Th^m Two elements a and b of an integral domain are associates iff one is unit times the other.

Proof Let the elements a & b of an integral domain R are associates

$\Rightarrow a|b$ & $b|a$ also $a, b \neq 0$

$\Rightarrow \exists\, x$ and $y \in R$ such that

$b = ax$ —① & $a = by$ —②

$\Rightarrow b = (by)x$ (from ① & ②)

$\Rightarrow 1 \cdot b = b(yx)$

$\Rightarrow b \cdot 1 - b(yx) = 0$

$\Rightarrow b(1 - yx) = 0$

$\Rightarrow 1 - yx = 0$ ($\because b \neq 0$ & R is integral dom)

$\Rightarrow yx = 1$

$\Rightarrow y$ & x are units in R.

So from ① $b = ax$ where x is unit

& from ② $a = by$ where y is unit.

Now conversely

Let $a = bu$ where u is unit in R.

Now $a = bu \Rightarrow b|a$

Also $a = bu \Rightarrow b = au^{-1}$ where $u^{-1} \in R$

$\Rightarrow a|b$

Hence $a \sim b$ Proved

Euclidean Algorithm for polynomial over a field.

If $d(x)$ be the greatest common divisor of two non-zero polynomials $f(x)$ and $g(x)$ over a field F, then there exists polynomials $m(x)$ and $n(x)$ over F s.t. $d(x) = m(x)f(x) + n(x)g(x)$

Proof Let F be a field and let $f(x)$ & $g(x) \in F[x]$ s.t. at least one of them is non-zero.

Let $S = \{ s(x).f(x) + r(x).g(x) : s(x), r(x) \in F[x] \}$

We claim that S is an ideal of $F[x]$

Let $p(x)$ & $q(x) \in S$

$\Rightarrow \exists$ $s(x), r(x)$ & $s_1(x)$ & $r_1(x) \in F[x]$ such that

$$p(x) = s(x).f(x) + r(x).g(x) \quad \text{—— (1)}$$

$$\& \quad q(x) = s_1(x) f(x) + r_1(x).g(x) \quad \text{—— (2)}$$

Now $p(x) - q(x) = \{s(x) - s_1(x)\} f(x) + \{r(x) - r_1(x)\} g(x)$

Since $s(x) - s_1(x)$ & $r(x) - r_1(x) \in F[x]$

$\Rightarrow p(x) - q(x) \in S$

Also let $\alpha(x) \in F[x]$ then

$$\alpha(x)\, p(x) = \alpha(x).\{s(x).f(x) + r(x).g(x)\}$$

$$= [\alpha(x).s(x)] f(x) + [\alpha(x).r(x)] g(x) \quad \text{—— (3)}$$

Since $\alpha(x).s(x)$ & $\alpha(x).r(x) \in F[x]$

so $\alpha(x).p(x) \in S$

Hence S is an ideal of $F[x]$

Now, since F is a field.

$\Rightarrow F$ is a commutative ring with unity

$\Rightarrow F[x]$ is a commutative ring with unity

$\Rightarrow F[x]$ is principal ideal ring
ie every ideal of $F[x]$ is principal ideal.

$\Rightarrow S$ is principal ideal of $F[x]$

$\Rightarrow \exists$ an element $d(x)$ such that

$$S = \{d(x)\} \text{ ie } S \text{ is generated by } d(x)$$

Since $d(x) \in S$

$\Rightarrow \exists\ m(x)\ \&\ n(x) \in F[x]$ such that

$$d(x) = m(x).f(x) + n(x).g(x) \quad \text{—— } (4)$$

Now we will prove that $d(x)$ is g.c.d of $f(x)$ & $g(x)$

Clearly $f(x)\ \&\ g(x) \in S$

$\because f(x) = 1.f(x) + 0.g(x)$

& $g(x) = 0.f(x) + 1\,g(x)$ where $0, 1 \in F[x]$

Since $f(x) \in S$ & S is generated by $d(x)$

$\Rightarrow \exists\ t(x) \in F[x]$ s.t. $f(x) = d(x).t(x)$

Similarly $\exists\ q(x) \in F(x)$ s.t $g(x) = d(x).q(x)$

$\Rightarrow d(x) \mid f(x)$ & $d(x) \mid g(x)$.

Also if $h(x) \mid f(x)$ & $h(x) \mid g(x)$

$\Rightarrow h(x) \mid m(x)f(x)$ & $h(x) \mid n(x).g(x)$

$\Rightarrow h(x) \mid m(x).f(x) + n(x).g(x)$

$\Rightarrow h(x) \mid d(x)$ (From 4)

So $d(x)$ is g.c.d of $f(x)$ and $g(x)$

(Proved)