MA3201 Rings and Modules, 2014

Key Definitions

Definition. A *ring* is a non-empty set R with two binary operations, $+$ (addition) and $\cdot$ (multiplication). We usually write $r \cdot s$ as just rs. These operations must satisfy the axioms:

(1) $(R, +)$ is an abelian group.
(2) *Associativity of multiplication*: $r(st) = (rs)t$ for all r, s, t in R.
(3) *Multiplication is distributive over addition on both sides*: $r(s+t) = rs + rt$ and $(s+t)r = sr + tr$ for all $r, s, t \in R$.
(4) *Multiplicative identity*: There is an element $1_R \in R$, such that $1_R r = r 1_R = r$ for all $r \in R$.

Lemma. Let R be a ring. Then $0_R = 1_R$ if and only if $R = \{0_R\}$.

Proof. Suppose that R is a ring and $1_R = 0_R$. Then, if $r \in R$, $r = r1_R = r0_R = 0_R$. Hence $R = \{0_R\}$. Conversely, if $R = \{0_R\}$, then $1_R \in R$, so $1_R = 0_R$. □

Rings satisfying the equivalent conditions in Lemma are called *zero rings*. An example of a zero ring is $\mathbb{Z}_1 = \{0\}$, the integers modulo 1. We also have, for any ring R, the quotient ring R/R, whose only element is the coset $0_{R/R} = 0 + R$.

Definition. A *commutative ring* is a ring in which the multiplication is commutative, i.e. $rs = sr$ for all $a, b \in R$.

For example, $\mathbb{Z}$ and $\mathbb{Z}[x]$ are commutative.

Definition. An *integral domain* is a ring R in which $\mathbf{1_R \neq 0_R}$ and $rs \neq 0_R$ for any non-zero elements $r, s \in R$.

Note that many mathematicians assume integral domains to be commutative, in addition to this.

Also, our definition means that integral domains must be non-zero. This is usually assumed because of a strong relationship with division rings and fields. Examples include $\mathbb{Z}$ and $\mathbb{Z}[x]$.

Definition. A *division ring* is a ring in which $1 \neq 0$ and every non-zero element has a multiplicative inverse.

Our definition means that division rings must be non-zero. Examples include $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$. The quaternions, $\mathbb{H}$, are an example of a non-commutative division ring. We are aiming for the Wedderburn-Artin theorem, which explains how a certain class of rings can be built up from division rings and matrix rings over division rings. From this point of view it is convenient to have that division rings are non-zero.

Definition. A *field* is a commutative division ring.

Thus, we also insist that fields are non-zero (i.e. that $1 \neq 0$ in a field). This definition ensures, for example, that the cardinality of a finite field is a positive power of a prime number (for example, the field $\mathbb{Z}_p$, for p a prime number, has p elements). Such fields will be discussed in the Galois Theory course, MA3202.

We shall also see that, for an ideal I, R/I is a field if and only if I is a maximal ideal. If we allowed zero fields, we would have to assume that I is proper (i.e. $I \neq R$) for this to hold.

Other examples of fields include $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.

Definition. Let R be a ring. Then a non-empty subset S of R is said to be a *subring* of R if and only if

(1) For all $r, s \in S$, $r - s \in S$.
(2) For all $r, s \in S$, $rs \in S$.
(3) $1_R \in S$.

Here, since we assume rings to always have an identity, it is natural to insist that the identity element of a ring lies in any subring. Since the multiplicative identity of a ring is unique, it will be the identity element for the subring also.

Definition. Let R and S be rings. A map $\varphi : R \to S$ with the properties:

(1) $\varphi(r + s) = \varphi(r) + \varphi(s)$ for all $r, s \in R$.
(2) $\varphi(rs) = \varphi(r)\varphi(s)$ for all $r, s \in R$.
(3) $\varphi(1_R) = 1_S$

is called a *ring homomorphism* (from R to S).

Similarly, here we insist that a ring homomorphism from R to S sends the multiplicative identity of R to the multiplicative identity of S.

Later in the course, we will also consider the following.

Definition. Let R be a ring. Then a (left) *R-module* is a pair consisting of an abelian group M and a map from $R \times M$ to M mapping (r, m) to rm, satisfying the axioms:

(1) $r(m_1 + m_2) = rm_1 + rm_2$ for all $r \in R$, $m_1, m_2 \in M$;
(2) $(r_1 + r_2)m = r_1m + r_2m$ for all $r_1, r_2 \in R$, $m \in M$;
(3) $(r_1r_2)m = r_1(r_2)m$ for all $r_1, r_2 \in R$, $m \in M$;
(4) $1_Rm = m$ for all $m \in M$.

Similarly, here, we insist that $1_Rm = m$ for all elements $m \in M$.

Sometimes algebraic objects which satisfy all of the axioms for a ring except the existence of a multiplicative identity, arise. For example, $2\mathbb{Z}$, the even integers.

Sometimes one ring can be contained in another ring but have a different identity element (see, for example, Exercise 3(b) and 6(b) on page 174 of the course book, from Problem Sheet 1). Such rings are not regarded as subrings in this course, since they do not satisfy the third axiom in the definition of a subring.

Remark. The rings we consider in this course are often known as *unital rings* or *rings with identity* to emphasize the fact that they have a multiplicative identity element (sometimes referred to as a unit element). Although our focus is on rings with identity, it is important to note that rings without identity are also studied.

Example: Let $\mathbb{F}$ be a field, and let Q be the quiver:

$$\begin{tikzcd} 1 \arrow[r, "\alpha"] & 2 \arrow[r, "\beta"] & 3 \end{tikzcd}$$

Let A be the subspace of $\mathbb{F}Q$ spanned by e_1, e_2, α. Then A does not contain $1_{\mathbb{F}Q} = e_1 + e_2 + e_3$ but does satisfy the first two axioms in the definition of a subring. Although A is not a subring of $\mathbb{F}Q$, it is a ring in its own right, with identity element $1_A = e_1 + e_2$. It is isomorphic to the path algebra of

$$\begin{tikzcd} 1 \arrow[r, "\alpha"] & 2 \end{tikzcd}$$

R. J. Marsh, 2014-09-02.