Math494: Honors Algebra II

Yanzhi Li

February 3, 2026

Abstract

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

Contents

Chapter 1

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.

1.1 Ring and Ring Homomorphism

Definition 1.1.1 (Ring). A Ring 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 1.1.1.

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

Example 1.1.1.

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 1.1.1. 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 1.1.2 (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 1.1.2.

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 1.1.2. 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 1.1.3. 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** Rings:

- Objects: rings.
- Morphisms: ring homomorphisms.
- composition: usual function composition.

Definition 1.1.3 (Ring Isomorphism). If R, S are rings, a ring isomorphism $R \to S$ 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 Rings.

We say R and S are isomorphic, write $R \cong S$ if $\exists$ ring isomorphism $R \to S$.

Proposition 1.1.2. 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 1.1.3 (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**.

1.2 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 **unitary ring**.

Definition 1.2.1 (Subring). Let R be a ring. A 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 1.2.1. 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 1.2.1. 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.

■

Example 1.2.1.

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

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

Proposition 1.2.2. If $f : R \to S$ is ring homomorphism, then $\mathrm{Im}(f) \subseteq S$ is a subring.

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

Definition 1.2.2 (Ideal). Suppose R be a ring and $I \subseteq R$ and $I \neq \emptyset$. Then

1. I is a <u>left ideal</u> (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 <u>right ideal</u> (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 <u>two-sided ideal</u> if it is both left and right ideal.

If R is **commutative**, then all the above definition coincide, so we simply say <u>ideal</u> in this case.

Remark 1.2.2.

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.

Example 1.2.2.

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 1.2.3. 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 1.2.4. 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 ring 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.

∎

1.3 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:

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

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:

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

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

- multiplication is associative.

$$\underbrace{\underbrace{(\overline{a}\overline{b})\overline{c}}_{=\overline{ab}\overline{c}=\overline{(ab)c}} = \underbrace{\overline{a}(\overline{b}\overline{c})}_{=\overline{a}\overline{bc}=\overline{a(bc)}}}_{\text{by associativity in } R} \qquad \forall\, \overline{a}, \overline{b}, \overline{c} \in {}^{R}\big/_{I}$$

- 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 1.3.1 (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**:

$$\begin{tikzcd} R \arrow[r, "\pi"] \arrow[d, "f"'] & R\,/\,I \arrow[dl, dashed, "\overline{f}"] \\ S & \end{tikzcd}$$

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:

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

■

1.4 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 1.4.1 (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 $\mathrm{Im}(f) \cong R/I$.

Remark 1.4.1. If f be arbitrary ring homomorphism, then $\mathrm{Im}(f) \subseteq S$ 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:

$$\begin{tikzcd} R \arrow[r, "\pi"] \arrow[d, "f"'] & R/I \arrow[dl, dashed, "\overline{f}"] \\ S & \end{tikzcd}$$

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. ■

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 1.4.1. We have an order preserving bijection:

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

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

$$ {}^{{}^{R}\!/_{I}}\!\big/_{{}^{I'}\!/_{I}} \cong {}^{R}\!/_{I'} $$

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

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

and the theorem implies:

$${}^{\mathbb{Z}}\big/_{n\mathbb{Z}}\big/_{(\overline{d})} \cong {}^{\mathbb{Z}}\big/_{d\mathbb{Z}}$$

1.5 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 1.5.1. 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. $(\sum_{i=0}^{n} a_i x^i) \cdot (\sum_{j=0}^{m} b_j x^j) := \sum_{k=0}^{m+n}(\sum_{i+j=k} a_i b_j)x^k$.

