

Rings

A ring is a non-empty set endowed with two binary operations (usually called addition and multiplication) and governed by a number of properties that control these operations. We will discuss these properties in three separate categories.

A) Addition Properties

Addition in a ring will be denoted either " $+$ " or " \oplus ". The elements in the ring must constitute an abelian group with respect to the addition operator. Hence, addition must be well defined and closed on the elements of the ring. There must be an identity element with respect to addition. We will call this element the "0" of the ring. Every element x must have an additive inverse. We will call this element " $-x$ ". Finally, addition must be associative and commutative. Hence, with respect to addition, all of our theorems concerning groups can be used.

B) Multiplication Properties

The multiplication operation in a ring will be denoted " \cdot ", " \odot " or by juxtaposition. Multiplication must be closed on the ring, well defined and associative. It need not be commutative. The set with its multiplication operator need not form a group. If there does exist a multiplicative identity, we call it the "unity of the ring" which we will symbolize "1.". If the ring possesses unity, an element x need not have a multiplicative inverse. If it does, we will denote this element " x^{-1} ". An element x that possesses a multiplicative inverse is called a unit. The two vocabulary terms, unity and unit, are often confused. For additional emphasis, let's review:

- a) The unity of a ring (if it has one) is the multiplicative identity which is denoted "1". Recall from the chapter on binary operations that a binary operation can have at most one identity.
- b) A unit of a ring with unity is an element that possesses a multiplicative inverse.

Properties Linking Multiplication and Addition

Within the set, multiplication must be left hand and right hand distributive over addition.

LHD For all x, y and z in the set:

$$x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$$

RHD For all x, y and z in the set:

$$(y \oplus z) \odot x = (y \odot x) \oplus (z \odot x)$$

At first glance, it does not seem necessary to state both properties. It would seem that **RHD** is a direct consequence of **LHD**. Remember that while addition must be commutative, multiplication does not need to be commutative. If multiplication is commutative, we call the ring a "commutative ring" and **RHD** is then a direct consequence of **LHD**. These two properties represent the first time we have axiomatically linked two different binary operations. This gives these properties added significance and shortly we will have a practice exercise to explore the difficulty of establishing them.

Some examples of rings:

- 1) The set of even integers under real number multiplication and addition form a commutative ring without unity.
- 2) The set of all 2×2 matrices form a non-commutative ring with unity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. The 0 of this ring is $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.
- 3) The integers (*mod n*) for any $n > 1$ (with 0 included in the set) form a commutative ring with unity. We will call this ring Z_n just as we did in the chapter concerning groups. However, you must remember that we are including 0 and both multiplication and addition when we view Z_n as a ring.

4) The complex number system (all numbers of the form $a + bi$ where a and b are real) forms a commutative ring with unity under the normal definition of complex number addition and multiplication. The 0 of this ring is $0 + 0i$ and the unity is $1 + 0i$.

5) The Generalized Quaternions are the set of all symbols of the form $a + bi + cj + dk$ where a, b, c and d are real numbers. Addition is defined component-wise. For example: $(2 + 3i + 4j + 5k) + (7 + 2i - j - 3k) = 9 + 5i + 3j + 2k$. Multiplication is performed using distribution and the defining equations of Q_8 . For example:

$$\begin{aligned} & (3 + 2i + 3j + 5k) \cdot (2 - 5i + 7j + 2k) \\ &= 3(2 - 5i + 7j + 2k) + 2i(2 - 5i + 7j + 2k) + 3j(2 - 5i + 7j + 2k) + \\ & \quad 5k(2 - 5i + 7j + 2k) \\ &= (6 - 15i + 21j + 6k) + (4i + 10 + 14k - 4j) + (6j + 15k - 21 + 6i) + \\ & \quad (10k - 25j - 35i - 10) \\ &= -15 - 40i - 2j + 45k \end{aligned}$$

This system forms a non-commutative ring with unity. The 0 of the ring is $0 + 0i + 0j + 0k$. the unity is $1 + 0i + 0j + 0k$.

We will see other examples of rings later. Let's try an exercise demonstrating our new distributive properties.

