

Math 28B: Introduction to Rings and Fields

Hussein Hijazi

Spring 2021

Lecture 1

Definition 1.1: Rings and Fields

A **ring** R is a set with two binary operations $+$, \cdot (addition and multiplication), i.e

$$+ : R \times R \rightarrow R$$

$$\cdot : R \times R \rightarrow R$$

such that:

(i) $(R, +)$ is an **abelian group**, i.e

- (Additive Identity) There exists a unique $0_R \in R$, such that $\forall a \in R$

$$a + 0_R = 0_R + a = a$$

- (Additive Inverse) $\forall a \in R$ there exists a unique $(-a) \in R$ such that

$$a + (-a) = (-a) + a = 0_R$$

- (Associativity) For all $a, b, c \in R$, $(a + b) + c = a + (b + c)$

- (Commutativity) For all $a, b \in R$, $a + b = b + a$

(ii) \cdot is **associative**, i.e $\forall a, b, c \in R$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

(iii) \cdot is **distributive** over $+$, i.e $\forall a, b, c \in R$

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Now we see variations and the extension of a ring, the field:

- We say R has an **identity element**, 1_R , if there exists a $1_R \in R$ such that $\forall a \in R$

$$a \cdot 1_R = 1_R \cdot a = a$$

- We say R is **commutative** if $\forall a, b \in R$

$$a \cdot b = b \cdot a$$

- If R is a commutative ring with $1_R \neq 0_R$, then we say R is a **field** if every non-zero element has a multiplicative inverse, i.e $\forall a \neq 0 \in R, \exists a^{-1} \in R$ such that

$$a \cdot (a^{-1}) = (a^{-1}) \cdot a = 1_R$$

For the rest of the notes, I will omit the R subscript from the additive and multiplicative identity, unless necessary. Anyways, now we can look at some examples of rings:

Example 1.1 $(\mathbb{Z}, +, \cdot)$, The integers with the usual addition and multiplication is a ring.

Example 1.2 $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ are fields.

Example 1.3 $(\mathbb{N}, +, \cdot)$ is **not** a ring, since there are no additive inverses.

Example 1.4 $(\mathbb{R}^3, +, \cdot)$ is **not** a ring. It has addition $\mathbf{v}, \mathbf{w} \in \mathbb{R}^3 \Rightarrow \mathbf{v} + \mathbf{w} \in \mathbb{R}^3$, but no proper multiplication operator. You can check that the cross product, \times , not distributive.

Definition 1.2: Unit

We say $a \in R$ is a **unit** if there exists a $b \in R$ such that $a \cdot b = b \cdot a = 1$.
Basically, a unit is an element whose multiplicative inverse is also in the ring.

Example 1.5 In \mathbb{R} , every element except 0 is a unit.

Example 1.6 In \mathbb{Z} , the only units are $\{1, -1\}$.

Now let us look at examples of rings other than the standard number types $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$:

Example 1.7 The integers modulo n are also a ring. This set is written as $\mathbb{Z}/n\mathbb{Z}$. To understand this, first define the set of multiples of an integer n as

$$n\mathbb{Z} := \{n \cdot a \mid a \in \mathbb{Z}\}$$

Then,

$$\mathbb{Z}/n\mathbb{Z} := \mathbb{Z}/\sim$$

where \sim is the equivalence relation for $x, y \in \mathbb{Z}$

$$x \sim y \iff x - y \in n\mathbb{Z}$$

which basically means two integers are equivalent if their difference is a multiple of n . Think about it like this, if x and y are multiples of n plus the same remainder, i.e

$$x = nk + r \quad y = nl + r$$

for some $k, l \in \mathbb{Z}$ then their difference is exactly a multiple of n ,

$$x - y = nk + r - (nl + r) = n(k - l) = nm$$

for $m \in \mathbb{Z}$. They are equivalent in the sense of producing the same remainder when n is divided by them. This can be written in modulo arithmetic as

$$x \equiv y \pmod{n}$$

So, $\mathbb{Z}/n\mathbb{Z}$ will contain equivalence classes of remainders when dividing any integer by n , and each of these classes contain all integers that produce such remainder

$$\mathbb{Z}/n\mathbb{Z} := \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$$

The numbers with bars indicate the equivalence classes generated when taking the integers modulo n . For example $\mathbb{Z}/3\mathbb{Z}$ are the integers modulo 3

$$\mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$$

where

$$\bar{0} = \{0, 3, 6, 9, \dots\}$$

$$\bar{1} = \{1, 4, 7, 10, \dots\}$$

$$\bar{2} = \{2, 5, 8, 11, \dots\}$$

Now, if $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$ and $a \in \bar{a}, b \in \bar{b}$ then we define

$$\bar{a} + \bar{b} = \overline{a + b}, \quad \bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

This set with the two operations is a ring. (Exercise to show these operations are well defined).

