1 Properties of Rings

We begin by talking about a few important properties.

1.1 Basic Rules of Multiplication

Theorem 1.1

For all $a \in R$, we have:

$$a0 = 0a = 0$$

Proof. We know that:

$$0a = (0 + 0)a = 0a + 0a$$

Subtracting both sides by $0a$ gives:

$$0 = 0a + (0a - 0a) \implies 0 = 0a$$

By symmetry, we can do the same for $0a$. Therefore, we are done. □

Theorem 1.2

For all $a, b \in R$, we have:

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

Proof. First, we have:

$$a(-b) + ab = a(-b + b) = a0 = 0$$

Now, if we add $-(ab)$ to both sides, we have:

$$a(-b) + ab + -(ab) = -(ab) \implies a(-b) = -(ab)$$

By symmetry, $(-a)b = -(ab)$ as well. □

Theorem 1.3

For all $a, b \in R$, we have:

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

Proof.

$$\begin{aligned}
(-a)0 &= 0 \\
&\iff (-a)(b + (-b)) = 0 \\
&\iff (-a)b + -a(-b) = 0 \\
&\iff -(ab) + -a(-b) = 0 \\
&\iff ab + -(ab) + -a(-b) = ab \\
&\iff -a(-b) = ab
\end{aligned}$$

So, we are done. □

Theorem 1.4

For all $a, b, c \in R$, we have:

$$a(b - c) = ab - ac \text{ and } (b - c)a = ba - ca$$

Proof.
$$\begin{aligned} a(b-c) &= ab + -(ac) \\ &= ab + (-a)c \\ &= ab - ac \end{aligned}$$
By symmetry, we can apply the other side as well. So, we are done. □

1.2 Rules of Multiplication with Unity Element

Theorem 1.5

For all $a \in R$ where R has a unity element 1, we have:
$$(-1)a = -a$$

Proof. Applying the theorem that we proved:
$$(-1)a = -(1a) = -a$$
So, we are done. □

Alternatively:

Proof. Since $(\mathbb{R}, +)$ is an abelian group, it suffices to prove that $(-1)a + a = 0$.
$$(-1)a + a = (-1)a + 1a = (-1+1)a = 0a = 0$$
So, we are done. □

Theorem 1.6

$$(-1)(-1) = 1$$

Proof. Applying the theorem that we proved:
$$(-1)(-1) = 1(1) = 1$$
So, we are done. □

1.3 Uniqueness of Unity and Inverses

Theorem 1.7

If a ring has a unity, it is unique. If a ring element has a multiplicative inverse, it is also unique.

Proof. We will prove both parts individually. Suppose R is a ring.

1. Suppose e and e' are unity elements in a ring R. Then, we know that:
    - $e = ee'$ since e' is a unity.
    - $e' = ee'$ since e is a unity.

Therefore:

$$e = ee' = e'$$

Which means that the unity must be unique.

2. Suppose $a \in R$ and further suppose that x and y are both multiplicative inverses of a. Then:

$$x = x1 = x(ay) = (xa)y = 1y = y$$

Therefore, $x = y$ and the two inverses are equal.

Therefore, we are done. $\square$

Important Note 1.1

Rings are not groups under multiplication. $R - \{0\}$ is not a group under multiplication. Rings may not have multiplicative cancellations.

To show that this is the case, consider the question: Which elements $a \in R$ satisfy $a^2 = a$?

- If R has unity, then $a = 1$.
- $a = 0$ is always a solution.

Now, consider $\mathbb{Z}/6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\}$. Then, $a^2 = a$ for $a = 0, 1, 3, 4$. The only units in this ring are 1 and 5.

2 Subring

Recall that, with groups, we have objects called *subgroups*. The same thing applies here: with rings, we have objects called *subrings*.

Definition 2.1: Subring

A nonempty subset S of a ring R is a **subring** of R if S itself is a ring with the operations of R.

2.1 Examples of Subrings

Below are some examples of subrings.