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

1. The following diagram is commutative:

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "i"'] & S \\ R[X] \arrow[ur, "\psi"'] & \end{tikzcd}$$

   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:

$$\begin{aligned}
PQ &= \sum_{k=0}^{m+n} \left(\sum_{i+j=k} \alpha_i \beta_j \right) x^k \\
\Rightarrow \psi(PQ) &= \sum_{k=0}^{m+n} \varphi \left(\sum_{i+j=k} \alpha_i \beta_j \right) a^k \\
&= \sum_{k=0}^{m+n} \left(\sum_{i+j=k} \varphi(\alpha_i) \cdot \varphi(\beta_j) \right) a^k \quad (\varphi \text{ is a ring homomorphism}) \\
\text{And} \quad \psi(P)\psi(Q) &= \left(\sum_{i=0}^{n} \varphi(\alpha_i) a^i \right) \cdot \left(\sum_{j=0}^{m} \varphi(\beta_j) a^j \right) \\
&= \sum_{i=0}^{n} \sum_{j=0}^{m} \varphi(\alpha_i)\varphi(\beta_j) a^j \\
&= \sum_{k \geq 0} \left(\sum_{i+j=k} \varphi(\alpha_i)\varphi(\beta_j) \right) a^{i+j=k} \quad (R \text{ is commutative}) \\
&= \psi(PQ)
\end{aligned}$$

■

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:

$$R[X_1, \dots, X_n] := (R[X_1, \dots, X_{n-1}])[X_n]$$

This is again a commutative ring.

Theorem 1.5.2 (Universal Property of R[$\mathbf{X}_1, \dots, \mathbf{X}_n$]). $\forall$ ring homomorphism $\varphi : R \to S$, R, S commutative, and $\forall\ a_1, \dots, a_n \in S$, there exists a **unique** ring homomorphism $\psi : R[X_1, \dots, X_n] \to S$, s.t.

1. the following diagram is commutative:

$$\begin{tikzcd}
R \arrow[r] \arrow[dr, "\varphi"'] & R[x_1] \arrow[r] & R[x_1, x_2] \arrow[r] & \dots \arrow[r] & R[x_1, \dots, x_n] \arrow[dlll, "\psi"] \\
 & S & & &
\end{tikzcd}$$

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

Example 1.5.1. $X_1^2 + X_1 X_3 + X_2^4 \in R[X_1, X_2, X_3]$

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

Example 1.5.2. If $\sigma \in S_n \Rightarrow \exists!$ ring homomoprhism, s.t. the following diagram is commutative:

$$\begin{tikzcd} R \arrow[r] \arrow[d] & R[X_1,\dots,X_n] \\ R[X_1,\dots,X_n] \arrow[ur, "f_\sigma"] & \end{tikzcd}$$

and $f_\sigma(x_i) = X_{\sigma(i)} \quad \forall i$. 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 $R[X_1,\dots,X_n]$ is just labelling anmd **doesn't matter with order** of $X_1,\dots,X_n$.

Notation. Every element of $R[X_1,\dots,X_n]$ can be written as

$$f = \sum_{u=(u_1,\dots,u_n)\in\mathbb{Z}^n_{\geq 0}} a_u X^u$$

where $X^u = X_1^{u_1}\cdots X_n^{u_n}$ with $a_u \in R$ which is a monomial.

Example 1.5.3.

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

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

Definition 1.5.2 (Ring of Formal Power Series). Suppose R a commutative ring, define the ring of formal power series 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:

$$\left(\sum_{i\geq 0} a_i x^i\right)\cdot\left(\sum_{j\geq 0} b_j x^j\right) := \sum_{k\geq 0} c_k x^k$$

$$\text{where} \qquad c_k = \sum_{i+j=k} a_i b_j \in R$$

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

1.5.1 R-Algebra

Definition 1.5.3 (R-Algebra). Suppose that R is a commutative ring, an R-Algebra 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 1.5.4.

1. $R[X]$, $R[[X]]$ have natural structures of R-Algebras $R[X_1,\dots,X_n]$.

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

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

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:

$$\begin{tikzcd} R \arrow[r] \arrow[dr] & S_1 \arrow[d, "u_1"] \\ & S_2 \end{tikzcd}$$

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

1.6 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 1.6.1 (Invertible). Fix a ring R, $a \in R$ is invertible if there exists $b \in R$, s.t. $ab = 1_R = ba$. b is the inverse of a and denoted as a^{-1}.

