14 Chapter

Definition 14.1. *Ideal*
A subring A of a ring R 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.

Theorem 14.1. *Ideal Test*
A nonempty subset A of a ring R is an ideal of R if

1. *$a - b \in A$ whenever $a, b \in A$.*

2. *ra and ar are in A whenever $a \in A$ and $r \in R$.*

EXAMPLE 1 For any ring R, $\{0\}$ and R are ideals of R. The ideal $\{0\}$ is called the *trivial* ideal.
EXAMPLE 2 For any positive integer n, the set $nZ = \{0, \pm n, \pm 2n, \dots\}$ is an ideal of $\mathbb{Z}$.
EXAMPLE 3 Let R be a commutative ring with unity and let $a \in R$. The set $\langle a \rangle = \{ra \mid r \in R\}$ is an ideal of R called the principal ideal generated by a. (Notice that $\langle a \rangle$ is also the notation we used for the cyclic subgroup generated by a. However, the intended meaning will always be clear from the context.) The assumption that R is commutative is necessary in this example.
EXAMPLE 4 Let $\mathbb{R}[x]$ denote the set of all polynomials with real coefficients and let A denote the subset of all polynomials with constant term 0. Then A is an ideal of $\mathbb{R}[x]$ and $A = \langle x \rangle$.
EXAMPLE 5 Let R be a commutative ring with unity and let $a_1, a_2, \dots, a_n$ belong to R. Then $I = \langle a_1, a_2, \dots, a_n \rangle = \{r_1a_1 + r_2a_2 + \cdots + r_na_n | r_i \in R\}$ is an ideal of R called the ideal generated by $a_1, a_2, \dots, a_n$. The verification that I is an ideal is left as an easy exercise.
EXAMPLE 6 Let $\mathbb{Z}[x]$ denote the ring of all polynomials with integer coefficients and let I be the subset of $\mathbb{Z}[x]$ of all polynomials with even constant terms. Then I is an ideal of $\mathbb{Z}[x]$ and $I = \langle x, 2 \rangle$ (see Exercise 39).
EXAMPLE 7 Let R be the ring of all real valued functions of a real variable. The subset S of all differentiable functions is a subring of R but not an ideal of R.

Theorem 14.2. *Existence of Factor Rings 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.*

Definition 14.2. *Prime Ideal, Maximal Ideal A prime ideal A of a commutative ring R is a proper ideal of R such 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 B is an ideal of R and $A \subseteq B \subseteq R$,then $B = A$ or $B = R$.*

EXAMPLE 13 Let n be an integer greater than 1. Then, in the ring of integers, the ideal $\langle n \rangle$ is prime if and only if n is prime (Exercise 9). (0 is also a prime ideal of $\mathbb{Z}$.)
EXAMPLE 14 The lattice of ideals of $\mathbb{Z}_{36}$ (Figure 14.1) shows that only $\langle 2 \rangle$ and $\langle 3 \rangle$ are maximal ideals.
EXAMPLE 15 The ideal $\langle x^2 + 1 \rangle$ is maximal in $\mathbb{R}[x]$. To see this, assume that A is an ideal of $\mathbb{R}[x]$ that properly contains $\langle x^2 + 1 \rangle$. We will prove that $A = \mathbb{R}[x]$ by showing that A contains some nonzero real number c. [This is the constant polynomial $h(x) = c$ for all x.] Then $1 = (1/c)\ c \in A$ and therefore, by Exercise 15, $A = \mathbb{R}[x]$. To this end, let $f(x) \in A$, but $f(x) \in \langle x^2 + 1 \rangle$. Then
$f(x) = q(x)(x^2 + 1) + r(x)$,
Where $r(x) \neq 0$ and the degree of $r(x)$ is less than 2. It follows that $r(x) = ax + b$, where a and b are not both 0, and

$$ax + b = r(x) = f(x) - q(x)(x^2 + 1) \in A.$$

EXAMPLE 16 The ideal $\langle x^2 + 1 \rangle$ is not prime in $\mathbb{Z}_2[x]$, since it contains $(x + 1)^2 = x^2 + 2x + 1 = x^2 + 1$ but does not contain $x + 1$.

Theorem 14.3. *R/A Is an Integral Domain If and Only If A Is Prime*
Let R be a commutative ring with unity and let A be an ideal of R. Then R/A is an integral domain if and only if A is prime.

Theorem 14.4. *R/A Is a Field If and Only if A is Maximal*
Let R be a commutative ring with unity and let A be an ideal of R. Then R/A is a field if and only if A is maximal.

EXAMPLE 17 The ideal $\langle x \rangle$ is a prime ideal in $\mathbb{Z}[x]$ but not a maximal ideal in $\mathbb{Z}[x]$. To verify this, we begin with the observation that $(x) = \{f(x) \in \mathbb{Z}[x] \mid f(0) = 0\}$ (see Exercise 31). Thus, if $g(x)h(x) \in \langle x \rangle$, then $g(0)h(0) = 0$. And since $g(0)$ and $h(0)$ are integers, we have $g(0) = 0$ or $h(0) = 0$.
To see that $\langle x \rangle$ is not maximal, we simply note that $\langle x \rangle \subseteq \langle x, 2 \rangle \subseteq \mathbb{Z}[x]$ (see Exercise 39).