## 30.4 Ideals, PID's, and Greatest Common Divisors

First, we introduce the fundamental concept of an ideal.

**Definition 30.4.** Given a ring $A$, an *ideal of* $A$ is any nonempty subset $\mathfrak{I}$ of $A$ satisfying the following two properties:

(ID1) If $a, b \in \mathfrak{I}$, then $b - a \in \mathfrak{I}$.

(ID2) If $a \in \mathfrak{I}$, then $ax \in \mathfrak{I}$ for every $x \in A$.

An ideal $\mathfrak{I}$ is a *principal ideal* if there is some $a \in \mathfrak{I}$, called a *generator*, such that

$$\mathfrak{I} = \{ax \mid x \in A\}.$$

The equality $\mathfrak{I} = \{ax \mid x \in A\}$ is also written as $\mathfrak{I} = aA$ or as $\mathfrak{I} = (a)$. The ideal $\mathfrak{I} = (0) = \{0\}$ is called the *null ideal* (or *zero ideal*).

An ideal $\mathfrak{I}$ is a *maximal ideal* if $\mathfrak{I} \neq A$ and for every ideal $\mathfrak{J} \neq A$, if $\mathfrak{I} \subseteq \mathfrak{J}$, then $\mathfrak{J} = \mathfrak{I}$. An ideal $\mathfrak{I}$ is a *prime ideal* if $\mathfrak{I} \neq A$ and if $ab \in \mathfrak{I}$, then $a \in \mathfrak{I}$ or $b \in \mathfrak{I}$, for all $a, b \in A$. Equivalently, $\mathfrak{I}$ is a prime ideal if $\mathfrak{I} \neq A$ and if $a, b \in A - \mathfrak{I}$, then $ab \in A - \mathfrak{I}$, for all $a, b \in A$. In other words, $A - \mathfrak{I}$ is closed under multiplication and $1 \in A - \mathfrak{I}$.

Note that if $\mathfrak{I}$ is an ideal, then $\mathfrak{I} = A$ iff $1 \in \mathfrak{I}$. Since by definition, an ideal $\mathfrak{I}$ is nonempty, there is some $a \in \mathfrak{I}$, and by (ID1) we get $0 = a - a \in \mathfrak{I}$. Then, for every $a \in \mathfrak{I}$, since $0 \in \mathfrak{I}$, by (ID1) we get $-a \in \mathfrak{I}$. Thus, an ideal is an additive subgroup of $A$. Because of (ID2), an ideal is also a subring.

Observe that if $A$ is a field, then $A$ only has two ideals, namely, the trivial ideal $(0)$ and $A$ itself. Indeed, if $\mathfrak{I} \neq (0)$, because every nonnull element has an inverse, then $1 \in \mathfrak{I}$, and thus, $\mathfrak{I} = A$.

**Definition 30.5.** Given a ring $A$, for any two elements $a, b \in A$ we say that $b$ *is a multiple of* $a$ *and that* $a$ *divides* $b$ if $b = ac$ for some $c \in A$; this is usually denoted by $a \mid b$.

Note that the principal ideal $(a)$ is the set of all multiples of $a$, and that $a$ divides $b$ iff $b$ is a multiple of $a$ iff $b \in (a)$ iff $(b) \subseteq (a)$.

Note that every $a \in A$ divides 0. However, it is customary to say that $a$ is a *zero divisor* iff $ac = 0$ for some $c \neq 0$. With this convention, 0 is a zero divisor unless $A = \{0\}$ (the trivial ring), and $A$ is an integral domain iff 0 is the only zero divisor in $A$.

Given $a, b \in A$ with $a, b \neq 0$, if $(a) = (b)$ then there exist $c, d \in A$ such that $a = bc$ and $b = ad$. From this, we get $a = adc$ and $b = bcd$, that is, $a(1 - dc) = 0$ and $b(1 - cd) = 0$. If $A$ is an integral domain, we get $dc = 1$ and $cd = 1$, that is, $c$ is invertible with inverse $d$. Thus, when $A$ is an integral domain, we have $b = ad$, with $d$ invertible. The converse is obvious, if $b = ad$ with $d$ invertible, then $(a) = (b)$.

It is worth recording this fact as the following proposition.