Introduction to Rings and Modules

Lecture 1, Wednsday March 15 2023

Ari Feiglin

1.1 Rings

The definition of mathematical objects is (usually) the product of decades of research, and are the abstraction of more specific exhaustively studied mathematical objects which have common characteristics with one another. When studying math, especially on an undergraduate level, we are more or less oblivious to this fact, as we are served these definitions on a silver platter and are not made aware of the arduous process which lead to the modern definition. The following definition is not universally accepted, as different authors may define the following mathematical object in different (non-equivalent) ways:

Definition 1.1.1:

A **ring** is a set R equipped with two binary operations $(+,\cdot)$ (remember that this is just a notation and does not necessarily correlate with real/complex addition and multiplication), which satisfy the following axioms:

(1) $(R,+)$ is an abelian group, ie:

- (i) $+$ is associative.
- (ii) There exists an identity element $0_R \in R$ such that for every $a \in R$, $a + 0_R = 0_R + a = a$.
- (iii) For every $a \in R$, a has an additive inverse $-a \in R$ such that $a + (-a) = (-a) + a = 0_R$.
- (iv) $+$ is commutative (abelian).

(2) $(R,\cdot)$ is a monoid, ie:

- (i) $\cdot$ is associative.
- (ii) There exists an identity element $1_R \in R$ such that for every $a \in R$, $a \cdot 1_R = 1_R \cdot a = a$.

(3) $\cdot$ and $+$ are distributive:

- (i) For every $a,b,c \in R$: $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$ (left distributivity).
- (ii) For every $a,b,c \in R$: $(b+c) \cdot a = (b \cdot a) + (c \cdot a)$ (right distributivity).

We say that a ring R is **commutative** if $(R,\cdot)$ is abelian (for every $a,b \in R : a \cdot b = b \cdot a$).

Note that multiplication in a ring need not be commutative.
For example, it is trivial to see why the following are true (the operations are obvious):

(1) $R = \mathbb{Z}$ is a commutative ring.

(2) $R = \mathbb{Z}_n \cong {}^{\mathbb{Z}}/_{n\mathbb{Z}}$ is a commutative ring.

(3) $R = M_n(\mathbb{R})$ ($M_n(\mathbb{R})$ is the set of all real square matrices of size $n \times n$) is a ring, and for $n \geq 2$ it is non-commutative.

(4) If S is a ring, $M_n(S)$ is also a ring (the operations defined on $M_n(S)$ are analogous to those defined when S is a field, it should be obvious why this is a ring).

Definition 1.1.2:

A similar mathematical object where $(R,\cdot)$ is instead a semigroup (it doesn't necessarily have an identity), is called an **rng** (a ring without an *i*dentity).

Definition 1.1.3:

Suppose R is a ring such that for every $0_R \neq a \in R$ has a multiplicative inverse, R is called a **division ring**. If furthermore multiplication is commutative, R is a **field**.

Note that a ring R is a division ring (respectively field) if $(R \setminus \{0_R\}, \cdot)$ is a group (respectively abelian group) or empty. We will soon show that $0_R = 1_R$ if and only if $|R| = 1$ (the trivial ring), so we can remove the "or empty" part of the previous observation if we assume R is non-trivial, and a trivial ring is trivially a field.
One example of a division ring is the *quaternions* which were defined in our Group Theory course, but another definition is $\mathbb{H}$ (the set of quaternions) is the real vector space with basis $\{1, \mathrm{i}, \mathrm{j}, \mathrm{k}\}$ such that:

$$\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = 1, \quad \mathrm{ij} = \mathrm{k}, \quad \mathrm{jk} = \mathrm{i}, \quad \mathrm{ki} = \mathrm{j}, \quad \mathrm{ji} = -\mathrm{k}, \quad \mathrm{kj} = -\mathrm{i}, \quad \mathrm{ik} = -\mathrm{j}$$

So:

$$\mathbb{H} = \{a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k} \mid a, b, c, d \in \mathbb{R}\}$$

It can be shown that $\mathbb{H}$ is a division ring, and it is obviously not a field since multiplication is not commutative (for example $\mathrm{ij} \neq \mathrm{ji}$).

