4.2 Every PID is a UFD

Recall that an ideal I of a commutative ring with identity R is *principal* if $I = \langle a \rangle$ for some $a \in R$, i.e.

$$I = \{ra : r \in R\}.$$

An integral domain R is a *principal ideal domain* if all the ideals of R are principal. Examples of PIDs include $\mathbb{Z}$ and $F[x]$ for a field F.

Definition 4.2.1 *A commutative ring R satisfies the* ascending chain condition *(ACC) on ideals if there is no infinite sequence of ideals in R in which each term properly contains the previous one. Thus if*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

is a chain of ideals in R, then there is some m for which $I_k = I_m$ for all $k \geq m$.

Note: Commutative rings satisfying the ACC are called *Noetherian*.

To understand what the ACC means it may be helpful to look at an example of a ring in which it does not hold.

Example 4.2.2 *Let $C(\mathbb{R})$ denote the ring of continuous functions from $\mathbb{R}$ to $\mathbb{R}$ with addition and multiplication defined by*

$$(f+g)(x) = f(x) + g(x); \quad (fg)(x) = f(x)g(x), \quad \text{for } f, g \in C(\mathbb{R}), x \in \mathbb{R}.$$

For $n = 1, 2, 3, \dots$, define I_n to be the subset of $C(\mathbb{R})$ consisting of those functions that map every element of the interval $\left[-\frac{1}{n}, \frac{1}{n}\right]$ to 0.

Then I_n is an ideal of $C(\mathbb{R})$ for each n and

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

is an infinite strictly ascending chain of ideals in $C(\mathbb{R})$ (i.e. every term is this chain is strictly contained in the next one). So the ACC is not satisfied in $C(\mathbb{R})$.

Example 4.2.3 *The ACC is satisfied in $\mathbb{Z}$.*

Proof: Let $I_1 \subseteq I_2 \subseteq \dots$ be an ascending chain of ideals in $\mathbb{Z}$. Choose k with $I_k \neq \{0\}$. Then $I_k = \langle n \rangle$ for some positive integer n. Now for an ideal $\langle m \rangle$ of $\mathbb{Z}$ we have $n \in \langle m \rangle$ if and only if $m|n$. Since n has only a finite number of divisors in $\mathbb{Z}$, this means only finitely many different ideals can appear after I_k in the chain.

Theorem 4.2.4 *Let R be a PID. Then the ACC is satisfied in R.*

Proof: Let $I_1 \subseteq I_2 \subseteq \dots$ be an ascending chain of ideals in $\mathbb{R}$. Let $I = \cup_{i=0}^{\infty} I_i$. Then

1. I is closed under addition and multiplication, for suppose a and b are elements of I. Then there are ideals I_j and I_k in the chain with $a \in I_j$ and $b \in I_k$. If $m \geq \max(j, k)$ then both a and b belong to I_m and so do $a + b$ and ab. So $a + b \in I$ and $ab \in I$.

2. $0 \in I$ since $0 \in I_i$ for each i.

3. Suppose $a \in I$. Then $a \in I_j$ for some j, and $-a \in I_j$. So $-a \in I$. Thus I is a subring of R.

4. Furthermore I is an ideal of R. To see this let $a \in I$. Then $a \in I_j$ for some j. If r is any element of R then $ra \in I_j$ and $ra \in I$. So whenever $a \in I$ we have $ra \in I$ for all $r \in R$. Thus I is an ideal of R.

Now since R is a PID we have $I = \langle c \rangle$ for some $c \in \mathbb{R}$. Since $c \in I$ there exists n with $c \in I_n$. Then $I_n = \langle c \rangle$ and $I_r = \langle c \rangle$ for all $r \geq n$. So the chain of ideals stabilizes after a finite number of steps, and the ACC holds in R.

Theorem 4.2.5 *Let R be a PID. Then every element of R that is neither zero nor a unit is the product of a finite number of irreducibles.*

Proof: Let $a \in R,\ a \neq 0,\ a \notin \mathcal{U}(R)$ (i.e. a not a unit).