Example 1.8 We can also have a rings of functions. Let R be a ring and X a set, define the set \mathfrak{F}

$$\mathcal{F} := \{f : X \rightarrow R\}$$

which is the set of functions which take elements of the set X to elements of the ring R . Then

$$\begin{array}{ll} (f + g) : X \rightarrow R & (f \cdot g) : X \rightarrow R \\ x \mapsto f(x) + g(x) & x \mapsto f(x) \cdot g(x) \end{array}$$

are operations which with \mathfrak{F} , form a ring.

Example 1.9 Define the set of continuous functions on the closed interval $[0, 1]$

$$C[0, 1] := \{f : [0, 1] \rightarrow \mathbb{R} | f \text{ continuous}\}$$

We know from calculus that if $f, g \in C[0, 1]$, then $f + g$ and $f \cdot g$ are also in $C[0, 1]$. Hence, $C[0, 1]$ is a ring.

Example 1.10 Sets of matrices can also be rings. Define

$$M_n(\mathbb{R}) := \{n \times n \text{ matrices with real coefficients}\}$$

Then for matrices A, B :

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}, B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix}$$

we have

$$A + B := \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \cdots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \cdots & a_{2n} + b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} + b_{n1} & a_{n2} + b_{n2} & \cdots & a_{nn} + b_{nn} \end{pmatrix}$$

$$A \cdot B := (a_{ik} \cdot b_{ki})$$

In the product, the notation indicates that each element is the dot product of a row vector in A and a column vector in B (the variable i indicates the i th row and i th column, while the k varies to multiply the k th element of each vector). This is the usual matrix multiplication we are all aware of.

Also, the additive and multiplicative identity are

$$0 = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, 1 = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

Lecture 2

Let's see some basic properties of a ring R :

(i) $0 \cdot a = a \cdot 0 = 0 \quad \forall a \in R$

Proof. Let a be in R , then:

$$\begin{aligned} 0 &= 0 + 0 \Rightarrow 0 \cdot a = (0 + 0) \cdot a \\ &\Rightarrow 0 \cdot a = 0 \cdot a + 0 \cdot a \\ &\Rightarrow 0 \cdot a + (-0 \cdot a) = 0 \cdot a + 0 \cdot a + (-0 \cdot a) \\ &\Rightarrow 0 = 0 \cdot a \end{aligned}$$

■

(ii) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b) \quad \forall a, b \in R$

Proof. Let a, b be in R , then:

$$a \cdot b + -(a \cdot b) = 0 \quad (\text{by definition})$$

then

$$\begin{aligned} a \cdot b + (-a) \cdot b &= (a + (-a)) \cdot b = 0 \cdot b = 0 \\ \Rightarrow -(a \cdot b) &= (-a) \cdot b \end{aligned}$$

■

(iii) $(-a) \cdot (-b) = a \cdot b \quad a, b \in R$

Proof. Let a, b be in R , then:

$$(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b))$$

But by definition we of additive inverse:

$$-(-(a \cdot b)) + (-a \cdot b) = 0$$

So

$$(-a) \cdot (-b) = -(-(a \cdot b)) = a \cdot b$$

■

(iv) If R has 1, then 1 is unique and $(-a) = (-1) \cdot a$

Proof. First, the multiplicative identity. Assume 1 and $1'$ are distinct identities. But

$$1 = 1 \cdot 1' = 1'$$

So, in fact, they are the same and it is unique.

Now, by definition additive inverses are unique, so $-a = (-1) \cdot a$ must both sum with a to 0. We check

$$a + (-1) \cdot a = 1 \cdot a + (-1) \cdot a = (1 + (-1)) \cdot a = 0 \cdot a = 0$$

which confirms it.

■

Definition 2.1: Zero Divisor

We say a non-zero element $a \in R$ is a **zero divisor** if $\exists b \neq 0$ such that $a \cdot b = 0$

Example 2.1 Recall that $M_2(\mathbb{R})$ is the set of 2x2 matrices with real valued entries and $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Then,

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

implies $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is a zero divisor.

Example 2.2 Let $\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$. Then

$$\bar{2} \cdot \bar{3} = \bar{0}$$

implies $\bar{2}$ is a zero divisor.

Claim: If $\bar{0} \neq \bar{a} \in \mathbb{Z}/n\mathbb{Z}$ is not a zero divisor, then it is a unit.

Proof. Let $a \in \mathbb{Z}$ with $a \neq 0$ be relatively prime to n . Then Euclid's algorithm (more specifically Bezout's Identity) constructs $x, y \in \mathbb{Z}$ such that

$$a \cdot x + n \cdot y = 1 \implies \bar{a} \cdot \bar{x} = \bar{1}$$

Hence, \bar{a} is a unit.