Proposition 1.1.4:

Suppose R is a ring, then for every $a \in R$:

$$a \cdot 0_R = 0_R \cdot a = 0_R$$

Proof:

This is quite simple:

$$a \cdot 0_R = a \cdot (0_R + 0_R) = a \cdot 0_R + a \cdot 0_R$$

So if we let $b = a \cdot 0_R$ (just to make it easier on the eyes), by the ring axioms, we have that:

$$b + b = b$$

and since by the ring axioms $-b \in R$, we have that:

$$b + b - b = b - b \Longrightarrow b = 0_R$$

that is, $a \cdot 0_R = 0_R$.
The proof for $0_R \cdot a = 0_R$ is similar.

■

Proposition 1.1.5:

If R is a ring, then $1_R = 0_R$ if and only if R is trivial.

Proof:

If R is trivial, this is trivial (there is only one element). To show the converse, notice that on one hand since 1_R is the multiplicative identity, for every $a \in R$, $1_R \cdot a = a$. But by above, $1_R \cdot a = 0_R \cdot a = 0_R$, so $a = 0_R$ for every $a \in 0_R$ and therefore R is trivial.

■

Definition 1.1.6:

A **left zero divisor** in a ring R is an element $0_R \neq a \in R$ such that there exists $0_R \neq b \in R$ such that $ab = 0_R$. Similarly, b is a **right zero divisor**. If an element is a left or right zero divisor, it is also simply known as a **zero divisor**.

Definition 1.1.7:

A commutative ring is known as an **integral domain** if it contains no zero divisors.

Proposition 1.1.8:

If R is a finite integral domain, then R is a field.

Proof:

Since R is necessarily commutative, all we need to show is that $(R, \cdot)$ is a group (the trivial case is trivial). We showed that a reducible monoid is a group in Group Theory, and $(R, \cdot)$ is a group by assumption, but we will prove this differently.
Let $0_R \neq a \in R$ then there exists two numbers $m < n$ such that $a^m = a^n$, so $a^m - a^n = 0_R$ (otherwise all a^m are distinct and then R is infinite). Notice that $a^m \neq 0_R$, this can be shown inductively since $a \neq 0_R$ and $a^{m-1} \neq 0_R$ and R has no zero divisors. So:

$$a^m(a^{n-m} - 1_R) = 0_R$$

which means that $a^{n-m} = 1_R$ and so $aa^{n-m-1} = a^{n-m-1}a = 1_R$ so $a^{n-m-1} = a^{-1}$, as required.

■

Proposition 1.1.9:

The axiom that $(R, +)$ is abelian follows from the rest of the axioms.

Proof:

Notice that:

$$a + a + b + b = a(1_R + 1_R) + b(1_R + 1_R) = (a + b)(1_R + 1_R) = (a + b)1_R + (a + b)1_R = a + b + a + b$$

and so by subtracting a from the left and b from the right, we have that:

$$a + b = b + a$$

■

If S is a ring, we define the *ring of polynomials* over S to be:

$$R = S[x] = \{a_0 + a_1x + \cdots + a_nx^n \mid n \in \mathbb{N}_{\geq 0}, a_i \in S\}$$

with the usual operations of polynomial addition and multiplication.
If we have two variables, x and y which commute, then we can define the two-variable polynomials over S to be all the polynomials with x and y:

$$S[x, y] = \big(S[x]\big)[y] = \big(S[y]\big)[x]$$

And we can inductively define $S[x_1, \ldots, x_n]$. The symbols x_i are called *indeterminates*.
If the two variables don't commute, this is denoted as $S\langle x, y\rangle$.
The ring of power series over a ring S is defined as:

$$S[\![x]\!] = \left\{ \sum_{k=0}^{\infty} a_k x^k \;\middle|\; a_k \in S \right\}$$

with the usual operations.
If S is a set, we can define operations over $\mathcal{P}\,S$ to turn it into a ring: $A + B = A \triangle B$ and $A \cdot B = A \cap B$.