Math494: Honors Algebra II

Yanzhi Li

January 18, 2026

Abstract

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

Contents

1 Ring Theory **2**

1.1 Ring and Ring Homomorphism . . . 2
1.2 Subrings and Ideals . . . 5
1.3 Quotient Rings . . . 7
1.4 Isomorphism Theorem . . . 8
1.5 Polynomial Ring and Formal Power Series Ring . . . 9
1.5.1 R-Algebra . . . 12
1.6 Fields and Integral Domain . . . 12
1.7 Ring Fraction . . . 14

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:

$$f : \mathbb{Z}/_{mn\mathbb{Z}} \to \mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}}$$
$$[a]_{mn} \to ([a]_m, [a]_n)$$

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 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 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 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 ideal 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 $\ker(f) = \{0\}$.

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.:

$$\begin{aligned} \pi : R &\to R\big/_I \\ a &\mapsto a + I \end{aligned}$$

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.

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

- distributivity holds by similar argument as above.
- identity element for multiplication.

$$\begin{aligned} \overline{1}\overline{a} &= \overline{1a} = \overline{a} \\ \overline{a}\overline{1} &= \overline{a1} = \overline{a} \end{aligned}$$

- 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:

$$R \Big/ I \Big/ I' \Big/ I \cong R \Big/ I'$$

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:

$$\begin{aligned} R &\xrightarrow{i} R[X] \\ a &\mapsto a \end{aligned}$$

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 ψ : $\psi(x^i) = a^i\ \forall i > 0$, 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:

$$R[X_1, \ldots, X_n] \coloneqq (R[X_1, \ldots, X_{n-1}])[X_n]$$

This is again a commutative ring.

Theorem 1.5.2 (Universal Property of $\mathbf{R[X_1, \ldots, X_n]}$). $\forall$ 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:

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

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

Example 1.5.1. $X_1^2 + X_1X_3 + X_2^4 \in R[X_1, X_2, X_3]$

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:

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

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 $R[X_1, \ldots, X_n]$ 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

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

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:

$$R[[X]] \coloneqq \{\sum_{i\geq 0} a_i x^i \mid a_i \in R,\ \forall\ i \geq 0\}$$

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 $\overline{a}\overline{b} = 0 \Leftrightarrow n \mid ab$. 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:

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

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:

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

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 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:

$$\begin{aligned} f &= a_0 + a_1 x + \cdots + a_m x^m \quad a_m \neq 0 \quad \deg(f) = m \\ g &= b_0 + b_1 x + \cdots + b_n x^n \quad b_n \neq 0 \quad \deg(g) = n \end{aligned}$$

then:

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

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

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 (Multiplication System). Fix R be commutative ring, $S \subseteq R$ be a multiplication 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

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

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

$$\color{blue}{s's''a}\color{black}{=s''sa'=ss'a''=}\color{red}{s'sa''}$$

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:

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

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

∎

Appendix