The following simple proposition gives a sufficient condition for an element $a \in A$ to be irreducible.

Proposition 32.1. *Let A be an integral domain. For any $a \in A$ with $a \neq 0$, if the principal ideal (a) is a prime ideal, then a is irreducible.*

Proof. If (a) is prime, then $(a) \neq A$ and a is not a unit. Assume that $a = bc$. Then, $bc \in (a)$, and since (a) is prime, either $b \in (a)$ or $c \in (a)$. Consider the case where $b \in (a)$, the other case being similar. Then, $b = ax$ for some $x \in A$. As a consequence,

$$a = bc = axc,$$

and since A is an integral domain and $a \neq 0$, we get

$$1 = xc,$$

which proves that $c = x^{-1}$ is a unit. $\square$

It should be noted that the converse of Proposition 32.1 is generally false. However, it holds for factorial rings, defined next.

Definition 32.2. A *factorial ring* or *unique factorization domain (UFD)* (or *unique factorization ring*) is an integral domain A such that the following two properties hold:

(1) For every nonnull $a \in A$, if $a \notin A^*$ (a is not a unit), then a can be factored as a product

$$a = a_1 \cdots a_m$$

where each $a_i \in A$ is irreducible ($m \geq 1$).

(2) For every nonnull $a \in A$, if $a \notin A^*$ (a is not a unit) and if

$$a = a_1 \cdots a_m = b_1 \cdots b_n$$

where $a_i \in A$ and $b_j \in A$ are irreducible, then $m = n$ and there is a permutation σ of $\{1, \ldots, m\}$ and some units $u_1, \ldots, u_m \in A^*$ such that $a_i = u_i b_{\sigma(i)}$ for all i, $1 \leq i \leq m$.

Example 32.1. The ring $\mathbb{Z}$ of integers if a typical example of a UFD. Given a field K, the polynomial ring $K[X]$ is a UFD. More generally, we will show later that every PID is a UFD (see Theorem 32.12). Thus, in particular, $\mathbb{Z}[X]$ is a UFD. However, we leave as an exercise to prove that the ideal $(2X, X^2)$ generated by $2X$ and X^2 is not principal, and thus, $\mathbb{Z}[X]$ is not a PID.

First, we prove that condition (2) in Definition 32.2 is equivalent to the usual "Euclidean" condition.