**UNIQUE FACTORIZATION DOMAINS**

BRIAN OSSERMAN

In this note, we prove the following theorem:

**Theorem.** If $R$ is a UFD, then $R[x]$ is also a UFD.

We follow the definitions and arguments in §12.3 (Gauss’s Lemma) of Artin *Algebra*, generalizing from the case $R = \mathbb{Z}$ which is given in the book.

**Definition.** Let $R$ be a UFD, and $f(x) \in R[x]$. We say $f(x)$ is **primitive** if there is no irreducible element $p \in R$ which divides $f(x)$.

Since $R$ has factorization into irreducibles, the definition is equivalent to requiring that no non-unit $x \in R$ divides $f(x)$. Also, recall that since $R$ is a UFD, irreducible is the same as prime for elements of $R$.

The basic tools we will use are reduction modulo $p$, and inclusion into the field of fractions.

The first statement we want is the following:

**Lemma (Gauss).** Let $p \in R$ be irreducible, and suppose for some $f(x), g(x) \in R[x]$, the product $f(x)g(x)$ is a multiple of $p$. Then either $f(x)$ or $g(x)$ is a multiple of $p$.

In particular, the product of primitive polynomials is primitive.

Note that the first statement of the lemma is just saying that $p$, which we already know is prime in $R$, is also prime in $R[x]$.

**Proof.** The second statement follows immediately from the first, if $f(x)$ and $g(x)$ are the primitive polynomials in question.

The proof of the first statement uses reduction modulo $p$. Given $f(x), g(x) \in R[x]$, suppose that $p$ divides $f(x)g(x)$. Now, since $p$ is prime, $R/(p)$ is an integral domain, and them so is $(R/(p))[x]$. We have a natural homomorphism

$$R[x] \to (R/(p))[x]$$

obtained by reducing each coefficient modulo $p$, and it is clear that a polynomial in $R[x]$ is in the kernel of this homomorphism if and only if it is a multiple of $p$. But now we are done: if $\bar{f}(x)$ and $\bar{g}(x)$ are the images of $f(x)$ and $g(x)$, then $\bar{f}(x)\bar{g}(x)$ is the image of $f(x)g(x)$, so by hypothesis, $\bar{f}(x)\bar{g}(x) = 0$. Since $(R/(p))[x]$ is an integral domain, we must have either $\bar{f}(x) = 0$ or $\bar{g}(x) = 0$, which means that one of $f(x)$ or $g(x)$ must be a multiple of $p$, as desired. \[\square\]

Next, let $K$ be the fraction field of $R$. Our next result is the following:

**Lemma.** If $f(x) \in K[x]$ has positive degree, it can be written as $cf_0(x)$, where $c \in K$, and $f_0(x) \in R[x]$ is primitive. Moreover, this is unique up to replacing $c$ by $cu$ and $f_0(x)$ by $u^{-1}f_0(x)$, for $u \in R^\times$.

**Proof.** To check existence, first we can multiply $f(x)$ by the product of the denominators of the coefficients to get a polynomial with coefficients in $R$. We can then factor the coefficients into irreducibles, and remove any common factors to obtain $f_0(x)$. The first step gives the denominator of $c$, while the second step gives the numerator. In this way, we write $f(x) = cf_0(x)$, as desired.

To see uniqueness, suppose also $f(x) = dq_0(x)$, where $d \in K$ and $q_0(x) \in R[x]$ is primitive. Then we have $\frac{c}{d}f_0(x) = g_0(x)$, so we want to show that for any two primitive polynomials $f_0(x), g_0(x)$ in
If $\alpha f_0(x) = g_0(x)$ for some $\alpha \in K$, then we must have $\alpha \in R^\times$. Write $\alpha = \frac{a}{b}$ for $a, b \in R$, and assume that $a, b$ have no common factors. We will prove that for any irreducible $p \in R$, neither $a$ nor $b$ can be a multiple of $p$. Multiplying our equation through by $b$, we have $af_0(x) = bg_0(x)$. If $p$ divides $a$, then $p$ doesn’t divide $b$, since we assume $a, b$ have no common factors. But $p$ divides $bg_0(x)$, so $p$ divides every coefficient of $bg_0(x)$. Since $R$ is a UFD, we conclude that $p$ must divide every coefficient of $g_0(x)$, contradicting that $g_0(x)$ is primitive. Thus, $p$ cannot divide $a$. Similarly $p$ cannot divide $b$, so we conclude that $a$ and $b$, and hence also $\alpha$, are units, as desired. \hfill $\square$

Putting the lemmas together, with some additional work we obtain the desired result.

