Let k be a field. Our goal is to show that the power series ring $R_m = k[[x_1, ..., x_m]]$ in m variables is a unique factorization domain (UFD). This result resembles the well known fact that a polynomial ring over a field is a UFD. Usually the polynomial case is derived by simple induction from the more general theorem that if A is a UFD then so is the polynomial ring in one variable $A[x]$. Unfortunately, an analogous statement for power series rings is false (i.e. there is a UFD A such that $A[[x]]$ is not a UFD). There is a notion of a regular ring (which extends the notion of a regular local ring) and it is true that if A is a regular UFD then so is $A[[x]]$ (and regular local rings are UFD), but it is not an easy result.

Our proof that R_m is a UFD will prosceed by induction on m. Note that R_m can be naturally identified with $R_{m-1}[[x_m]]$. Assuming that R_{m-1} is a UFD, the polynomial ring $R_{m-1}[x]$ is a UFD and our strategy is to relate the arithmetic of R_m to the one of $R_{m-1}[x]$ and derive that R_m is a UFD.

The following exercises should be a good way of getting acquainted with the power series rings.

Exercise. Show that if A is a ring then a power series $\sum_{k=0}^{\infty} a_k x^k \in A[[x]]$ (one variable) is invertible iff a_0 is invertible in A. Conclude that an element in R_m is invertible iff its constant term is non-zero. Conclude that R_m is a local ring with maximal ideal $M_m =< x_1, ..., x_m >$.

Exercise. Show that if A is a domain then so is $A[[x]]$. Prove that if A is Noetherian then so is $A[[x]]$ (this is an analog of Hilbert's basis theorem for polynomial rings). Hint. For an ideal I of $A[[x]]$ consider the ideals I_k of A consisting of all a such that there is a power series in I which starts with aX^k.

We focus now on the ring R_m which we will often identify with $R_{m-1}[[x_m]]$. We set $M = M_{m-1}$ for the maximal ideal of R_{m-1} and $M^k[[x_m]]$ for elements in R_m whose all coefficients (as power series in x_m) belong to M^k. The key to our proof is the following

Theorem 1. (Weierstrass Division Theorem) *Let k be a field and let $R_m = k[[x_1, ..., x_m]]$. Suppose that $f \in R_m$ is of the form $f = ux_m^s - w$, where $s \geq 0$ is an integer, u is a unit of R_m, and $w \in M[[x_m]]$ is a polynomial in x_m of degree $< s$. For any $g \in R_m$ there are unique $h \in R_m$ and $r \in R_{m-1}[x]$ such that r is a polynomial in x_m of degree $< s$ and $g = hf + r$.*

Proof: Note that any element g in R_m can be uniquely written as $g = A(g)x_m^s + B(g)$ with $A(g) \in R_m$ and $B(g) \in R_{m-1}[x_m]$ a polynomial in x_m of degree $< s$. Clearly both A and B are k-linear functions of g. Define $T : R_m \longrightarrow R_m$ by $T(g) = A(g)u^{-1}f + B(g)$. Clearly T is a k-linear map. We will show that T is an isomorphism (of k-vector spaces) by finding its inverse. The idea is to make sense of the following formal identity:

$$T^{-1} = (I - (I - T))^{-1} = \sum_{i=0}^{\infty} (I - T)^i,$$

where I is the identity. Note that $g - T(g) = A(g)(X_m^s - u^{-1}f) = A(g)u^{-1}w$. If $g \in M^k[[x_m]]$ for some $k \geq 0$ then clearly $A(g) \in M^k[[x_m]]$ and therefore $A(g)u^{-1} \in M^k[[x_m]]$ and $A(g)u^{-1}w \in M^{k+1}[[x_m]]$ (since w has coefficients in M), i.e. $g - T(g) \in M^{k+1}[[x_m]]$. Let $S(g) = g - T(g) = (I - T)(g)$. Thus $S^j(g) \in M^j[[x_m]]$ for any $g \in R_m$ and all j. Note now that for any sequence h_i of elements of R_m such that $h_i \in M^i[[x_m]]$, the sum $\sum_{i=0}^{\infty} h_i$

