Theorem 32.10. *If A is a UFD then the polynomial ring $A[X]$ is also a UFD.*

Proof. As we said earlier, the factorization property (1) is easier to prove than uniqueness. Assume that $f(X)$ has degree m and let f_m be the coefficient of X^m in $f(X)$. Either f_m is a unit or it is the product of $n \geq 1$ irreducible elements. If f_m is a unit we set $n = 0$. We proceed by induction on the pair (m, n), using the well-founded ordering on pairs, i.e.,

$$(m, n) \leq (m', n')$$

iff either $m < m'$, or $m = m'$ and $n < n'$. If $f(X)$ is a nonnull polynomial of degree 0 which is not a unit, then $f(X) \in A$, and $f(X) = f_m = a_1 \cdots a_n$ for some irreducible $a_i \in A$, since A is a UFD. This proves the base case.

If $f(X)$ has degree $m > 0$ and $f(X)$ is reducible, then

$$f(X) = g(X)h(X),$$

where $g(X)$ and $h(X)$ have degree $p, q \leq m$ and are not units. There are two cases.

(1) f_m is a unit (so $n = 0$).

If so, since $f_m = g_p h_q$ (where g_p is the coefficient of X^p in $g(X)$ and h_q is the coefficient of X^q in $h(X)$), then g_p and h_q are both units. We claim that $p, q \geq 1$. Otherwise, $p = 0$ or $q = 0$, but then either $g(X) = g_0$ is a unit or $h(X) = h_0$ is a unit, a contradiction.

Now, since $m = p + q$ and $p, q \geq 1$, we have $p, q < m$ so $(p, 0) < (m, 0)$ and $(q, 0) < (m, 0)$, and by the induction hypothesis, both $g(X)$ and $h(X)$ can be written as products of irreducible factors, thus so can $f(X)$.

(2) f_m is not a unit, say $f_m = a_1 \cdots a_n$ where $a_1, \ldots, a_n$ are irreducible and $n \geq 1$.

(a) If $p, q < m$, then $(p, n_1) < (m, n)$ and $(q, n_2) < (m, n)$ where n_1 is the number of irreducible factors of g_p or $n_1 = 0$ if g_p is irreducible, and similarly n_2 is the number of irreducible factors of h_p or $n_2 = 0$ if h_p is irreducible (note that $n_1, n_2 \leq n$ and it is possible that $n_1 = n$ if h_q is irreducible or $n_2 = n$ if g_p is irreducible). By the induction hypothesis, $g(X)$ and $h(X)$ can be written as products of irreducible polynomials, thus so can $f(X)$.

(b) If $p = 0$ and $q = m$, then $g(X) = g_p$ and by hypothesis g_p is not a unit. Since $f_m = a_1 \cdots a_n = g_p h_q$ and g_p is not a unit, either h_q is not a unit in which case, by the uniqueness of the number of irreducible elements in the decomposition of f_m (since A is a UFD), h_q is the product of $n_2 < n$ irreducible elements, or $n_2 = 0$ if h_q is irreducible. Since $n \geq 1$, this implies that $(m, n_2) < (m, n)$, and by the induction hypothesis $h(X)$ can be written as products of irreducible polynomials. Since $g_p \in A$ is not a unit, it can also be written as a product of irreducible elements, thus so can $f(X)$.

The case where $p = m$ and $q = 0$ is similar to the previous case.