Basic definitions concerning rings.

Definition: A nonempty set R is said to be a ***ring*** if there are two binary operations on R, denoted by $+$ and $\cdot$, which satisfy the following requirements:

(a) If $a, b \in R$, then $a + b \in R$.

(b) For all $a, b \in R$, $\quad a + b \;=\; b + a$.

(c) For all $a, b, c \in R$, $\quad (a + b) + c \;=\; a + (b + c)$.

(d) There exists an element $0 \in R$ such that $a + 0 = a$ for all $a \in R$.

(e) For any $a \in R$, there exists an element $b \in R$ such that $a + b = 0$.

(f) If $a, b \in R$, then $a \cdot b \in R$.

(g) For all $a, b, c \in R$, $\quad (a \cdot b) \cdot c \;=\; a \cdot (b \cdot c)$.

(h) For all $a, b, c \in R$, $\quad a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.

Standard notation and terminology.

We will sometimes refer to 0 as the *additive identity element of* R. If $a \in R$, then the element b satisfying $a + b = 0$ is denoted by $-a$. We refer to $-a$ as the *additive inverse of* a. If $a, b \in R$, then $a + (-b)$ is denoted by $a - b$.

Requirements (a) - (e) mean that R is an abelian group under the operation $+$. We will refer to R under $+$ (ignoring the operation $\cdot$) as the *underlying additive group of* R.

Additional definitions.

A subset S of a ring R is said to be a ***subring of*** R if S is a ring under the operations $+$ and $\cdot$, restricted to pairs of elements of S.

If R and R' are rings, then we say that R and R' are ***isomorphic*** if there exists a bijective map $\phi : R \to R'$ such that, for all $a, b \in R$, $\quad \phi(a+b) = \phi(a) + \phi(b)$ and $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$.

Suppose that R and R' are rings. A map $\phi : R \to R'$ is said to be a ***ring homomorphism*** if, for all $a, b \in R$, $\quad \phi(a + b) = \phi(a) + \phi(b)$ and $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$.

Suppose that R is a ring. A nonempty subset I of R is said to be an ***ideal of*** $\boldsymbol{R}$ if I satisfies the following two requirements:

(i) If $a, b \in I$, then $a + b \in I$ and $a - b \in I$.

(ii) If $a \in I$ and $r \in R$, then $r \cdot a \in I$ and $a \cdot r \in I$.

Some important types of rings.

Assume that R is a ring.

Rings with identity. If there exists an element $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$, then we say that R is a ***ring with identity***. The element 1, if it exists, is referred to as the *identity element* of R, and will sometimes be denoted by 1_R.

Suppose that R is a ring with identity. An element $a \in R$ is said to be an *invertible element of* R if there exists an element $b \in R$ such that $a \cdot b = 1$ and $b \cdot a = 1$. We refer to b as the *multiplicative inverse* of a. An invertible element of R is also often called a *unit of* R. The set of invertible elements of R is denoted by $R^\times$.

Commutative rings. If $a \cdot b = b \cdot a$ for all $a, b \in R$, then we say that R is a ***commutative ring***.

Rings with or without zero-divisors.. If there exist elements $a, b \in R$ such that $a \neq 0,\ b \neq 0$, but $ab = 0$, then we say that R is a ***ring with zero-divisors***. If no such pair of elements $a, b \in R$ exist, then we say that R is a ***ring without zero-divisors***.

Integral domains. Suppose that R is a commutative ring without zero-divisors, that R has an identity 1_R, and that $1_R \neq 0_R$. We then say that R is an ***integral domain***.

Division rings. Assume that R is a ring with identity 1_R and that $1_R \neq 0_R$. Assume also that, for all $a \in R$ such that $a \neq 0$, there exists an element $b \in R$ such that $a \cdot b = b \cdot a = 1$. We will then say that R is a ***division ring***.

Fields. If R is a commutative division ring, then we say that R is a ***field***.