Definition 12.1 (Ring). *A ring R is a set with two binary operations: addition (denote by $a+b$) and multiplication (denote by ab), such that for any a b $c \in R$:*

1. $a + b = b + a$
2. $(a + b) + c = a + (b + c)$
3. *An identity of addinition* 0*, that is,* $a + 0 = a$.
4. *An inverse of* a*, denote by* $-a$*, such that* $a + (-a) = 0$
5. $(ab)c = a(bc)$
6. $a(b + c) = ab + ac$ *and* $(a + b)c = ac + bc$

We can observe that ring is a group under addition and some rules about multiplication (i.e. multiplication is associative and is left/right distributive over addition).

We use $n \cdot a$ to indicate the "sum" of n a rather than na, since na is used by multiplication.

From the definition, we can get some faimilar properties.

Theorem 12.1. *Let a b $c \in R$ where R is ring, then*

1. $a0 = 0a = 0$
2. $a(-b) = (-a)b = -(ab)$
3. $(-a)(-b) = ab$
4. $a(b - c) = ab - ac$ *and* $(a - b)c = ac - bc$
5. *If R has a unity element* 1*, then* $(-1)a = -a$
6. *If R has a unity element* 1*, then* $(-1)(-1) = 1$

Proof. Newline please!

1. Let $b \in R$, $a(b+0) = ab+a0$ and $a(b+0) = a(b)$. Therefore $ab+a0 = ab$, then $a0 = 0$, same for $0a$.
2. $a(b + (-b)) = ab + a(-b)$ and $a(b + (-b)) = a0 = 0$. Therefore $0 = ab + a(-b)$, then $a(-b) = -(ab)$, same for $(-a)b$.

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

4. $a(b-c) = a(b+(-c)) = ab + a(-c) = ab + -(ac) = ab - ac$, same for $(a-b)c$.

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

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

□

Theorem 12.2. *If a ring has a unity, then it is unique. If a ring element has a multiplicative inverse, then it is unique.*

Proof. Suppose 1 and m are the unity of some ring, then $1m = 1$ and $1m = m$, since they are unity.

For any ring element r, and a b are the inverse of r, then $(ar)b = b$ and $a(rb) = a$, therefore $a = b$. □

Definition 12.2 (Subring). *A subset $S \subseteq R$ is a subring of R if $(S, +, \times)$ is a ring.*

Lemma 12.1 (Subring Test). *A non-empty set $S \subseteq R$ is a subgring of R if:*

- *For any a $b \in S$, $a - b \in S$.*
- *For any a $b \in S$, $ab \in S$.*