# The Foundations of Algebra's Prequisite Course

Shi Boyuan

September 23, 2025

# Contents

# Chapter 1

# The Foundations of Algebra

## 1.1 The Prerequisite Course

**Preliminaries.** *This Course is taught by Luosw and its purpose is to introduce basic concepts in fundations of algebra*

What is mathematics? Bourbaki says: In mathematics we study
Structures defined on sets
Maps preserving structures

### 1.1.1 Classical set Theory

Learning classical set theory can be divided into two parts
The relation and operation between sets
$\subseteq \quad \times \quad \sqcup \quad P(S) \ \ or \ \ 2^S \quad \cup \quad \cap$
The set-functions
$A \longleftrightarrow B \quad A \hookrightarrow B \quad A \twoheadrightarrow B$

**Relations and Operations between sets**

Definition 1.1.1 Direct Product

Direct Product ($\times$)

Definition 1.1.2 Disjoint union or coproduct

Disjoint union or coproduct ($\sqcup$)

**Remark 1.1.1.** *There are some relations between product and coproduct.An explanation will be given later.*

**Remark 1.1.2.** *if $A \cap B = \emptyset$,then $A \cup B = A \sqcup B$*

Definition 1.1.3 Power Sets

Power Sets, $P(A)$ or $2^A$

**Remark 1.1.3.** *$P(\mathbb{N})$is special.It's the first uncountable set discovered by our mankind*

**Mapping between Sets**

Definition 1.1.4 Set-function

Set-functions, Def by $\mathbb{A} \times \mathbb{B}$,$f : A \to B$

Definition 1.1.5 Image

Image

Definition 1.1.6 Injection and surjection

Injection and surjection
Injective $f : A \hookrightarrow B$
Surjective $f : A \twoheadrightarrow B$

Definition 1.1.7 Bijection or isomorphism

Bijection or isomorphism $f : A \leftrightarrow B$

**Example 1.1.1.** *$A \to 0 \times A$ is bijection,and $A \cong \{0\} \times A$*
*$\mathbb{A} \hookrightarrow \{0, 1\} \times \mathbb{A}, a \longmapsto (0, a)$,which is a injection*

$$A \underset{construct\ a\ isomorphism}{\xrightarrow{\sim}} \{0\} \times A \underset{inclusion}{\overset{\iota}{\hookrightarrow}} \{0, 1\} \times A$$

*so we find a decomposition of injection*

**Equivalence Relation**

**Example 1.1.2.** *construct relation $<$ in $\mathbb{Z}$*

Definition 1.1.8 Relation

Relation: A relation on a set $\mathbb{S}$ is defined by $\mathbb{R} \in \mathbb{S} \times \mathbb{S}$, If $(a, b) \in \mathbb{R}$,we say "a and b are related by $\mathbb{R}$" and we write aRb or $(a, b) \in \mathbb{R}$

**Example 1.1.3.** *" = " in S:* $\{(a, a) \mid a \in \mathbb{S}\} \subset \mathbb{S} \times \mathbb{S}$

Definition 1.1.9 Equivalence Relation

Equivalence Relation:If $\mathbb{R}$ is a relation on $\mathbb{S}$, satisfying
1.(reflexivity) $aRa$
2.(symmetry) $aRb \Longrightarrow bRa$
3.(transitivity) $aRb, bRc \Longrightarrow aRc$

**Remark 1.1.4.** *The definition's goal is to classify the set by the relation!*

Definition 1.1.10 Equivalence Class

Equivalence Class, $[a]_{\sim}$

Consider $\{[a]_{\sim} \mid a \in \mathbb{S}\}$ as a Classification of sets

Definition 1.1.11 Quotient Set

Quotient Set: $S/\sim = \{[a]_{\sim} \mid a \in \mathbb{S}\}$

**Example 1.1.4.** $\mathbb{R}/= \cong \mathbb{R}$

**Example 1.1.5.** *Canonical Projection*
$\Pi : S \twoheadrightarrow S/\sim, s \longmapsto \Pi(s) = [s]_{\sim}$

**Example 1.1.6.** $\mathbb{R}^2$,$\sim$: $x = x'$

$$\mathbb{R}^2 \twoheadrightarrow \mathbb{R}^2/\sim \xrightarrow{\sim} \mathbb{R}$$

