Prove \( R \text{ U.F.D} \Rightarrow RC \text{K} \text{ U.F.D} \)

Recall we proved:

**Gauss's Lemma**

Let \( R \) be a U.F.D with quotient field \( \mathbb{Q} \). Let \( p(x) \in RC \text{K} \). Then if \( p(x) \) is reducible in \( \mathbb{Q} \text{K} \), it is also reducible in \( RC \text{K} \).

**Greatest Common Divisors in UFD's**

Let \( R \) be an integral domain.

**Definition** Let \( a \neq 0 \in R \). We say \( d \mid a \) is a divisor of \( a \) if \( a = bd \) for some \( b \in R \).

Now let \( a, b \) be nonzero elements of \( R \).

A **gcd** or greatest common divisor...
of \( a, b \) is an element \( d \) such that

(i) \( d \mid a \) and \( d \mid b \)

(ii) If \( c \mid a \) and \( c \mid b \) then \( c \mid d \)

**Lemma**

Let \( a, b \) be nonzero elements of \( \mathbb{R} \). Suppose \( d_1 \) and \( d_2 \) are both gcd \( a, b \). Then \( d_1 \) is an associate of \( d_2 \) i.e. \( d_1 = u d_2, u \in \mathbb{R} \) a unit.

If we have \( d_1 \mid d_2 \) and \( d_2 \mid d_1 \), by definition, so

\[
d_1 = \alpha d_2, \quad d_2 = \beta d_1
\]

\[
\Rightarrow \quad d_1 = \alpha \beta d_1
\]

Let \( d_1 \) be so by cancellation \( \alpha \beta = 1 \)

So \( \alpha, \beta \) are units and \( d_1 \) is an associate of \( d_2 \).
Then let \( R \) be a UFD. Then any two non-zero elements \( a, b \in R \) have a GCD.

**Proof**

Factorize \( a = u_1 x_1 \cdots x_r \)

\( b = u_2 y_1 \cdots y_s \)

\( u_1, u_2 \) units, \( x_1, y_1 \) irreducible.

Let \( \mathcal{P} = \{ P_1, \ldots, P_n \} \) be a collection of pairwise non-associate irreducible elements s.t. each irreducible factor of \( a \) and \( b \) is an associate of some \( P_i \).

This set can be formed as such:

If \( P_i = x_i \). Then let \( P_2 \) be the first element of \( \{ x_2, \ldots, x_i, y_1, \ldots, y_s \} \) not an associate of \( x_i \).
Let $p_3$ be the first element after $p_2$ not an associate of $p_1, p_2$ etc... so we can write

$$a = c_1 \cdot p_1 \cdots p_n$$

$$b = c_1 \cdot p_1 \cdots p_n$$

for integers \( c_i, p_i \geq 0 \)

Set \( d = \min \{ p_1, p_2 \cdots p_n \} \) so... we claim \( d \) is a gcd of \( a, b \).

Obviously \( d | a, d | b \).

Suppose \( e | a, e | b \).

Let \( e = e_1 e_2 \cdots e_{n+1} \in \mathbb{Z} \) be a factorization of \( e \)
Each \( q_i \mid e \Rightarrow q_i \mid a, q_i \mid b \)

But \( q_i \) is prime (i.e., \( \mathbb{Z}_{p_i} \) prime in \( \mathbb{Z}_{p_i} \))

So \( q_i \) must divide some irreducible \( p_j \)

i.e., \( q_i \) and \( p_j \) are associated.

So we can write

\[
e = c_1 \cdot p_1 \cdots p_n
\]

\( c_i \) are units \( \Rightarrow c_i \geq 0 \) integers

But \( e \mid a, e \mid b \Rightarrow c_i \leq e_i \)

\( c_i \leq e_i \)

So \( c_i \leq \min \{e_i, f_i\} \Rightarrow e_i \)

\[\Rightarrow e \mid d.\]

Definition: let \( R \) be a U.F.D.
A polynomial \( p(x) \in \mathbb{F}[x] \) is said to be primitive if the gcd of its coefficients is 1.

