
> $$\text{RHS} = \underbrace{af(u) = f(au)}_{f \text{ is morphism of } R-\text{module}} = \text{LHS}$$
>
> $\blacksquare$

> **Theorem 0.24.1** (**First Isomprhism Theorem**)**.** If $f : M \to M'$ is a surjective morphism of R-modules, the universal property of $M/\ker(f) \Rightarrow$ there exists a unique morphism of R-modules
>
> $$M\big/_{\ker(f)} \to M'$$
> $$\overline{u} = u + \ker(f) \mapsto u$$

> And this is an isomprhism of R-modules. It is clear that it is a <u>bijection</u> as we know from the case of abelian groups.

0.24.1 Submodules of M/N

Proposition 0.24.2. If $N \subseteq M$ is a submodule of a left R-module, then we have an order preserving bijection as follow:

$$\left\{ \begin{array}{c} \text{Submodules of} \\ M/N \end{array} \right\} \xrightleftharpoons[\pi(K) \rightsquigarrow N \subseteq K \subseteq M]{T \subseteq M/N \rightsquigarrow \pi^{-1}(T)} \left\{ \begin{array}{c} \text{Submodules of } M \\ \text{containing } N \end{array} \right\}$$

where

$$\pi : M \to {}^{M}\!/\!_{N}$$

Proof. We know this for abelian groups, it is only left to check they maps R-modules to R-modules, namely

1. If $T \subseteq M/N$ be R-submodule $\Rightarrow \pi^{-1}(T) \subseteq M$ is an R-submodule.

2. If $K \subseteq M$ be R-submodule $\Rightarrow \pi(K) \subseteq M/N$ is an R-submodule.

and we can use some beautiful tricks to prove it.

1. Have

$$\pi^{-1}(T) = \ker\left(M \xrightarrow{\pi} {}^{M}\!/\!_{N} \to {}^{M}\!/\!_{N}\big/{}_{T} \right)$$

2. Have

$$\pi(K) = \operatorname{Im}\left(K \hookrightarrow M \longrightarrow {}^{M}\!/\!_{N} \right)$$

■

Remark 0.24.1. If $N \subseteq K \subseteq M \Rightarrow$

$$\begin{array}{ccc}
K & \longrightarrow M \longrightarrow & M/N \\
\| & & \cup \text{I} \\
K & \longrightarrow & \pi(K)
\end{array}$$

and by first isomorphism theorem, we have

$$\pi(K) \cong {}^{K}\!/\!_{N}$$

Theorem 0.24.2 (Third Isomorphism Theorem). If $N \subseteq K \subseteq M$ be an R-submodule of M, then:

$$ {}^{M}\!/\!_{N}\Big/{}_{{}^{K}\!/\!_{N}} \cong {}^{M}\!/\!_{K}$$

Proof. Consider

$$\begin{array}{ccc}
M & \longrightarrow & M/K \\
\downarrow & \nearrow{}_{\varphi} & \\
M/N & &
\end{array}$$

where
$$M\big/_N \xrightarrow{\varphi} M\big/_K$$
$$u + N \mapsto u + K$$

see that φ is surjective, with

$$\ker(\varphi) = K\big/_N$$

and the first isomorphism theorem yields the result. ∎

Exercise. If M, N are left R-modules, have

$$\mathrm{Hom}_R(M, N) = \{f : M \to N \mid f \text{ is morphism of } R - \text{modules}\}$$

What structure does $\mathrm{Hom}_R(M, N)$ have? What operations can you put on it?

The answer is that it is always an abelian group, sometimes an R-module (if R is commutative!)

Remark 0.24.2. If R ring, M, N are (left) R-modules, then

- $\mathrm{Hom}_R(M, N)$ is an abelian group with operation defined:

$$(f + g)(m) := f(m) + g(m), \quad \forall m \in M$$

one can check that $f + g \in \mathrm{Hom}_R(M, N)$ and this operation makes $\mathrm{Hom}_R(M, N)$ an abelian group. The 0 element is given by the constant 0 map.

