<u>Field of Quotient of UFD</u>: If R is a unique factorisation domain, then R is necessarily an integral domain. Therefore R has a field of quotients. We will denote this field of quotient of R by F. We can consider $R[x]$ to be subring of $F[x]$

<u>Thm.</u> If R is integral domain (not necessarily UFD) and F is its field of quotients, then any element $f(x)$ in $F[x]$ can be written as

$$f(x) = \frac{f_0(x)}{a} \quad \text{where } f_0(x) \in R[x] \text{ and } a \in R.$$

<u>Proof</u> Let F be field of quotient of integral domain R.

Then $F = \{p/q : p, q \in R \text{ s.t. } q \neq 0\}$

Let $f(x) \in F[x]$ ie $\exists \frac{a_0}{b_0}, \frac{a_1}{b_1}, \cdots \frac{a_n}{b_n} \in F$ s.t

$$f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \frac{a_2}{b_2}x^2 + \cdots + \frac{a_n}{b_n}x^n$$

where $b_0, b_1 \cdots b_n$ are non-zero

Clearly $a_0, a_1, a_2, \cdots a_n$ & $b_0, b_1, \cdots b_n$ all are elements of R and inverses of $b_0, b_1, b_2 \cdots b_n$ exist as they are non-zero elements of F.

$\Rightarrow b_0 \cdot b_1 \cdot b_2 \cdots b_n$ is also non-zero element of R

$\Rightarrow$ Inverse of $b_0 \cdot b_1 \cdot b_2 \cdots b_n$ also exist.

So we can write

$$f(x) = \frac{b_0 b_1 b_2 \cdots b_n}{b_0 b_1 b_2 \cdots b_n}\left[\frac{a_0}{b_0} + \frac{a_1}{b_1}x + \cdots + \frac{a_n}{a_n}x^n\right]$$

$$= \frac{(a_0 b_1 b_2 \cdots b_n) + (b_1 a_2 b_2 \cdots b_n)x + \cdots + (b_0 b_1 \cdots b_{n-1} a_n)x^n}{b_0 b_1 b_2 \cdots b_n}$$

$$= \frac{f_0(x)}{a}$$

Obviously $f_0(x) = (a_0 b_1 b_2 \cdots b_n) + (b_0 a_1 b_2 \cdots b_n)x + \cdots + (b_0 b_1 \cdots b_{n-1} a_n)x^n$ is an element of $R[x]$ and $a = b_0 b_1 b_2 \cdots b_n$ is in R.

Proved

Thm (Gauss Lemma):

Let F be the field of quotient of UFD "R". If the primitive polynomial $f(x) \in R[x]$ can be factorised as a product of two polynomials having coeffients in F, then it can be factorised as a product of two polynomials having coefficient in R.

Proof Let F be field of quotients of UFD "R".

Let $f(x) \in R[x]$ be primitive

Let $f(x) = g(x) \cdot h(x)$ where $g(x)$ & $h(x)$ have coeffients — ① in F. ie $g(x), h(x) \in F[x]$

∴ We can write

$$g(x) = \frac{g_0(x)}{a} \quad \& \quad h(x) = \frac{h_0(x)}{b}$$

Where $g_0(x)$ & $h_0(x) \in R[x]$ and $a, b \in R$

From ① $\Rightarrow f(x) = \frac{g_0(x)}{a} \cdot \frac{h_0(x)}{b} = \frac{1}{ab} g_0(x) \cdot h_0(x)$ — ②

Let $\alpha = c(g_0)$ and $\beta = c(h_0)$

then we can write

$$g_0(x) = \alpha \cdot g_1(x) \quad \& \quad h_0(x) = \beta h_1(x)$$

where $g_1(x)$ and $h_1(x)$ are primitive in $R[x]$

From ② we have

$$f(x) = \frac{\alpha\beta}{ab} g_1(x).h_1(x)$$

$$\Rightarrow ab\, f(x) = \alpha\beta\, g_1(x).h_1(x)$$

Since $g_1(x)$ and $h_1(x)$ are both primitive members of $R[x]$, therefore $g_1(x).h_1(x)$ is also a primitive member of $R[x]$. Therefore we conclude that $f(x)$ and $g_1(x)\,h_1(x)$ are associates in $R[x]$. Thus $\exists$ a unit $u \in R[x]$ such that

$$f(x) = u.\,g_1(x).\,h_1(x)$$

Now $u \in R[x]$ is unit $\Rightarrow u \in R$

Also $g_1(x) \in R[x]$

$$\Longrightarrow u.g_1(x) \in R[x]$$

Also $h_1(x) \in R[x]$

Hence $f(x)$ can be factorised as product of two polynomials having coefficients in R.

$$\text{as } f(x) = (u g_1(x)).\,(h_1(x))$$

Proved

Note: <u>Above theorem can be stated for set of integers I as</u>

"If a primitive polynomial $f(x) \in I(x)$ can be factorised as a product of two polynomials having rational coefficients then it can also be factorised as a product of two polynomials having integer coefficients.