**Proposition**

Let \( R \) be a U.F.D and \( \mathbb{Q} \) its field of fractions. Let \( p(x) \in \mathbb{F}[x] \) be primitive. Then \( p(x) \in \mathbb{F}[x] \) is irreducible if and only if \( p(x) \in \mathbb{Q}[x] \) is irreducible in \( \mathbb{Q}[x] \).

**Proof**

If \( p(x) \in \mathbb{Q}[x] \) is reducible then by Gauss' lemma, \( p(x) \in \mathbb{F}[x] \) is reducible.

Conversely, suppose \( p(x) = A(x)B(x) \in \mathbb{F}[x] \).
is reducible, where $A(x), B(x)$ are not units. Since $p(x)$ is primitive, neither $A(x)$ nor $B(x)$ can be constant polynomials (else the coefficients would be divisible by this non-unit constant).

Thus $A(x), B(x)$ are nonunits in $\mathbb{Q}[x]$ (as they are nonconstant)
so $p(x) \in \mathbb{Q}[x]$ is reducible.

Tim

Let $R$ be a UFD. Then $R[x]$ is a UFD.

Proof

Let $p(x) \in R[x]$. Let $d \in R$ be the
gcd of the coefficients of $p(x)$. 
\[ p(x) = d q(x) = q(x) \text{ primitive} \]

If \( R \) is a UFD, \( d \in R \Rightarrow \text{can factor} \ \ d \in R \\
\] 

as a product \( d = u_1 d_1 \cdots d_n \), \( d_i \) irreducible

Further \( d_i \in R[\mathbb{C}] \) still irreducible

(\( u \) is constant) and the factorization

\( d = u_1 d_1 \cdots d_n \in R[\mathbb{C}] \) is still

esentially unique for the same reason.

So it suffices to show that the

primitive polynomial \( q(x) \) has an essentially

unique factorization.

Let \( Q \) be the field of fractions of \( R \),

then \( Q[\mathbb{C}] \) is a P.I.D. and so

\( Q[\mathbb{C}] \) is a U.F.D.

Now recall that in the course of
Proving Gauss’s Lemma we showed, if \( p(x) = A(x) B(x) \), \( A(x), B(x) \in \Omega[x] \) nonunits,

then there exist \( \alpha, \beta \in \Omega \) s.t.

\[ a(x) := \alpha A(x) \in \mathcal{R}[x] \]

\[ b(x) := \beta B(x) \]

and \( p(x) = a(x) b(x) \) is reducible.

Thus if \( p(x) \) is a \( \mathcal{R}[x] \) monic

\[ p(x) = A_1(x) \cdots A_n(x) \]

is a factorization into irreducibles in \( \mathcal{R}[x] \).

If \( \mathcal{Q}[x] \)
we have a factorization

\[ p(x) = q_1(x) \cdots q_m(x) \in \mathcal{Q}[x] \]

\[ q_i(x) \in \mathcal{Q}[x] \]

\[ q_i(x) = \alpha \in \mathcal{Q} \]

\[ q_i(x) = \alpha A_i(x) \]

\[ \alpha, \alpha \in \mathcal{Q}, \alpha \]
For $f(x)$ primitive
\[ p(x) \quad \text{primitive} \quad \Rightarrow q_i(x) \quad \text{primitive} \quad \forall 1 \leq i \leq n \]

As $A_i(x) \in \mathbb{Q}[x] \text{ is irreducible,}$

so is $q_i(x) \in \mathbb{Q}[x] \Rightarrow q_i(x) \text{ is irreducible}$

is irreducible (by Prop. above)

so we have a factorization of $p(x)$ by irreducible

Next time $p(x) = q_1(x) \ldots q_n(x) \in \mathbb{Q}[x]$ is

unique.