Let R be the set of all integers. Let \oplus be defined by: $a \oplus b = a + b + 1$ (e.g. $2 + 4 = 7$). Let \odot be defined by: $a \odot b = a + b + ab$ (e.g. $2 \odot 4 = 14$). Is \odot left hand distributive over \oplus ? We must show: $x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$

$$\begin{aligned} \text{Consider first: } & x \odot (y \oplus z) \\ &= x \odot (y + z + 1) \\ &= (x + y + z + 1) + (xy + xz + x) \\ &= 2x + y + z + xy + xz + 1 \\ \text{Now let's consider: } & (x \odot y) \oplus (x \odot z) \\ &= (x + y + xy) \oplus (x + z + xz) \\ &= (x + y + xy) + (x + z + xz) + 1 \\ &= 2x + y + z + xy + xz + 1 \end{aligned}$$

This matches the result for $x \odot (y \oplus z)$. $\therefore \odot$ is left hand distributive over \oplus . Since \odot is commutative, \odot is also right hand distributive over \oplus .

In the definition of a ring, all we know about 0 is that it is the additive identity. It has no defined special properties with respect to multiplication.

Theorem: For any ring R , $x \cdot 0 = 0$ for all x in R .

Proof: Consider $x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$ by LHD

However, $x \cdot (0 + 0) = x \cdot 0$ since 0 is the additive identity.

$$\therefore x \cdot 0 + x \cdot 0 = x \cdot 0$$

$$\Rightarrow x \cdot 0 + x \cdot 0 = x \cdot 0 + 0 \text{ (because 0 is the additive identity)}$$

Since R with addition forms a group, we can use LHC on addends.

$$\therefore x \cdot 0 = 0$$

QED

The fact that $0 \cdot x = 0$ for every x in R can be proven in much the same way.

For any ring R , we can define a third binary operation called subtraction. If x and y are in R , we define $x - y$ to mean $x + (-y)$. Recall that $-y$ is the symbol we use in rings for the additive opposite of y .

Theorem: In any ring R , $x(-y) = -xy$ for any x and y in R .

Proof: Consider $xy + x(-y)$

$$= x(y + (-y))$$

LHD

$$= x \cdot 0$$

Definition of an additive inverse

$$= 0$$

Previous Theorem

$$\therefore xy + x(-y) = 0$$

However, $xy + (-xy) = 0$ by the definition of an additive inverse

$$\therefore xy + x(-y) = xy + (-xy)$$

By LHC on the addition operator:

$$x(-y) = -xy$$

QED

It is a simple matter to prove that $(-x)y$ is also $-xy$ using the same ideas as were used in the previous proof.

Theorem: In any ring R , $(-x) \cdot (-y) = xy$ for any x and y in R .

Proof: Consider $(-x)y + (-x)(-y)$

$$= (-x)(y + (-y))$$

LHD

$$= (-x) \cdot 0$$

Definition of an additive inverse

$$= 0$$

Previous Theorem

However $(-x)y = -xy$ by previous theorem

$$\therefore (-x)y + xy = 0$$

$$\therefore (-x)y + (-x)(-y) = (-x)y + xy$$

$$\therefore (-x)(-y) = xy \text{ by } \span style="border: 1px solid black; padding: 2px;">LHC$$

QED

The next concept that we want to introduce concerning rings in general may seem quite alien to you after your experience with high school algebra. Let's solve a type of problem that you've encountered frequently.

Problem: In the real number system, solve $x^2 - x - 12 = 0$

Solution:

$$x^2 - x - 12 = 0$$

$$(x - 4)(x + 3) = 0$$

$$\text{Either } x - 4 = 0 \text{ or } x + 3 = 0$$

$$\text{Either } x = 4 \text{ or } x = -3$$

One of the key steps in this solution hinges on the following property of the reals: If $a \cdot b = 0$ then either $a = 0$ or $b = 0$. In general, rings don't always possess this property.

Definition: An element $a \neq 0$ in a ring R is called a left zero divisor if and only if there exists an element $b \neq 0$ in R such that $a \cdot b = 0$.

