Content:

Theorem	If R is a PID, then R is a UFD.
Goal	$R[x]$ is a UFD if R is a UFD.
Definition	primitive polynomial
Lemma	Gauss' Lemma. If R is a UFD and $f(x), g(x) \in R[x]$ are both primitive, then $f(x)g(x)$ is primitive.
Definition	content
Example 1	$f(x) = \frac{7}{10}x^2 + \frac{28}{15}x + \frac{7}{15} = \frac{7}{30}(3x^2 + 8x + 2)$
Lemma 3	Let R be a UFD, $Q = \text{Frac}(R)$, $f(x) \in Q[x]$. Then there is a factorization $f(x) = c(f)f^*(x)$ such that $c(f) \in Q$, $f^*(x)$ is primitive in $R[x]$. This factorization is unique up to units.
Example 2	$g(x) = 6x^2 + 18x + 12 \in \mathbb{Z}[x]$; $h(x) = 12x + 20 \in \mathbb{Z}[x]$ $c(g) = 6$; $c(h) = 4$; $c(gh) = 24$
Lemma 4	If $f(x), g(x) \in R[x]$, then $c(fg)$ and $c(f)c(g)$ are associates in R and $(fg)^*$ and f^*g^* are associates in $R[x]$.
Example 3	$5x^2 + 3x + 4 =$ _____$(ax^2 + b + c)$ where $ax^2 + b + c$ is primitive in $\mathbb{Z}[x]$.
Lemma 5	Let $f(x) \in Q[x]$ such that $f(x) = qf^*(x)$ where $q \in Q$ and $f^*(x)$ is primitive in $R[x]$. Then $f(x) \in R[x] \Leftrightarrow q \in R$.
Example 4	$5x^2 + 3x + 4 = bg(x)$ where $g(x) \in \mathbb{Z}[x]$. Does $5x^2 + 3x + 4 \mid g(x)$?
Lemma 6	Let $f(x), g(x) \in R[x]$. If $f(x)$ is primitive and $f(x) \mid bg(x)$, $b \in R$, $b \neq 0$, then $f(x) \mid g(x)$.

Announcements Exam 1 will cover through $R[x]$ a UFD.
6.2 #17, 18i, 29 are pertinent to the exam.

Recall

Lemma 1 In an integral domain in which criteria (1) for UFD is satisfied, then R is a UFD $\Leftrightarrow$ (p) is prime for all irreducible elements p.

Lemma 2 (1) If R is a commutative ring with unity and $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$ is an ascending chain of ideals in R, then $\cup_{n \geq 1} I_n$ is an ideal in R.
(2) If R is a PID, then it has no infinitely strictly increasing chain of ideals.
(3) If R is a PID and $r \in R$, $r \neq 0$, $r \notin U(R)$, then r is a product of irreducibles.

Theorem If R is a PID, then R is a UFD.

Proof:
By Lemma 2 any non-zero non-unit in a PID can be factored into irreducibles. To prove R is a UFD we need only show that for any irreducible p, (p) is a prime ideal. In a PID, irreducible elements are prime, hence (p) is prime. So by Lemma 1, we have a UFD.

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

Definition Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$. We say $f(x)$ is *primitive* if the coefficients of $f(x)$ are relatively prime (i.e. gcd $(a_0, \ldots, a_n)$ is a unit.

Examples

	Primitive	**Not Primitive**
$\mathbb{Z}[x]$	$2x + 1$ $2x^2 + 6x + 5$	$2x + 4$
$\mathbb{Q}[x]$	$2x + 4$	
Over a field	Everything	
$R[x]$ (R a UFD)	Every monic polyn.	

Question If $f(x) \in R[x]$ and $f(x)$ is irreducible, is $f(x)$ primitive?
Answer Homework 6.29

Lemma Gauss' Lemma
If R is a UFD and $f(x), g(x) \in R[x]$ are both primitive, then $f(x)g(x)$ is primitive.

Proof:
Assume $f(x), g(x)$ are primitive, but $f(x)g(x)$ is not.
So there is an irreducible element $p \in R$ such that p divides all the coefficients in $f(x)\, g(x)$.
Define π: $R[x] \to R/(p)[x]$ by
$\pi(a_0 + a_1x + \cdots + a_nx^n) = (a_0 + (p)) + (a_1 + (p))x + \cdots$
So $\pi(f(x)\, g(x)) = 0 + (p)$ since all coefficients are divisible by p.
But $\pi(f(x)\, g(x)) = \pi(f(x))\pi(g(x)) = 0$.
Since $f(x)$ and $g(x)$ are primitive, then $\pi(f(x)) \neq 0$ and $\pi(g(x)) \neq 0$.
Thus, $R/(p)[x]$ contains zero divisors.
But this is a contradiction as R is a UFD and p is irreducible, hence (p) is prime by Lemma 1. Thus $R/(p)$ is an integral domain
And this gives us that $f(x)g(x)$ is primitive.