On the other hand, if $\gcd(a, n) > 1$, then let $\gcd(a, n) = d$. Hence, since n is a multiple d we can write for some $q, k \in \mathbb{Z}$

$$n = d \cdot q \quad a = d \cdot k$$

Then,

$$\bar{a} \cdot \bar{q} = \overline{a \cdot q} = \overline{d \cdot k \cdot q} = \overline{n \cdot k} = \bar{n} = \bar{0}$$

Thus, \bar{a} is a zero divisor. ■

Corollary 2.1

If n is prime, then $\mathbb{Z}/n\mathbb{Z}$ is a field.

Proof. If $0 < m < n$ and n is prime, then $\gcd(m, n) = 1$. From the previous claim, this would mean every element is a unit and therefore $\mathbb{Z}/n\mathbb{Z}$ is a field. ■

Example 2.3 $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ are fields but $\mathbb{Z}/4\mathbb{Z}$ is not (since $\bar{2} \cdot \bar{2} = \bar{0}$, therefore $\bar{2}$ is a zero divisor and not a unit).

Claim: If $a \in R$ is a zero divisor, then it is not a unit

Proof. Let $b \neq 0$ and $a \cdot b = 0$.

Assume $\exists c \in R$ such that $a \cdot c = 1 = c \cdot a$, then

$$c \cdot a \cdot b = c \cdot (a \cdot b) = c \cdot 0 = 0$$

but similarly,

$$c \cdot a \cdot b = (c \cdot a) \cdot b = 1 \cdot b = b$$

contradicting the fact of $b \neq 0$. Hence our assumption is wrong and a is not a unit. ■

Definition 2.2: Group of Units

If R is a ring with $1 \neq 0$, we denote the set of units by

$$R^\times := \{a \in R \mid \exists b \in R \quad a \cdot b = b \cdot a = 1\}$$

Claim: (R^\times, \cdot) is a group.

Proof. We check the properties of a group

- (i) $1 \in R^\times$ ($1 \cdot 1 = 1$)
- (ii) $\forall a \in R^\times, a \cdot 1 = 1 \cdot a = a$
- (iii) Associativity follows since \cdot is associative in R
- (iv) $\forall a \in R^\times$, by the definition of R^\times there exists $b \in R$ such that

$$a \cdot b = b \cdot a = 1$$

but this is the same as

$$b \cdot a = a \cdot b = 1$$

hence b , the inverse of a , is also a unit and therefore $b \in R^\times$. ■

A field F is a commutative ring with $1 \neq 0$ such that $F^\times = F \setminus \{0\}$

Definition 2.3: Integral Domain

We say a commutative ring R with $1 \neq 0$ is an **integral domain** if it has no zero divisors

Example 2.4 $\mathbb{Z}/4\mathbb{Z}$ is **not** an integral domain. ($\bar{2} \cdot \bar{2} = \bar{0} \implies \bar{2}$ is a zero divisor)

Example 2.5 $M_2(\mathbb{R})$ is **not** an integral domain. Then,

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

implies $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is a zero divisor.

Example 2.6 \mathbb{Z} is an integral domain

Proposition 2.1: Cancellation Law

Let R be a ring and $a, b, c \in R$.

Suppose a is not a zero divisor, then

$$ab = ac \implies b = c$$

Proof. If $a \neq 0$, then $a \cdot (b - c) = 0$. Since we supposed a is not a zero divisor then it must be

$$b - c = 0 \implies b = c$$

■

Example 2.7 To show why a must **not** be a zero divisor, consider $\mathbb{Z}/4\mathbb{Z}$. We have $\bar{2} \cdot \bar{2} = \bar{0}$ and $\bar{2} \cdot \bar{0} = \bar{0}$. So

$$\bar{2} \cdot \bar{2} = \bar{2} \cdot \bar{0}$$

but

$$\bar{2} \neq \bar{0}$$

Corollary 2.2

If R is a finite (as a set) integral domain then R is a field

Proof. Fix $a \in R$ and $a \neq 0$. Then define a map

$$\begin{aligned} f_a : R &\rightarrow R \\ x &\mapsto a \cdot x \end{aligned}$$

Claim: f_a is an injective map by cancellation

Proof. Suppose $f_a(x) = f_a(y)$, then

$$a \cdot x = a \cdot y \implies x = y$$

hence, it is injective.

■

By the Pigeonhole Principle f_a is also surjective. This bijection implies that there exists $x \in R$ such that $a \cdot x = 1$. Hence, a is a unit and is an element of the group of units, i.e. $a \in R^\times$.

Since every non-zero a is shown to be in R^\times this way, they are all units, and hence R is a field (since every element in the ring has a multiplicative inverse).