- We have
$$\mathrm{Hom}_R(M, N) \times \mathrm{Hom}_R(N, P) \to \mathrm{Hom}_R(M, P)$$
$$(f, g) \mapsto g \circ f$$

is additive in each factor. We want to make $\mathrm{Hom}_R(M, N)$ an R-module, we define:

$$(af)(u) := af(u) = f(au) \quad \forall a \in R, u \in M, f \in \mathrm{Hom}_R(M, N)$$

It is easy to see that af is additive, and need to see it is compatible with scalar multiplication:

$$(af)(bu) \stackrel{?}{=} b(af)(u) \quad \forall b \in R$$

see that

$$\mathrm{LHS} = af(bu) = (ab)f(u)$$
$$\mathrm{RHS} = (ba)f(u)$$

If R is commutative, thus making $\mathrm{LHS} = \mathrm{RHS}$, and makes $\mathrm{Hom}_R(M, N)$ an R-module.

- Let R being commutative, we have:

$$\mathrm{Hom}_R(R, M) \cong M$$
$$f \mapsto f(1)$$

which is isomorphism as R-module. Note that this is because if we choose $f : R \to M$ being morphism of R-modules, then $f(a) = af(1) \ \forall a \in R$. And thus the whole M is generated by $f(1)$.

0.25 Operations on Submodules

As submodules can be view as somekind of generalization of ideals, the construction in this section is pretty much like what we have done for the operation for ideals.

0.25.1 Intersection

Definition 0.25.1. If $(N_i)_{i \in I}$ be family of submodules of M, then

$$\bigcap_{i \in I} N_i \subseteq M$$

is a submodule, which is easily checked.

0.25.2 Submodule Generated by a Subset

Definition 0.25.2. If $A \subseteq M$ be any subset of the module, define:

$$\langle A \rangle := \bigcap_{\substack{N \subseteq M \\ N \text{ is a submodule} \\ A \subseteq N}} N$$

this is the smallest submodule of M conatining A, and is called the submodule generated by A. There is also a more explicit description of $\langle A \rangle$

$$\langle A \rangle = \left\{ \sum_{i=1}^{r} \lambda_i x_i \mid r \geq 0, x_i \in A, \lambda_i \in R \, \forall \, i \right\}$$

Proof. One can easily check that RHS is indeed a submodule, and it contains A, so it is immediate that $\langle A \rangle \subseteq$ RHS. If $A \subseteq M'$ where where M' being submodule of $M \Rightarrow$ RHS $\subseteq M' \Rightarrow$ RHS $\subseteq \langle A \rangle$. ∎

Note.

- $A \subseteq M$ is a system of generators of M if $\langle A \rangle = M$.

- M is called finitely generated if it has a finite system of generators.

0.25.3 The Sum of Submodules

Definition 0.25.3. Given a family $(M_i)_{i \in I}$ of submodules of M, define the sum of those submodules

$$\sum_{i \in I} M_i := \langle \bigcup_{i \in I} M_i \rangle$$

one can check that it also has a expclit description:

$$\sum_{i \in I} M_i = \left\{ \sum_{i \in I} x_i \mid x_i \in M_i \, \forall \, i \in I \text{ and only finitely many } x_i \text{ are non-zero.} \right\}$$

Notation. If $I = \{1, \ldots, n\}$, we write $M_1 + \cdots + M_n$.

Theorem 0.25.1 (**Second Isomorphism Theorem**)**.** If $M_1, M_2 \subseteq M$ are submodules, then:

$$M_1 \Big/ M_1 \cap M_2 \cong M_1 + M_2 \Big/ M_2$$

Proof. Consider the composition defined as follows:

$$f : M_1 \overset{i}{\hookrightarrow} M_1 + M_2 \overset{\pi}{\to} M_1 + M_2 \Big/ M_2$$

