MA542 Lecture

Timothy Kohl

Boston University

January 22, 2025

Rings

Definition

A ring is a set R together with two binary operations, addition (denoted $a+b$) and multiplication (denoted $a \cdot b$ or ab) such that for all $a, b, c \in R$.

1. $a+b=b+a$ (commutativity of addition)
2. $(a+b)+c=a+(b+c)$ (associativity of addition)
3. There is an additive identity $0 \in R$ such that $a+0=a$ for all $a \in R$.
4. For each $a \in R$, there is an element $b \in R$ such that $a+b=0$, where we denote b by $-a$. (the additive inverse)
5. $a(bc)=(ab)c$ (associativity of multiplication)
6. $a(b+c)=ab+ac$ (distributivity of multiplication over addition)

We note that axioms 1-4 make $(R, +)$ into an abelian group.

It is the addition of the multiplication that makes R into a ring.

The most basic example is the integers $\mathbb{Z}$ with the usual arithmetic of addition and multiplication that we're all familiar with.

Indeed the formalizing and axiomitization of the rules of arithmetic which gives us the definition of ring.

Beyond the integers, there are a number of natural and familiar generalizations.

- $\mathbb{Q}$ the rational numbers with the usual addition/multiplication
- $\mathbb{R}$ the real numbers with the usual addition/multiplication
- $\mathbb{C} = \{a + b\ i \mid a, b \in \mathbb{R},\ i^2 = -1\}$ the complex numbers
  where $(a + bi) + (c + di) = (a + c) + (b + d)i$
  and (because $i^2 = -1$) $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$

Exercise: Verify that $\mathbb{C}$ is a ring.

We also note that for any integer $n \geq 1$ the abelian group $\mathbb{Z}_n$ becomes a ring if we define multiplication 'mod n'.

Example: Consider $\mathbb{Z}_4$ whose structure we can examine by viewing the following tables:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Recall from basic group theory that the group table (Cayley table) of a group is a latin square, namely each element in the group appears exactly once in each row and each column.

This is clearly the case for $(\mathbb{Z}_4, +)$ however it is *not* the case for the $(\mathbb{Z}_4, \cdot)$ table which highlights an important fact we'll explore more subsequently,namely that for a ring $(R, +, \cdot)$ one has that $(R, \cdot)$ does *not* yield a group structure, even though it is closed and associative under multiplication.

Two other observations regarding the multiplicative structure of a ring:

- There may or may not be a multiplicative identity element.
- Even if there is a multiplicative identity, not all elements in the ring have a multiplicative inverse.

More on this later.

Also, while R is an abelian group with respect to addition, it is not required that the multiplication be commutative.

Ex: a non-commutative ring

$$R = M_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z} \right\}$$

with addition and multiplication being the usual matrix addition and multiplication.

In linear algebra one learns that for $A, B, C \in M_2(\mathbb{Z})$

$$\begin{aligned}
A + B &= B + A \\
A + (B + C) &= (A + B) + C \\
0 &= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \text{ is the additive identity} \\
A &= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \\
&\downarrow \\
-A &= \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} \text{ is the additive inverse}
\end{aligned}$$

Moreover, one shows that matrix multiplication defined as

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} ax + bz & ay + bw \\ cx + dz & cy + dw \end{bmatrix}$$

is associative, and distributes over matrix addition.

However, as you may already know, for matrices A, B it is generally the case that $AB \neq BA$.

So one may divide rings into two major categories, commutative vs. non-commutative. (We generally don't call a ring 'abelian'.)

In a ring like $\mathbb{Z}$ for example, there is a multiplicative identity 1 which has the property that

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

for all $a \in R$.

We call 1 the unity element.

One typically uses the symbol '1' for such an element, with some exceptions, for example in $M_2(\mathbb{Z})$ the matrix

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ the identity matrix}$$

which one may verify has the property that $A \cdot I = A$ and $I \cdot A = A$ for all $A \in M_2(\mathbb{Z})$.

While (most) rings have unity, it is not required in the definition of a ring.

For example, $R = 2\mathbb{Z}$, the set of even integers under the usual addition and multiplication, has no unity element.

i.e. It's **never** true that $(2m)(2n) = 2n$ for any non-zero m, n!

i.e. $1 \notin 2\mathbb{Z}$.

Other examples of rings.

$$\mathbb{Z}[x] \leftarrow \left\{ \begin{array}{c} \text{polynomials with integer coefficients} \\ \text{with usual polynomial addition/multiplication} \end{array} \right\}$$

$$\mathbb{R}[x] \leftarrow \left\{ \text{ same thing but with real coefficients} \right\}$$

$$C^0(\mathbb{R})$$

$$= \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ continuous}\}$$

where $(f+g)(a) = f(a) + g(a)$ and $(f \cdot g)(a) = f(a)g(a)$

similarly

$$C^1(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ differentiable}\}$$

with the same 'pointwise' addition and multiplication

We saw earlier the definition of the complex numbers:

$$
\begin{aligned}
\mathbb{C} &= \{a + b\ i \mid a, b \in \mathbb{R},\ i^2 = -1\} \\
(a+bi) + (c+di) &= (a+c) + (b+d)i \\
(a+bi)(c+di) &= (ac-bd) + (ad+bc)i \\
(0+0i) + (a+bi) &= a + bi \\
(1+0i)(a+bi) &= a + bi
\end{aligned}
$$

where, in particular, the multiplication is keyed to the fact that $i^2 = -1$.

Moreover, $\mathbb{C}$ can also be viewed as a vector space in that every $z \in \mathbb{C}$ is of the form $z = a + bi = a \cdot 1 + b \cdot i$.

i.e. every element of $\mathbb{C}$ is a linear combination of $\{1, i\}$