4.4 Lecture 18: Every PID is a UFD

Theorem 60. *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:

   $$\langle a \rangle \subset \langle c_1 \rangle \subset \langle c_2 \rangle \dots$$

   This chain must end after a finite number of steps at an ideal $\langle c_r \rangle$ with c_r irreducible. Then

   $$a = p_1 p_2 \dots p_r c_r$$

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

This was mentioned in Lecture 15.

Proof. Suppose that $p|ab$ for some elements $a, b \in R$. If $p|a$ there is nothing to do, so suppose $p \not| a$. Then $a \notin \langle p \rangle$ and $\langle a, p \rangle = \{sa + tp : s, t \in R\}$ is an ideal of R that strictly contains $\langle p \rangle$. However $\langle p \rangle$ is a maximal ideal of R since p is irreducible and R is a PID. It follows that $1_R \in \langle a, p \rangle$, so $1_R = xa + yp$ for some $x, y \in R$. Then $b = xab + ybp$, and p divides b since p divides ab and p divides ybp. We conclude that p is prime in R. □

Theorem 62. *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 $s \geqslant r$. 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. □

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, let $f(X)$ be a non-zero non-unit element of $\mathbb{Z}[X]$. If $f(X)$ is constant, then it is an integer and factorizes uniquely as a product of irreducibles in $\mathbb{Z}$. Prime integers (and their negatives) are irreducible elements of $\mathbb{Z}[X]$, so a constant element of $\mathbb{Z}[X]$ has a unique factorization in $\mathbb{Z}[X]$ (since it can have no factor of degree higher than 0).

No suppose $f(X)$ is not constant and first suppose that $f(X)$ is primitive (the gcd of its coefficients is 1). By Gauss's Lemma (Lecture 9), $f(X)$ is a product of irreducible polynomials in $\mathbb{Q}[X]$ that belong to $\mathbb{Z}[X]$. All of these factors are primitive in $\mathbb{Z}[X]$ since their product is primitive. This factorization of $f(X)$ is unique in $\mathbb{Q}[X]$, hence also in $\mathbb{Z}[X]$. If $h(X)$ and $g(X)$ are primitive in $\mathbb{Z}[X]$ and associate elements in $\mathbb{Q}[X]$, then $h(X) = \pm g(X)$, so $h(X)$ and $g(X)$ are assoicates in $\mathbb{Z}[X]$ also.

Finally, let $f(X)$ be any non-constant polynomial in $\mathbb{Z}[X]$. The irreducible elements of $\mathbb{Z}[X]$ are $\pm p$ for primes p, and primitive non-constant polynomials in $\mathbb{Z}[X]$ that are irreducible in $\mathbb{Q}[X]$. We can write $f(X) = df_1(X)$, where $d \in \mathbb{Z}$ is the gcd of the coefficients of $f(X)$ and $f_1(X) \in \mathbb{Z}[X]$ is primitive. Any factorization of $f(X)$ as a product of irreducible elements of $\mathbb{Z}[X]$ has factors of degree 0 whose product is $\pm d$, and primitive irreducible factors in $\mathbb{Z}[X]$, whose product is $\pm f_1(X)$. It follows that the factorization is unique, since (non-zero non-unit) integers and primitive non-constant polynomials both factorize uniquely in $\mathbb{Z}[X]$.