*Appearently,* $\mathbb{R}^2 \underset{f}{\twoheadrightarrow} \mathbb{R}$*,Thus we find a dexcomposition of a surjection*

**Example 1.1.7.** *we can use* $\mathbb{Z}\times\mathbb{Z}\setminus\{0\}, (p,q) \sim (p',q') \Longleftrightarrow pq' = qp'$,$(\mathbb{Z}\times\mathbb{Z}\setminus\{0\})/\sim$ *to construct a isomorphism to* $\mathbb{Q}$

**Proposition 1.1.1.** *If* $\mathbb{A} \xrightarrow{f} \mathbb{B}$ *is a set-function, we define a relation* $\sim_f$ *on* $\mathbb{A}$ *by* $a \sim_f b \overset{def}{\Longleftrightarrow} f(a) = f(b)$*, then* $\sim_f$ *is an equivalence relation.*

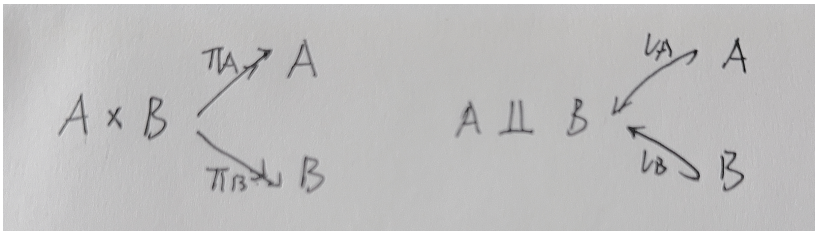
*Proof.* 1.reflexivity:...
2.symmetry:...
3.transitivity:... □

**Theorem 1.1.2.** ***Canonical Decomposition***

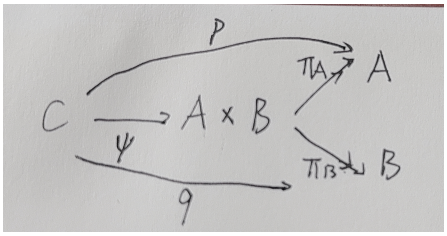
$$\mathbb{A} \underset{\Pi}{\overset{projection}{\Longrightarrow}} \mathbb{A}/\sim_f \underset{\sim}{\overset{isomorphism}{\longrightarrow}} Imf \underset{\iota}{\overset{inclusion}{\hookrightarrow}} \mathbb{B} \Longleftrightarrow \mathbb{A} \xrightarrow{f} \mathbb{B}$$

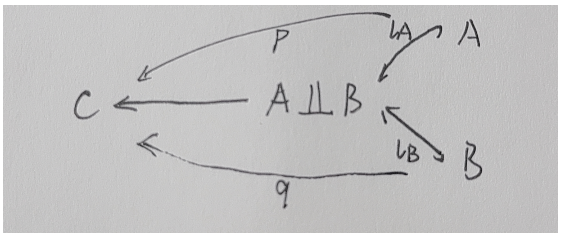
**Remark 1.1.5.** *This conclusion is so fucking elegant!!!*
*In group theory,*$A/kerf \cong imf$

**Remark 1.1.6.** *product* $\longleftrightarrow$ *coproduct*
*The product has a special property called universal property*




*If there exists* $\mathbb{C}$ *and two set-functions* $p : \mathbb{C} \longrightarrow \mathbb{A}$, $q : \mathbb{C} \longrightarrow \mathbb{B}$,*then exists a* ***unique*** $\phi : \mathbb{C} \longrightarrow \mathbb{A} \times \mathbb{B}$,*satisfying the diagram commutes*