The definition of a right zero divisor is similar. If an element of a ring is either a left zero divisor or a right zero divisor, we simply refer to it as a zero divisor.

Example 1 Since $\begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ in the ring of 2×2 matrices, both $\begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 3 & 4 \end{pmatrix}$ are zero divisors in this ring.

Example 2 In Z_6 , $2 \cdot 3 = 0$. Therefore both 2 and 3 are zero divisors in Z_6 .

Theorem: If an element $a \neq 0$ is a unit in a ring R with unity, then a can not be a zero divisor.

Proof: Suppose not. Suppose a is a left zero divisor. Then there exists an element $b \neq 0$ in R such that $a \cdot b = 0$. Since a is a unit, a^{-1} exists. Consider: $a \cdot b = 0$

$$\Rightarrow a^{-1}(a \cdot b) = a^{-1} \cdot 0$$

$$\Rightarrow a^{-1}(a \cdot b) = 0$$

$$\Rightarrow (a^{-1} \cdot a)b = 0$$

$$\Rightarrow 1 \cdot b = 0$$

$$\Rightarrow b = 0$$

$$\longrightarrow \longleftarrow$$

The proof for right zero divisors is similar.

QED

Note that in one of our examples it is no accident that $\begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 3 & 4 \end{pmatrix}$ are nonsingular. Similarly, 2 and 3 do not have multiplicative inverses in Z_6 .

Definition: A ring R is said to possess the left hand multiplicative cancellation property if and only if whenever $a \cdot b = a \cdot c$ and $a \neq 0$ then $b = c$. A ring R is said to possess the right hand multiplicative cancellation property if and only if whenever $b \cdot a = c \cdot a$ and $a \neq 0$ then $b = c$.

Theorem: A ring does not possess zero divisors if and only if both right hand and left hand multiplicative cancellation laws are possessed by the ring.

Proof: First, let's suppose that the ring has no zero divisors and prove that left hand multiplicative cancellation holds.

$$\text{Suppose } ab = ac \text{ where } a \neq 0$$

$$\Rightarrow ab - ac = 0$$

$$\begin{aligned} &\Rightarrow a(b - c) = 0 \\ &\Rightarrow \text{either } a = 0 \text{ or } b - c = 0 \\ &\text{Since } a \neq 0, b - c = 0 \\ &\therefore b = c \end{aligned}$$

Right hand multiplicative cancellation can be established in the same manner.

Next, let's suppose both right and left hand multiplicative cancellation laws hold in R . Let $a \neq 0$ be an element of R . Suppose a is a left zero divisor. Therefore, there exists $b \neq 0$ such that $a \cdot b = 0$.

$$\begin{aligned} &\therefore a \cdot b = a \cdot 0 \\ &\Rightarrow b = 0 \\ &\longrightarrow \longleftarrow \end{aligned}$$

The fact that there are no right hand zero divisors can be established similarly.

QED

Let's focus on the rings Z_n . From them we will extract a brand new family of groups!

Theorem: An element a in Z_n is a divisor of 0 if and only if a and n are not relatively prime.

Proof: Suppose a and n are relatively prime. Suppose b is an element of Z_n and $a \cdot b = 0$. This implies that $a \cdot b$ is a multiple of n . Therefore, n divides $a \cdot b$. Since a and n are relatively prime, n must divide b . $\therefore b = 0$. Therefore, a is not a divisor of 0.

Conversely, suppose a and n are not relatively prime. Let g be the greatest common divisor of a and n . Note that g must be larger than 1 and $g \in Z_n$. $\left(\frac{a}{g}\right)n$ is a multiple of n and $\frac{a}{g}$ is an element of Z_n .

$$\therefore \frac{a}{g}n = 0.$$

However, $\left(\frac{a}{g}\right) \cdot n = a \cdot \left(\frac{n}{g}\right)$

$$\therefore a \cdot \frac{n}{g} = 0$$

Since $\frac{n}{g}$ is also an element of Z_n , a is a divisor of 0.