Definition 1.6.2 (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.

Example 1.6.1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields, $\mathbb{Z}$ is not a field.

Definition 1.6.3 (Zero-Divisor). If R is a commutative ring, $a \in R$ is a zero-divisor if $\exists\ b \neq 0$ in R, s.t. $ab = 0$. Otherwise, we say a is a non-zero-divisor.

Definition 1.6.4 (Integral Domain). A ring R is an integral domain or simply a domain 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 1.6.1. 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 1.6.2. If $n > 0$, then $\mathbb{Z} / n\mathbb{Z}$ is a domain if and only if n is **prime number**.

Proof. Suppose $\overline{a}, \overline{b} \in \mathbb{Z} / n\mathbb{Z}$, with $\overline{a}, \overline{b} \neq 0 \Leftrightarrow a \nmid a, n \nmid b$, 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 1.6.1. 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:

$$\begin{aligned} b &= (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0 \\ \Rightarrow b &= 0 \end{aligned}$$

■

Proposition 1.6.2. 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 function given by:

$$\begin{aligned} f &: R \to R \\ f(b) &= ab \end{aligned}$$

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

Remark 1.6.2. 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 1.6.5 (Degree of R[X]). Fix R to be a commutative ring. If $f \in R[X]$, $f \neq 0$, write:

$$f = a_0 + a_1x + \cdots + a_nx^n$$

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

Remark 1.6.3. $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$

Proposition 1.6.3. 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 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.

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:

$$\begin{aligned} fg &= \sum_{k\geq 0}\left(\sum_{i+j=l} a_ib_j\right)x^k \\ &= \underbrace{a_mb_n}_{\neq 0}x^{m+n} + \text{ lower degree monomials} \end{aligned}$$

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

Corollary 1.6.1. 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. ■

1.7 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 1.7.1 (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:

$$(a_1, s_1) \sim (a_2, s_2) \Leftrightarrow s_2a_1 = s_1a_2$$
$$\text{denoted as} \qquad \frac{a_1}{s_1} = \frac{a_2}{s_2}$$

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

$$\begin{aligned} (a, s) \sim (a', s') &\quad (a', s') \sim (a'', s'') \\ \Leftrightarrow s'a = sa' &\quad s''a' = s'a'' \end{aligned}$$

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 1.7.2. 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.

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:

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

We now interest in:

$$\begin{aligned} t_1t_2s'(s''a - sa'') &= t_2s''\underbrace{t_1(s'a - sa')}_{=0} + \underbrace{t_2t_1s''sa' - t_1t_2s'sa''}_{=t_1s\,\underbrace{t_2(s''a' - s'a'')}_{=0}} \\ &= 0 \\ &\Rightarrow (a, s) \sim (a'', s'') \end{aligned}$$

note that $t_1t_2s' \in S$ since $s', t_1, t_2 \in S$ and S being a multiplication system.

∎

And thus we denote:

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

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

$$\begin{aligned} \frac{a_1}{s_1} + \frac{a_2}{s_2} &:= \frac{s_2a_1 + s_1a_2}{s_1s_1} \\ \frac{a_1}{s_1} \cdot \frac{a_2}{s_2} &:= \frac{a_1a_2}{s_1s_2} \end{aligned}$$

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:

$$\frac{s_2a_1 + s_1a_2}{s_1s_2} = \frac{t_2b_1 + t_1b_2}{t_1t_2} \tag{1.1}$$

$$\frac{a_1a_2}{s_1s_2} = \frac{b_1b_2}{t_1t_2} \tag{1.2}$$

Proof of Equation 1.1. By our hypothesis, there exists $u, v \in S$, s.t.:

$$\begin{aligned} u(t_1a_1 - s_1b_1) &= 0 \\ v(t_2a_2 - s_2b_2) &= 0 \end{aligned}$$