■

Definition 2.4: Subring

A subring S of a ring R is a subgroup that is closed under multiplication. That is $S \subset R$ such that $\forall a, b \in S$,

$$\left. \begin{array}{ll} \text{(i)} & a + b \in S \quad (\text{closure under } +) \\ \text{(ii)} & 0 \in S \quad (\text{additive identity}) \\ \text{(iii)} & -a \in S \quad (\text{additive inverse}) \\ \text{(iv)} & a \cdot b \in S \quad (\text{closure under } \cdot) \end{array} \right\} S \text{ is a subgroup}$$

Proposition 2.2: Subring Criterion

If $S \subset R$ is a subset of a ring such that $\forall a, b \in S$

- (i) $S \neq \emptyset$
- (ii) $a - b \in S$
- (iii) $a \cdot b \in S$

then S is a subring.

Proof. Suppose $a, b \in S$ and the conditions above are true, then

- (i) $a - a = 0 \in S$
- (ii) $0 - a = -a \in S$
- (iii) $a - b = a + (-b) \in S$
- (iv) $a \cdot b \in S$

thus satisfying the definition of a subring. ■

Example 2.8 $\mathbb{Z} \subset \mathbb{Q}, \mathbb{Q} \subset \mathbb{R}, \mathbb{Z} \subset \mathbb{R}$ are all subrings.

Example 2.9 $2\mathbb{Z} \subset \mathbb{Z}$ is a subring and more generally $n\mathbb{Z} \subset \mathbb{Z}$ is a subring.

Example 2.10 $C[0, 1] \subset \mathcal{F} := \{f : [0, 1] \rightarrow \mathbb{R}\}$ is a subring.

Definition 2.5: Subfield

If F is a field and $F' \subset F$ is a subring such that

- (i) $1 \in F'$
- (ii) $\forall a \in F', a^{-1} \in F'$

then we say F' is a **subfield** of F .

Warning: Not all subrings of fields are subfields! (e.g $\mathbb{Z} \subset \mathbb{R}$)

Claim: If $R \subset F$ is a subring of a field with $1 \in R$, then R is an integral domain.

Lecture 3

Polynomial Rings

Fix a commutative ring R with 1 (e.g. $R = \mathbb{Z}$, $R = \mathbb{Q}$, etc) Let X be an indeterminate (this means X is just a symbol without an exact representation, compared to when you think x is a variable representing a number).

Definition 3.1: Polynomial Ring

A **polynomial** in X with coefficients in R is a formal, finite sum

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0, \quad a_i \in R, i \in \{0, \dots, n\}$$

Note: If $a_n \neq 0$ and $a_m = 0, \quad \forall m > n$. Then we say the **degree** of the polynomial is n . If $a_k = 1$, we often omit it from the notation, e.g

$$X^2 + 2$$

has a 1 "missing" in front of X^2 .

If $a_n = 1$, we say the polynomial is **monic**

Definition 3.2: Set of Polynomials and Constant Polynomial

The **set of polynomials** in X w/ coefficients in R is denoted

$$R[X] := \{a_n X^n + \cdots + a_0 \mid a_i \in R\}$$

If the degree of $p \in R[X]$ is zero, we say p is a **constant** polynomial.

Observe that there is an obvious inclusion map from a ring into the ring of polynomials, by taking each element $a \in R$ to the constant polynomial $a \in R[X]$.

$$R \rightarrow R[X]$$

$$a \mapsto a$$

Claim: $R[X]$ is a ring.

Proof. We check the ring properties

(i) Closure under addition

$$\begin{aligned} & (a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0) + (b_n X^n + b_{n-1} X^{n-1} + \cdots + b_1 X + b_0) \\ &= (a_n + b_n) X^n + (a_{n-1} + b_{n-1}) X^{n-1} + \cdots + (a_1 + b_1) X + (a_0 + b_0) \end{aligned}$$

(ii) Closure under multiplication

$$\begin{aligned} & (a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0) \cdot (b_m X^m + b_{m-1} X^{m-1} + \cdots + b_1 X + b_0) \\ &= (a_0 \cdot b_0) + (a_1 \cdot b_0 + a_0 \cdot b_1) X + (a_2 \cdot b_0 + a_1 \cdot b_1 + a_0 \cdot b_2) X^2 \\ & \quad + \cdots + \left(\sum_{k=0}^l a_k \cdot b_{l-k} \right) X^l + \cdots + (a_n \cdot b_m) X^{n+m} \end{aligned}$$

■

Example 3.1 $\mathbb{Z}[X], \mathbb{Q}[X], \mathbb{Z}/3\mathbb{Z}[X]$, which are rings of polynomials with coefficients in different number systems. In particular, we may write $\mathbb{Z}/3\mathbb{Z}$ coefficients without the "overbar" notation,

$$X + 2, X^3 + 2X^2 + 1 \in \mathbb{Z}/3\mathbb{Z}[X]$$

Factoring polynomials depends on the coefficient ring. For example

$$X^2 - 2 \in \mathbb{Z}[X]$$

$$X^2 - 2 = (X + \sqrt{2}) \cdot (X - \sqrt{2}) \in \mathbb{R}[X]$$

Here we can see that $X^2 - 2$ can not be factored further in the integers, but in the real numbers it can.