QED

We define U_n to be the set of all non-zero elements of Z_n that are not zero divisors. In other words, U_n is the set of elements in Z_n that have the property that each is relatively prime to n .

Theorem: U_n forms a group under modular multiplication.

Proof: We already know that multiplication is well defined and associative. We know that 1 is an element of U_n by the very definition of U_n . We must show that U_n is closed under multiplication and that each element in U_n has a multiplicative inverse that is in U_n .

Closure

Let a and b be elements of U_n . Suppose $a \cdot b$ is not an element of U_n . Therefore, there exists $c \neq 0$ in U_n such that $(ab) \cdot c = 0$.

$$\Rightarrow a \cdot (b \cdot c) = 0$$

Since a is not a zero divisor, we conclude that $bc = 0$. Since b is not a zero divisor, we conclude that $c = 0 \longrightarrow \longleftarrow$

$$\therefore a \cdot b \text{ is an element of } U_n.$$

Existence of a Multiplicative Inverse in U_n

Let $a \in U_n$. If $a = 1$ then a is self-invertible. Suppose $a \neq 1$. Let the elements of U_n be $\{a_1, a_2, a_3, \dots, a_t\}$. Note that one of these elements must be 1 and that there are precisely t elements in U_n . Consider the set of products: $\{aa_1, aa_2, aa_3, \dots, aa_t\}$ Are they distinct?

$$\text{Suppose } aa_i = aa_j$$

$$\Rightarrow aa_i - aa_j = 0$$

$$\Rightarrow a(a_i - a_j) = 0$$

$$\text{Since } a \text{ is not a zero divisor, } a_i - a_j = 0$$

$$\Rightarrow a_i = a_j$$

$$\therefore \text{ these products are distinct.}$$

There are t different answers. By closure from the first half of this proof, each of these t elements are in U_n .

$$\therefore \text{ one of these products has to be 1.}$$

$$\therefore a \cdot a_k = 1 \text{ for some } k.$$

$$\therefore \text{ the inverse of } a \text{ is } a_k \text{ which is also an element of } U_n.$$

QED

It's interesting to construct an actual example and identify it.

U_{15} is the set $\{1, 2, 4, 7, 8, 11, 13, 14\}$. These are precisely the elements of Z_{15} that are relatively prime to 15. U_{15} has to be an 8 element group under modular multiplication. By the Fundamental Theorem of Abelian Groups, U_{15} has to be an isomorphic copy of $Z_8, Z_2 \times Z_4$ or $Z_2 \times Z_2 \times Z_2$.

Let's construct a table for U_{15} :

U_{15}	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

Z_8 only has 2 self-invertible elements. U_{15} has 4 self-invertible elements. $\therefore U_{15} \not\cong Z_8$.
 $Z_2 \times Z_2 \times Z_2$ has the property that all elements are self-invertible. $Z_2 \times Z_2 \times Z_2$ is isomorphic to K_8 . $\therefore U_{15} \not\cong Z_2 \times Z_2 \times Z_2$.

$\therefore U_{15}$ is an isomorphic copy of $Z_2 \times Z_4$. We have discovered an elegant and easy way to construct a model of $Z_2 \times Z_4$.

1. Let R be a ring. Prove that $a^2 - b^2 = (a + b)(a - b)$ for every a and b in R if and only if R is a commutative ring.
2. Construct U_{12} . What group is this group isomorphic to?
3. A Boolean Ring is a ring which has the property that $x^2 = x$ for every x in the ring. Prove that in a Boolean Ring $x = -x$ for every x .
4. Prove that every Boolean Ring is a commutative ring.
5. An element x of a ring is said to be idempotent if $x^2 = x$ and nilpotent if $x^n = 0$ for some integer n . Prove that a non-zero idempotent element can not be nilpotent.
6. Prove that every non-zero nilpotent element is a zero divisor.
7. Prove that $\begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}$ is a nilpotent element in the ring of 2×2 matrices.
8. Find a non-zero idempotent element other than $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ in the ring of 2×2 matrices.
9. Prove that the only ring R where $a + b = a \cdot b$ for every a and b in R is the trivial ring $R = \{0\}$.