# 3 Ideals and Factor Rings

**Definition 3.1** A subring $A$ of a ring is called a (two-sided) *ideal* of $R$ if for every $r \in R$ and every $a \in A$ both $ra$ and $ar$ are in $A$. $R$ and $\{0\}$ are always ideals. $\{0\}$ is called a *trivial ideal*. When an ideal $A \neq R$, $A$ is called a *proper ideal*.

**Proposition 3.1** *A nonempty subset $A$ of a ring $R$ is an ideal of $R$ if*

(i) $a - b \in A$ *whenever* $a, b \in A$.

(ii) $ra$ *and* $ar$ *are in* $A$ *whenever* $a \in A$ *and* $r \in R$.

**Example 3.1** 1. For $n \in \boldsymbol{N}$, $n\boldsymbol{Z}$ is an ideal of $\boldsymbol{Z}$.

2. Let $R$ be a commutative ring with unity[9]. The set $\langle a \rangle = \{ra \mid r \in R\}$ is an ideal of $R$ called the *principal ideal generated by* $a$.

3. Let $R$ be a commutative ring with unity and $a_1, a_2, \ldots, a_n \in R$. Then

$$I = \langle a_1, a_2, \ldots, a_n \rangle = \{r_1 a_1 + r_2 a_2 + \cdots + r_n a_n \mid r_i \in R\}$$

is an ideal of $R$ called the *ideal generated by* $a_1, a_2, \ldots, a_n$. (Exercise 3)

4. Let $R = \boldsymbol{Z}[x]$. Consider $\langle x \rangle$, $\langle f \rangle$, $\langle x, 2 \rangle$.

**Theorem 3.2** *Let $R$ be a ring and let $A$ be a subring of $R$. The set of cosets $\{r + A \mid r \in R\}$ is a ring under the operations: $(s+A)+(t+A) = s+t+A$ and $(s+A)(t+A) = st+A$ if and only if $A$ is an ideal of $R$.*

*Proof.* Recall that $A$ is a subgroup of an Abelian group (with respect to addition) $R$, $A$ is a normal subgroup of $R$ and for $x, y \in R$, $x + A = y + A$ if and only if $x - y \in A$.

Since $A$ is a subring, it is an additive subgroup and $R/A$ is an Abelian group as all subgroups of an Abelian group is normal. Suppose $s + A = s' + A$ and $t + A = t' + A$. Then there exist $a \in A$ and $b \in A$ such that $s = s' + a$, $t = t' + b$. Thus

$$st = (s' + a)(t' + b) = s't' + s'b + at' + ab.$$

Thus if $A$ is an ideal, the right hand side is in $s't' + A$. If there is an element $a' \in R$ such that $s'b \notin A$ for some $b \in A$. Then by setting $a = 0$, $st - s't' \notin A$ and the product is not well-defined. ∎

When $A$ is an ideal of a ring $R$, the ring defined above is called the *factor ring* and denoted by $R/A$. Clearly $A = 0 + A$ is the zero element in $R/A$. When $R$ has a unity 1, then $R/A$ has a unity if $A$ is a proper ideal and $1 + A$ is the unity in $R/A$. Note that by definition, unity is a nonzero element.

Note that

$$(s + A)(r + A) = \{xy \mid x \in s + A, y \in r + A\} \neq sr + A, \text{ even if}$$

$$(s + A) + (r + A) = \{x + y \mid x \in s + A, y \in r + A\} = s + r + A.$$

[9] If $R$ does not have unity, $Ra$ is not the smallest ideal containing $a$, which is called the ideal generated by $a$.

**Definition 3.2** A *prime ideal* $A$ of a commutative ring $R$ is a proper ideal of that $a, b \in R$ and $ab \in A$ imply $a \in A$ or $b \in A$. A *maximal* ideal of a commutative ring $R$ is a proper ideal of $R$ such that, whenever $A$ is an ideal of $R$ and $A \subseteq B \subseteq R$, then $B = A$ or $B = R$.

**Theorem 3.3** *Let $R$ be a commutative ring with unity and let $A$ be an ideal of $R$. Then*

(i) *$R/A$ is an integral domain if and only if $A$ is prime.*

(ii) *$R/A$ is a field if and only if $A$ is maximal.*

*In particular, if $A$ is maximal, $A$ is prime.*

*Proof.* Since unity is a nonzero element, if $R/A$ is an integral domain or a field, $R \neq A$ and $A$ is a proper ideal. So to prove this theorem, we may assume from the beginning that $A$ is a proper ideal.

(i) Suppose $A$ is a prime ideal. For $a, b \in R$, by definition $(a + A)(b + A) = ab + A$. So $(a + A)(b + A) = A(= 0_{R/A})$ if and only if $ab \in A$. Since $A$ is prime, $a \in A$ or $b \in A$ and $a + A = A$ or $b + A = A$. Conversely, supper $R/A$ is an integral domain. Suppose $ab \in A$ for some $a, b \in R$. Then $(a + A)(b + A) = ab + A = A = 0_{R/A}$. Hence this implies $a + A = A$ or $b + A = A$. Thus $a \in A$ or $b \in A$ and $A$ is a prime ideal.

(ii) Suppose $R/A$ is a field and $B$ is an ideal such that $A \subset B \subset R$. Assume $A \neq B$ and show $B = R$. Since $A \neq B$, there exists $b \in B \setminus A$. Then $b + A \neq A = 0_{R/A}$, there exists $c + A \in R/A$ such that $(b + A)(c + A) = bc + A = 1 + A = 1_{R/A}$. Therefore, $1 - bc \in A \subset B$ and $R = R1 \subset B \subset R$. Therefore $B = R$. Conversely, assume $A$ is maximal. We will show that every nonzero element in $R/A$ has its multiplicative inverse. Let $b + A \neq A = 0_{R/A}$. Then $b \notin A$ and $\langle b \rangle + A = R$ as $A$ is a maximal ideal and $b \notin A$. Hence there exists $r \in R$ such that $rb + a = 1$. Therefore, $(r + A)(b + A) = rb + A = 1 + A$ and $R/A$ is a field. ■

**Example 3.2** In $R = \boldsymbol{Z}[x]$. $A = \langle x \rangle$ is a prime ideal but not maximal as $\langle 2, x \rangle$ is an ideal properly containing $A$. See Exercise 37. What about $\langle 2 \rangle$? Note that $A = \{f(x) \in \boldsymbol{Z}[x] \mid f(0) = 0\}$, and there is a one-to-one correspondence between $\boldsymbol{Z}[x]/\langle x \rangle$ and $\boldsymbol{Z}$. $\boldsymbol{Z}[x]/\langle 2, x \rangle$ and $\boldsymbol{Z}_2$ which is a field. These are discussed in the next section.