Proposition 2 (The Division Algorithm). *Let k be a field and let g be a nonzero polynomial in $k[x]$. Then every $f \in k[x]$ can be written as*

quotient

$$f = qg + r,$$

remainder

where $q, r \in k[x]$, and either $r = 0$ or $\deg(r) < \deg(g)$. Furthermore, q and r are unique, and there is an algorithm for finding q and r.

Proof:

Alg to find q, r

$LT(g) \nmid LT(r)$

$\Updownarrow$

$\deg(r) < \deg(g)$

Output: q, r

$q := 0$

$r = f$

While $r \neq 0$ and $LT(g) \mid LT(r)$ Do:

$$q := q + \frac{LT(r)}{LT(g)}$$

$$r := r - \frac{LT(r)}{LT(g)} g$$

Return q, r

Why this works:

- $f = \tilde{q} g + \tilde{r}$, true for $\tilde{q} = 0, \tilde{r} = f$
- when we redefine q, r, $f = qg + r$ still holds since

$$f = qg + r = \left(\tilde{q} + \frac{LT(\tilde{r})}{LT(g)}\right) g + \left(\tilde{r} - \frac{LT(\tilde{r})}{LT(g)} g\right)$$

Show alg. terminates (not infinite loop)

since either $r - \frac{LT(r)}{LT(g)} g = 0$ or

has smaller degree than r.

to see why...

$r = c_0 x^m + \cdots + c_m$, $LT(r) = c_0 x^m$

$g = d_0 x^l + \cdots + d_l$, $LT(g) = d_0 x^l$

suppose $m \geq l$ (since otherwise we are done)

Then

$$r - \frac{LT(r)}{LT(g)} g = (c_0 x^m + \cdots) - \frac{c_0}{d_0} x^{m-l} (d_0 x^l + \cdots)$$

"new" r

$\therefore$ $\deg(r)$ must drop at each step (or $r = 0$)

Since $\deg r$ is finite there are finitely many steps $\therefore$ alg terminates. ■

Cor] $f \in K[x]$, K a field. f has at most $\deg(f)$ roots in K.

Cor] $K[x]$ is a principal ideal (K a field), i.e. every ideal I has the form $I = (f)$ for some $f \in K[x]$.

f is unique (up to a constant).

Q: How do we find the principle generator of an Ideal $I \subseteq k[x]$?

A: greatest common divisor = gcd

Def: $\gcd(f,g)$, $f,g \in k[x]$ is a poly. h s.t.

- h divides f and h divides g
- If $p|f$, $p|g \Rightarrow p|h$

write $h = \gcd(f,g)$

Prop] $f, g \in K[x]$

(i) $\gcd(f, g)$ exists and is unique (up to scalar)

(ii) $(\gcd(f,g)) = (f, g)$

(iii) $\exists$ an alg. to find $\gcd(f,g)$

Proof: (i)/(ii) in text.

Euclidean Algorithm

Input: f, g

Output: $h = \gcd(f,g)$

$h := f$
$s := g$

while $s \neq 0$ do — remainder of dividing h by s

  rem $:= h \,\%\, s$

  $h := s$

  $s :=$ rem

Return h:

$g = q'r + r'$

$\gcd(f,g) = \gcd(g, r)$ $\deg(g) > \deg(r) > \deg(r')$

$= \gcd(r, r') = \cdots$

$s = r''' = 0$ eventually

$f = qg + r$

$\gcd(f,g) = \gcd(f - qg, g) = \gcd(r, g)$

$\Updownarrow$

$(f, g) = (f - qg, g)$

By this we eventually

$\gcd(h, 0) = \gcd(f, g) \;\therefore\; \gcd(f,g) = h$

Def: $h = \gcd(f_1, \ldots, f_s)$, $f_i \in k[x]$

(i) h divides (each of) $f_1, \ldots, f_s$

(ii) If p divides $f_1, \ldots, f_s \Rightarrow p \mid h$

Prop) $f_1, \ldots, f_s \in k[x]$ $s \geq 2$

- $\gcd(f_1, \ldots, f_s)$ exists and is unique (upto scalar)
- $(\gcd(f_1, \ldots, f_s)) = (f_1, \ldots, f_s)$
- $s \geq 3$ then $\gcd(f_1, \ldots, f_s) = \gcd(f_1, \gcd(f_2, \ldots, f_s))$
- There is an alg to find $\gcd(f_1, \ldots, f_s)$.

Application:

Ideal membership problem in $k[x]$

$(f_1, \ldots, f_s) \leq k[x]$, $f \in k[x]$

Q: is $f \in (f_1, \ldots, f_s)$

A: $(f_1, \ldots, f_s) = (\gcd(f_1, \ldots, f_s))$, let $h = \gcd(f_1, \ldots, f_s)$ and apply Div. Alg.

$f = qh + r$

If $r = 0 \Rightarrow f \in (h)$

i.e. $f = 0 \in k[x]/(h)$

if $r \neq 0$ then $f \notin (h)$.