Consider:

$$t_1t_2(s_2a_1 + s_1a_2) - s_1s_2(t_2b_1 + t_1b_2) = t_2s_2(t_1a_1 - s_1b_1) + t_1s_1(t_2a_2 - s_2b_2)$$

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 1.2. Similarly:

$$t_1t_2a_1a_2 - s_1s_2b_1b_2 = t_2a_2(t_1a_1 - s_1b_1) + s_1b_1(t_2a_2 - s_2b_2)$$

Multiply $uv \in S$, we get 0. ■

Proposition 1.7.1. 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 $(+)$:

$$\begin{aligned}\left(\frac{a_1}{s_1} + \frac{a_2}{s_2}\right) + \frac{a_3}{s_3} &= \frac{s_2a_1 + a_2s_1}{s_1s_2} + \frac{a_3}{s_3} \\ &= \frac{s_3s_2a_1 + s_3a_2s_1 + a_3s_1s_2}{s_1s_2s_3} \\ &= \frac{a_1}{s_1} + \left(\frac{a_2}{s_2} + \frac{a_3}{s_3}\right) \qquad \text{by symmetry}\end{aligned}$$

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

Remark 1.7.1. $S^{-1}R$ has a canonical structure of R-Algebra with the following canonical ring homomorphism:

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

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

Remark 1.7.2. $a \in \ker(\varphi) \Leftrightarrow \frac{a}{1} = \frac{0}{1} \Leftrightarrow \exists\, s \in S$, s.t. $sa = 0$.

Hence: φ is not injective if and only if $\exists\, s \in S$, which is a **zero divisor**.

Remark 1.7.3. $S^{-1}R = \{0\}$ iff $0 \in S$, it tells us in general we don't care about the case where $0 \in S$.

Example 1.7.1. Let R be a integral domain, 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 $s_2a_1 - s_1a_2 = 0$.

Example 1.7.2. 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;

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[dr, "\psi"'] & S^{-1}R \arrow[d, dashed, "f"] \\ & T \end{tikzcd}$$

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
$$f(1) = 1$$

■

1.8 Prime Ideals and Maximal Ideals

In this section we shall discuss prime ideals and maximal ideals

leave some overview!

1.8.1 Prime Ideals

Definition 1.8.1 (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 1.8.1. 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 1.8.1. If $R = \mathbb{Z}$, then

1. $\{0\}$ is a prime ideal ($\mathbb{Z}$ 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:

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

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

Example 1.8.2. 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** 1.8.1:

$$R[x] \big/ (x) \cong R$$

Consider the R-algebra homomorphism:

$$\begin{gathered} R[x] \xrightarrow{\varphi} R \\ \varphi(x) = 0 \\ a_0 + a_1 x + \cdots + a_n x^n \to a_0 \end{gathered}$$

This is a surjective homomorphism, with kernel being:

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

Then by isomorphism theorem 1.4.1, yields the result. ■

Question 1.8.1. What about now consider $(x - a) \subseteq R[x]$?

Note. There exists a R-Algebra isomorphism:

$$\begin{aligned} f : R[x] &\to R[x] \\ f(x) &= (x-a) \end{aligned}$$

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 1.8.2 (Coprime 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 coprime if:

$$I_1 + I_2 = R$$

Theorem 1.8.1 (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:

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

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:

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

and proceed on induction on n. ■

1.8.2 Maximal Ideals

Definition 1.8.3 (Maximal Ideal). An ideal $M \subseteq R$ is a maximal ideal if:

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

Lemma 1.8.1. 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 1.8.1. 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** 1.8.1. ∎

Corollary 1.8.2. Every maximal ideal is prime ideal.

Proof. This follows since **every field is a domain**. And by **Corollary** 1.8.1 and **Proposition** 1.8.1. ∎

Example 1.8.3. The following are ideals that are prime but not maximal:

1. $\{0\} \subseteq \mathbb{Z}$ is a prime ideal, but not maximal ideal.
2. $(x) \subseteq \mathbb{Z}[x]$ is a prime ideal, but not maximal ideal.

why?

Theorem 1.8.2. 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 1.8.2 (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 1.8.2. 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** 1.8.2.