Similarly, $X^2 + 1 \in \mathbb{Z}[X], X^2 + 1 \in \mathbb{R}[X]$. These polynomials doesn't factor in either ring, but it does factor in $\mathbb{C}[X]$

$$X^2 + 1 = (X + i)(X - i)$$

it also factors in $\mathbb{Z}/2\mathbb{Z}[X]$

$$X^2 + 1 = (X + 1)(X + 1) \pmod{2}$$

Because $X^2 + 2X + 1 \equiv X^2 + 1 \pmod{2}$

Proposition 3.1

Let R be an integral domain and $p(X), q(X) \in R[X]$

- (i) $\deg(p(X) \cdot q(X)) = \deg p(X) + \deg q(X)$.
- (ii) $R[X]^\times = R^\times$
- (iii) $R[X]$ is an integral domain

Proof.

(i) The leading term is

$$(a_n \cdot b_m)X^{n+m}$$

Since R is an integral domain and $a_n, b_m \neq 0$. Then $a_n \cdot b_m \neq 0$ (This also proves (iii))

(ii) Suppose $p(X) \in R[X]^\times$, say $p(X) \cdot q(X) = 1$.

Then

$$\deg(p \cdot q) = \deg(1) = 0 \implies \deg(p) + \deg(q) = 0 \implies \deg(p) = \deg(q) = 0 \implies p(X) \in R$$

i.e $p(X)$ is a constant polynomial whose constant coefficient, say p , is from the ring R .

Hence, since $p(X)$ is a unit, so is p . ■

Example 3.2 Consider $2X^2 + 1, 2X^5 + 3X \in \mathbb{Z}/4\mathbb{Z}[X]$

$$(2X^2 + 1) \cdot (2X^5 + 3X) = 2 \cdot 2X^7 + \text{lower terms} = 0 \cdot X^7 + \text{lower terms}$$

This implies

$$\deg((2X^2 + 1) \cdot (2X^5 + 3X)) < \deg(2X^2 + 1) + \deg(2X^5 + 3X)$$

When R isn't an integral domain, the degree of the product of polynomials can be less than the degree of their sum (in general, the degree is at most the sum).

Ring Homomorphisms

Definition 3.3: Ring homomorphism and isomorphism

Let R, S be rings. A **ring homomorphism** is a map $f : R \rightarrow S$ such that

$$(i) \ f(a +_R b) = f(a) +_S f(b) \quad (\text{Group homomorphism})$$

$$(ii) \ f(a \cdot_R b) = f(a) \cdot_S f(b)$$

If f is a bijective ring homomorphism, we say it is a **ring isomorphism**.

We say, in this case R is **isomorphic** to S as rings and write

$$R \cong S$$

Definition 3.4

The **kernel** of a ring homomorphism $f : R \rightarrow S$ is the subset

$$\text{Ker } f := f^{-1}(0_S) \subset R$$

Proposition 3.2

Let R, S be rings and $f : R \rightarrow S$ a homomorphism, then

(i) $\text{Im } f \subset S$ is a subring

(ii) $\text{Ker } f \subset R$ is a subring

where Im is the image of f and Ker is the kernel.

Moreover, if $r \in R$, $a \in \text{Ker } f$ then $r \cdot a \in \text{Ker } f$.

(this is a stronger property of the kernel, which shows it is more than just a subring, since it is also closed under multiplication with elements from outside the kernel, in particular from the ring).

Both proofs rely on using the Subring Criterion Test mentioned in Lecture 2.

Proof (i). First, we check show that it is non empty.

Claim: $f(0_R) = 0_S$ and in particular $\text{Im } f \neq \emptyset$.

Proof. By definition of ring homomorphism

$$f(0_R) = f(0_R + 0_R) = f(0_R) + f(0_R) \implies 0_S = f(0_R)$$

Where we have subtracted (in S) $f(0_R)$ from both sides. ■

Suppose now $f(a), f(b) \in \text{Im } f$, then

$$f(a) \cdot f(b) = f(a \cdot b) \in \text{Im } f$$

which shows the product is also in the image.

Finally, what's left to show is that the difference is also in the image. To see $f(a) - f(b) \in \text{Im } f$, it suffices to see that $-f(b) = f(-b)$.

Claim: $-f(b) = f(-b)$

Proof. Again using the ring homomorphism definition

$$0 = f(0_R) = f(b + (-b)) = f(b) + f(-b) \implies f(-b) = -f(b)$$

Therefore, with the subring criterion satisfied, then $\text{Im } f$ is a subring in S .

Proof (ii). Since $f(0_R) = 0_S \implies 0_R \in \text{Ker } f$, hence $\text{Ker } f$ is nonempty. Suppose $a, b \in \text{Ker } f$, then

$$f(a - b) = f(a) - f(b) = 0 - 0 = 0 \implies a - b \in \text{Ker } f$$

and

$$f(a \cdot b) = f(a) \cdot f(b) = 0 \cdot 0 = 0 \implies a \cdot b \in \text{Ker } f$$

Hence, $\text{Ker } f$ is a subring in R .