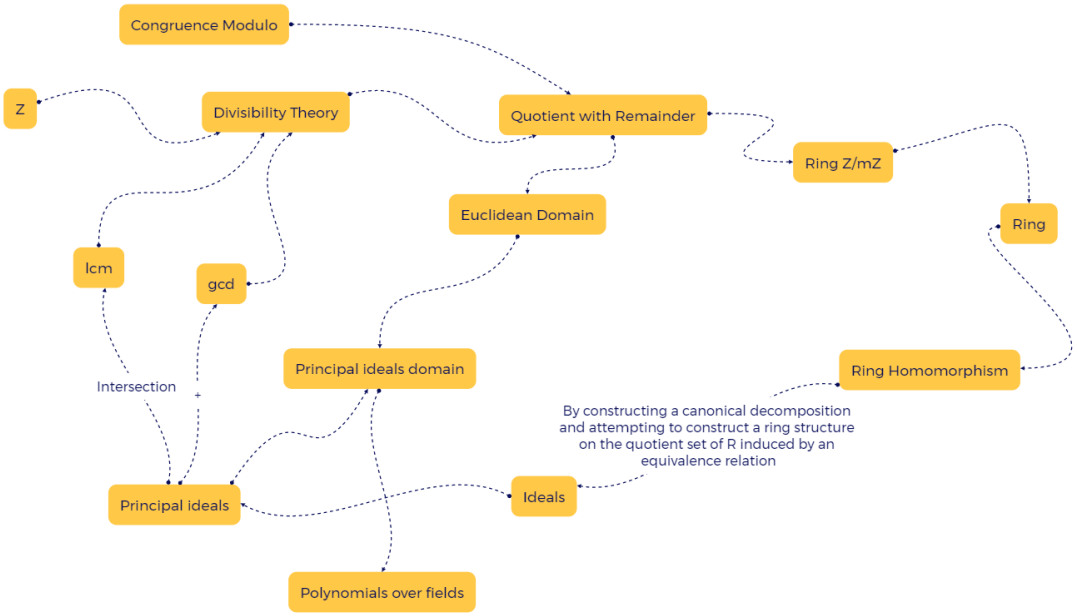



*These pictures is a interpretation to the special property*

### 1.1.2 Elementary Number Theory

This is the main content of this section.




#### Divisibility Theory

The Divisibility Theory is derived from the concept of division.

> Definition 1.1.12 Divisible
>
> Divisible:$b \mid a$,and we say " a is divisible by b ",we call b is a divisor of a

**Proposition 1.1.3.** *There is some property, but I think it's not significant*

**Remark 1.1.7.** $a \mid b, b \mid a \Longleftrightarrow |a| = |b|$

If not divisible?

#### Quotient with Remainder

**Theorem 1.1.4.** *Let* $a \in \mathbb{Z}, b \in \mathbb{Z}\backslash 0$,*then exists unique* $(q, r) \in \mathbb{Z}^2$ *satisfying* $a = bq + r$ *and* $0 \leq r < |b|$

*Proof.* I think it's easy □

### 1.1.3 Ring

**Congruence Modulo**

Definition 1.1.13 Congruence Modulo

Congruence Modulo :$\equiv_m$

Consider the quotient set of $\mathbb{Z}$ by $\equiv_m$,

$$\mathbb{Z}/\equiv_m = \left\{[0]_{\equiv_m}, [1]_{\equiv_m}, ..., [m-1]_{\equiv_m}\right\}$$

$$\mathbb{Z} = \bigsqcup_{i=0}^{m-1} [i]_{\equiv_m} = \bigsqcup_{i=0}^{m-1} \overline{i}$$

what is addition and multiplication?,we can define it as a mapping f,$f : \mathbb{S} \times \mathbb{S} \mapsto \mathbb{S}$,and now we have the definition of these calculations, naturally we will put these calculations(additions and multiplications) on sets, we still need The Addition and Multiplication in $\mathbb{Z}$'s beautiful properties in new defined operations

