3.2 Principal Ideal Domains

Definition 3.2.1 *A* principal ideal domain *(PID) is an integral domain in which every ideal is principal.*

Lemma 3.2.2 *$\mathbb{Z}$ is a PID.*

NOTE: Showing that $\mathbb{Z}$ is a PID means showing that if I is an ideal of $\mathbb{Z}$, then there is some integer n for which I consists of all the integer multiples of n.

Proof: Suppose that $I \subseteq \mathbb{Z}$ is an ideal. If $I = \{0\}$ then I is the principal ideal generated by 0 and I is principal. If $I \neq \{0\}$ then I contains both positive and negative elements. Let m be the least positive element of I. We will show that $I = \langle m \rangle$.
Certainly $\langle m \rangle \subseteq I$ as I must contain all integer mulitples of m. On the other hand suppose $a \in I$. Then we can write

$$a = mq + r$$

where $q \in \mathbb{Z}$ and $0 \leqslant r < m$. Then $r = a - qm$. Since $a \in I$ and $-qm \in I$, this means $r \in I$. It follows that $r = 0$, otherwise we have a contradiction to the choice of m. Thus $a = qm$ and $a \in \langle m \rangle$. We conclude $I = \langle m \rangle$. □

Note: In fact every subring of $\mathbb{Z}$ is an ideal - think about this.

Lemma 3.2.3 *Let F be a field. Then the polynomial ring $F[x]$ is a PID.*

NOTE: Recall that $F[x]$ has one important property in common with $\mathbb{Z}$, namely a division algorithm. This is the key to showing that $F[x]$ is a PID.
Proof: Let $I \subseteq F[x]$ be an ideal. If $I = \{0\}$ then $I = \langle 0 \rangle$ and I is principal. If $I \neq \{0\}$, let $f(x)$ be a polynomial of minimal degree m in I. Then $\langle f(x) \rangle \subseteq I$ since every polynomial multiple of $f(x)$ is in I.
We will show that $I = \langle f(x) \rangle$. To see this suppose $g(x) \in I$. Then

$$g(x) = f(x)q(x) + r(x)$$

where $q(x), r(x) \in F[x]$ and $r(x) = 0$ or $\deg(r(x)) < m$. Now

$$r(x) = g(x) - f(x)q(x)$$

and so $r(x) \in I$. It follows that $r(x) = 0$ otherwise $r(x)$ is a polynomial in I of degree strictly less than m, contrary to the choice of $f(x)$.
Thus $g(x) = f(x)q(x)$, $g(x) \in \langle f(x) \rangle$ and $I = \langle f(x) \rangle$. □

QUESTION FOR THE SEMINAR: If R is a ring (not a field) it is not always true that $R[x]$ is a PID.
Find an example of a non-principal ideal in $\mathbb{Z}[x]$.