Now suppose $r \in R$

$$f(r \cdot a) = f(r) \cdot f(a) = f(r) \cdot 0 = 0$$

which proves the additional property.

Example 3.3 Consider the map which takes even numbers to 0 and odd numbers to 1.

$$\begin{aligned} f : \mathbb{Z} &\rightarrow \mathbb{Z}/2\mathbb{Z} \\ a &\mapsto a \pmod{2} \end{aligned}$$

Check the possible situations (these show the sums and products follow the homomorphism properties)

Addition	$\begin{aligned} \bar{0} + \bar{0} &= \bar{0} & \text{even} + \text{even} &= \text{even} \\ \bar{0} + \bar{1} &= \bar{1} & \text{even} + \text{odd} &= \text{odd} \\ \bar{1} + \bar{1} &= \bar{0} & \text{odd} + \text{odd} &= \text{even} \end{aligned}$
Multiplication	$\begin{aligned} \bar{0} \cdot \bar{0} &= \bar{0} & \text{even} \cdot \text{even} &= \text{even} \\ \bar{0} \cdot \bar{1} &= \bar{0} & \text{even} \cdot \text{odd} &= \text{even} \\ \bar{1} \cdot \bar{1} &= \bar{1} & \text{odd} \cdot \text{odd} &= \text{odd} \end{aligned}$

Therefore $\text{Ker } f = \{\text{evens}\} = 2\mathbb{Z}$ and observe that

$$f^{-1}(\bar{1}) = \{\text{odds}\} = 1 + 2\mathbb{Z} = \{1 + 2n | n \in \mathbb{Z}\} = 1 + \text{Ker } f$$

Example 3.4 The following is a non-example. Consider

$$\begin{aligned} f_n : \mathbb{Z} &\rightarrow \mathbb{Z} \\ a &\mapsto n \cdot a \end{aligned}$$

Then

$$f_n(a + b) = n \cdot (a + b) = n \cdot a + n \cdot b = f_n(a) + f_n(b)$$

But

$$f_n(a \cdot b) = n(a \cdot b) \stackrel{?}{=} n^2(a \cdot b) = (n \cdot a) \cdot (n \cdot b) = f_n(a) \cdot f_n(b)$$

So f_n is a ring homomorphism if and only if $n^2 = n$ (i.e $n = 0, 1$). f_0 is the constant map zero and f_1 is the identity.

Therefore f_2, f_3, \dots are **NOT** ring homomorphisms. In particular, it shows that a group homomorphism is not necessarily a ring homomorphism.

Example 3.5 Here is a polynomial homomorphism which maps a polynomial to its own constant term

$$\begin{aligned}\phi : \mathbb{R}[X] &\rightarrow \mathbb{R} \\ p(X) &\mapsto p(0)\end{aligned}$$

This can easily be checked

$$\begin{aligned}\phi(p + q) &= (p + q)(0) = p(0) + q(0) = \phi(p) + \phi(q) \\ \phi(p \cdot q) &= (p \cdot q)(0) = p(0) \cdot q(0) = \phi(p) \cdot \phi(q)\end{aligned}$$

Its kernel (which are polynomials who have 0 as a root) can be written

$$\begin{aligned}\text{Ker}\{p \in \mathbb{R}[X] \mid p(0) = 0\} &= \{p \in \mathbb{R}[X] \mid p(x) = x \cdot p'(x) \text{ for some } p' \in \mathbb{R}[X]\} \\ (p' \text{ is not the derivative, just another polynomial}).\end{aligned}$$

Question: What about

$$\begin{aligned}\phi_1 : \mathbb{R}[X] &\rightarrow \mathbb{R} \\ p(x) &\mapsto p(1)\end{aligned}$$

Lecture 4

Quotient Rings

Recall that given a ring homomorphism $f : R \rightarrow S$, the kernel of f , $\text{Ker } f$, is a subring of R .

Definition 4.1: Coset and Quotient Ring

Given a ring homomorphism $f : R \rightarrow S$, let $I = \text{Ker } f$ and $r \in R$.