Definition 1.1.14 Ring

Ring:A set $\mathbb{R}$ with two calculations $+, \cdot$ satisfying:
1.$(a+b)+c = a+(b+c)$
2.There exists $0_R$
3.There exists $-a$
4.$a+b = b+a$
5.$(a \cdot b) \cdot c = a \cdot (b \cdot c)$
6.There exists $1_R$
7.$(a+b) \cdot c = ac + bc$ and $a \cdot (b+c) = ab + ac$
Then we call $(\mathbb{R}, +, \cdot)$ is a ring
If $\cdot$ satisfies: 8.$ab = ba$, then we call $(\mathbb{R}, +, \cdot)$ is a commutative ring

Because we define ring from the addition and multplication in $\mathbb{Z}$, so we can easily know that $(\mathbb{Z}, +, \cdot)$ is a ring
We can see that the calculation on the ring is the addition and multiplication inherited from the integer, so this can inspire us to define the calculation in $\mathbb{Z}/m\mathbb{Z}$,which is very Apparent, and our result is as follows.

Definition 1.1.15 The Operations on $\mathbb{Z}/\equiv_m$

$$\mathbb{Z}/\equiv_m \times \mathbb{Z}/\equiv_m \overset{+_{\mathbb{Z}/\equiv_m}}{\longrightarrow} \mathbb{Z}/\equiv_m$$

$$(\overline{a}, \overline{b}) \overset{+_{\mathbb{Z}/\equiv_m}}{\mapsto} \overline{a +_{\mathbb{Z}} b}$$

$$\mathbb{Z}/\equiv_m \times \mathbb{Z}/\equiv_m \overset{\cdot_{\mathbb{Z}/\equiv_m}}{\longrightarrow} \mathbb{Z}/\equiv_m$$

$$(\overline{a}, \overline{b}) \overset{\cdot_{\mathbb{Z}/\equiv_m}}{\mapsto} \overline{a \cdot_{\mathbb{Z}} b}$$

This is the inheritance from $\mathbb{Z}$, so we can know that $(\mathbb{Z}/\equiv_m, +, \cdot)$ is a ring without proof

$$\mathbb{Z}/\equiv_m \underset{Algebra\ Structure}{\xrightarrow{+,\cdot}} \mathbb{Z}/m\mathbb{Z} = \left\{\overline{0}, \overline{1}, ..., \overline{m-1}\right\}$$

**Example 1.1.8.** *Table of addition/multiplication*

### Ring Homomorphism

Ring Homomorphism is a mapping that don't change the operation on rings

Definition 1.1.16 Ring Homomorphism

Ring Homomorphism:Keep Operation structures and $1_{\mathbb{S}}$

we know the canonical decomposition in mapping between sets, but how will the cannonical decomposition be when we are talking in rings?

$$\mathbb{R}_1 \xrightarrow{\theta} \mathbb{R}_2 \Longleftrightarrow \mathbb{R}_1 \underset{\Pi}{\twoheadrightarrow} \mathbb{R}_1/\sim_\theta \xrightarrow{\sim} im\theta \underset{\iota}{\longrightarrow} \mathbb{R}_2$$

The $\theta$ is a **ring homomorphism**
we hope that every step of supra is a ring homomorphism, Firstly,if we want the $\Pi$ to be a ring homomorphism,we need $\mathbb{R}_1/\sim_\theta$ to be a ring at least

$$\mathbb{R}_1/\sim_\theta \overset{Algebra\ Structure}{\underset{+,\cdot}{\longrightarrow}} Ring$$

Like The Operations on $\mathbb{Z}/\equiv_m$, we can use $\mathbb{R}_1$ to define the $\mathbb{R}_1/\sim_\theta$,definition are given as follows.

