Lecture 11: Introduction to Rings

Lecture: Sujata Ghosh *Scribe: Aranya Kumar Bal, Sandeep Chatterjee*

1 Topics for this lecture

In this lecture, we shall talk about the following

1. Rings
2. Special Types of Ring
3. Subrings

2 Rings

Definition 2.1 *A ring is a non-empty set, R, with two binary operations on R, one denoted by $+$ (addition) and the other denoted by $\cdot$ (multiplication), such that the following conditions are satisfied:*

1. $(R, +)$ *forms a commutative group.*
2. $\cdot$ *is associative in R.*
3. *For all $a, b, c \in R$:*

$$\left.\begin{aligned} &(i)\ a \cdot (b + c) = a \cdot b + a \cdot c \quad (1)\\ &(ii)\ (b + c) \cdot a = b \cdot a + b \cdot c \quad (2)\end{aligned}\right\} \textit{distributivity}$$

We denote this ring by $(R, +, \cdot)$.

- R is said to be a commutative ring if $\forall a, b \in R$, $a \cdot b = b \cdot a$.
- R is said to be a ring with an identity if there exists an element 1, say, in R, such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$.

Examples

1. $(\mathbb{Z},\ +,\ \cdot)$, $(\mathbb{Q},\ +,\ \cdot)$, $(\mathbb{R},\ +,\ \cdot)$
2. $\left(M_n(\mathbb{R}),\ \underset{m\times a}{+},\ \underset{m\times m}{\cdot}\right)$
3. $(2\mathbb{Z},\ +,\ \cdot)$
4. $(\mathbb{Z}/n\mathbb{Z},\ +_n,\ \cdot_n)$

Exercise: Check if $(\mathbb{Z}/n\mathbb{Z}, +_n, \cdot_n)$ forms a ring. Use the fact that

$$(a + n\mathbb{Z}) +_n (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}$$
$$(a + n\mathbb{Z}) \cdot_n (b + n\mathbb{Z}) = (a \cdot b) + n\mathbb{Z}$$

Different Types of Rings

In fact, the definition of a ring becomes more succinct if we define a couple more algebraic structures.

A set S with a binary operation $\cdot$ is called a *semi-group* if $\cdot$ is closed in S and is associative.

It is called a *monoid* if it is a semi-group and has an identity element.

[Note that a group is just a monoid with inverses.]

Then we call a set R with binary operations $+$ and $\cdot$ a ring if $(R, +)$ is a group, $(R, \cdot)$ is a semi-group and $+$ distributes over $\cdot$.

When we later define fields, you will see that it is $(F, +, \cdot)$ such that $(F, +)$ is a group, $(F, \cdot)$ is also a group and $+$ distributes over $\cdot$.

5. **Polynomial Rings**

   Take any ring $(R, +, \cdot)$. Consider a polynomial in x over ring R, say $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$, where a_i's belong to R.

   Define $+$ and $\cdot$ as follows:

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i$$
$$[n \geq m,\ b_i = 0 \text{ for } i > m]$$
$$\sum_{i=0}^{n} a_i x^i \cdot \sum_{j=0}^{m} b_j x^j = \sum_{k=0}^{l} c_k x^k,\ c_k = \sum_{i+j=k} a_j b_i$$

   Now, consider the collection of all such polynomials over ring R and denote it by $R[x]$, and consider $+$ and $\cdot$ as defined above. Then, $(R[x], +, \cdot)$ forms a ring.

   This ring is called the polynomial ring over R.

   Definition 2.2 *Let $(R; +, \cdot)$ be a ring. A polynomial, $f(x)$, over R is an expression of the form*

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

where $n \geq 0$, and $a_0, a_1, a_2, \ldots, a_n \in R$. The set of all polynomials in the indeterminate x with coefficients in R is polynomial ring, denoted by $R[x]$.

Exercise: Show that $(R[x], +, \cdot)$ forms a ring, where R is any ring.

