Temos que o anel de polinômio $R[x]$ é também um DFU, a idéia básica da prova:

Dado um polinômio $f(x)$, seus fatores estão repetidam entre como um polinômio de baixo grau até $f(x)$ ser escrito como um produto de irredutíveis.

Para provar unicidade, considere $f(x)$ como um polinômio em $F[x]$, onde F é um corpo de quocientes de R.

Use o fato que $F[x]$ é DFU, para mostrar que fatoração em $R[x]$ é única.

Exemplo 1: O polinômio $3x^2+6$ não pode ser fatorado como um produto de 2 polinômios de baixo grau em $\mathbb{Z}[x]$, e é irredutível em $\mathbb{Q}[x]$. Mas $3x^2+6$ é irredutível em $\mathbb{Z}[x]$, porque $3x^2+6 = 3(x^2+2)$ e nem 3 nem (x^2+2) é uma unidade em $\mathbb{Z}[x]$.

$$3x^2+6 = 3(x^2+2) = \underbrace{3x^0}_{p(x)} \cdot \underbrace{(x^2+2)}_{q(x)}$$

$3x^2+6 = 0$

$\Delta = -48$, raízes $\in \mathbb{C}$, logo não pode ser fatorado em 2 polinômios em $\mathbb{Z}[x]$.

Lema de Gauss: Um polinômio em $\mathbb{Z}[x]$ de grau ≥ 1 é irredutível em $\mathbb{Z}[x] \longleftrightarrow$ é primitivo e é irredutível em $\mathbb{Q}[x]$.

Temos que o primeiro passo é examinar a função dos polinômios constantes em $R[x]$.

"As unidades em $R[x]$ são as unidades em R", e

"o polinômio constante irredutível em $R[x]$ são os elementos irredutíveis de R"

Por exemplo, as unidades de $\mathbb{Z}[x]$ são ± 1. O polinômio constante "3" é irredutível em $\mathbb{Z}[x]$, assim ele é uma unidade em $\mathbb{Q}[x]$.

Os fatores constantes irredutíveis de um polinômio em $R[x]$ pode ser encontrado por fatoração por qualquer constante e expressando eles como produtos de elementos irredutíveis em R.

Exemplo 2: Em $\mathbb{Z}[x]$,

$$6x^2+18x+12 = 6(x^2+3x+2) = 2.3(x^2+3x+2)$$

Temos que 2,3 são irredutíveis em $\mathbb{Z}[x]$

x^2+3x+2, é um polinômio cujos os divisores constantes em $\mathbb{Z}[x]$ são as unidades ± 1.

$x^2+3x+2=0 \longrightarrow (x+2).(x+1)$

$\Delta = 9 - 8 = 1$

$x = \dfrac{-3 \pm 1}{2}$

$x' = -2, \; x'' = -1$

$6x^2+18x+12 = 2.[3.(x+2).(x+1)]$

Temos R sendo um domínio de fatoração única, um polinômio diferente de zero em $R[x]$ é dito ser primitivo, se somente se, as constantes que divide ele são unidades em R.

Um polinômio é primitivo cujos coeficientes tem máximo divisor comum igual a um.

Por exemplo: x^2+3x+2 e $3x^4-5x^3+2x$ são primitivos em $\mathbb{Z}[x]$.

$p(x) = x^2+3x+2$; $mdc(1,3,2) = 1$ ✓
$q(x) = 3x^4-5x^3+2x$; $mdc(3,-5,2) = 1$ ✓

Já os polinômios primitivos de grau $\emptyset$ são unidades.

$3x^0 + 0x^0 = 3$; unidades em $\mathbb{Z}$

Todo polinômio primitivo de grau 1, deve ser irredutível pelo teorema:

Teorema 2.2: Temos p sendo um elemento diferente de zero, não unidade em um domínio de integridade R. Então p é irredutível $\forall\, p = rs \longrightarrow r$ ou s é uma unidade.

Por que toda fatoração inclui uma constante e cada constante deve ser uma unidade.

Contudo, polinômios primitivos de alto grau não precisa ser irredutível:

Exemplo: $x^2+3x+2=(x+1)(x+2)$ em $\mathbb{Z}[x]$.

Por outro lado, um polinômio irredutível de grau positivo, não tem divisores constantes exceto unidades.

"Um polinômio primitivo de grau positivo é primitivo"

Além do mais, como exemplo:

"Todo polinômio diferente de zero $f(x) \in R[x]$, fatores como $f(x) = c\, g(x)$ com $g(x)$ primitiva."

Para provar esta afirmação, temos $\underline{c}$ sendo um MDC dos coeficientes de $f(x)$.

Então: $f(x) = c\, g(x)$ $\forall g(x)$

Agora vamos mostrar que $g(x)$ é primitiva.

Se $d \in R$ divide $g(x)$, então $g(x) = d\, h(x)$ sendo que $f(x) = cd\, h(x)$.

Então cd é um divisor constante de $f(x)$, ele deve dividir os coeficientes de $f(x)$ e, deve dividir o mdc $\underline{c}$.

Assim $cdu = c$ $\forall u \in R$, e sendo $c \neq 0_R$, temos que $du = 1_R$ e d é uma unidade.
Portanto $g(x)$ é primitiva.

Teorema 10.32:

Temos R sendo um domínio de fatoração única, então todo $f(x)$ diferente de zero e não unidade em $R[x]$ é um produto de polinômios irredutíveis.

Lema 10.33:

Temos R sendo um domínio de fatoração única e $g(x), h(x) \in R[x]$. Se p é um elemento irredutível de R que divide $g(x)h(x)$, então p divide $g(x)$ ou p divide $h(x)$.

Corolário 10.34: Lema de Gauss

Temos R sendo um domínio de fatoração única, então o produto de polinômios primitivos em $R[x]$ é primitivo.

Teorema 10.35:

Temos R sendo um domínio de fatoração única e (r, s) elementos diferentes de zero de R.
Temos $f(x)$ e $g(x)$ sendo polinômios primitivos em $R[x]$ sendo que: $r f(x) = s g(x)$.
Então r e s são associados em R e $f(x)$ e $g(x)$ são associados em $R[x]$.

Corolário 10.36: Temos R sendo um domínio de fatoração única e F seu corpo de quocientes. Temos $f(x), g(x)$ sendo polinômios

primitivos em $R[x]$. Se $f(x)$ e $g(x)$ estão associados em $F[x]$, então eles estão associados em $R[x]$.

Corolário 10.37:

Temos R sendo um domínio de fatoração única e F seu corpo de quocientes. Se $f(x) \in R[x]$ tem grau positivo e é irredutível em $R[x]$, então $f(x)$ é irredutível em $F[x]$.

Teorema 10.38:

Se R é um domínio de fatoração única, então ele é $R[x]$.

Corolário 10.39:

$\mathbb{Z}[x]$ é um domínio de fatoração única, que não é um domínio de ideal principal.