

Lecture 6 (Rings and Integral Domains)

Definition 6.1 (Rings) A ring is a set R equipped with two operations, addition and multiplication such that:

R(1) R is abelian group under addition.

R(2) Multiplication is associative.

R(3) Multiplication distributes over addition, on the left and on the right.

If the multiplication is commutative then R is called a *commutative ring*

Notes and Observations Addition is usually denoted $+$ and multiplication denoted by juxtaposition. The ring axioms say for all $a, b, c \in R$

- R(1) • $a + (b + c) = (a + b) + c$.
 • $a + b = b + a$.
 • There is a $0 \in R$ such that $a + 0 = 0 + a = a$ for all $a \in R$
 • Every element $a \in R$ has an additive inverse $-a$ such that $a + (-a) = 0$.

R(2) $a(bc) = (ab)c$

R(3) $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

If $ab = ba$ for all $a, b \in R$, the ring is called *commutative*.

Examples 6.2

1. \mathbb{Z} , $2\mathbb{Z}$, \mathbb{Q} , \mathbb{R} , \mathbb{C} are all commutative rings with the usual $=$ and multiplication.
2. $M_n(\mathbb{Z})$ matrices with integer entries, $M_n(\mathbb{Q})$ matrices with rational entries, $M_n(\mathbb{R})$ matrices with real entries, $M_n(\mathbb{C})$ matrices with complex entries are non-commutative rings.

The above rings are all infinite.

3. For $m = 2, 3, 4, \dots$, $\mathbb{Z}_m = \{0, 1, 2, \dots, m - 1\}$ the distinct possible remainders on division by m with $+$ and multiplication taken modulo m are commutative rings. These rings are all finite.
4. The zero ring $R = \{0\}$ has $0 + 0 = 0$ and $0 \times 0 = 0$.

Definition 6.3 (Identity Elements) An element of a ring R is called an identity if it is an identity for the ring multiplication: $ia = ai$ for all $a \in R$.

Exercise An identity if it exist is unique. [See Tutorial 3].

Notation If the ring R has an identity element it is denoted 1_R or simply 1

The rings in in Example 6.2 all have an identity element except $2\mathbb{Z}$.

Note The zero ring has identity element 0 . Conversely if $1 = 0$ then for all $a \in R$, $a = a1 = a0 = 0$. So R is the zero ring.

Definition 6.4 (Inverses) For $a \in R$ a ring with an identity element 1 , an element b is called a left inverse of a if $ba = 1$, and right inverse if $ab = 1$ and a two sided inverse if it is both a left and right inverse.

Lemma 6.5 If an element $a \in R$ a ring with an identity element has a left and a right inverse, they are equal and are a two-sided inverse of a .

Proof Hint: Suppose $ba = 1$, and $ac = 1$ and consider $a(bc)$ and $(ab)c$. \square

Corollary If an element a in a ring R has a two-sided inverse it is unique.

Notation If $a \in R$ has a two-sided inverse it is denoted a^{-1} .

Definition 6.6 (Fields) A commutative ring with an identity such that $1 \neq 0$ in which all nonzero elements have an inverse is called a *field*.

Recall that in a field $ab = 0$ implies $a = 0$ or $b = 0$. This is not the case in arbitrary rings. In \mathbb{Z}_6 , $2 \times 3 = 0$, but $2 \neq 0$ and $3 \neq 0$. Recall also non-zero matrices can multiply to give a zero matrix e.g. in $M_2\mathbb{Z}$,

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Definition 6.7 (Zero Divisors) In a ring R and $a \neq 0$ and $b \neq 0$ in R satisfy $ab = 0$, (a, b) is called a pair of zero divisors.

If the ring is commutative then we can simply refer to a and b as zero divisors.

Definition 6.8 (Integral Domains) A commutative ring with 1 with no zero divisors is called an *integral domain*.

Examples For example every field is an integral domain.

The integers \mathbb{Z} are the proto-typical integral domain.