

(R3) $*$ is distributive w.r.t. $+$.

The identity element for addition is denoted 0 , and the additive inverse of $a \in A$ is denoted by $-a$. More explicitly, the axioms of a ring are the following equations which hold for all $a, b, c \in A$:

$$a + (b + c) = (a + b) + c \quad (\text{associativity of } +) \quad (2.1)$$

$$a + b = b + a \quad (\text{commutativity of } +) \quad (2.2)$$

$$a + 0 = 0 + a = a \quad (\text{zero}) \quad (2.3)$$

$$a + (-a) = (-a) + a = 0 \quad (\text{additive inverse}) \quad (2.4)$$

$$a * (b * c) = (a * b) * c \quad (\text{associativity of } *) \quad (2.5)$$

$$a * 1 = 1 * a = a \quad (\text{identity for } *) \quad (2.6)$$

$$(a + b) * c = (a * c) + (b * c) \quad (\text{distributivity}) \quad (2.7)$$

$$a * (b + c) = (a * b) + (a * c) \quad (\text{distributivity}) \quad (2.8)$$

The ring A is *commutative* if

$$a * b = b * a \quad \text{for all } a, b \in A.$$

From (2.7) and (2.8), we easily obtain

$$a * 0 = 0 * a = 0 \quad (2.9)$$

$$a * (-b) = (-a) * b = -(a * b). \quad (2.10)$$

Note that (2.9) implies that if $1 = 0$, then $a = 0$ for all $a \in A$, and thus, $A = \{0\}$. The ring $A = \{0\}$ is called the *trivial ring*. A ring for which $1 \neq 0$ is called *nontrivial*. The multiplication $a * b$ of two elements $a, b \in A$ is often denoted by ab .

Example 2.6.

1. The additive groups $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, are commutative rings.
2. For any positive integer $n \in \mathbb{N}$, the group $\mathbb{Z}/n\mathbb{Z}$ is a group under addition. We can also define a multiplication operation by

$$\bar{a} \cdot \bar{b} = \overline{ab} = \overline{ab \bmod n},$$

for all $a, b \in \mathbb{Z}$. The reader will easily check that the ring axioms are satisfied, with $\bar{0}$ as zero and $\bar{1}$ as multiplicative unit. The resulting ring is denoted by $\mathbb{Z}/n\mathbb{Z}$.²

3. The group $\mathbb{R}[X]$ of polynomials in one variable with real coefficients is a ring under multiplication of polynomials. It is a commutative ring.

²The notation \mathbb{Z}_n is sometimes used instead of $\mathbb{Z}/n\mathbb{Z}$ but it clashes with the notation for the *n-adic integers* so we prefer not to use it.