UFDs Have UFD Polynomial Rings

Theorem 1 *R a UFD implies $R[X]$ a UFD.*

Proof First, suppose $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$, for $a_j \in R$. Then define the content of $f(X)$ to be $\mathrm{cont}(f(X)) = \gcd(a_0, \ldots, a_n) = d$ in R. (So $\mathrm{cont}(f(X))$ is well-defined up to a unit factor in R.)

(Existence) If $p \in R$ is irreducible then p is also irreducible in $R[X]$. If $f(X) \in R[X]$, write $f(X) = dF(X)$, where $d = \mathrm{cont}(f(X))$. Then $\mathrm{cont}(F(X)) = 1$. We can certainly factor d into a product of irreducibles in R. Either $F(X)$ is irreducible in $R[X]$ or it factors properly as a product of lower degree polynomials (since $\mathrm{cont}(F(X)) = 1$). All the factors will also have content 1 (since a divisor of any factor would divide F). We can only lower degree of factors finitely often, so we get a factorization of $F(X)$, and hence $f(X)$, as a product of irreducibles in $R[X]$.

(Uniqueness) It suffices to prove each irreducible element of $R[X]$ generates a prime ideal in $R[X]$. If $p \in R$ is irreducible, this is clear, since $R[X]/pR[X] = (R/p)[X]$, which is an integral domain.

Lemma 1 *If* $\mathrm{cont}(F(X)) = \mathrm{cont}(G(X)) = 1$, $F(X), G(X) \in R[X]$, *then* $\mathrm{cont}(F(X)G(X)) = 1$. *More generally, for* $f(X), g(X) \in R[X]$, $\mathrm{cont}(f(X)g(X)) = \mathrm{cont}(f(X))\,\mathrm{cont}(g(X))$.

Proof Suppose irreducible $p \in R$ divides all coefficients of $F(X)G(X)$. Then $F(X)G(X) = 0$ in $(R/p)[X]$, which is an integral domain. Thus p either divides all coefficients of $F(X)$ or p divides all coefficients of $G(X)$, since one of $F(X), G(X)$ must be 0 in $(R/p)[X]$. But this contradicts the assumption $\mathrm{cont}(F) = \mathrm{cont}(G) = 1$.

In the general case, write $f = dF$, $g = d'G$, where $\mathrm{cont}(F) = \mathrm{cont}(G) = 1$. Then $fg = dd'FG$, so, by the first part of the Lemma, $\mathrm{cont}(fg) = dd' = \mathrm{cont}(f)\,\mathrm{cont}(g)$. ∎

Lemma 2 (Gauss) *Let K be the field of fractions of R. If $P(X) \in R[X]$ is irreducible then $P(X)$ is also irreducible in $K[X]$. More generally, if $P(X) \in R[X]$ factors in $K[X]$ then $P(X)$ factors in $R[X]$ with factors of the same degrees as the $K[X]$ factors.*

Proof Every element of $K[X]$ can be written $A(X)/a$, where $A(X) \in R[X]$ and $a \in R$. Suppose in $K[X]$ we have $P(X) = (A(X)/a)(B(X)/b)$, with $a, b \in R$ and $A(X), B(X) \in R[X]$. Then $abP(X) = A(X)B(X) \in R[X]$. Consider an irreducible factor p of ab in R. Then $A(X)B(X) = 0$ in $(R/p)[X]$. Thus p either divides all coefficients of $A(X)$ or p divides all coefficients of $B(X)$. We can then cancel a factor p in the $R[X]$ equation $abP(X) = A(X)B(X)$. By induction on the number of prime factors of ab in R, conclude $P(X) = A'(X)B'(X) \in R[X]$, where $\deg A' = \deg A$ and $\deg B = \deg B'$. ∎

Now we finish the proof of the theorem by showing $(P(X)) \subset R[X]$ is a prime ideal if $P(X)$ is irreducible in $R[X]$. Suppose $P(X)Q(X) = F(X)G(X) \in R[X] \subset K[X]$. Since $K[X]$ is a UFD, the Gauss Lemma implies $P(X)$ divides $F(X)$ or $G(X)$ in $K[X]$. Say in $K[X]$ we have $F(X) = P(X)(S(X)/s)$, with $S(X) \in R[X]$, $s \in R$. Then in $R[X]$ we have $P(X)S(X) = sF(X)$. Then s divides $\mathrm{cont}(P(X)S(X)) = \mathrm{cont}(S(X))$ by the first Lemma. So $S(X)/s$ is in $R[X]$ and $F(X)$ is in the ideal $(P(X)) \subset R[X]$. ∎