- This is surjective: given every element in $M_1 + M_2 / M_2$ is of the form $\pi(u_1 + u_2)$ with $u_i \in M_i$. But

$$\pi(u_1 + u_2) = \pi(i(u_1)) = \pi(u_1) = f(u_1)$$

- $\ker(f) = \{u \in M_1 \mid i(u) \in M_2\} = M_1 \cap M_2.$

and by first isomorphism theorem, yield:

$$M_1 \Big/ M_1 \cap M_2 = M_1 \Big/ \ker(f) \cong M_1 + M_2 \Big/ M_2$$

∎

0.25.4 Internal Direct Sums

Definition 0.25.4. If $M_1, M_2 \subseteq M$ being submodules, we have a morphism of R-modules

$$f : M_1 \oplus M_2 \longrightarrow M$$
$$(u_1, u_2) \longmapsto u_1 + u_2 \qquad u_i \in M_i$$

Say M is the <u>internal direct sum</u> of M_1, M_2 (write $M = M_1 \oplus M_2$) if f is an **isomorphism**. Which is equivalent to say

- f is surjective, $\Leftrightarrow M = M_1 + M_2$.

- f is injective, $\Leftrightarrow$

$$\begin{aligned} \ker(f) &= \{0\} \\ &= \{(u, v) \mid u_i \in M_i, u_2 = -u_1\} \\ &= \{(x, -x) \mid x \in M_1 \cap M_2\} \\ &\Leftrightarrow M_1 \cap M_2 = \{0\} \end{aligned}$$

Conclusion 0.25.1.

$$M = M_1 \oplus M_2 \Leftrightarrow \begin{cases} M_1 + M_2 = M \\ M_1 \cap M_2 = \{0\} \end{cases}$$

0.25.5 Functors Between R-**mod** and R / I-**mod**

Suppose $I \subseteq R$ be a 2-sided ideal, and M is a left R-module, s.t. $\forall\, a \in I, u \in M, au = 0$.

Claim. We have a natural structure of R / I-module on M, given by:

$$\overline{a}u := au \quad \forall\, \overline{a} \in R \Big/ I, u \in M$$

To check that this is well-defined, we need to check

$$\overline{a_1} = \overline{a_2} \Rightarrow a_1 u = a_2 u \quad \forall\, u \in M$$

see that:

$$\overline{a_1} = \overline{a_2} \Rightarrow a_1 - a_2 \in I \Rightarrow (a_1 - a_2)u = 0 \Rightarrow a_1 u = a_2 u$$

Suppose M is any left R-module, $I \subseteq R$ be an left ideal, define

$$IM := \langle \{au \mid a \in I, u \in M\} \rangle$$

$$\overset{\text{exer!}}{=\!=\!=\!=} \left\{ \sum_{i=1}^{r} a_i u_i \mid r \geq 0, a_i \in I, u_i \in M \;\forall\; i \right\}$$

Consider $\overline{M} := M \,/\, IM$, this satisfies:

$$\lambda \in I, \overline{u} \in \overline{M} \Rightarrow \lambda \overline{u} = \overline{\lambda u} = 0$$

Conclusion 0.25.2. If I is a two-sided ideal $\Rightarrow \overline{M}$ has a natural structure of $R\,/\,I$-module.

Note. The submodules are the same (whether viewed over R or over $R\,/\,I$).

Exercise. Show that we get in this way, a **functor**

$$R - \underline{\text{mod}} \to {}^{R}\!\big/_{I} - \underline{\text{mod}}$$

We need to check: if $f : M \to N$ is a morphism of R-modules, then we get a morphism of $R\,/\,I$-modules

$$M\big/_{IM} \to N\big/_{IN}$$
$$\overline{u} \mapsto \overline{f(u)}$$

0.26 Free Modules

It is difficult to studyy on modules where R is not a field, because in general there is no basis for such kinds of modules. Free modules along with their basis along us to understand ideal of rings in a larger context.

Definition 0.26.1 (**Free Modules**). Fix R be ring, and left R-module M. $A \subseteq M$ is linearly independent (over R) if for every relation
$$\sum \lambda_i x_i = 0$$
with $\lambda_i \in R$ and distinct $u_i \in A$ with all but **finitely many** $\lambda_i = 0$, $\Rightarrow \lambda_i = 0 \;\forall\; i$.
$\quad A \subseteq M$ is a basis of M if A is linearly independent and $\langle A \rangle = M$. M is free R-modules if it has a basis.

Remark 0.26.1. Keep in mind, if $R \neq$ field $\Rightarrow$ "**most**" R modules are **not free**.