**Proof of the Theorem.** First, we verify that factorizations into irreducibles exist in $R[x]$. This is more or less clear: certainly, each time we factor out a positive-degree polynomial, the degree goes down, so this can only happen finitely many times. On the other hand, since factorizations into irreducibles exist in $R$, if we first factor out the common irreducible factors of the coefficients of a polynomial, then there are no further constant factors to remove, so the only further factorizations have to involve polynomials of positive degree.

Knowing that factorizations into irreducibles exist, in order to prove that $R[x]$ is a UFD, by the lemma we proved earlier (in the process of showing that every PID is a UFD) we just need to prove that irreducible elements are prime. Thus, let $f(x)$ be an irreducible element of $R[x]$. If $f(x)$ is constant, then it is prime by the first statement of Gauss’ Lemma. If $f(x)$ is nonconstant, then it clearly must be primitive, and we claim that in fact, it must be irreducible in $K[x]$. Suppose we have written $f(x) = g(x)h(x)$ for $g(x), h(x) \in K[x]$ nonconstant. By the previous lemma, we can write $g(x) = cg_0(x)$ and $h(x) = dh_0(x)$ for $c, d \in K$ and $g_0(x), h_0(x) \in R[x]$ primitive. Then $f(x) = cd(g_0(x)h_0(x))$. By Gauss’ Lemma, $g_0(x)h_0(x)$ is primitive, so by the uniqueness in the previous lemma, we conclude that $f(x)$ is a unit times $g_0(x)h_0(x)$, so we get a factorization of $f(x)$ in $R[x]$, contradicting irreducibility.

Now, since $K[x]$ is a PID, we know that $f(x)$ is prime in $K[x]$. It then suffices to prove that if a primitive polynomial $f(x) \in R[x]$ is prime in $K[x]$, then it is prime in $R[x]$. Suppose $f(x)$ divides $g(x)h(x)$ for some $g(x), h(x) \in R[x]$. Then since $f(x)$ is prime in $K[x]$, it must divide either $g(x)$ or $h(x)$ in $K[x]$. Without loss of generality, suppose that it divides $g(x)$, so that $g(x) = f(x)q(x)$ for some $q(x) \in K[x]$. We will prove that $q(x) \in R[x]$, so that $f(x)$ divides $g(x)$ in $R[x]$, and $f(x)$ is prime in $R[x]$, which will complete the proof of the theorem. By the previous lemma, we can write $g(x) = cg_0(x)$, and $q(x) = dq_0(x)$, where $c, d \in K$ and $g_0(x), q_0(x) \in R[x]$ are primitive. Note that since $g(x) \in R[x]$, we must have $c \in R$, as otherwise the primitivity of $g_0(x)$ would create denominators in $g(x)$. Then $cg_0(x) = df(x)q_0(x)$, and $f(x)q_0(x)$ is primitive in $R[x]$ by Gauss’ Lemma, so by the uniqueness in the previous lemma, for some unit $u \in R$ we have $d = cu$. But then $d \in R$, so $q(x) = dq_0(x) \in R[x]$, as desired. \hfill $\square$

Note that the proof of the theorem also gives a description of the irreducible elements of $R[x]$: they consist of constants which are irreducible in $R$, and nonconstant primitive polynomials which are irreducible in $K[x]$.

Applying the theorem inductively, we conclude that

**Corollary.** $\mathbb{Z}[x_1, \ldots, x_n]$ is a UFD, and $F[x_1, \ldots, x_n]$ is a UFD for any field $F$.

**Example.** $\mathbb{Z}[x]$ is not a PID: for instance, the ideal $(2, x)$ (which is the ideal of polynomials with even constant term) is not the set of multiples of any one element. Similarly, if $F$ is a field, $F[x_1, x_2]$ is not a PID: the ideal $(x_1, x_2)$ is not principal. Thus, we now have many examples of UFDs which are not PIDs.