3.2 Lecture 11: Principal Ideal Domains

Definition 38. *A* principal ideal domain *(PID) is an integral domain in which every ideal is principal.*

Lemma 39. *$\mathbb{Z}$ 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 $I = \langle m \rangle$. □

Lemma 40. *Let $\mathbb{F}$ be a field. Then the polynomial ring $\mathbb{F}[X]$ is a PID.*

NOTE: Recall that $\mathbb{F}[X]$ has one important property in common with $\mathbb{Z}$, namely a division algorithm. This is the key to showing that $\mathbb{F}[X]$ is a PID.
Proof: Let $I \subseteq \mathbb{F}[X]$ 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 $I = \langle f(X) \rangle$. □

Note Not every integral domain is a PID. For example $\mathbb{Z}[X]$ is not. Let I be the ideal of $\mathbb{Z}[X]$ consisting of all elements whose constant term is a multiple of 3 (check that this is an ideal). The I includes both 3 and $X + 3$. If $I = \langle \alpha \rangle$ for some $\alpha \in \mathbb{Z}[X]$, then $\alpha \in \mathbb{Z}$ since 3 is a multiple of α in $\mathbb{Z}[X]$. The possibilities are ± 3 and ± 1. If $\alpha = 3$ or -3, then $X + 3$ is not a multiple of α in $\mathbb{Z}[X]$. If $\alpha = 1$ or -1, then $\langle \alpha \rangle = \mathbb{Z}[X] \neq 1$. It follows that I is not a principal ideal.