Example 0.26.1.

- Suppose $a \in R \backslash \{0\}$ and R be commutative ring, a is not a unit. Then
$$M = {}^{R}\!\big/_{(a)} \neq 0$$
  don't have a basis since every element $u \in M$ sarisfies $au = 0 \Rightarrow$ there is no non-empty linearly independent subset $\Rightarrow M \neq$ free R-modules.

- R is free module as a left R-module with basis being 1.

By combining the universal property of direct sums and the description of R-module morphism $R \to N$, implies the **Universal Property** of $R^{(I)}$: $\forall$ R-module N, and $\forall \, (u_i)_{i \in I}$, $u_i \in N \; \forall \, i$, $\exists \, ! \, R$ -module homomorphism $f : R^{(I)} \to N$, s.t. $f(e_i) = u_i \; \forall \, i$. Basically we only need to specify where e_i goes to secure the whole morphism.

Note.

-
$$\text{Im}(f) = \left\{ \sum a_i u_i \mid a_i \in R, \text{ only finitely many } \neq 0 \right\}$$
$$= \text{submodule } \langle \{ u_i \mid i \in I \} \rangle$$
$$= \sum_{i \in I} R u_i$$

$\Rightarrow \{ u_i \mid i \in I \}$ is system of generator of N iff f is surjective.

- f injective iff the $u_i, i \in I$ are **linearly independent**.

- f is isomorphism iff the $u_i, i \in I$ form a **basis** of N.

- In particular, <u>a module is free</u> iff it is **isomorphic to some** $R^{(I)}$.

Theorem 0.26.1 (Linear Algebra Facts).

- Every vector space over a field has a basis.

- Moreover, any basis have the same cardinality.

When over a ring R:

- We saw that many R-modules are **not free**.

- If R commutative, then can reduce modulo a maximal ideal to show that any 2 basis of a free left R-module have the same cardinality.

- If R is not commutative, then it can happen that

$$R \cong R \oplus R$$

as left R-module.

The above statements will be proved in **Practice Set 2**, and supply here later.

0.27 Nakayama's Lemma

Basically Nakayama's Lemma gives us some idea on how to relate module of arbitrary ring to a module of a field.

Lemma 0.27.1 (Nakayama's Lemma). Let's fix $R, \underline{m}$ a local ring being $R \neq \{0\}$ is commutative and the only maximal ideal is $\underline{m}$. If M is a finitely generated R-module, such that $M = \underline{m}M$, then $M = \{0\}$.

One may wonder the significance of Nakayama's Lemma, basically it gives us a functor

$$F : R - \underline{\text{mod}} \to {}^{R}/{\underline{m}} - \underline{\text{mod}}$$

$$F(M) = {}^{M}/{\underline{m}M}$$

While we lose some information when applying F, the lemma says that:

$$F(M) = \{0\} \Rightarrow M = \{0\}$$

thus we can recover some of the information.

Corollary 0.27.1. If M is finitely generated over R, and $(R, \underline{m})$ is local, have $N \subseteq M$ be submodule, then $M = N + \underline{m}M \Rightarrow M = N$.

Proof. Apply **Nakayama's Lemma** to $\overline{M} = M \,/\, N$, which is finitely generated as well, have:

$$\underline{m} \cdot {}^{M}/{N} = {}^{(\underline{m}M + N)}/{N} = {}^{M}/{N}$$

$$\Rightarrow {}^{M}/{N} = \{0\} \Rightarrow M = N$$

where $\underline{m}M + N$ being the smallest submodule containing $\underline{m}M$ and N. ∎

Corollary 0.27.2. If M is finitely generated over R, and $(R, \underline{m})$ being local ring, then $u_1, \ldots, u_n \in M$ is a system of generators iff $\overline{u_1}, \ldots, \overline{u_n} \in M \,/\, \underline{m}M$ is a system of generators over $R \,/\, \underline{m}$.