The **coset** of $r \in R$ with respect to f (or w.r.t I) is the set

$$r + I := \{r + x \mid x \in I = \text{Ker } f\}$$

The **quotient ring** of R by I is the set

$$R/I := \{r + I \mid r \in R\}$$

Proposition 4.1

Given a ring homomorphism $f : R \rightarrow S$ with $I = \text{Ker } f$, the quotient ring R/I is a ring with operations

$$(r + I) + (s + I) := (r + s) + I$$

$$(r + I) \cdot (s + I) := (r \cdot s) + I$$

Note: If I is understood, we will often write \bar{r} for $r + I$, e.g

$$(r + I) + (s + I) = (r + s) + I$$

becomes

$$\bar{r} + \bar{s} = \overline{r + s}$$

Lemma 4.1

If $r, s \in R$ and $(r + I) \cap (s + I) \neq \emptyset$, then $r + I = s + I$

Proof. Suppose $x \in (r + I) \cap (s + I)$, then

$$x \in r + I \implies x = r + a, a \in I$$

$$x \in s + I \implies x = s + b, a \in I$$

These together lead to three equivalent equations

$$r + a = s + b \iff r = s + (b - a) \iff s = r + (a - b)$$

Since $I \subset R$ is a subring then we know $b - a, a - b \in I$. Then the previous equations imply

$$r \in s + I, s \in r + I$$

Now take any element $c \in I$, then

$$r + c = (s + (b - a)) + c = s + (b - a + c) \in s + I \implies r + I \subset s + I$$

where the last implication comes from the fact that $b - a + c$ are elements in I and as such their combination is as well.

With similar logic we see that

$$s + c = (r + (a - b)) + c = r + (a - b + c) \in r + I \implies s + I \subset r + I$$

Hence, $r + I = s + I$. ■

Example 4.1 Let f be the homomorphism from the integers to the integers mod 2, i.e

$$\begin{aligned} f : \mathbb{Z} &\rightarrow \mathbb{Z}/2\mathbb{Z} \\ n &\mapsto n \bmod 2 \end{aligned}$$

Immediately we know that the kernel is the set of even integers, $\text{Ker } f = 2\mathbb{Z}$.

Consider the coset of $1 \in \mathbb{Z}$ which is $1 + 2\mathbb{Z}$, then

$$1 + 2\mathbb{Z} = 3 + 2\mathbb{Z} = -7 + 2\mathbb{Z} = 29 + 2\mathbb{Z}$$

where the equivalence follows from Lemma 4.1.

Lemma 4.2

If

$$\begin{aligned} r + I &= r' + I \\ s + I &= s' + I \end{aligned}$$

then

$$\begin{aligned} (r + s) + I &= (r' + s') + I \\ (r \cdot s) + I &= (r' \cdot s') + I \end{aligned}$$

i.e, $+, \cdot$ are well-defined in R/I

Proof. Let $r, r', s, s' \in R$, then

$$\begin{aligned} r + I = r' + I &\implies r = r' + x, x \in I \\ s + I = s' + I &\implies s = s' + y, y \in I \end{aligned}$$

Then their sum

$$r + s = (r' + x) + (s' + y) = (r' + s') + (x + y) \implies r + s \in (r' + s') + I$$

On the other hand $r + s = r + s + 0 \in (r + s) + I$, hence

$$[(r + s) + I] \cap [(r' + s') + I] \neq \emptyset$$

By Lemma 4.1, it is immediate that

$$(r + s) + I = (r' + s') + I$$

Similarly,

$$r \cdot s = (r' + x) \cdot (s' + y) = r' s' + r' y + x s' + x y \in r' \cdot s' + I$$
■

Observe that R/I consists of the equivalence classes in R of the equivalence relation given by

$$x \sim y \iff x - y \in I$$

Proof of Prop 4.1.

We check that the quotient is a ring

$$\bar{0} + \bar{a} = \overline{0 + a} = \bar{a} = \overline{a + 0} = \bar{a} + \bar{0} \quad (\bar{0} \in R/I \text{ is the additive identity})$$

$$\bar{a} + \overline{(-a)} = \overline{a + (-a)} = \bar{0} = \overline{(-a) + a} = \overline{(-a)} + \bar{a}$$

$$\bar{a} + \overline{(b + c)} = \overline{a + (b + c)} = \overline{(a + b) + c} = \overline{(a + b)} + \bar{c} = (\bar{a} + \bar{b}) + \bar{c}$$

$$\bar{a} \cdot \overline{(b \cdot c)} = \overline{a \cdot (b \cdot c)} = \overline{(a \cdot b) \cdot c} = \overline{a \cdot b} \cdot \bar{c} = (\bar{a} \cdot \bar{b}) \cdot \bar{c}$$

$$\bar{a} \cdot \overline{(b + c)} = \overline{a \cdot (b + c)} = \overline{a \cdot b + a \cdot c} = \overline{a \cdot b} + \overline{a \cdot c} = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}$$

■

Definition 4.2: Ideal

Let R be a ring and $I \subset R$.

We say I is a

(i) **Left ideal** if I is a subring such that for all $a \in R, x \in I$

$$a \cdot x \in I$$

(ii) **Right ideal** if I is a subring such that for all $a \in R, x \in I$

$$x \cdot a \in I$$

(iii) **Ideal** if I is both a left and right ideal (sometimes called a **two-sided ideal**).

Observe that if $f : R \rightarrow S$ is a ring homomorphism then $\text{Ker } f$ is an ideal in R .

