1.2 Lecture 2: The axioms of a ring

NOTE: In this section and throughout these lecture notes, please do not confuse the symbol R, which is used for a general ring, with the symbol $\mathbb{R}$ which is used for the set of real numbers.

Definition 1. *A* ring *is a non-empty set* R *equipped with two binary operations called addition* $(+)$ *and multiplication* $(\times)$*, satisfying the following properties :*

The first four are concerned with the operation that is called addition.

- A1 Addition is associative.
  $(r+s)+t = r+(s+t)$ for all $r, s, t \in R$.
- A2 Addition is commutative. $r+s = s+r$ for all $r, s \in R$.
- A3 R contains an identity element for addition, denoted by 0_R and called the *zero element* of R.
  $r + 0_R = 0_R + r = r$ for all $r \in R$.
- A4 Every element of R has an inverse with respect to addition. (The additive inverse of r is often denoted by $-r$).
  For every $r \in R$, there exists an element $-r \in R$ for which $r + (-r) = 0_R$.

NOTE : Axioms A1 to A4 could be summarized by saying that R is an *abelian group* under addition. (If this remark is not helpful for you, disregard it for now).

The next two are about properties of the multiplication operation

- M1 Multiplication is associative.
  $(r \times s) \times t = r \times (s \times t)$ for all $r, s, t \in R$.
- M2 There is an identity element in R for the multiplication operation (often denoted 1 or 1_R and sometimes referred to as *unity*).

$$1_R \times r = r \times 1_R = r \text{ for all } r \in R.$$

The last two axioms are concerned with the manner in which the two operations must interact.

- D1 $r \times (s+t) = (r \times s) + (r \times t)$ for all $r, s, t \in R$.
- D2 $(r+s) \times t = (r \times t) + (s \times t)$ for all $r, s, t \in R$.
  These are the *distributive laws* for multiplication over addition.

REMARKS

1. Some authors omit axiom M2 from the list, and allow a structure that satisfies all the other axioms to qualify for the title "ring". Under this relaxed definition, the set of even integers for example would be a ring. This inconsistency is an inconvenience but not a major problem. If you are reading a text, just check what definition the author is using, to avoid confusion.
2. A ring is called *commutative* if its multiplication is commutative.
3. The term "ring" was introduced by David Hilbert in the late 19th century, when he referred to a "Zahlring" or "number ring".

Our first theorem about rings is the following consequence of the ring axioms.

Theorem 2. *Let R be a ring. Then for all elements r of R we have*

$$0_R \times r = 0_R \text{ and } r \times 0_R = 0_R.$$

i.e. multiplying any element of R by the zero element results in the zero element as the product.

Proof : Let $r \in R$. We have

$$\begin{aligned}(0_R \times r) + (0_R \times r) &= (0_R + 0_R) \times r \\ &= 0_R \times r.\end{aligned}$$

Adding the additive inverse of the element $0_R \times r$ to both sides of this equation gives

$$0_R \times r = 0_R.$$

A similar argument shows that $r \times 0_R = 0_R$. □

THREE REMARKS

1. Deducing the truth of a statement like Theorem 2 from the axioms of a ring is tricky. The proof may not be too hard to follow, but could you have come up with it yourself? If you were trying to, where could you start? Of the eight axioms for rings, which might be likely to be helpful in proving the two (left and right) statements of Theorem 2? The statement is about how the zero element behaves under multiplication. According to the ring axioms, the zero element is special because of how it behaves under addition. To deduce something about its role in multiplication, it must be that we have to look at how addition and multiplication interact, and the two axioms that deal with that are the *distributive laws*.

2. The next two remarks are about the philosophy of abstract algebra and how the subject progresses. The definition of a ring is a list of technical properties. The motivation for that is the ubiquity of objects having these properties, like the ones in Lecture 1. When defining the concept of a ring (or group or vector space), the goal is a set of axioms that exactly captures the crucial unifying properties of those objects that you wish to study. In familiar number systems like the integers, the rational numbers and the real numbers, we are all used to Theorem 2, which says "multiplying by zero gives zero". We can notice that this also holds in the polynomial ring $\mathbb{Q}[x]$ and in the ring of matrices $M_2(\mathbb{R})$. We might well speculate that in any ring, it's probably true that multiplying by the zero element always results in the zero element. But could this just be a feature of how multiplication is defined in polynomial rings and matrix rings? Before we can assume it in *every ring* and build it into our mental schemes for thinking about rings, we must *deduce it as a consequence of the ring axioms*.

3. Looking at Definition 1, you could ask why these eight axioms in particular are chosen for the definition of a ring. Does it look like an arbitrary selection of rules? Why do we insist that every element have an inverse for addition, but not for multiplication? Why does addition have to be commutative but not multiplication? What happens if we add more axioms, or drop some? People do these things and they lead to different areas of study within abstract algebra. Relaxing the addition axioms in various ways leads to different types of algebraic structures such as *near–rings* and *semirings*. If you drop the requirement that multiplication must be associative then you are studying *non-associative rings* – people do study all of these variants and some of them have important connections to other areas of mathematics. You can even relax the distributive laws and people do this too. However *rings* themselves as defined in Definition 1 are of paramount importance in mathematics.

   If you want more instead of fewer axioms, you can insist that multiplication be commutative as well as associative, then you are studying *commutative rings*. Some of our lectures will concentrate on commutative rings. If you further insist that every (non-zero) element have an inverse for multiplication, then you are studying *fields*. Fields are examples of rings, and field theory is a big subject. A crucial practice in studying abstract algebra is to be absolutely clear on the precise axioms that determine the class of objects that you are studying.

Exercise Could you have a ring in which the zero element and the multiplicative element are the same element? What could such a ring look like? How many other elements could it have? (Use Theorem 2.)