6. **Ring of Endomorphisms**

   - A homomorphism from a group G to itself is called an endomorphism.
   - Let $(G, +)$ be a commutative group. Let $f : G \to G$ and $g : G \to G$ be two endomorphisms. Define $+_e$ and $\cdot_e$ as follows:

$$f +_e g \text{ is defined by } (f +_e g)(a) = f(a) + g(a)$$
$$f \cdot g \text{ is defined by } (f \cdot g)(a) = f(g(a))$$

Different Types of Rings

Rings can be given different flavours to suit our taste.

In what follows, let R be a non-trivial ring.

- If there is an element $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for each element $a \in R$, we say that R is a ring with unity or identity, sometimes also called an unital ring.
- A ring R for which $ab = ba$ for all a, b in R is called a commutative ring.
- A ring R is called a domain if, for every $a, b \in R$ such that $ab = 0$, either $a = 0$ or $b = 0$.
- A domain R is called an integral domain if R is commutative.

In a unital ring R, an element $x \in R$ is called an unit if there exists $y \in R$ such that $xy = 1$.

- A unital ring is called a division ring (also sometimes called a skew-field) if every element is a unit.
- A commutative division ring is called a field.

So we have several ways to go from general rings to a field; first attach an identity, then make it commutative and finally make every element a unit

$$\text{Rings} \to \text{Unital rings} \to \text{Commutative unital ring} \to \text{Fields}$$

or first attach an identity to the ring, then make everything a unit, and then make things commute

Rings → Unital rings → Division Ring → Fields

You can try and find several other ways.

In terms of inclusiveness:

Fields ⊂ Division Rings ⊂ Domains ⊂ Rings

Fields ⊂ Integral Domains ⊂ Domains ⊂ Rings

3 End(G)

We defined two operations on the set of all endomorphisms on a group. Let us verify they actually form a ring.
Let End(G) denote the collection of all endomorphisms over G.

1. Is $(\text{End}(G), +_e)$ a commutative group?

   (a) Let $f, g \in \text{End}(G)$.

   $$\begin{aligned}(f +_e g)(a_1 + a_2) &= f(a_1 + a_2) + g(a_1 + a_2) \\ &= f(a_1) + f(a_2) + g(a_1) + g(a_2) \\ &= f(a_1) + g(a_1) + f(a_2) + g(a_2) \\ &= (f +_e g)(a_1) + (f +_e g)(a_2)\end{aligned}$$

   So, $f +_e g \in \text{End}(G)$.

   (b) Associativity of $+_e$ follows from associativity of $+$ in G.

   (c) Consider the zero map $\mathcal{O} : G \to G$, where $\mathcal{O}(a) = e_G$ for all $a \in G$. Then, $\mathcal{O}$ is the identity element.

   (d) Take $f \in \text{End}(G)$. Then, $f^{-1} : G \to G$ is defined by $f^{-1}(a) = -f(a)$, for all $a \in G$. Then,

   $$(f + f^{-1})(a) = e_G \text{ for all } a \in G$$
   $$\Rightarrow f + f^{-1} = \mathcal{O} \in \text{End}(G)$$

   (e) $(f + g)(a) = f(a) + g(a) = g(a) + f(a) = (g + f)(a)$ for all $a \in G$. So, $(f + g) = (g + f)$, where $f, g \in \text{End}(G)$.

   So, $(\text{End}(G), +)$ forms a commutative group.

2. Does $f \cdot g \in \text{End}(G)$? For any $a \in G$, $f \cdot g(a) = f(g(a))$. So, $f \cdot g \in \text{End}(G)$ as composition of homomorphisms is a homomorphism.

3. Is $\cdot$ associative? Yes, as composition of maps is associative.

4. Does the distributive laws hold? Take $f, g, h \in \text{End}(G)$. To show:

   (a) $f \cdot (g + h) = f \cdot g + f \cdot h$

   (b) $(g + h) \cdot f = g \cdot f + h \cdot f$

   (a) $$\begin{aligned}(f \cdot (g + h))(a) &= f(g + h)(a)\\ &= f(g(a) + f(h(a))\\ &= f(g(a)) + f(h(a))\\ &= f \cdot g(a) + f \cdot h(a), \text{ for all } a \in G\end{aligned}$$

   Hence, $f(g + h) = f \cdot g + f \cdot h$. Similarly, (b) holds. So, $(\text{End}(G), +, \cdot)$ forms a ring.