Let $\mathcal{J}' \subseteq \mathcal{J}$ be a totally orderded 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** 1.8.2: there exists $M \in \mathcal{J}$ to be the maximal element, and this is a maximal ideal that containing I. ∎

Corollary 1.8.3. 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 1.8.2. 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. ∎

1.9 Local Ring

In this section we shall discuss local rings.

leave some overview!

Definition 1.9.1 (Local Ring). A commutative ring R is a local ring if R has a **unique** maximal ideal.

Proposition 1.9.1. 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** 1.8.2, 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 $\lightning$.
- 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 $\lightning$.

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** 1.8.3, then M is a maximal ideal, and in fact the unique one. See that any maximal ideal $M' \subseteq M \Rightarrow M' = M$. ■

Example 1.9.1.

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

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

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

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

Example 1.9.2. 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.

1.10 Radical Ideals

In this section we shall discuss radical rings.

leave some overview!

Definition 1.10.1 (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 1.10.2 (Reduced Ring). Let R commutative ring, R is called a reduced ring if $\{0\}$ is a radical ideal.

Theorem 1.10.1. 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 1.10.1.

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 1.10.1.

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

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

Proof. First note that:

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

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 $S = \{1, f, f^2, \ldots\}$.

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** 1.8.2 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:

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

■

Corollary 1.10.1. 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 $I = \mathrm{rad}(I)$. ■

Corollary 1.10.2. A ring R is reduced if and only if

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

1.11 Operations with Ideals

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

1.11.1 Sum of Ideals

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

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

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

such here means corresponding left/right/2-sided

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.

Proposition 1.11.1 (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 1.11.1.

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

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

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

Remark 1.11.1.

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

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

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

Example 1.11.3. If R is commutative, a principal ideal in R is an ideal generated by 1 element: (a), $a \in R$.

1.11.2 Product of Ideals

Let R be commutative ring, $I_1, \dots, I_n \subseteq R$ 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:

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

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, as 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 $I \cdot S$:

$$IS := \{\sum_{j=1}^{n} a_j f(b_j) \mid n \in \mathbb{Z}_{>0},\; a_j \in S,\; b_j \in I\} \tag{1.3}$$

Example 1.11.4. Suppose that $S = T^{-1}R$ where $T \subseteq R$ be a multiplicative system. Let $I \subseteq R$ be an ideal. See that:

$$IS = T^{-1}I = \{\frac{a}{s} \mid a \in I,\; s \in T\}$$

1.12 Spectrum of a Commutative Ring

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

Definition 1.12.1. Given a commutative ring R, define:

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

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

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

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

Proposition 1.12.1 (Zariski Topology). We have a topology on $\operatorname{Spec} R$, s.t. the **closed sets** are the $V(I)$ for $I \subseteq R$. The topology it forms is called Zariski Topology.

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. $x_1x_2 \in I_1 \cap I_2$ (follows by ideal property) but $x_1x_2 \notin P$ since P is prime ideal, and reason by contraposition. This leads to contradiction $\lightning$. 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 1.12.1. Let $R = \mathbb{Z} \Rightarrow$ the prime ideals are precisely $\{\{0\}, p\mathbb{Z}$ for p prime.$\}$. Then:

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

see next time every ideal is principal in this case

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

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

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

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

is given by:

1. For every $X \in \operatorname{Ob}(\mathcal{C})$, we have $F(X) \in \operatorname{Ob}(\mathcal{D})$.
2. For all $X, Y \in \operatorname{Ob}(\mathcal{C})$, we have a map

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

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**:

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

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:

$$(f^{\#})^{-1}(V(I)) = \{P \subseteq S \mid P \text{ prime. } f^{\#}(P) \supseteq I \Leftrightarrow f^{-1}(P) \supseteq I \Leftrightarrow P \supseteq f(I) \Leftrightarrow P \supseteq IS \ \ 1.3\}$$

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 1.12.1. 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: $\mathbb{K}[x_1, \ldots, x_n] \,/\, I$ where $\mathbb{K}$ be a field, and in this case, it indeed **gives a functor**.