Definition 1.1.17 The Operations on $\mathbb{R}_1/\sim_\theta$

$$\mathbb{R}_{\sim_\theta} \times \mathbb{R}_{\sim_\theta} \xrightarrow{+_{\mathbb{R}_{\sim_\theta}}} \mathbb{R}_{\sim_\theta}$$
$$[r_1]_{\sim_\theta} +_{\mathbb{R}_1/\sim_\theta} [r_2]_{\sim_\theta} = [r_1 +_{\mathbb{R}_1} r_2]_{\sim_\theta}$$
$$\mathbb{R}_{\sim_\theta} \times \mathbb{R}_{\sim_\theta} \xrightarrow{\cdot_{\mathbb{R}_{\sim_\theta}}} \mathbb{R}_{\sim_\theta}$$
$$[r_1]_{\sim_\theta} \cdot_{\mathbb{R}_1/\sim_\theta} [r_2]_{\sim_\theta} = [r_1 \cdot_{\mathbb{R}_1} r_2]_{\sim_\theta}$$

**Remark 1.1.8.** *we need to prove that the results do not change with the change of the representative element we selected.How to prove it, by using the definition!*

**Remark 1.1.9.**

$$a \sim_\theta b \Longleftrightarrow \theta(a-b) = 0_{\mathbb{R}_2}$$

Definition 1.1.18 Kernel

Kernel: $Ker(\theta) = \{r_1 \in \mathbb{R}_1 \mid \theta(r_1) = 0\}$

**Proposition 1.1.5.** $a \sim_\theta b \Longleftrightarrow a - b \in Ker(\theta)$

**Remark 1.1.10.**

$$\mathbb{R}_1 \longrightarrow \mathbb{R}_1/\sim_\theta \underset{Algebra\ Structure}{\xrightarrow{+,\cdot}} \mathbb{R}_1/Ker(\theta)$$

*we all know* $\mathbb{R}_1/\sim_\theta$ *is quotient set and* $\mathbb{R}_1/Ker(\theta)$ *is quotient ring*
$\mathbb{I} \underset{Find\ Ring\ Structure}{\xrightarrow{?}} \mathbb{R}/\mathbb{I}$
*Firstly, we can define a equivalence relation* $a \sim_I b \overset{def}{\Longleftrightarrow} a - b \in \mathbb{I}$*, so we can define a* $[..]_{\mathbb{I}}$*, so that we can define* $\mathbb{R}/\mathbb{I}$
*1.Reflexibility:* $0 \in \mathbb{I}$
*2.Reflexivity:* $a \in \mathbb{I} \Longrightarrow -a \in \mathbb{I}$
*3.Transitivity:* $a, b \in \mathbb{I} \Longrightarrow a + b \in \mathbb{I}$
*Under the above constraints,we can make* $\mathbb{R}/\mathbb{I}$ *a quotient set, but we still need to add some operations*$(+, \cdot)$ *on it to make it a quotient ring,and this operation will stricter the constraints. Finally, we call* $\mathbb{I}$ *the* $\mathbb{R}$*'s ideal.*

**Ideal**

Definition 1.1.19 The Operations on $\mathbb{R}/\mathbb{I}$

$$[r_1]_{\sim_{\mathbb{I}}} +_{\mathbb{R}/\mathbb{I}} [r_2]_{\sim_{\mathbb{I}}} = [r_1 +_{\mathbb{R}} r_2]_{\sim_{\mathbb{I}}}$$
$$[r_1]_{\sim_{\mathbb{I}}} \cdot_{\mathbb{R}/\mathbb{I}} [r_2]_{\sim_{\mathbb{I}}} = [r_1 \cdot_{\mathbb{R}} r_2]_{\sim_{\mathbb{I}}}$$

Others, we need to prove the results do not change with the change of the representative element we selected

