Th^m. Let R be a UFD. Prove that every non-zero element of $f(x)$ of $R[x]$ can be written as $f(x) = g f_1(x)$ where $g = c(f)$ and $f_1(x)$ is primitive. Also prove that this decomposition of $f(x)$ as an element of R by a primitive in $R[x]$ is unique apart from the distinction between associates.

Proof Let R be a UFD and let

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in R[x]$$

Since R is UFD, therefore the elements $a_0, a_1, \cdots a_n$ of R must possess a GCD. Let $g \in R$ be the GCD of these elements.

$$\Rightarrow a_i = g b_i \quad \forall\, i = 0, 1, 2, \cdots n$$

$$\Rightarrow f(x) = g b_0 + g b_1 x + g b_2 x^2 + \cdots + g b_n x^n$$

$$= g(b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n)$$

$$= g \cdot f_1(x)$$

Where $f_1(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n$

Since g is GCD of $a_1, a_2 \cdots a_n$ therefore the elements $b_0, b_1, b_2 \cdots b_n$ has non common factor other than units of R

$$\Rightarrow f(x) \text{ is primitive in } R[x]$$

Thus we have $f(x) = g \cdot f_1(x)$ where $g \in R$

MoizKCC

and $f_1(x) \in R[x]$ is primitive.

Now we will prove the uniqueness.

Let if possible $f(x) = h f_2(x)$ where $h \in R$ and $f_2(x) \in R[x]$ is primitive.

$$\Rightarrow g \cdot f_1(x) = h f_2(x) \quad \text{——— (1)}$$

Since $f_1(x)$ & $f_2(x)$ are both primitive,

The content on LHS of eqn (1) is g

The content on RHS of eqn (1) is h.

But content of a polynomial is unique upto associates

Therefore g and h are associates.

$$\Rightarrow g = hu \quad \text{where } u \text{ is unit in } R.$$

Eqn (1) becomes

$$hu \cdot f_1(x) = h f_2(x)$$

$$\Rightarrow u f_1(x) = f_2(x)$$

$\Rightarrow f_1(x)$ & $f_2(x)$ are associates.

Hence the theorem

MOIZ KCC

$\Rightarrow (m) \subseteq (l)$

$\Rightarrow l / m.$

Hence by defn of LCM, l is LCM of a & b

(Proved)

Note: This result can be generalised as any n non-zero elements $a_1, a_2, \cdots a_n$ in PID have HCF & LCM.

Thm: The product of two primitive polynomials over UFD R is primitive polynomial in $R[x]$.

Proof: Let R be UFD and let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ and $g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m$. be two primitive polynomials in $R[x]$

ie HCF of $a_0, a_1, \cdots a_n = 1$ $\longrightarrow (1)$ & HCF of $b_0, b_1, \cdots b_m = 1$ $\longrightarrow (2)$

Let $h(x) = f(x).g(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{m+n} x^{m+n}$.

We want to prove that $h(x)$ is also a primitive

Let us assume that $h(x)$ is not a primitive polynomial

ie let us assume that $\exists$ a prime element $p \in R$ which divides each c_{i+j}, $i = 0, 1, \ldots n$, $j = 0, 1, \ldots m$.

As HCF of $a_0, a_1, \ldots a_n = 1$

$\Rightarrow p$ does not divide each a_i $i = 0, 1, 2, \ldots n$

Let a_r be the first coefficient of $f(x)$ such that p does not divide a_r. Similar b_s be the first coefficient of $g(x)$ such that p does not divide b_s.

$\Longrightarrow p$ does not divide $a_r . b_s$.

Now consider the coefficient of x^{r+s} in $h(x)$.

We have

$$c_{r+s} = a_r \cdot b_s + (a_{r-1} b_{s+1} + a_{r-2} b_{s+2} + \cdots + a_0 \cdot b_{s+r}) + (a_{r+1} b_{s-1} + a_{r+2} b_{s-2} + \cdots + a_{r+s} \cdot b_0)$$

$$\Rightarrow a_r \cdot b_s = c_{r+s} - (a_{r-1} b_{s+1} + a_{r-2} b_{s+2} + \cdots + a_0 b_{s+r}) - (a_{r+1} b_{s-1} + a_{r+2} b_{s-2} + \cdots + a_{r+s} \cdot b_0) \quad \text{—③}$$

By choice of a_r, p is divisor of $a_0, a_1 \cdots a_{r-1}$

$$\Rightarrow p \mid (a_{r-1} \cdot b_{s+1} + a_{r-2} b_{s+2} + \cdots + a_0 b_{s+r})$$

By choice of b_s, p is divisor of $b_0, b_1 \cdots a_{s-1}$

$$\Rightarrow p \mid (a_{r+1} b_{s-1} + a_{r+2} b_{s-2} + \cdots + a_{r+s} b_0)$$

Also $p \mid c_{r+s}$

So by eq③ $p \mid a_r \cdot b_s$ which is a contradiction.

Hence $h(x)$ must be primitive.

Thm: If R is UFD and $f(x), g(x) \in R[x]$ then

$$c(f \cdot g) = c(f) \cdot c(g). \text{ (upto units)}$$

where $c(f)$ denotes content of $f(x)$.

Proof Let $f(x) = a f_1(x)$ & $g(x) = b g_1(x)$

where $a = c(f)$ & $b = c(g)$ and $f_1(x)$ & $g_1(x)$ are primitive

$$\Rightarrow f(x)\, g(x) = ab\, f_1(x) \cdot g_1(x)$$

$$\Rightarrow c(f \cdot g) = ab\, c(f_1 g_1)$$

$$\Rightarrow c(f \cdot g) = ab \cdot 1 \quad (\because f_1 \,\&\, g_1 \text{ are primitive} \Rightarrow f_1 g_1 \text{ is primitive} \Rightarrow c(f_1 g_1) = 1)$$

$$\Rightarrow c(f \cdot g) = c(f) \cdot c(g)$$

(within units)

Proved

MoizKCC