1. First we show that a has an irreducible factor. If a is irreducible, this is certainly true. If not then we can write $a = a_1 b_1$ where neither a_1 nor b_1 is a unit. Then $a \in \langle a_1 \rangle$, and $\langle a \rangle \subset \langle a_1 \rangle$. This inclusion is strict for $\langle a \rangle = \langle a_1 \rangle$ would imply $a_1 = ac$ and $a = acb_1$ for some $c \in R$. Since R is an integral domain this would imply that b_1 is a unit, contrary to the fact that the above factorization of a is proper.

   If a_1 is not irreducible then we can write $a_1 = a_2 b_2$ for non-units a_2 and b_2 and we obtain
   $$\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle,$$
   where each of the inclusions is strict. If a_2 is not irreducible we can extend the above chain, but since the ACC is satisfied in R the chain must end after a finite number of steps at an ideal $\langle a_r \rangle$ generated by an irreducible element a_r. So a has a_r as an irreducible factor.

2. Now we show that a is the product of a finite number of irreducible elements of R. If a is not irreducible then by the above we can write $a = p_1 c_1$ where p_1 is irreducible and c_1 is not a unit. Thus $\langle a \rangle$ is strictly contained in the ideal $\langle c_1 \rangle$. If c_1 is not irreducible then $c_1 = p_2 c_2$ where p_2 is irreducible and c_2 is not a unit. We can build a strictly ascending chain of ideals :
   $$\langle a \rangle \subset \langle c_1 \rangle \subset \langle c_2 \rangle \ldots$$
   This chain must end after a finite number of steps at an ideal $\langle c_r \rangle$ with c_r irreducible. Then
   $$a = p_1 p_2 \ldots p_r c_r$$
   is an expression for a as the product of a finite number of irreducibles in R.

□

So in order to show that every PID is a UFD, it remains to show uniqueness of factorizations of the above type.

Lemma 4.2.6 *Let I be an ideal of a PID R. Then I is maximal if and only if $I = \langle p \rangle$ for an irreducible element p of R.*

Proof: Suppose I is maximal and write $I = \langle p \rangle$ for some $p \in R$. If p is reducible then $p = ab$ for non-units a and b of R, and $\langle p \rangle \subseteq \langle a \rangle$. Furthermore $\langle p \rangle \neq \langle a \rangle$ since $a \in \langle p \rangle$ would imply $a = pc$ and $p = pcb$ which would mean that b is a unit in R. Also $\langle a \rangle \neq R$ since a is not a unit of R. Thus reducibility of p would contradict the maximality of I.

On the other hand suppose p is irreducible and let I_1 be an ideal of R containing $I = \langle p \rangle$. Then $I_1 = \langle q \rangle$ for some $q \in R$ and $p \in I_1$ means $p = rq$ for some $r \in R$. Then either q is a unit or r is a unit. In the first case $I_1 = R$ and in the second case $q = r^{-1}p$ and $q \in \langle p \rangle$ implies $\langle q \rangle = \langle p \rangle$ and $I_1 = I$. Thus I is a maximal ideal of R. □

Note: The notation $a|b$ (a divides b) in an integral domain R means $b = ac$ for some $c \in R$.

Lemma 4.2.7 *Let R be a PID and let p be an irreducible in R. Then p is a prime in R.*

Proof: Let a and b be elements of R for which $p|ab$. By Lemma 4.2.6 $I = \langle p \rangle$ is a maximal ideal of R. Thus I is a prime ideal of R by Corollary 3.4.5. Now $ab \in I$ implies either $a \in I$ or $b \in I$. Thus either $p|a$ or $p|b$ in R. $\square$.

So in a PID the notions of prime and irreducible coincide.