Proof. The "only if" part is clear. Now suppose that $\overline{u_1}, \ldots, \overline{u_n} \in M \,/\, \underline{m}M$ is a system of generators. Let $N = \sum_{i=1}^{n} R u_i$ be submodule of M, thus system of generators gives us:

$$M = \underline{m}M + N \xrightarrow{\text{Cor } 0.27.1} N = M$$

thus $u_1, \ldots, u_n$ is system of generators of M. ∎

Proof of Nakayama's Lemma 0.27.1. Let's choose $u_1, \ldots, u_n$ be system of generators of M. Have $M = \underline{m}M \Rightarrow$

$$\forall i, u_i = \sum_{j=1}^{d_i} a_{ij} v_{ij} \quad a_{ij} \in \underline{m}, v_{ij} \in M$$

and can write

$$v_{ij} = \sum_{k=1}^{n} b_{ijk} u_k \quad b_{ijk} \in R$$

thus

$$u_i = \sum_{j=1}^{d_i} a_{ij} \sum_{k=1}^{n} b_{ijk} u_k$$

$$= \sum_{k=1}^{n} c_{ik} u_k \qquad c_{ik} = \sum_{j=1}^{d_i} a_{ij} b_{ijk} \in \underline{m}$$

using the matrix notation, let $C = (c_{ij})_{1 \leq i,j \leq n}$, have:

$$(I_n - C) \cdot \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = 0$$

Multiply on the left by the classical adjoint of $(I_n - C)$, yields that:

$$\det(I_n - C) \cdot I_n \cdot \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = 0 \Rightarrow \det(I_n - C) \cdot u_i = 0 \; \forall \; i$$

Notice that:

$$\det(I_n - C) = \begin{vmatrix} 1 - c_{11} & -c_{12} & \cdots & -c_{1n} \\ -c_{21} & 1 - c_{22} & \cdots & -c_{2n} \\ & & \ddots & \\ -c_{n1} & -c_{n2} & \cdots & 1 - c_{nn} \end{vmatrix} = 1 + \alpha \text{ for some } \alpha \in \underline{m}$$

Since $(R, \underline{m})$ is local and $\alpha \in \underline{m}$ with $\underline{m}$ contains all it's invertible elements, thus $1 + \alpha$ is invertible. Thus $u_i = 0 \; \forall \; i \Rightarrow M = \{0\}$. ∎

Check proof here.

Definition 0.27.1 (**Noetherian (Artinian) Module**). M is a Noetherian (Artinian) R-module if $\nexists$ infinitely **strictly increasing (resp. decreasing)** sequence of submodules of M.

Note. By definition, R is left Noetherian/Artinian iff R is Noetherian/Artinian as left R-module.

Proposition 0.27.1. For a left R-module M, **TFAE**:

1. M is Noetherian.

2. Every non-empty family of submodules of M contains a maximal element w.r.t. inclusion.

3. Every submodule of M is finitely generated.

Proof. Follows the same word by word as for the case $M = R$. See the proof for **Proposition** 0.13.1.
∎

Proposition 0.27.2. If M is a left R-module and $N \subseteq M$ is a submodule, then M is Noetherian (Artinian) iff N and $M \, / \, N$ are Noetherian (resp. Artinian).

Proof. We'll treat the Noetherian case, the Artinian case is similar. If M is Noetherian, this impiles:

- N is Noetherian, since every sequence of submodules of N is also a sequence of submodules of M.

- $qoMN$ is Noetherian: Let

$$\pi : M \hookrightarrow {}^M/_N$$

be the canonical morphism. Given a sequence of submodules of $M \, / \, N$ denoted as:

$$Q_1 \subseteq Q_2 \subseteq \cdots \subseteq {}^M/_N$$

thus have:

$$\pi^{-1}(Q_1) \subseteq \pi^{-1}(Q_2) \subseteq \cdots \subseteq M$$

be seuquence of submodules of M. Since M is Noetherian, then there exists n_0, s.t. $\pi^{-1}(Q_n) = \pi^{-1})(Q_{n+1}) \; \forall \; n \geq n_0$, thus:

$$Q_n = \pi(\pi^{-1}(Q_n)) = \pi(\pi^{-1}(Q_{n+1})) = Q_{n+1} \; \forall \; n \geq n_0$$

