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 $+, \bullet$ (addition and multiplication), i.e

$$+ : R \times R \to R$$
$$\bullet : R \times R \to R$$

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

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

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 $\forall a \in R$
$$a \bullet 1_R = 1_R \bullet a = a$$
- We say R is **commutative** if $\forall a, b \in R$
$$a \bullet b = b \bullet a$$
- 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
$$a \bullet (a^{-1}) = (a^{-1}) \bullet a = 1_R$$

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

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

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

Example 1.4 $(\mathbb{R}^3, +, \bullet)$ 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

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

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

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

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

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

where

$$\overline{0} = \{0, 3, 6, 9, \dots\}$$
$$\overline{1} = \{1, 4, 7, 10, \dots\}$$
$$\overline{2} = \{2, 5, 8, 11, \dots\}$$

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

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

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 $\mathfrak{F}$

$$\mathcal{F} \coloneqq \{f : X \to R\}$$

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

$$\begin{aligned} (f+g) :&X \to R \\ &x \mapsto f(x)+g(x) \end{aligned} \qquad \begin{aligned} (f \bullet g) :&X \to R \\ &x \mapsto f(x) \bullet g(x) \end{aligned}$$

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

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

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

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

Example 1.10 Sets of matrices can also be rings. Define

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

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

$$\begin{aligned} A+B &\coloneqq \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \cdots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & \cdots & a_{2n}+b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}+b_{n1} & a_{n2}+b_{n2} & \cdots & a_{nn}+b_{nn} \end{pmatrix} \\ A \bullet B &\coloneqq (a_{ik} \bullet b_{ki}) \end{aligned}$$

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 ith row and ith column, while the k varies to multiply the kth 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 divsor.

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

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

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

<u>**Claim:**</u> If $\overline{0} \neq \overline{a} \in \mathbb{Z}/n\mathbb{Z}$ 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

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

Hence, $\overline{a}$ 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 $q, k \in Z$

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

Then,

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

Thus, $\overline{a}$ 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 $\overline{2} \cdot \overline{2} = \overline{0}$, therefore $\overline{2}$ 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

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

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

Proof. We check the properties of a group

(i) $1 \in R^\times \quad (1 \cdot 1 = 1)$

(ii) $\forall a \in \mathbb{R}^\times$, $a \cdot 1 = 1 \cdot a = a$

(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. ($\overline{2} \cdot \overline{2} = \overline{0} \implies \overline{2}$ 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 divsor.

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 $a \bullet (b - c) = 0$. 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 $\overline{2} \bullet \overline{2} = \overline{0}$ and $\overline{2} \bullet \overline{0} = \overline{0}$. So

$$\overline{2} \bullet \overline{2} = \overline{2} \bullet \overline{0}$$

but

$$\overline{2} \neq \overline{0}$$

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

$$\begin{aligned} f_a : & R \to R \\ & x \mapsto a \bullet x \end{aligned}$$

<u>**Claim:**</u> f_a is an injective map by cancellation

> ***Proof.*** Suppose $f_a(x) = f_a(y)$, then
>
> $$a \bullet x = a \bullet y \implies x = y$$
>
> hence, it is injective. ■

By the Pigeonhole Principle f_a is also surjective. This bijection implies that there exists $x \in R$ such that $a \bullet x = 1$. 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 $\forall a, b \in S$,

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

Proposition 2.2: Subgroup 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) $a \bullet b \in S$

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) $a \bullet b \in S$

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 $C[0, 1] \subset \mathcal{F} \coloneqq \{f : [0, 1] \to \mathbb{R}\}$ 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.
