Theorem (Division Alg.)

$\frac{f(x)}{g(x)}$

Let $f(x), g(x) \in F[x]$ where F is a field and $g \neq 0$

$\exists$ unique $q(x), r(x) \in F[x]$ s.t.

$$f(x) = g(x)\,q(x) + r(x)$$

where either $\deg(r(x)) < \deg(g(x))$ or $r(x) = 0$.

Proof:

- If $f(x) = 0$ then $0 = 0 \cdot g(x) + 0$

  $\therefore$ $q = r = 0$

Suppose $f(x) \neq 0$ Say $\deg(f(x)) = n$, $\deg(g(x)) = m$

If $m > n$ then take $q(x) = 0$, $r(x) = f(x)$

Assume $m \leq n$ do induction on n

Say $f(x) = a_n x^n + \cdots + a_1 x + a_0$

$g(x) = b_m x^m + \cdots + b_1 x + b_0$

Let

$$\hat{f}(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$$

$\deg(\hat{f}) < n$ or $\hat{f} = 0$ (by induction we may assume that quo. and remainder exist $\deg < \deg(g)$)

$\therefore$ by induction $\exists\ \tilde{q}(x), r(x)$ s.t.

$$\hat{f}(x) = \tilde{q}(x)\,g(x) + r(x)$$ where either $r = 0$ or $\deg(r) < \deg(g)$

Set

$$q(x) = \hat{q}(x) + \frac{a_n}{b_m} x^{n-m}$$

This is why we need a field

Then

$$= g \cdot \hat{q} + g \frac{a_n}{b_m} x^{n-m} + r(x) = \hat{f} + g \frac{a_n}{b_m} x^{n-m}$$
$$= f.$$

$$f(x) = g(x) q(x) + r(x)$$

we know $r = 0$ or $\deg(r) < \deg(g)$.

Now show uniqueness of q, r

Suppose $\exists$ q_1, r_1 s.t. $f(x) = g(x) q_1(x) + r_1(x)$
with $\deg(r_1(x)) < \deg(g(x))$
or $r_1 = 0$.

So then

$$\underbrace{f(x) = g(x)\, q(x) + r(x) = g(x)\, q_1(x) + r_1(x)}$$

$$g(x)\left[q(x) - q_1(x)\right] = r_1(x) - r(x)$$

$g \neq 0$

$$\deg\left(g(x)\left[q(x) - q_1(x)\right]\right) \overset{\geq \deg(g(x))}{=} \deg\left(r_1(x) - r(x)\right) \geq \deg(g(x))$$

But $\deg(r(x)) < \deg(g)$ and $\deg(r_1(x)) < \deg(g(x))$

This is a contradiction $\Rightarrow$ $r_1(x) = r(x)$
and $q_1(x) = q(x)$

$\blacksquare$

Ex) Polynomial Long divison ← Division Alg.

Suppose we want to divide $x^3 - x^2 + 2x - 3$ by $x-2$

$$
\begin{array}{rrrrrrrrr}
 & & & x^2 & + & x & + & 4 & \\
\cline{4-9}
x & - & 2 \,\big) & x^3 & - & x^2 & + & 2x & - \; 3 \\
 & & & x^3 & - & 2x^2 & & & \\
\cline{4-9}
 & & & & & x^2 & + & 2x & - \; 3 \\
 & & & & & x^2 & - & 2x & \\
\cline{6-9}
 & & & & & & & 4x & - \; 3 \\
 & & & & & & & 4x & - \; 8 \\
\cline{8-9}
 & & & & & & & & 5
\end{array}
$$

Let $p(x) \in F[x]$, $\alpha \in F$

α a root/zero of $p(x) \iff p(\alpha) = 0$

$\iff p(x) \in \ker(\phi_\alpha)$

Corol) Let F be a feild. $\alpha \in F$ is a zero of $p(x) \in F[x]$ iff $x - \alpha$ is a factor of $p(x)$ in $F[x]$.

Proof: First suppose $\alpha \in F$, $p(\alpha) = 0$

By the div. alg $\exists\, q(x), r(x) \in F[x]$ s.t

$$p(x) = (x-\alpha)q(x) + r(x)$$

and $\deg(r(x)) < \deg(x-\alpha) = 1 \implies r(x) = b \in F$

$$\therefore \; P(x) = (x-\alpha)q(x) + b$$

$$0 = P(\alpha) = 0 \cdot \overset{0}{q(x)} + b \implies b = 0.$$

$$\therefore \; p(x) = (x-\alpha)q(x)$$

Suppose $(x-\alpha)$ is a factor of $p(x)$

$\Rightarrow$ $p(x) = (x-\alpha)\, q(x)$ for some $q(x) \in F(x)$

$\Rightarrow$ $p(\alpha) = (\alpha - \alpha)\, q(\alpha) = 0.$ ∎

<u>Corol</u> Let F be a field. A non-zero poly. $p(x)$ of degree n in $F[x]$ can have at most n distinct zeros in F.

<u>Proof:</u> Do induction on $\deg(p(x))$

special case

[• If $\deg(p(x)) = 0 \Rightarrow p(x) = c \in F$ $\therefore$ has no zeros

base case

[• If $\deg(p(x)) = 1 \Rightarrow p(x) = ax + b$ for some $a, b \in F$

Since F is a feild $0 = p(\alpha) = a\alpha + b \Rightarrow \alpha = (-b)a^{-1}$

$\therefore$ p has exactly 1 root

Assume $\deg(p(x)) > 1$. If $p(x)$ has no zeros in F we are done.

Suppose $\alpha \in F$ is a root of p.

$\Rightarrow$ $p(x) = (x-\alpha)\, q(x)$ for some $q \in F[x]$

Since F is a feild $\Rightarrow$ F is a int. domain

$$\deg(q(x)) = n-1$$

Let $\beta \neq \alpha$ be another root of $p(x)$

$p(\beta) = (\beta - \alpha)\, q(\beta) = 0$, since $\alpha \neq \beta$ and F is a feild

$$\Rightarrow \quad q(\beta) = 0$$

by induction, since $\deg(q) = n-1$

then q has at most $n-1$ roots

$\therefore$ p has at most n roots $\blacksquare$.

Let F be a field. A monic polynomial $d(x)$ is a <u>greatest common divisor</u> of $p(x), q(x) \in F[x]$

if $d(x) \mid p(x)$ and $d(x) \mid q(x)$ and if for any other $\tilde{d}(x)$ which divides p, q $\Rightarrow$ $\tilde{d}(x) \mid d(x)$

$$d(x) = \gcd(p(x), q(x))$$

- $p(x), q(x)$ are <u>relitivley prime</u> if $\gcd(p(x), q(x)) = 1$.