Theorem : Division Alg. in $K[x_1, \ldots, x_n]$

$F = f_1, \ldots, f_s$, $>$ mon. ord

Any $f \in K[x_1, \ldots, x_n]$ can be written as

$$f = q_1 f_1 + \cdots + q_s f_s + r$$

where either $r = 0$ OR None of the monomials of r are divisable by any of $LT(f_1), \ldots, LT(f_s)$

Further if $q_i f_i \neq 0 \Rightarrow$ multdeg $(f) \geq$ multdeg $(q_i f_i)$.

Proof:

Input : $f_1, \ldots, f_s, f$
Output : $q_1, \ldots, q_s, r$
$q_1 := 0; \ldots; q_s := 0; r := 0$
$p := f$
WHILE $p \neq 0$ DO
  $i := 1$
  divisionoccurred := false
  WHILE $i \leq s$ AND *divisionoccurred* = false DO
    IF $\mathrm{LT}(f_i)$ divides $\mathrm{LT}(p)$ THEN
      $q_i := q_i + \mathrm{LT}(p)/\mathrm{LT}(f_i)$
      $p := p - (\mathrm{LT}(p)/\mathrm{LT}(f_i))f_i$
      divisionoccurred := true
    ELSE
      $i := i + 1$
  IF *divisionoccurred* = false THEN
    $r := r + \mathrm{LT}(p)$
    $p := p - \mathrm{LT}(p)$
RETURN $q_1, \ldots, q_s, r$

intermediate q, r at each step

$f = q_1 f_1 + \cdots + q_s f_s + p + r$

← Checks if we have done division

Exactly one of div or rem occurs in each iteration

division step

rem. step

no $LT(f_i)$ divides $LT(p)$

$\therefore$ move $LT(p)$ into rem.

TO Prove we get what we want

$f = q_1 f_1 + \cdots + q_s f_s + p + r$ holds at every step

- Division step: $\Rightarrow$ $LT(f_i) \mid LT(p)$ for some i

$$q_i f_i + p = \underbrace{\left(q_i + \frac{LT(p)}{LT(f_i)}\right)}_{\text{new } q_i} f_i + \underbrace{\left(p - \frac{LT(p)}{LT(f_i)} f_i\right)}_{\text{new } p}$$

new step

$$p + r = \underbrace{(p - LT(p))}_{\text{new } p} + \underbrace{(r + LT(p))}_{\text{new } r}$$

$\therefore$ $f = q_1 f_1 + \cdots + q_s f_s + p + r$ holds

Must check that alg terminates

div step

$$p' = p - \frac{LT(p)}{LT(f_i)} f_i \qquad \text{(new } p\text{)}$$

new step

$$p' = p - LT(p)$$

$$\text{multdeg}(p') < \text{multdeg}(p)$$

$\therefore$ by well ordering alg. must terminate

(since otherwise we would have an infinite decreasing sequence)

Ideal membership

divide f by $F = f_1, \dots, f_s$ if $r = 0$

then $f = q_1 f_1 + \cdots + q_s f_s \Rightarrow f \in (f_1, \dots, f_s)$

$\therefore$ $r=0$ is sufficient, is it is nessesary for $f \in (f_1, \dots, f_s)$?

NO $\not\Rightarrow$

$f = xy^2 - x$

[Ex] $f_1 = xy - 1$, $f_2 = y^2 - 1 \in k[x,y]$ with lex

- div f by $F = f_1, f_2$ gives

$$xy^2 - x = f = \underbrace{y}_{=q_1} \cdot f_1 + \underbrace{0}_{=q_2} \cdot f_2 + \underbrace{(-x+y)}_{=r}$$

div f by $F = f_2, f_1$ gives

$$f = x \cdot f_1 + 0 \cdot f_2 + 0$$

$$\therefore \quad f \in (f_1, f_2)$$

Point is: Div. alg. only sometimes solves Ideal Membership

Always solve if $I = \langle$Groebner basis$\rangle$.

Monomials Ideals + Dickson Lemma

- For mon. ideals we can solve ideal description ↑ show all mon. ideals have a finite basis

Def: Let $A \subseteq \mathbb{N}^n$ (possibly infinite)

$I = (x^\alpha \mid \alpha \in A) \subseteq k[x_1, \dots, x_n]$

is a monomial ideal.

Ex] $I = (x^2z,\ y^3z,\ x^2yz,\ z^7) \subseteq k[x,y,z]$

Lemma] $I = (x^\alpha \mid \alpha \in A)$ a monomial ideal

$x^\beta \in I$ iff x^β is divisable by x^α for some $\alpha \in A$.

Proof: $\in$

If $x^\alpha \mid x^\beta$ for some $\alpha \in A \Rightarrow x^\beta = x^\gamma \cdot x^\alpha$

$\therefore x^\beta \in I$.

$\Rightarrow x^\beta \in I$

$x^\beta = \sum h_i x^{\alpha(i)}$ $\quad h_i \in k[x_1,\dots x_n]$, $\alpha(i) \in A$

But x^β is a monomial $\therefore x^\beta = h_i x^{\alpha(i)}$ for some i

∎

$x^\beta \in I \iff x^\beta = x^\gamma x^\alpha$ for some $\gamma \in \mathbb{N}^n$

$\Rightarrow \alpha + \mathbb{N}^n = \{\alpha + \gamma \mid \gamma \in \mathbb{N}^n\}$

↑ all exponents of monomials in I

Ex] $I = (x^4y^2,\ x^3y^4,\ x^2y^5)$