Definition Let R be a UFD and $Q = \text{Frac}(R)$. If $f(x) \in Q[x]$ is non-zero and $f(x) = c(f)f^*(x)$ where $c(f) \in Q$ and $f^*(x)$ is primitive in $R[x]$ we say $c(f)$ is the *content* of $f(x)$ and $f^*(x)$ is the *associated primitive polynomial.*

Example 1 To motivate Lemma 3:

$$f(x) = \frac{7}{10}x^2 + \frac{28}{15}x + \frac{7}{15} \in \mathbb{Q}[x].$$
$$= \frac{1}{30}(21x^2 + 56x + 14) \text{ where } 21x^2 + 56x + 14 \in \mathbb{Z}[x].$$
$$= \frac{7}{30}(3x^2 + 8x + 2) \text{ where } 3x^2 + 8x + 2 \text{ is primitive in } \mathbb{Z}[x].$$

Lemma 3 Let R be a UFD, $Q = \text{Frac}(R)$, $f(x) \in Q[x]$. Then there is a factorization $f(x) = c(f)f^*(x)$ such that $c(f) \in Q$, $f^*(x)$ is primitive in $R[x]$. This factorization is unique up to units.

Proof:
p. 332 Read it.
Clearing denominators, there is $b \in R$ with $bf(x) \in R[x]$.
If d is the gcd of the coefficients of $bf(x)$, then
$(b/d)f(x) \in R[x]$ is a primitive polynomial.
If we define $c(f) = d/b$ and $f^*(x) = (b/d)f(x)$, then
$f^*(x)$ is primitive and $f(x) = c(f)f^*(x)$.
To prove uniqueness, suppose that $c(f)f^*(x) = f(x) = qg^*(x)$, where $c(f), q \in Q$ and $f^*(x), g^*(x) \in R[x]$ are primitive.
Exercise 6.17 on page 339 (If R is a UFD, $Q = \text{Frac}(R)$, then each nonzero $a/b \in Q$ has an expression in lowest terms.) allows us to write $q/c(f)$ in lowest terms: $q/c(f) = u/v$, where u and v are relatively prime elements of R.
Thus the equation $vf^*(x) = ug^*(x)$ holds in $R[x]$.
Equating like coefficients, v is a common divisor of each coefficient of $ug^*(x)$. And since u and v are relatively prime, we have v a common divisor of the coefficients of $g^*(x)$ by Exercise 6.18(i) on page 339 (If $a, b, c \in R$ a UFD and a and b are relatively prime, then $a|bc \Rightarrow a \mid c$.)
But $g^*(x)$ is primitive, and so v is a unit. A similar argument shows that u is a unit. Therefore, $q/c(f) = u/v = w$, a unit in R.
So then we have $wc(f) = q$ and $f^*(x) = wg^*(x)$, as desired.

Example 2 To motivate Lemma 4:
$g(x) = 6x^2 + 18x + 12 \in \mathbb{Z}[x]$; $h(x) = 12x + 20 \in \mathbb{Z}[x]$
$c(g) = 6$; $c(h) = 4$; $c(gh) = 24$

Lemma 4 If $f(x), g(x) \in R[x]$, then $c(fg)$ and $c(f)c(g)$ are associates in R and $(fg)^*$ and f^*g^* are associates in $R[x]$.

Proof:
$f(x)g(x) = c(fg)(f(x)g(x))^* = c(f)f^*(x)c(g)g^*(x) = c(f)c(g)f^*(x)g^*(x)$.
Note that $f^*(x)g^*(x)$ is primitive by Gauss' Lemma.
By Lemma 3, $c(fg)$ and $c(f)c(g)$ are associates and $(f(x)g(x))^*$ and $f^*(x)g^*(x)$ are associates.

Example 3 To motivate Lemma 5:
$5x^2 + 3x + 4 =$ _____$(ax^2 + b + c)$ where $ax^2 + b + c$ is primitive in $\mathbb{Z}[x]$.

Question Is it possible to fill the blank with a non-unit? No.