is a well defined element of R_m (since any monomial in $x_1, ..., x_m$ appears in only a finite number of the h_i's; more precisely, only monomials of degree $\geq i$ can appear in h_i). In particular, for any $g \in R_m$ the sum $\sum_{i=0}^{\infty} S^i(g)$ is a well defined element of R_m and it is now straightforward to verify that $T^{-1} = \sum_{i=0}^{\infty} S^i$. To finish the proof of the theorem note that $g = hf + r$ as claimed in the theorem iff $g = T(hux_m^s + r)$, so the existence and uniqueness follows from the fact that T is an isomorphism. $\square$

Before we make use of the last theorem let us discuss the assumption about f. We say that $f \in R_m$ is **regular of order** s at x_m if f satisfies the assumption of the theorem, i.e. if $f = ux_m^s - w$ for some integer $s \geq 0$, a unit u of R_m and a polynomial $w \in M[[x_m]]$ of degree $< s$. Equivalently, the monomial x_m^s appears in f with non-zero coefficient and $s \geq 0$ is smallest integer with this property (so s, u, w are uniquely determined by f). Another equivalent condition is that $f(0, ..., 0, x_m)$ is a non-zero power series in x_m and x_m^s is the lowest power of x_m appearing in $f(0, ..., 0, x_m)$ with non-zero coefficient. It follows that if f is regular at x_m and $f = gh$ then both g and h are regular at x_m as well. The assumption that f is regular is not very restrictive. If k is an infinite field then any f becomes regular after a linear change of variables. In fact, $f = \sum_{j=0}^{\infty} F_j(x_1, ..., x_m)$, where F_j is a homogeneous polynomial of degree j. Let s be smallest such that $F_s \neq 0$. Since k is infinite, there is $0 \neq a = (a_1, a_2, ..., a_m) \in k^m$ such that $F_s(a_1, ..., a_m) \neq 0$. There is an invertible matrix $B = (b_{i,j})$ such that $B(0, 0, ..., 0, 1) = a$. The map sending x_i to $\sum_{j=1}^{m} b_{i,j} x_j$ defines an automorphism of R_m and the image of f is regular of order s.

Exercise. The above argument does not work for finite fields. Show that the map sending x_i to $x_i + x_m^{n_i}$ for $i < m$ and fixing x_m defines an automorphism of R_m and given f one can choose $n_1, ..., n_{m-1}$ such that f is mapped to a regular element.

In order to formulate our next result we need one more definition. A polynomial in $R_{m-1}[x_m]$ is called a **Weierstrass polynomial of degree** s if it is monic of degree s and all its coefficients (except the leading one) are in M.

Theorem 2. (Weierstrass Preparation Theorem). *Let $f \in R_m$ be regular of order s at x_m. Then there is unique Weierstrass polynomial p of degree s such that $f = vp$ for some v invertible in R_m.*

Proof: This result is a direct consequence of the Weierstrass Division Theorem. Write $p = x_m^s + q$, so q has degree $< s$ and all coefficients in M. The equality $f = vp$ is equivalent to $X^s = v^{-1}f - q$. By Weierstrass Division theorem, $x_m^s = hf + r$ for unique $h \in R_m$ and $r \in R_{m-1}[x_m]$ of degree $< s$. We need to show that h is invertible and $r \in M[x_m]$. Note that

$$x_m^s = h(0, ..., 0, x_m)f(0, ..., 0, x_m) + r(0, ..., 0, x_m) = h(0, ..., 0, x_m)x_m^s u(0, ..0, x_m) + r(0, ..., 0, x_m),$$

(where $f = ux_m^s - w$). It follows that $r(0, ..., 0, x_m) = 0$ and $h(0, ..., 0, x_m)$ has non-zero constant term. In other words, $r = q$ has all its coefficients in M and $h = v^{-1}$ is invertible. $\square$

Corollary 1. *Let $f, g \in R_m$ be Weierstrass polynomials. Suppose that $f = gh$ for some $h \in R_m$. Then h is a Weierstrass polynomial.*

Proof: Since f is regular at x_m, so is h. Thus $h = uq$ for some Weierstrass polynomial q and invertible u. We have $f = ugq$. The uniqueness in Weierstrass Preparation Theorem implies $u = 1$. $\square$

Exercise. Let $f, g \in R_{m-1}[x_m]$ be polynomials. Suppose that g is Weierstrass and $f = gh$ for some $h \in R_m$. Show that h is a polynomial in $R_{m-1}[x_m]$.

