# MTH 339



## Introduction to Rings

**Def** Ring

A ring is a set with two binary operations, addition (denoted by $a+b$) and multiplication (denoted by $ab$), such that for all $a, b, c$ in $R$:

1. $a+b = b+a$
2. $(a+b)+c = a+(b+c)$
3. There is an additive identity $0$, meaning $a+0=a$ for all $a \in R$.
4. There is an element $-a$ in $R$ such that $a+(-a)=0$.
5. $a(bc) = (ab)c$
6. $a(b+c) = ab+ac$ and $(b+c)a = ba+ca$.

( $R$ is an Abelian group under addition, also having an associative multiplication that is left and righ distributive over addition).

Note: Multiplication is not necessarily commutative.

When multiplication is commutative, we say the ring is <u>commutative</u>.

A ring does not need to have an identity under multiplication. If it does, we call such an element <u>unity</u> or <u>identity</u>.

If $R$ is a commutative ring with unity, an element does not need to have a multiplicative inverse.

If an element $a$ does have $a^{-1}$, we call $a$ a <u>unit</u>.

<u>Example:</u>

1. $\mathbb{Z}$ under addition and multiplication is a commutative ring with unity 1. The units of $\mathbb{Z}$ are $-1$ and $1$.

2. $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ under addition and multiplication modulo $n$ is a commutative ring with unity 1. The sets of units is $U(n)$.

3. The set $\mathbb{Z}[x]$ of all polynomials in the variable $x$ with integer coefficients under ordinary addition and multiplication is a commutative ring with unity $f(x) = 1$

**Example:** The set $2\mathbb{Z}$ of even integers under ordinary addition and multiplication is a commutative ring without unity.

**Properties of Rings:**

Let $a, b$, and $c$ belong to a ring $R$. Then

1. $a0 = 0a = 0$
2. $a(-b) = (-a)b = -(ab)$
3. $(-a)(-b) = ab$
4. $a(b-c) = ab - ac$ and $(b-c)a = ba - ca$

Furthermore, if $R$ has a unity element $1$, then

5. $(-1)a = -a$
6. $(-1)(-1) = 1$

**Proof:** 1. : $0 + a0 = a0 = a(0+0) = a0 + a0$

$\Rightarrow$ $0 = a0$ by cancellation

2. : $a(-b) + ab = a(-b+b) = a0 = 0$

$\Rightarrow$ $a(-b) = -ab$.

(3.-6. are exercises) ($\rightarrow$ Do now!)

Clearly, if $R$ has a unity, it is unique and if $a \in R$ is a unit, then its inverse is unique as well.

Remark: Usually, a ring is not a group under multiplication. In particular, it might not have a unity and cancellation might not hold.

Subring: A subset $S$ of $R$ is a subring of $R$ if $S$ itself is a ring with the operations of $R$.

Subring test. A nonempty subset $S$ of $R$ is a subring if $S$ is closed under subtraction and multiplication – that is, if $a-b$ and $ab$ are in $S$ whenever $a$ and $b$ are in $S$.

Proof: Follows from one-step subgroup test.

Example: $\{0, 2, 4\}$ is a subring of $\mathbb{Z}_6$.

Note: $1$ is the unity in $\mathbb{Z}_6$, but $4$ is the unity in $\{0, 2, 4\}$

Example: $\mathbb{Z}[i] = \{ a + bi \mid a, b \in \mathbb{Z} \}$

is a subring of the complex numbers $\mathbb{C}$.

Example: The set of all diagonal matrices of the form

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \;\middle|\; a, b \in \mathbb{Z} \right\}$$

is a subring of the ring of all $2 \times 2$ matrices over $\mathbb{Z}$.

$\boxed{\text{MTH 339 - Do now}}$

1./ Complete proofs for 3.-6. in the theorem of the properties of rings.

2./ Which of the following subsets of $\mathbb{Z}[x]$ are subrings?

a. All elements of $\mathbb{Z}[x]$ that have all coefficients even.

b. $\{ f(x) \in \mathbb{Z}[x] \mid f'(0) = 0 \}$ where $f'(x)$ is the derivative of $f$.

c. All elements of $\mathbb{Z}[x]$ whose coefficient of $x^2$ is 0.

3./ Consider the ring $\mathbb{Z}_p$. Show:

a. $a^2 = a$ implies $a = 0$ or $a = 1$

b. $ab = 0$ implies $a = 0$ or $b = 0$

c. $ab = ac$ and $a \neq 0$ imply $b = c$

# MTH 339 - HW

1./ Show that a ring that is cyclic under addition is commutative.

2./ Let $R$ be a commutative ring with unity and let $\mathcal{U}(R)$ denote the set of units of $R$. Prove that $\mathcal{U}(R)$ is a group under multiplication.

3./ Determine $\mathcal{U}(\mathbb{Z}[x])$ and $\mathcal{U}(\mathbb{R}[x])$.

4./ Suppose $R$ is a ring such that $x^4 = x$ for all $x$ in $R$. Prove that $2x = 0$ for all $x$ in $R$.

5./ Find an integer $n > 1$ such that $a^n = a$ for all $a$ in $\mathbb{Z}_6$. Do the same for $\mathbb{Z}_{10}$. Show that no such $n$ exists for $\mathbb{Z}_m$ when $m$ is divisible by the square of some prime.