1.13 Noetherian Rings

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

Definition 1.13.1 (Noetherian Rings and Artirian 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 Artirian ring if there exists **no** strictly decreasing sequence

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

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

Example 1.13.1.

1. A field is both noetherian and artirian.
2. Every finite ring is both noetherian and artirian.
3. $\mathbb{Z}$ is not a artirian 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 1.13.1. 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.:
$$a_{n+1} \notin \sum_{i=1}^{n} Ra_i\ \forall\, n$$
This implies that the sequence of ideals $\left(\sum_{i=1}^{n} Ra_i\right)$ 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** 1.8.2, 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:

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

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

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

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 1.13.1 (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** 1.13.1.

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 1.13.1. $J = (a_1, \ldots, a_m)$.

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:

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

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

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

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 1.13.1. 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** 1.13.1 and induction on n and the fact that $\mathbb{K}$ is a Noetherian ring. ∎

1.14 PIDs and Euclidean Domains

Definition 1.14.1 (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 1.14.1 (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 1.14.2 (Euclidean Domain). A domain R is an Euclidean Domain 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 $N(r) < N(b)$).

Proposition 1.14.1. Every Euclidean Domain R is a PID.

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 $N(b)$ $\lightning$. So this case cannot happen.

■

Example 1.14.2.

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:

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

This implies that:

$$\begin{aligned}\underbrace{a+bi}_{\in\mathbb{Z}[i]} &= \underbrace{(c+di)}_{\in\mathbb{Z}[i]}\cdot\underbrace{(\alpha+\beta i)}_{\in\mathbb{Z}[i]}+r\\ &\text{where } r=(c+di)(\gamma+\delta i)\\ &\Rightarrow r\in\mathbb{Z}[i]\end{aligned}$$

thus:

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

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:

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

We verify the condition by showing the following proposition.

Proposition 1.14.2. Let R be any commutative ring, $f,g\in R[x]$ and $g\neq 0$. Let

$$g = a_nx^n+\cdots+a_1x+a_0$$

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 $m:=\deg(f)\geq n\Rightarrow f=b_mx^m+$ lower order term. Consider

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

see that $\deg(f')<\deg(f)\Rightarrow\exists\, q',r'$, s.t. $f'=q'g+r'\Rightarrow f=\left(b_ma_n^{-1}x^{m-n}+q'\right)g+r'$, which leads to contradiction $\lightning$, 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 $\deg(r)<n=\deg(g)$. ∎

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 domain, and it is crucial that a_n is invertible here.

Remark 1.14.1. 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.

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

Definition 1.15.1. 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 1.15.1.

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:
   $$a + b\sqrt{d} = \frac{p_1q_2 + p_2q_1\sqrt{d}}{q_1q_2} \text{ with } p_1q_2 + p_2q_1\sqrt{d} \text{ and } q_1q_2 \in \mathbb{Z}[\sqrt{d}]$$
   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 $\mathbb{Q}[\sqrt{d}]$.
5. Define:
$$\mathbb{Z}[\sqrt{d}] \xrightarrow{\varphi} \mathbb{Z}[\sqrt{d}]\varphi(a + b\sqrt{d}) \quad = a - b\sqrt{d}$$
when d is negative, this is exactly the conjugation for complex number. See that φ is actually a **ring homomorphism** and in particular $\varphi \circ \varphi = \mathrm{Id} \Rightarrow \varphi$ 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.
   $$N(uv) = N(u)N(v) \quad \forall\, u, v \qquad (\star\star)$$
   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** 1.13.1, $\mathbb{Z}[x]$ 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 1.15.1. $u = a + b\sqrt{d}$ 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 1.15.2 (Gauss Integers: $d = -1$). The 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 unit (invertible elments in a ring) if and only if $a^2+b^2 = 1 \Rightarrow$ the units are exactly $\pm 1, \pm i$.

Appendix