Corollary 2. *Let $f \in R_m$ be a Weierstrass polynomial of degree s. Suppose that $f = gh$ for some $g, h \in R_m$. There is an invertible element $u \in R_m$ such that ug, $u^{-1}h$ are Weierstrass polynomials.*

Proof: Note that Weierstrass polynomials are regular at x_m. Thus both g, h are regular at x_m. By the Weierstrass Preparation Theorem, there is an invertible elements u such that ug is a Weierstrass polynomial. Since $f = (ug)(u^{-1}h)$, $u^{-1}h$ is a Weierstrass polynomial by Corollary 1. □

Lemma 1. *A Weierstrass polynomial f of degree $s > 0$ is irreducible in R_m iff it is irreducible in $R_{m-1}[x_m]$. Furthermore, every Weierstrass polynomial is a product of irreducible Weierstrass polynomials.*

Proof: If f is reducible in R_m then it is reducible in $R_{m-1}[x_m]$ by Corollary 2. Suppose that $f = gh$ is reducible in $R_{m-1}[x_m]$. Since f is monic, the leading coefficients of g, h are invertible in R_{m-1} and we may assume that both g, h are monic of degrees i and $s - i$ respectively. Now $x_m^s = f(0, ..., 0, x_m) = g(0, ..., 0, x_m)h(0, ..., 0, x_m)$. Since $g(0, ..., 0, x_m)$, $h(0, ..., 0, x_m)$ are monic polynomials in $k[x_m]$ of degrees i, $s - i$ respectively, we must have $g(0, ..., 0, x_m) = x_m^i$, $h(0, ..., 0, x_m) = x_m^{s-i}$. Thus both g and h are Weierstrass polynomials. In particular, neither g nor h is a unit of R_m. Thus f is not irreducible in R_m. This proves the first part. For the second part note, the we have seen that a Weierstrass polynomial which is not irreducible, factors into a product of Weierstrass polynomials of lower degrees. It follows that if f is factored into largest possible number of Weierstrass polynomials then each factor is irreducible. □

Now we can prove our main result.

Theorem 3. *The ring R_m is a UFD.*

Proof: The proof is by induction on m. For $m = 0$, $R_m = k$ is a field, hence UFD. Suppose that R_{m-1} is UFD. Then so is the polynomial ring $R_{m-1}[x_m]$. In order to show that R_m is a UFD we need to show that each element factors as a product of irreducible elements (this is always true in Noetherian rings, but we are not going to use here the fact that R_m is Noetherian) and each irreducible element is prime.

Let $f \in R_m$ be irreducible and suppose that $f|gh$. As we have seen, there is an automorphism of R_m which takes gh to an element regular at x_m. So we may assume that gh is regular and therefore also f, g, h are regular at x_m. Thus $f = up$, $g = vq$, $h = wr$, where u, v, w are units in R_m and p, q, r are Weierstrass polynomials. Since f is irreducible, p is irreducible in R_m and hence in $R_{m-1}[x_m]$ (Lemma 1). Also, $p|qr$ in R_m so also $p|rq$ in $R_{m-1}[x_m]$ (Corollary 1). But $R_{m-1}[x_m]$ is a UFD and p is irreducible, so $p|r$ or $p|q$. Thus $f|g$ or $f|h$ which shows that f is prime.

If $f \in R_m$ is arbitrary, then as before, we may assume f is regular and $f = up$ with u invertible and p a Weierstrass polynomial. Since p factors as a product of irreducible Weierstrass polynomials and each of them is irreducible in R_m, we get a factorization of f into irreducible elements. □

Exercise. Use the Weierstrass theorems (and Hilbert's basis theorem) to give an inductive proof that R_m are Noetherian rings.