Theorem 4.2.8 *Every PID is a UFD.*

Proof: Let R be a PID and suppose that a non-zero non-unit element a of R can be written in two different ways as a product of irreducibles. Suppose

$$a = p_1 p_2 \dots p_r \text{ and } a = q_1 q_2 \dots q_s$$

where each p_i and q_j is irreducible in R, and $s \geq r$. Then p_1 divides the product $q_1 \dots q_s$, and so p_1 divides q_j for some j, as p_1 is prime. After reordering the q_j if necessary we can suppose $p_1|q_1$. Then $q_1 = u_1 p_1$ for some unit u_1 of R, since q_1 and p_1 are both irreducible. Thus

$$p_1 p_2 \dots p_r = u_1 p_1 q_2 \dots q_s$$

and

$$p_2 \dots p_r = u_1 q_2 \dots q_s.$$

Continuing this process we reach

$$1 = u_1 u_2 \dots u_r q_{r+1} \dots q_s.$$

Since none of the q_j is a unit, this means $r = s$ and $p_1, p_2, \dots, p_r$ are associates of $q_1, q_2, \dots, q_r$ in some order. Thus R is a unique factorization domain. $\square$

Note: It is not true that every UFD is a PID.
For example $\mathbb{Z}[x]$ is not a PID (e.g. the set of polynomials in $\mathbb{Z}[x]$ whose constant term is even is a non-principal ideal) but $\mathbb{Z}[x]$ *is* a UFD.

To see this note that irreducible elements in $\mathbb{Z}[x]$ are either integers of the form $\pm p$ for a prime p, or primitive irreducible polynomials of degree ≥ 1. (Recall that a polynomial in $\mathbb{Z}[x]$ is primitive if the gcd of its coefficients is 1.) Let $f(x)$ be a non-zero non-unit in $\mathbb{Z}[x]$.

If $f(x) \in \mathbb{Z}$, then $f(x)$ has a unique factorization as a product of primes. If not then $f(x) = dh(x)$, where d is the gcd of the coefficients in $f(x)$ and $h(x) \in \mathbb{Z}[x]$ is primitive. So $h(x)$ is the product of a finite number of primitive irreducible polynomials in $\mathbb{Z}[x]$, and f(x) is the product of a finite number of irreducible elements of $\mathbb{Z}[x]$. Now suppose that

$$f(x) = p_1 \dots p_k f_1(x) \dots f_r(x) = q_1 \dots q_l g_1(x) \dots g_s(x),$$

where $p_1, \dots, p_k, q_1, \dots, q_l$ are irreducibles in $\mathbb{Z}$ and $f_1(x), \dots, f_r(x), g-1(x), \dots, g_s(x)$ are primitive irreducible polynomials in $\mathbb{Z}[x]$. Then $p_1 \dots p_k = \pm$(the gcd of the coefficients in $f(x)$), and $p_1 \dots p_k = \pm q_1 \dots q_l$. Thus $l = k$ and $p_1, \dots, p_k$ are associates in some order of $q_1, \dots, q_k$. Now

$$f_1(x) \dots f_r(x) = \pm g_1(x) \dots g_s(x).$$

Then each $f_i(x)$ and $g_j(x)$ is irreducible not only in $\mathbb{Z}[x]$ but in $\mathbb{Q}[x]$ and since $\mathbb{Q}[x]$ is a UFD this means that $s = r$ and $f_1(x), \dots, f_r(x)$ are associates (in some order) of $g_1(x), \dots, g_r(x)$. After reordering the $g_j(x)$ we can suppose that for $i = 1, \dots, r$ $f_i(x) = u_i(g_i(x)$ where u_i is a non-zero rational number. However since $f_i(x)$ and $g_i(x)$ are both primitive polynomials in $\mathbb{Z}[x]$, we must have $u_i = \pm 1$ for each i, so $f_i(x)$ and $g_i(x)$ are associates not only in $\mathbb{Q}[x]$ but in $\mathbb{Z}[x]$.

Thus $\mathbb{Z}[x]$ is a UFD.