Conversely, suppose N and M/N are Noetherian, and suppose we have sequence of submodules of M denoted as:
$$P_1 \subseteq P_2 \subseteq \cdots \subseteq M$$
thus we have sequence of submoduels of N denoted as:
$$P_1 \cap N \subseteq P_2 \cap N \subseteq \cdots \subseteq N$$
Since N is Noetherian, there exists n_1, s.t.
$$P_n \cap N = P_{n+1} \cap N \; \forall \, n \geq n_1 \tag{6}$$
M/N is Noetherian implies that after enlarging n_1, may assume:
$$\pi(P_n) = \pi(P_{n+1}) \; \forall \, n \geq n_1$$
and note that:
$$\pi(P_n) = {}^{(P_n + N)}\!/_N \Rightarrow P_n + N = P_{n+1} + N \; \forall \, n \geq n_1 \tag{7}$$
where $P_n + N$ is the smallest submodules of M conatins both P_n and N. By **Equation** 6 and **Equation** 7, we have:
$$P_n = P_{n+1} \; \forall \, n \geq n_1$$
Now if
$$u \in P_{n+1} \xRightarrow{\text{eq } 7} u = v + w, \; v \in P_n, w \in N$$
$$\text{with } w = \underbrace{u}_{\in P_{n+1}} - \underbrace{v}_{\in P_n \subseteq P_{n+1}} \Rightarrow w \in P_{n+1} \cap N$$
$$\xRightarrow{\text{eq } 6} w \in P_n \cap N \subseteq P_n$$
$$\Rightarrow u = v + w \in P_n$$
∎

Note. We have:
$$\pi^{-1}(\pi(P_n)) = P_n + N$$
the $\supseteq$ is clear, for $\subseteq$, see that $a \in \pi^{-1}(\pi(P_n))$, then there exists $b \in P_n$, $a - b \in N \Rightarrow a \in P_n + N$.

Corollary 0.27.3. If M, N are left R-modules, then $M \oplus N$ is Noetherian (Artinian) iff both M, N are Noetherian (Artinian).

Proof. Use the surjective morphism:
$$M \oplus N \xrightarrow{p} M$$
$$p(u, v) = u$$
see that we have $\ker(p) \cong N$ and by proposition we are done. ∎

Now we want to relate the Noetherian module by Noetherian ring.

Corollary 0.27.4. If R is left Noetherian ring, then a left R-module M is Noetherian iff M is finitely generated.

Note. It allow us to only need to check itself being Noetherian instead of checking all its submodules.

Proof. The $\Rightarrow$ part is clear, consider the $\Leftarrow$ part. By hypothesis, R is Notherian as a left R-module,

thus by **Corollary** 0.27.3 and using induction on n, see that:

$$R^n \text{ is a Noetherian module.} \left(\bigoplus_{i=1}^{n} R \right)$$

If M is a finitely generated R-module, and $u_1, \ldots, u_n \in M$ are its generators, we define;

$$\varphi : R^n \to M$$
$$\varphi(e_i) = u_i \quad \forall\, 1 \le i \le n$$
$$e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \text{ with } 1 \text{ at the } i\text{-th position}$$

we can do this since φ is a free module, and we only need to specify where its basis goes. Since $u_1, \ldots, u_n$ generates M this means φ is surjective. Since R^n is Noetherian $\xrightarrow{\text{prop } 0.27.2}$ M is Noetherian.

∎

Exercise. An artinian R-module might not be finitely generated. Consider

$$M := \mathbb{C}[x]_x \big/ \mathbb{C}[x]$$

being module over $R := \mathbb{C}[x]$, where $\mathbb{C}[x]_x$ being $\mathbb{C}[x]$ localized over x, being the Laurent polynomials (Poly of the form $\frac{1}{x^n}$). Check that M is Artinian, but not finitely generated.

0.28 More Catgeorical Terminology

Definition 0.28.1 (**Kernel**)**.** If $f : M \to N$ be morphism of left R-module, a <u>kernel</u> of f is a morphism of left R-modules

$$K \xrightarrow{u} M$$

such that:

- $f \circ u = 0$.