*Proof.* we know

$$r_1 \sim_I r_1', r_2 \sim_I r_2'$$

then proof

$$[r_1 + r_2]_{\sim_I} = [r_1' + r_2']_{\sim_I}$$

this is easy by the Transitivity
The next

$$r_1'r_2' - r_1r_2 \in \mathbb{I} \Longrightarrow -r_2'(r_1 - r_1') - r_1(r_2 - r_2') \in \mathbb{I}$$

so we have a new constraint

$$\forall a \in \mathbb{I}, c \in \mathbb{R}, ca \in \mathbb{I}$$

□

Definition 1.1.20 Ideal

Ideal: we assume $\mathbb{R}$ is a commutative ring
**I stuck here for about 3 minutes to think about why $\mathbb{R}$ is a commutative ring and finally I got the reason, This is because when we are deriving from $r_1'r_2' - r_1r_2$, we use the commutative law**
We call $\mathbb{I}$ an ideal of $\mathbb{R}$ iff

$$\forall a, b, \in \mathbb{I}, a + b \in \mathbb{I}$$

$$\forall a \in \mathbb{I}, c \in \mathbb{R}, ca \in \mathbb{I}$$

**I stuck here for about 5 minutes to think about how can we get a $-1$ from $\mathbb{R}$ and finally I get: we can pick the $1_{\mathbb{R}}$ to the $-1_{\mathbb{R}}$**

**Example 1.1.9.** *1.$Ker(\theta) \subset \mathbb{R}_1 \Longrightarrow Ker(\theta)$ is an ideal of $\mathbb{R}_1$*
*2.$\mathbb{R} \overset{\Pi}{\twoheadrightarrow} \mathbb{R}/\mathbb{I}$,then $Ker\Pi = \mathbb{I}$*
*3.Ideal $\Longleftrightarrow$ Kernel*

**Example 1.1.10.** *Using $\mathbb{Z}/m\mathbb{Z}$ as a example*

$$\mathbb{Z} \longrightarrow \mathbb{Z}/\equiv_m \longrightarrow \mathbb{Z}/m\mathbb{Z}$$

*In fact, $m\mathbb{Z}$ is an ideal of $\mathbb{Z}$*
*so $r\mathbb{R}$ is an ideal of $\mathbb{R}$*

Definition 1.1.21 Principle Ideal

Principle Ideal:$(r) = \{r \cdot r' \mid r' \in \mathbb{R}\}$, we call $(r)$ the principle ideal generated by r

**Proposition 1.1.6.** *Any ideal $\mathbb{I} \subset \mathbb{Z}$ is principle,so $\mathbb{Z}$ is **principle ideal domain**(PID)*

Can we generate new ideals from given ideals ?

**Proposition 1.1.7.** *If $\mathbb{I}_1, \mathbb{I}_2 \subset \mathbb{R}$ ideal,then*

$$\mathbb{I}_1 \cap \mathbb{I}_2, \mathbb{I}_1 + \mathbb{I}_2, \mathbb{I}_1 \cdot \mathbb{I}_2 = \{a_1b_1 + a_2b_2 + ... + a_nb_n \mid a_1...a_n \in \mathbb{I}_1, b_1...b_n \in \mathbb{I}_2\}$$

*is ideal*

From this, we can easily construct a connection between ideal and number theory

Definition 1.1.22 From ideal to number theory

Under $\mathbb{Z}$

$$(a) \subset (b) \longrightarrow b \mid a$$

$$(a) + (b) = (d) \longrightarrow d = gcd(a, b)$$

$$(a) \cap (b) = (l) \longrightarrow l = lcm(a, b)$$

**Theorem 1.1.8.** *Bezout's theorem:*
*Given $a, b \in \mathbb{Z}$,then there exists $s, t \in \mathbb{Z}$,such that*

$$as + bt = gcd(a, b)$$

*If there exists $d' \mid a, d' \mid b.$ satisfying $d' = as + bt \Longrightarrow d' = gcd(a, b)$*