Unique factorization in polynomial rings

Let R be an integral domain and let F be its field of fractions. We know that $F[x]$ is a Euclidean Domain, hence a PID (Problem 71), hence a UFD (Problem 78). Thus, if $p(x) \in R[x]$, then $p(x)$ factors uniquely in $F[x]$. In general, the situation in $R[x]$ can be much more complex:

(127) Let $R = \mathbb{R}[t^2, t^3]$ and let F be the fraction field of R. Show that the polynomial $x^2 - t^2$ factors in $F[x]$, but is irreducible in $R[x]$.

(128) Let $R = \mathbb{R}[t^2, t^3]$ and let F be the fraction field of R. Give two different irreducible factorizations of the polynomial $x^6 - t^6$ over $R[x]$. You may find it helpful to know that the factorization of $x^6 - t^6$ over $F[x]$ is $(x-t)(x+t)(x^2 + tx + t^2)(x^2 - tx + t^2)$.

As the rest of this worksheet will show, if R is a UFD, then life is much nicer. For the rest of this worksheet:

Assume that R is a UFD.

We begin with a problem from the homework:

(129) Let $p \in R$ be a prime element. Let $a(x)$ and $b(x)$ be polynomials in $R[x]$. Show that, if $a(x)b(x) \in pR[x]$, then either $a(x) \in pR[x]$ or $b(x) \in pR[x]$.

We define a polynomial $a_n x^n + \cdots + a_1 x + a_0$ in $R[x]$ to be ***primitive*** if $\mathrm{GCD}(a_n, \cdots, a_1, a_0) = 1$.

(130) Let $a(x)b(x) = c(x)$ with $a(x)$, $b(x)$ and $c(x) \in R[x]$. Show that, if $c(x)$ is primitive then $a(x)$ and $b(x)$ are primitive.

(131) (**Gauss's Lemma**[1]) Let $a(x)b(x) = c(x)$ with $a(x)$, $b(x)$ and $c(x) \in R[x]$. Show that, if $a(x)$ and $b(x)$ are primitive, then $c(x)$ is primitive.

(132) Let $a(x)b(x) = c(x)$ with $a(x) \in R[x]$ primitive, $b(x) \in F[x]$ and $c(x) \in R[x]$. Show that $b(x) \in R[x]$.

(133) Let $p(x) \in R[x]$. Show that the following are equivalent:
  (a) $p(x)$ is irreducible in $R[x]$.
  (b) $p(x)$ is prime in $R[x]$.
  (c) One of the following two conditions holds:
    - $p(x)$ is a constant polynomial whose value is a prime element p of R.
    - $p(x)$ is primitive in $R[x]$, and is prime in $F[x]$.

  Helpful reminder: R and $F[x]$ are UFD's, so prime and irreducible are synonyms in those two rings.

We are now set to prove:

(134) **IMPORTANT RESULT:** Show that, if R is a UFD, then $R[x]$ is a UFD.

In particular, $\mathbb{Z}[x_1, \ldots, x_n]$ and $k[x_1, \ldots, x_n]$ are UFD's for any field k and any number of variables.

[1] Carl Friedrich Gauss, German mathematician, 1777-1855, plausible candidate for the greatest mathematician of all time. This is one of three results I know of named "Gauss's Lemma".