Math494: Honors Algebra II

Yanzhi Li

January 12, 2026

Abstract

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

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:

$$[a] + [b] \coloneqq [a + b]$$
$$[a] \cdot [b] \coloneqq [ab]$$

   where $[a] \coloneqq a + n\mathbb{Z}$, 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:

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

   with "usual" addition and mult. for matrices:

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

   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 $n \ge 2$, 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.**:

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

   define the operations **componentwise**:

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

   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:

$$\underbrace{f(f^{-1}(ab))}_{=ab} = \underbrace{f\big(f^{-1}(a)\cdot f^{-1}(b)\big)}_{=f(f^{-1}(a))\cdot f(f^{-1}(b))=ab}$$

■

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

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

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

Definition 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:

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

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

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

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:

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

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

- multiplication is associative.

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

- 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**:

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

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

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

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

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

- $\overline{f}(u \cdot v) = \overline{f}(u)\overline{f}(v)\ \forall\ u, v \in R/I$.
- $\overline{f}(1_{R/I}) = 1_S$.

the second assertion follows directly:

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

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

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

■

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:

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

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

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:

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

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:

$$\left.\left.R\middle/I\middle/I'\middle/I\right.\right. \cong \left.R\middle/I'\right.$$

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:

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

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:

$$(\overline{d}) \coloneqq \{\overline{d}a \mid a \in \left.\mathbb{Z}\middle/n\mathbb{Z}\right.\} = \left.(d)\middle/(n)\right.$$

and the theorem implies:

$$\left.\left.\mathbb{Z}\middle/n\mathbb{Z}\middle/(\overline{d})\right.\right. \cong \left.\mathbb{Z}\middle/d\mathbb{Z}\right.$$

Appendix