- u is universal with this property. Namely if $v : Q \to M$ is such that $f \circ v = 0$, then there exists a unique morphism $g : Q \to K$, such that the following diagram is commutative:

$$
\begin{array}{ccc}
K & \xrightarrow{\ u\ } & M \\
& \nwarrow_{g} \quad \nearrow_{v} & \\
& Q &
\end{array}
$$

As usual, if $K' \xrightarrow{u'} M$ also satisfies this, then we have:

$$
\begin{array}{ccc}
K & \xrightarrow{\ u\ } & M \\
{\scriptstyle \simeq}\downarrow{\scriptstyle \theta} & \nearrow_{u'} & \\
K' & &
\end{array}
$$

there exists a unique isomorphism θ, s.t. $u' \circ \theta = u$.

Claim. Let:

$$\ker(f) \xhookrightarrow{i} M \xrightarrow{f} N$$

then i is a kernel of f.

- Clearly: $f \circ i = 0$.

- if $v : Q \to M$, s.t. $f \circ v = 0 \Rightarrow \text{Im}(f) \subseteq \ker(f)$, thus existence and uniqueness of g is clear. Uniqueness yield since i is injective.

Definition 0.28.2 (**Cokernel**). Let $f : M \to N$ be a morphism of R-modules. A <u>cokernel</u> of f is a morphism $p : N \to C$, such that:

- $p \circ f = 0$.

- p is universal with this property. Namely, if $q : N \to Q$ is such that $q \circ f = 0$, then there exists a unique morphism $h : C \to Q$, such that the following diagram commutes:

$$M \xrightarrow{f} N \xrightarrow{p} C$$
$$q \searrow \quad \downarrow h$$
$$Q$$

As usual, if $p' : N \to C'$ also satisfies this property, then we have the following diagram:

$$M \xrightarrow{f} N \xrightarrow{p} C$$
$$p' \searrow \quad \downarrow \theta$$
$$C'$$

where there exists a unique isomorphism θ, s.t. $\theta \circ p = p'$.

Claim. The projection morphism:

$$p : N \to \left. N \middle/ f(M) \right.$$

is a cokernel of f.

- Clearly: $p \circ f = 0$.

- For any other $p' : N \to C'$ with $p' \circ f = 0$, we have the commutative diagram:

$$M \xrightarrow{f} N \xrightarrow{p} N / f(M)$$
$$p' \searrow \quad \downarrow g$$
$$C'$$

See that $p' \circ f = 0 \Rightarrow f(M) \subseteq \ker(p') \Rightarrow$ existence + uniqueness of g follows from the universal property of quotient module.

Definition 0.28.3 (**Exact Sequence**). A sequence of morphisms of R-modules is <u>exact at A_2</u> if $\text{Im}(f_1) = \ker(f_2)$:

$$\cdots \to A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} A_3 \to \cdots$$

and is <u>exact</u> if it is exact everywhere.

Definition 0.28.4 (**Short Exact Sequence**). A <u>short exact sequence</u> is a sequence:

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

which is <u>exact</u>, which is equivalent to saying:

$$\begin{cases} \ker(f) = 0 \Leftrightarrow f \text{ is injective.} \\ \text{Im}(f) = \ker(g) \\ \text{Im}(g) = M'' \Leftrightarrow g \text{ is surjective.} \end{cases}$$

which is equivalent to saying f gives an isomorphism of M' onto a submodule of $f(M')$ of M and g induces an isomorphism:

$$M\big/ f(M') \cong M''$$

Exercise. Given a short exact sequence as follows:

$$0 \longrightarrow M' \underset{p}{\overset{f}{\rightleftarrows}} M \underset{i}{\overset{g}{\rightleftarrows}} M'' \longrightarrow 0$$

then **t.f.a.e.**

1. $\exists$ morphism $p : M \to M'$, s.t. $p \circ f = \text{Id } M'$.

2. $\exists$ morphism $i : M'' \to M$, s.t. $g \circ i == \text{Id}_{M''}$.

3. $\exists$ submodule $N \subseteq M$, s.t.
$$M = f(M') \oplus N$$
   and g induces an isomorphism $N \cong M''$.

such a short exact sequence is called **split exact sequence**.

Appendix