Note: We may define R/I for **any** ideal $I \subset R$, whether or not $I = \text{Ker } f$ for some ring homomorphism $f : R \rightarrow S$.

Theorem 4.1: The First Isomorphism Theorem

If $f : R \rightarrow S$ is a ring homomorphism and $I = \text{Ker } f$. Then

$$R/I \cong \text{Im } f$$

as rings.

Proof. We first prove a smaller claim.

Claim: If $r \in R$, then

$$r + I = f^{-1}(f(r)) = \{x \in R \mid f(x) = f(r)\}$$

If $r \in R$, then

$$r + I = f^{-1}(f(r)) = \{x \in R \mid f(x) = f(r)\}$$

(Here f^{-1} is the preimage, not the inverse).

Proof. If $a \in I$, then

$$f(r + a) = f(r) + f(a) = f(r) \implies r + a \in f^{-1}(f(r)) \implies r + I \subset f^{-1}(f(r))$$

Similarly, if $x \in f^{-1}(f(r))$, then

$$f(r) = f(x) \implies f(r) - f(x) = 0 \implies f(r - x) = 0$$

This last equality means $r - x$ (and $x - r$) $\in \text{Ker } f$, hence

$$x - r \in \text{Ker } f \implies x = r + (x - r) \in r + I \implies f^{-1}(f(r)) \subset r + I$$

Therefore, both inclusions are proved and $r + I = f^{-1}(f(r))$. ■

There is a bijective map

$$\begin{aligned} \bar{f} : R/I &\rightarrow \text{Im } f \\ \bar{r} &\mapsto f(r) \end{aligned}$$

The point being that \bar{r} is independent of the representative $r \in R$. ■

Theorem 4.2

If $I \subset R$ is an ideal, then the **quotient map**

$$\begin{aligned} f : R &\rightarrow R/I \\ r &\mapsto \bar{r} \end{aligned}$$

is a surjective ring homomorphism with $\text{Ker } f = I$

Proof. Firstly, f is clearly surjective because every element of $r \in R$ will be an element of its own equivalence class.

It remains to show that this is a homomorphism.

$$f(a + b) = \overline{a + b} = \bar{a} + \bar{b} = f(a) + f(b)$$

$$f(a \cdot b) = \overline{a \cdot b} = \bar{a} \cdot \bar{b} = f(a) \cdot f(b)$$

For the kernel, by definition of the map $f(a) = \bar{a}$, but if we also have that $f(a) = \bar{0}$ then by definition of equivalence classes $\bar{a} = \bar{0}$ because if $a \sim 0$ then $\bar{a} = \bar{0}$.

Therefore $a \in I = \text{Ker } f$. ■

Example 4.2 For any integer $n \in \mathbb{Z}$, we have that

$$n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$$

is an ideal in \mathbb{Z} .

Furthermore, the quotient ring of \mathbb{Z} by $n\mathbb{Z}$ is exactly the ring $\mathbb{Z}/n\mathbb{Z}$.

Example 4.3 Let $R = \mathbb{Z}[X]$ and define

$$I := \{p(X) \in R \mid \text{all nonzero terms have degree at least } 2\}$$

e.g $7x^2 + 3x^3 + 10x^9 \in I$

Note: $0 \in I$ because it has **no** terms with non-zero coefficient.

Exercise: Prove that I is an ideal. Now consider two polynomials $p(x), q(x) \in R$ and $\overline{p(x)} = \overline{q(x)}$, then by definition of equivalence, $p - q \in I$.

So $p - q$ consists of terms of *at least* degree 2, i.e the degree 0 and degree 1 parts of p, q agree, e.g

$$5 + x + 7x^3 = 5 + x - 21x^5 + 7x^{19}$$

This implies that the polynomials of degree at most 1 represent *distinct* cosets in R/I , e.g

$$5 + x, -7 + 2x, 11 - 4x$$

Therefore, there is a bijection between

$$R/I \iff \{a + bx | a, b, \in \mathbb{Z}\}$$

Observe that R/I has zero divisors: $\overline{x} \cdot \overline{x} = \overline{x^2} = \overline{0}$.

Example 4.4 Let R be a ring and X a non-empty set. Consider the ring

$$\mathcal{F}(X, R) := \{f : x \rightarrow R\}$$

For a fixed element $a \in X$, the **evaluation map** at a is

$$\begin{aligned} \text{Ev}_a : \mathcal{F}(X, R) &\rightarrow R \\ f &\mapsto f(a) \end{aligned}$$

Exercise: Ev_a is a ring homomorphism.

Moreover, Ev_a is a *surjective* ring homomorphism and

$$\text{Ker}(\text{Ev}_a) := \{f \in \mathcal{F}(X, R) | f(a) = 0\}$$

In particular, by the First Isomorphism Theorem we have

$$\mathcal{F}(X, R) / \text{Ker}(\text{Ev}_a) \cong R$$