Unique Factorization Domains

A *unique factorization domain (UFD)* is an integral domain R such that every $a \neq 0$ in R can be written

$$a = up_1 \dots p_k$$

where u is a unit and p_1, p_2,…,p_k are primes in R.

Note that the factorization is essentially unique (by the same argument used to prove uniqueness of factorization in PIDs).

Note also that if R is a UFD, any finite collection $a_1, \dots, a_n \in R$ has a highest common factor. For we can take out prime factors until we write $a_i = rb_i$ where the $b_1, \dots, b_n$ have no proper factors in common. Then r is the (unique up to units) highest common factor. We write $r = \mathrm{hcf}(a_1, \dots, a_n)$, but note that unless R is a PID we will not in general have $r = \lambda_1 a_1 + \dots + \lambda_n a_n$ for $\lambda_i \in R$.

Observe that if R is an integral domain then R is a UFD iff it satisfies the following condition:

> Every $a \neq 0$ in R can be written as a product $a = up_1 \dots p_k$ where u is a unit and p_i is irreducible for each i. Moreover, this factorization is essentially unique in the sense that if we also have $a = vq_1 \dots q_l$ then $k = l$ and, after renumbering the q_i, we have $p_i \sim q_i$ for all i.

Furthermore, every irreducible in a UFD is prime.

Our aim is to prove that the ring of polynomials over a unique factorization domain is itself a UFD. Along the way, we shall prove Gauss' Lemma that the product of primitive polynomials in a UFD is itself primitive. (Recall that a polynomial over a UFD is said to be *primitive* if the greatest common divisor of its coefficients is 1.) The proof of the main theorem takes R a UFD and considers F its field of fractions. Now, R[X] is a subring of $F[X]$ and $F[X]$ is a PID and so is a UFD. We show that factorization in $R[X]$ is determined by

(i) factorization in $F[X]$; and

(ii) factorization in R.

Lemma 1 (Gauss)**.** *A product of primitive polynomials is primitive.*

Proof. Suppose

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_0$$

and

$$g(X) = b_m X^m + b_{m-1} X^{m-1} + \dots + b_0$$

are primitive. Take p prime and i, j largest such that $p \nmid a_i$ and $p \nmid b_j$. Now c_{i+j}, the $(i+j)$th coefficient of the product fg is

$$c_{i+j} = a_i b_j + (a_{i+1} b_{j-1} + \dots) + (a_{i-1} b_{j+1} + \dots),$$

a sum of $a_i b_j$ and terms divisible by p. As p is prime, $p \nmid a_i b_j$ and so $p \nmid c_{i+j}$. As p was an arbitrary prime, this shows that the product is primitive. $\square$

Lemma 2. *(i)If u is a unit in R then u is a unit in $R[X]$.*

(ii) If p is a prime in R then p is a prime in $R[X]$.

(iii) Suppose $f(X)$ is a primitive polynomial in $R[X]$ which is irreducible and so prime in $F[X]$. Then f is prime in $R[X]$.

Proof. (i) Suppose u is a unit in R. Then there exists $v \in R$ such that $uv = 1$. But then $uv = 1$ in $R[X]$ so u is a unit in $R[X]$.

(ii) The argument is the same as that used to prove Gauss' Lemma. Suppose p is prime in R. To show that p is prime in $R[X]$, it is enough to show that if

$$p \nmid a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0$$

and

$$p \nmid b_m X^m + b_{m-1} X^{m-1} + \ldots + b_0$$

then

$$p \nmid (a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0)(b_m X^m + b_{m-1} X^{m-1} + \ldots + b_0).$$

So suppose

$$p \nmid a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0$$

and

$$p \nmid b_m X^m + b_{m-1} X^{m-1} + \ldots + b_0.$$

Pick i greatest such that $p \nmid a_i$ and j greatest such that $p \nmid b_j$. Then, writing c_k for the coefficient of X^k in the product,

$$p \nmid c_{i+j} = \sum_{r+s=i+j} a_r b_s$$

and so

$$p \nmid c_{n+m} X^{n+m} + c_{n+m-1} X^{n+m-1} + \ldots + c_0.$$

(iii) Suppose $f(X)|g(X)h(X)$ in $R[X]$; then $f|gh$ in $F[X]$ and so $f|g$ or $f|h$ in $F[X]$. Assume wlog $f|g$ in $F[X]$, so we have $g = fk$ with $k \in F[X]$. Write $g = a\tilde{g}$ and $k = \frac{b}{c}\tilde{k}$ where $a, b, c \in R$ and $\tilde{g}, \tilde{k} \in R[X]$ are primitive. Then we have $a\tilde{g} = \frac{b}{c} f\tilde{k}$ or $ac\tilde{g} = bf\tilde{k}$. Now, as f, $\tilde{g}$ and $\tilde{k}$ (and hence $f\tilde{k}$ by Gauss) are primitive, we have $ac \sim b$, i.e. $b = uac$ for some unit u. Then $\tilde{g} = uf\tilde{k}$ and so $g = a\tilde{g} = fua\tilde{k}$ and so $f|g$ in $R[X]$. This show that f is prime in $R[X]$. $\square$

Theorem 3. *If R is a UFD then so is $R[X]$, the ring of polynomials over R.*

Proof. Take a (non-zero) polynomial $f \in R[X]$. We can factorize it into irreducibles=primes in $F[X]$ (as $F[X]$ is a PID and so a UFD), and we may as well take the irreducibles to be primitive polynomials in $R[X]$. So we can write

$$f(X) = \tfrac{r}{s} g_1(X) g_2(X) \ldots g_k(X)$$

where $g_i \in R[X]$ is primitive and irreducible in $F[X]$ (and so prime in $R[X]$). Now $f(X) = a\tilde{f}(X)$ for some $a \in R$ and primitive $\tilde{f} \in R[X]$, and so

$$a\tilde{f} = \tfrac{r}{s} g_1 g_2 \ldots g_k$$

or

$$as\tilde{f} = rg_1g_2\dots g_k$$

so, as $\tilde{f}$, g_1, g_2, ..., g_k are primitive, $as \sim r$ and we can write $r = uas$ where $u \in R$ is a unit. Then

$$f = uag_1g_2\dots g_k.$$

But now we can factorize $a = va_1a_2\dots a_l$ where $v \in R$ is a unit and $a_i \in R$ is prime, and so we have a complete factorization:

$$f = \underbrace{(uv)}_{\text{unit by 2(i)}} \underbrace{a_1a_2\dots a_l}_{\text{primes by 2(ii)}} \underbrace{g_1g_2\dots g_k}_{\text{primes by 2(iii)}}.$$

□