MTHSC 412 Section 5.1 – Rings

Kevin James

Definition

A set R together with two binary operations $+$ and $*$ is a *ring* if

1. $(R, +)$ is an abelian group.
2. R is closed under $*$ and $*$ is associative.
3. The following distributive laws hold for all $x, y, z \in R$.
   1. x(y+z) = xy + xz.
   2. (x+y)z = xz + yz.

Note

Some authors also include the requirement that there be an identity with respect to $*$. We will call such a ring a ring with unity.

Example

1. $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$ and $\mathbb{C}$ are all rings.
2. $M_n(\mathbb{R})$ is a ring.
3. In fact if R is a ring then $M_n(R)$ is a ring.

Definition

Suppose that $S \subseteq R$ where $(R, +, *)$ is a ring. If $(S, +, *)$ is also a ring then we say that S is a subring of R.

Theorem

Suppose that $(R, +, *)$ is a ring and that $S \subseteq R$. Then S is a subring of R if the following conditions hold.

1. $S \neq \emptyset$.
2. *For all* $x, y \in S$, $(x + y), xy \in S$.
3. *For all* $x \in S$, $-x \in S$.

Theorem

Suppose that $(R, +, *)$ is a ring and that $S \subseteq R$. Then S is a subring of R if the following conditions hold.

1. $S \neq \emptyset$.
2. *For all* $x, y \in S$, $(x - y), xy \in S$.

Example

1. $R = \{a + b\sqrt{2} \mid a, b \in \mathbb{R}\}$ is a subring of $\mathbb{R}$.
2. $\mathbb{Z}_n$ is a finite ring.
3. Let U be a nonempty set. Then $\mathcal{P}(U)$ is a ring with operations $A + B = (A \cup B) - (A \cap B)$ and $AB = A \cap B$.

Definition

Let R be a ring. If there exists an element $e \in R$ such that $x * e = e * x = x$ for all $x \in R$, then we cal e a *unity or multiplicative identity* and say that R is a *ring with unity*. If $*$ is commutative then we say that R is a *commutative ring*.

Example

1. $\mathbb{Z}$ is a commutative ring with unity.
2. $E = \{2k \mid k \in \mathbb{Z}\}$ is a commutative ring without unity.
3. $M_n(\mathbb{R})$ is a non-commutative ring with unity.
4. $M_n(E)$ is a non-commutative ring without unity.

Theorem

If R is a ring with unity then the unity is unique.

Definition

Let R be a ring with unity e and let $a \in R$. If there exists $x \in R$ such that $ax = xa = e$ then x is a *multiplicative inverse* of a and a is called a *unit* or an *invertible element* in R.

Theorem

Suppose that R is a ring with a unity e. If $a \in R$ has a multiplicative inverse then that inverse is unique and will be denoted a^{-1}.

Other facts that we know about rings because of their group structure under $+$ are:

1. The zero element in R is unique.
2. For each $x \in R$ there is a unique $-x$.
3. For each $x \in R$, $-(-x) = x$.
4. For any $x, y \in R$, $-(x + y) = -y - x$.
5. For $a, x, y \in R$, $a + x = a + y \Rightarrow x = y$.

Theorem

If R is a ring and $a \in R$ then $a \cdot 0 = 0 \cdot a = 0$.

Definition

Let R be a ring and let $a \in R$. If $a \neq 0$ and if there is $0 \neq b \in R$ such that $ab = 0$ or $ba = 0$ then a is called a *zero divisor*.

Example

5 is a zero divisor in $\mathbb{Z}_{10}$ because $2 * 5 = 0$ in $\mathbb{Z}_{10}$.

Theorem

Suppose $x, y, z \in R$ then the following are true.

1. $(-x)y = -(xy) = x(-y)$.
2. $(-x)(-y) = xy$.
3. $x(y - z) = xy - xz$.
4. $(x - y)z = xz - yz$.