Lemma 5 Let $f(x) \in Q[x]$ such that $f(x) = qf^*(x)$ where $q \in Q$ and $f^*(x)$ is primitive in $R[x]$. Then $f(x) \in R[x] \Leftrightarrow q \in R$.

Proof:
$\Leftarrow$: $q \in R$ and $f^*(x) \in R[x]$. So $qf^*(x) \in R[x]$ by closure.
$\Rightarrow$: Assume $f(x) \in R[x]$.
Then $f(x) = c(f)f^*(x)$ where $c(f) = d$ is a gcd of the coefficients of $f(x)$, and $f^*(x)$ is primitive. By lemma 3, we have uniqueness, hence for some $u \in U(R)$, $q = ud \in R$.

Example 4 To motivate Lemma 6:
$5x^2 + 3x + 4 = bg(x)$ where $g(x) \in \mathbb{Z}[x]$. Does $5x^2 + 3x + 4 \mid g(x)$?

Lemma 6 Let $f(x), g(x) \in R[x]$. If $f(x)$ is primitive and $f(x) \mid bg(x)$, $b \in R$, $b \neq 0$, then $f(x) \mid g(x)$.

Proof:
p. 332 Read it.
Since $bg(x) = h(x)f(x)$, we have $bc(g)g^*(x) = c(h)h^*(x)f(x)$.
By uniqueness, $g^*(x)$ and $h^*(x)f(x)$ are associates, and so $f(x) \mid g^*(x)$.
But $g(x) = c(g)g^*(x)$, and so $f(x) \mid g(x)$.

Lemma 3 Let R be a UFD, $Q = \text{Frac}(R)$, $f(x) \in Q[x]$. Then there is a factorization $f(x) = c(f)f^*(x)$ such that $c(f) \in Q$, $f^*(x)$ is primitive in $R[x]$. This factorization is unique up to units.

Proof:

Denote $[a, b] \in Q$ by $\frac{a}{b}$.

$f(x) \in Q[x] \Rightarrow f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x^1 + \frac{a_2}{b_2}x^2 + \cdots + \frac{a_n}{b_n}x^n$

where $a_0, a_1, a_2, \ldots, a_n, b_0, b_1, b_2, \ldots, b_n \in R$.

Then $f(x) = \frac{d}{b}(a_0' + a_1'x + a_2'x^2 + \cdots + a_n'x^n) = \frac{d}{b}f^*(x)$

where $b = \text{lcm}\,(b_0, b_1, b_2, \ldots, b_n)$ and $d = \gcd(a_0, a_1, a_2, \ldots, a_n)$.
So then $f^*(x)$ is primitive.

Thus for $c(f) = \frac{d}{b}$, we have $f(x) = \frac{d}{b}f^*(x)$.

To prove uniqueness, suppose that $c(f)f^*(x) = f(x) = qg^*(x)$, where $c(f), q \in Q$ and $f^*(x), g^*(x) \in R[x]$ are primitive.
Since $c(f), q \in Q$, then

$c(f) = \frac{a}{b}$ and $q = \frac{c}{d}$ for some non-zero $a, b, c, d \in R$.

So $\frac{bd}{1} \bullet \frac{a}{b}f^*(x) = \frac{bd}{1} \bullet \frac{c}{d}g^*(x)$ holds and gives us
$ad \bullet f^*(x) = bc \bullet g^*(x)$.
And by Exercise 6.17 on page 339 (If R is a UFD, $Q = \text{Frac}(R)$, then each nonzero $a/b \in Q$ has an expression in lowest terms.)
we have $\frac{bc}{ad} = \frac{u}{v}$ where $u, v \in$ R and u and v are relatively prime.
Thus the equation $vf^*(x) = ug^*(x)$ holds in $R[x]$.
Equating coefficients of like terms, v is a common divisor of each coefficient of $ug^*(x)$. And since u and v are relatively prime, we have v a common divisor of the coefficients of $g^*(x)$ by Exercise 6.18(i) on page 339 (If $a, b, c \in R$ a UFD and a and b are relatively prime, then $a|bc \Rightarrow a \mid c$.)
But $g^*(x)$ is primitive, and so v is a unit. A similar argument shows that u is a unit. Therefore, $\frac{bc}{ad} = \frac{u}{v} = \frac{w}{1}$ where w is a unit in R.
So then we have $f^*(x) = wg^*(x)$, hence $c(f)f^*(x) = c(f)wg^*(x) = qg^*(x)$.
Thus, by cancellation we have $c(f)wg = q$, as desired.
$\therefore$ The factorization is unique.