Rings

Definition: Ring

A *ring* R is a non-empty set equipped with the binary operations of addition $(+)$ and multiplication $(\cdot)$ such that:

1). R is an additive abelian group.

2). Multiplication is associative.

3). The distributive laws hold. $\forall\, r, s, t \in R$:

Left: $r(s+t) = rs + rt$

Right: $(s+t)r = sr + tr$

A ring with *unity* is a ring with multiplicative identity element $1 \in \mathbb{R}$ such that $\forall\, r \in R$:

$$1r = r1 = r$$

We normally assert that $1 \neq 0$ in order to exclude $R = \{0\}$.

A commutative ring is a ring with commutative multiplication.

Example

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

2). $R[x]$ (formal polynomial ring)

3). $R[x, y]$ (algebraically independent, commuting variables)

4). $R[\![x]\!]$ (formal power series ring)

5). $M_n(R)$

6). $\mathbb{Z}/n\mathbb{Z}$

7). $\mathbb{Z} \times \mathbb{Z}$

8). $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ (Gaussian Integers)

9). $\mathbb{Z}[\omega] = \{a + b\frac{-1+\sqrt{3}}{2} \mid a, b \in \mathbb{Z}\}$ (Eisenstein Integers)

Definition: Quaternion Group

The *quaternion group*, denoted by Q_8, is given by:

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

where $i^2 = j^2 = k^2 = ijk = (-1)$

Note that $ij = k$ and $ji = -k$, so Q_8 is not commutative.

Definition: Hamilton Ring of Quaternions

The *Hamilton Ring of Quaternions*, denoted by $\mathbb{H}$, is given by:

$$\mathbb{H} = \{a + ib + cj + dk \mid a, b, c, d \in \mathbb{R}\}$$

Note that $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$.

Theorem

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

$$0r = r0 = 0$$

Proof

$0r = (0 + 0)r = 0r + 0r$
$0r = 0r + 0$
$0r + 0r = 0r + 0$

$\therefore 0r = 0$

$r0 = r(0 + 0) = r0 + r0$
$r0 = r0 + 0$
$r0 + r0 = r0 + 0$

$\therefore r0 = 0$

Definition: Subring

To say that S is a *subring* of a ring R, denoted $S \leq R$, means that $S \subseteq R$ and S is also a ring using the same operations as R.

Theorem: Subring Test

Let R be a ring and S a non-empty subset of R. $S \leq R \iff \forall\, x, y \in S$:

1). $x + (-y) \in S$

2). $xy \in S$

Proof

Assume $x, y \in S$

$\implies$ Assume $S \leq R$

S is a ring, so $-y \in S$
By additive closure: $x + (-y) \in S$
By multiplicative closure: $xy \in S$

$\Longleftarrow$ Assume that the two closure conditions hold

Since $x + (-y) \in S$, by the subgroup test, S is an additive subgroup of R. Moreover, S inherits additive commutativity from R, so S is an additive abelian subgroup of R.

Since $xy \in S$, S is closed under multiplication. Moreover, S inherits multiplicative associativity and the distributive laws from R.

$\therefore S \leq R$