What happens when $G = \mathbb{Z}$? If $G = \mathbb{Z}$, then any $f \in \text{End}(\mathbb{Z})$ is given by $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$, where for any $k \in \mathbb{Z}$,

$$\begin{aligned}f(k) &= f(1 + 1 + \ldots + 1) \ (k \text{ times})\\ &= f(1) + f(1) + f(1) + \ldots + f(1) \ (k \text{ times})\\ &= k \cdot f(1)\end{aligned}$$

So, any endomorphism f on $(\mathbb{Z}, +)$ is fully given by $f(1)$.

Exercise: Prove that Composition of homomorphisms is also a homomorphism.

Exercise: Show that $(g + h) \cdot f = g \cdot f + h \cdot f$.

Exercise*: Prove that $f(k) = k \cdot f(1)$ for $k \in \mathbb{Z}^-$.

4 Subrings

A subring S of a ring R is a ring with the operations on R restricted to S.

Homework: Find all subrings of $(\mathbb{Z}, +, \cdot)$.

5 Miscellaneous facts about small rings

The smallest possible group: $\{e\}$

What about smallest possible ring? Clearly $\{0\}$ is a ring. In fact, this ring has both identities, and they are the same.

What happens if $R \neq \{0\}$, that is, there is at least one non-zero element in R? We will show that in such a ring, if 1 exists, then for sure $1 \neq 0$. To prove this, we need a small lemma first.

Lemma 5.1 *In a ring R, $a \cdot 0 = 0$ for all $a \in R$.*

Proof. We use the fact that $0 + 0 = 0$. Then we have

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

Since $+$ forms a group, it is cancellative and hence by cancelling a $a \cdot 0$ on both sides, we get $0 = a \cdot 0$. □

Claim 5.2 *If $R \neq \{0\}$, then $1 \neq 0$ in R.*

Proof. Suppose not. Now since $R \neq \{0\}$, there is $a \in R$ such that $a \neq 0$. Then $0 = a \cdot 0 = a \cdot 1 = a$ which is a contradiction. □

Fun ring fact

One can wonder why we want the addition to be abelian in a ring. Let's see how far exploration can take us.

Call $(R, +, \cdot)$ a *near-ring* if R satisfies the following:

- $(R, +)$ forms a group
- $(R, \cdot)$ forms a semi-group
- $+$ distributes over $\cdot$.

Note the difference with a ring; in a ring, $+$ forms an abelian group, here we remove that restriction. We do get a nice result though.

Proposition 5.3 *A near ring with identity is a unital ring.*

Proof. Let 1 be the identity. Then for any x and y

$$(1 + 1)(x + y) = 1(x + y) + 1(x + y) = x + y + x + y$$

$$(1 + 1)(x + y) = (1 + 1)x + (1 + 1)y = x + x + y + y$$

Equating them and cancelling terms gives $y+x = x+y$ and thus $+$ is abelian. Hence R is a unital ring. □

If $\cdot$ does not have an identity, can we still force a near ring to be a ring? No, as the following construction shows.

Take the set as S_3, the symmetric group on 3 elements. Let $+$ be the group operation on S_3 and $\cdot$ be defined as $a \cdot b = e$ for any $a, b \in S_3$. One can verify this is a near-ring but not a ring.

In fact, in the above example $\cdot$ is commutative. We can have non-commutative near rings as well. Consider the following example. Take the set as S_3 like above. Let $+$ be the group operation on S_3 again but let $\cdot$ be defined as $a \cdot b = aba^{-1}b^{-1}$ for any $a, b \in S_3$. One can verify this is a near-ring but not a ring, and in fact is a non-commutative near-ring.