**Content:**

Theorem In a UFD, gcd's always exist.

Theorem $R[x]$ is a UFD if $R$ is a UFD.

**Example** gcd(3240, 765450)

$3240 = 2^2 \cdot 3^4 \cdot 5$

$765450 = 2 \cdot 3^7 \cdot 5^2 \cdot 7$

To find gcd(3240, 765450) we take the minimum power of all primes and multiply them together.

So to find the gcd $(r, s)$ where $r = u\, p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$ and $s = v\, p_1^{j_1} p_2^{j_2} \cdots p_t^{j_t}$ do the same thing.

Moral of the story: In a UFD, gcd's always exist.

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

**Proof**:

Let $f(x) \in R[x]$. We need to show $f(x)$ can be expressed as a product of irreducibles. Assume $f(x) \notin U(R[x]), f(x) \neq 0$.

Induct on deg $f$.

If deg $f = 0$, then $f \in R$. Since $R$ is a UFD, $f$ can be factored into irreducibles.

Let deg $f(x) = k$.

Assume $k > 0$ and we have irreducible factorization for any deg f < k.

Then by Lemma 5 If $f(x) = c(f)f^*(x)$ where $f^*(x)$ is primitive in $R[x]$, then $f(x) \in R[x] \Leftrightarrow c(f) \in R$.) we have $f(x) = c(f)f^*(x)$ where $c(f) \in R$.

Since $f(x) \in R[x]$, $c(f) \in R$, and $R$ is a UFD, then $c(f)$ can be expressed as a product of irreducibles or $c(f)$ is a unit in $R$.

If $f^*(x)$ is irreducible then $c(f)f^*(x)$ is a product of irreducibles and we're done. So assume $f^*(x)$ is not irreducible.

Then $\exists\, g(x), h(x)$ such that deg $g(x)$, deg $h(x) <$ deg $f^*(x)$ and $f^*(x) = g(x)h(x)$. (This is simply by definition of reducibility in an integral domain.) Then, by our induction hypothesis, $g(x)$ and $h(x)$ can be expressed as a product of irreducibles, hence $f(x)$ can.

$\therefore$ We have criterion (1) of UFD.

To prove $R[x]$ is a UFD, we'll use Lemma 1 (If R is an integral domain in which criterion (1) of UFD is satisfied, the R is a UFD $\Leftrightarrow$ (p) is a prime ideal for all irreducible elements p $\in$ R). In other words, we need to show that for any irreducible polynomial, $p(x) \in R[x]$, we get that $(p(x))$ is prime. We'll show that if $p(x) \mid f(x)g(x)$ then $p(x) \mid f(x)$ or $p(x) \mid g(x)$.

Assume $p(x) \mid f(x)g(x)$ in R[x].

Case 1: Assume deg $p(x) = 0$. Then $p(x) = p \in R$.

So, $p \mid f(x)g(x)$
$\Rightarrow p \mid c(fg)[f(x)g(x)]^*$
$\Rightarrow p$ divides all the coefficients of $f(x)g(x)$.
$\Rightarrow p$ divides $c(fg)$
$\Rightarrow p \mid c(f)c(g)$ (since $c(fg)$ is an associate of $c(f)c(g)$, Lemma 4)
$\Rightarrow p \mid c(f)$ or $p \mid c(g)$ (by Lemma 1, ie. (p) is a prime ideal)
$\Rightarrow p \mid f(x)$ or $p \mid g(x)$, as desired.

Case 2: Assume deg $p(x) > 0$.

Let $I = (p(x), f(x))$
Let $m(x) \in I$ of minimal degree.
Let $Q = \text{Frac}(R)$ and use the division algorithm.
Then $\exists!\ q'(x), r'(x) \in Q[x]$ such that
$f(x) = m(x)q'(x) + r'(x)$ for $r'(x) = 0$ or deg $r'(x) <$ deg $m(x)$.
And $q'(x) = c(q')g^*(x)$; $r'(x) = c(r')r^*(x)$ for $g^*(x), r^*(x) \in R[x]$.
$\exists\ b \in R$ such that $bf(x) = m(x)q(x) + r(x)$ where
$q(x) = bq'(x)$ and $r(x) = br'(x)$ and $q(x), r(x) \in R[x]$.
Now we have $bf(x) \in I$ and $m(x)g(x) \in I$, so $r(x) \in I$.
Hence $m(x) \mid bf(x)$.
Recall $(2x + 4) \mid 2(x + 2)$ but $(2x + 4) \nmid (x + 2)$. So we need $m(x)$ to be primitive. So here we can use $m(x) = c(m)m^*(x)$.
Then by Lemma 6(If $f(x)$ is primitive and $f(x) \mid bg(x)$, $b \in R$, $b \neq 0$, then $f(x) \mid g(x)$.), $m^*(x) \mid f(x)$ since $m^*(x)$ is primitive.
Similarly $m^*(x) \mid p(x)$.
Since $p(x)$ is irreducible (by assumption) $m^*(x) \in U(R[x])$ or $m^*(x)$ and $p(x)$ are associates.
If $m^*(x)$ and $p(x)$ are associates, then $p(x) \mid m^*(x)$.
Since $m^*(x) \mid f(x)$ we get $p(x) \mid f(x)$.
If $m^*(x) \in U(R[x])$, then $m^*(x) = m^* \in U(R)$,
Since $m(x) = c(m)m^*(x)$, then $m(x)$ and $c(m)$ are associates in $R$. (I don't think Lemma 5 applies here as stated in the lecture notes.) Thus, $m^* \in R \Rightarrow m(x) = m \in R$.

Since $m \in I$ (by definition), $\exists\ a(x), b(x) \in R[x]$ such that
$m = p(x)a(x) + f(x)b(x)$.
So $mg(x) = p(x)a(x)\,g(x) + f(x)\,g(x)b(x)$.
Thus, $p(x) \mid mg(x)$.
Since $p(x)$ is irreducible and deg $p(x) > 0$, then $p(x)$ is primitive by Exercise 6.29 ($f(x) \in R[x]$ is irreducible in $R[x] \Leftrightarrow f(x)$ is primitive and $f(x)$ is irreducible in $Q[x]$).
Thus, $p(x) \mid g(x)$.
So, by Lemma 1, $R[x]$ is a UFD.