Rings

Definition

Let R be a non-empty set equipped with two binary operators: addition and multiplication. To say that $\langle R, +, \cdot \rangle$ is a *ring* means:

1). $\langle R, + \rangle$ is an abelian group

2). Multiplication is associative

3). The left and right distributive rules hold: $\forall\, a, b, c \in R$:

$$a(b + c) = ab + ac$$

$$(a + b)c = ac + bc$$

Example

The following are all rings:

1). The trivial ring: $\{0\}$

2). $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

3). $n\mathbb{Z}$

4). $\mathbb{Z}_n$

5). $M_n(R), R$ is a ring

6). A direct product of rings: $\prod_{i \in I} R_i$, with component-wise operators

7). The set F of real-valued functions such that:

  a). $(f + g)(x) = f(x) + g(x)$

  b). $(fg)(x) = f(x)g(x)$

Theorem

Let R be a ring. $\forall\, a, b \in R$:

1). $a0 = 0a = 0$

2). $(-a)b = a(-b) = -(ab)$

3). $(-a)(-b) = ab$

Proof

1). Assume $a \in R$

$a0 = a(0+0) = a0 + a0$
$\therefore a0 = 0$ (cancellation)

$0a = (0+0)a = 0a + 0a$
$\therefore 0a = 0$ (cancellation)

2). Assume $a, b \in R$

$(-a)b + ab = (-a+a)b = 0b = 0$
So $(-a)b$ is an inverse of ab
But inverses are unique
$\therefore (-a)b = -(ab)$

$a(-b) + ab = a(-b+b) = a0 = 0$
So $a(-b)$ is an inverse of ab
But inverses are unique
$\therefore a(-b) = -(ab)$

3). Assume $a, b \in R$

$(-a)(-b) = a[-(-b)] = ab$

Notation

Let R be a ring, $a \in R$, and $n \in \mathbb{Z}$:

$$n \cdot a = \begin{cases} a + a + \cdots + a & n > 0 \\ (-a) + (-a) + \cdots + (-a) & n < 0 \\ 0 & n = 0 \end{cases}$$

This helps distinguish these cases from multiplication between two elements of R.