0.1 Introduction to Rings

At this point, we have now studied one kind of algebraic structure - groups. Groups are rather general things, but their flexibility means that we can say less about them. We now introduce a second kind of algebraic structure – rings.

Consider the integers, $\mathbb{Z}$. Within the integers, we have 2 operations: that of addition, and of multiplication. Adding 2 integers certainly yields another integer, and multiplying two integers also yields another integer. From elementary school, we also know that given integers a, b, c, we have

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

the distributive law. We also have the property that 1 multiplied by any integer simply yields that integer itself.

Motivated by this example, we can now define a

Definition 0.1 (Ring). A **ring** is a set R equipped with 2 binary operations $+, \cdot$ such that R forms an abelian group under $+$, and

1. **(Associativity)** For all $a, b, c \in R$, we have $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
2. **(Distributivity)** For all $a, b, c \in R$, we have
$$a \cdot (b + c) = a \cdot b + a \cdot c \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$
The former is called left distributivity, and the latter is right distributivity.
3. **(Unity)** There is an element $1 \in R$ such that for all $a \in R$, $1 \cdot a = a \cdot 1 = a$.

Whenever possible, we shall drop the use of $\cdot$ to make it less messy, and simply write $a(b + c)$ to mean $a \cdot (b + c)$. Note that what we have just defined here is a ring with unity. Some authors (e.g. [Gal20]) defines what is generally called a Rng, a ring without unity.

Given some $a \in R$, if there is an element b such that $ab = ba = 1$, then a is said to be a *unit* and we write $b = a^{-1}$. The following proposition justifies this notation.

Proposition 0.2 (Uniqueness of units and unity). Let R be a ring. Then, the unity of R is unique, and units are unique.

Proof. Repeat the proof for groups. □

Example 0.3 (The integers)**.** It is not too hard to verify that $\mathbb{Z}$ forms a ring. In fact, it is arguably the most important ring of all. //

The multiplication in a ring need not be commutative at all. If a ring has commutative multiplication, we call it a commutative ring.

Example 0.4 (Square matrices)**.** Let $\mathcal{M}_n(\mathbb{F})$ denote the set of $n \times n$ matrices with entries from $\mathbb{F}$. For a concrete example, let $\mathbb{F} = \mathbb{R}$, and let $R = \mathcal{M}_n(\mathbb{R})$. Then R forms a ring under usual matrix addition and multiplication. This ring is also noncommutative when $n > 1$, which we leave for the reader to verify. //

Example 0.5 (Any field)**.** Any field whatsoever is a ring. Some fields that may come to your mind are $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. It is not too hard to check that these are all in fact, rings. We also have the relationship $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, and they are all subrings of each other in that way. //

We haven't defined what a subring is yet, but we shall now. Intuitively, a subring S of a ring R should form a ring as well, but with the operations of R. That means S has to contain the additive identity of R, the multiplicative identity of R, and remain closed under addition and multiplication.

Exercise 0.6. Formulate the definition of a subring.

We shall now see some basic properties of rings. These properties will allow us to use the familiar rules from multiplication and subtraction of integers that we are used to.

Proposition 0.7 (Basic properties of rings)**.** Let R be a ring, and let $a, b, c \in R$. Then, the following are true:

1. $a0 = 0a = 0$;
2. $a(-b) = (-a)b = -(ab)$;
3. $(-a)(-b) = ab$;
4. $a(b-c) = ab - ac$, $(b-c)a = ba - ca$;
5. $(-1)a = -a$;
6. $(-1)(-1) = 1$.

Proof. We will prove this without making use of the element $1 \in R$, so that this proposition remains true for rngs. For the first one, notice that

$$0 + a0 = a0 = a(0+0) = a0 + a0.$$

Subtract $a0$ on both sides to obtain the result. The other way is similar.

For 2, we have

$$a(-b) + ab = a(-b+b) = a0 = 0.$$

Adding $-(ab)$ to both sides yields $a(-b) = -(ab)$. Switch the roles of a and b to get the other one. □

Exercise 0.8. Complete the proof of Proposition 0.7 without making use of the unity 1, except in rules 5 and 6.

This proposition is useful and not difficult to prove.

Proposition 0.9 (Subring test)**.** Let $S \subseteq R$ be a subset of R. Then S is a subring of R if and only if S contains 1, and given $a, b \in S$, we have $a - b \in S$ and $ab \in S$.

Exercise 0.10. Supply the proof of Proposition 0.9.