2.1.1 Example 1: Simple Subrings

The trivial subring $\{0\}$ is a subring of any ring R. This is because:

$$0(0) \in R \qquad 0 - 0 \in R$$

Any ring R is a subring of itself. This is because for any $a, b \in R$, we know that $a - b = a + (-b) \in R$ and $ab \in R$.

2.1.2 Example 2: Integers

For any positive integer n, the set below is a subring of the integers $\mathbb{Z}$:

$$n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \dots\}$$

Take any $a, b \in \mathbb{Z}$. Then, suppose we have an and bn. We know that:

$$an - bn = (a - b)n \in \mathbb{Z}$$

$$an(bn) = anbn$$

Since $anb \in \mathbb{Z}$, it follows that $(anb)n \in n\mathbb{Z}$.

2.1.3 Example 3: Rational Numbers

The ring $\mathbb{Q}$ is a subring of $\mathbb{R}$.

2.1.4 Example 4: Gaussian Integers

Consider the Gaussian integers:

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

This is a subring of $\mathbb{C}$. Note that $i^2 = -1$ so:

$$(a + bi)(c + di) = ac + adi + bci + bdi^2 = ac + adi + bci - bd = (ac - bd) + (ad + bc)i$$

2.1.5 Example 5: Integers with Square Root 2

Consider the following set:

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

This is a subring of $\mathbb{R}$. This is because:

$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd$$

Note that we can apply the same work used in the previous example.

2.1.6 Example 7: Diagonal Matrices

The set of diagonal matrices is a subring of $M_2(\mathbb{Z})$.

$$\left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \mid a, d \in \mathbb{Z} \right\}$$

2.2 Subring Test

Theorem 2.1: Subring Test

A nonempty subset S of a ring R is a subring if S is closed under subtraction and multiplication; that is, if $a - b \in S$ and $ab \in S$ whenever $a, b \in S$.

Proof. If S is a subring, then it is a ring and so S must be closed under subtraction and multiplication.

Suppose S is closed under subtraction and multiplication. Then, we know the following properties (inherited from R):

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

We need to check if S has 0. Since S is not empty, pick some $a \in S$. Then, it follows that:

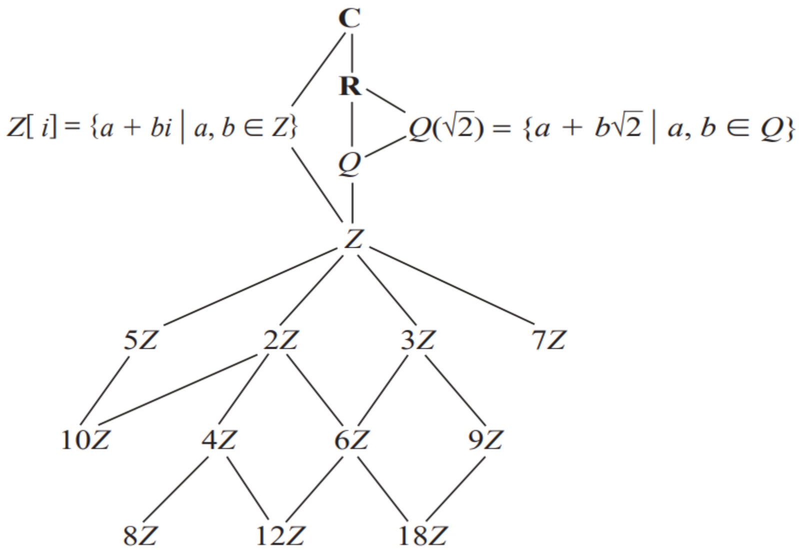
$$a - a = 0 \in S$$

So, the additive identity exists. Now, if $a \in S$, then $-a = 0 - a \in S$, so additive inverses exist.

Finally, we need to show that addition is closed. We know that subtraction is closed, so if $a, b \in S$, then $-b \in S$ and $a + b = a - (-b) \in S$. □

2.3 Subring Lattice

If we are dealing with a lot of subrings, we can use a *subring lattice* to better show the relationship between these rings. An example of a subring lattice is:



We used some of the examples discussed above.