Groeb 1

§1 Term order on monomials

$x_1, \cdots, x_n$ variables $\quad \underline{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}, \quad \alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{N}^n$

Def 1 A <u>term order</u> on $\underline{x}^{\mathbb{N}^n} = \{\underline{x}^\alpha : \alpha \in \mathbb{N}^n\}$ = monomials in $x_1, \cdots, x_n$ is a linear order $<$ on $\underline{x}^{\mathbb{N}^n}$ which satisfies conditions (i) and (ii) below

(i) $1 < \underline{x}^\beta \quad \forall \beta \in \mathbb{N}^n \setminus \{0\}$

(ii) If $\underline{x}^\alpha < \underline{x}^\beta$, then $\underline{x}^\alpha \cdot \underline{x}^\gamma < \underline{x}^\beta \cdot \underline{x}^\gamma \quad \forall \gamma \in \mathbb{N}^n$

Example 1 The <u>lexicographic order</u> on $\underline{x}^{\mathbb{N}^n}$ with $x_1 > x_2 > \cdots > x_n$:

$\underline{x}^\alpha <_{lex} \underline{x}^\beta \iff \exists\, i$ with $1 \le i \le n$ s.t. $\alpha_j = \beta_j \quad \forall j = 1, \cdots, i-1$, and $\alpha_i < \beta_i$

i.e. $\beta - \alpha = (\underbrace{0, 0, \cdots, 0}_{i-1}, >0, *, \cdots, *)$

Example 2 The <u>degree lexicographic order</u> on $\underline{x}^{\mathbb{N}^n}$ with $x_1 > x_2 > \cdots > x_n$:

$\underline{x}^\alpha <_{deglex} \underline{x}^\beta \iff$ either $\alpha_1 + \cdots + \alpha_n < \beta_1 + \cdots + \beta_n$,

or $\alpha_1 + \cdots + \alpha_n = \beta_1 + \cdots + \beta_n$ and $\underline{x}^\alpha <_{lex} \underline{x}^\beta$

Example The <u>reverse lexicographic order</u> on $\underline{x}^{\mathbb{N}^n}$ with $x_1 > x_2 > \cdots > x_n$:

$\underline{x}^\alpha <_{revlex} \underline{x}^\beta \iff$ either $\alpha_1 + \cdots + \alpha_n < \beta_1 + \cdots + \beta_n$,

or $\alpha_1 + \cdots + \alpha_n = \beta_1 + \cdots + \beta_n$, and $\exists\, i$ with $1 \le i \le n$ s.t.

$\alpha_i > \beta_i$ and $\alpha_j = \beta_j \quad \forall j \ge i+1$. i.e. $\beta - \alpha = (*, \cdots, *, \underset{i}{<0}, 0, \cdots 0)$

Lemma 1 Let $<$ be a term order on $\underline{x}^{\mathbb{N}^n}$.

1) If $\underline{x}^\alpha \mid \underline{x}^\beta$, then $\underline{x}^\alpha \le \underline{x}^\beta$

2) The liner order $<$ on $\underline{x}^{\mathbb{N}^n}$ is a well-ordering

Let $<$ be a term order on $\underline{x}^{\mathbb{N}^n}$

Def Let k be a field, and write $k[\underline{x}] = k[x_1, \cdots, x_n]$. Let $f \in k[x_1, \cdots, x_n]$, $f \neq 0$

$f = a_1 \underline{x}^{\alpha_1} + \cdots + a_r \underline{x}^{\alpha_r} \quad r \ge 1, \ a_1, \cdots, a_r \neq 0, \ \underline{x}^{\alpha_1} > \underline{x}^{\alpha_2} > \cdots > \underline{x}^{\alpha_r}$

(1) $lm(f) = \underline{x}^{\alpha_1}$ = the leading monomial of f

(2) $lc(f) = a_1$ = the leading coefficient of f

(3) $lt(f) = a_1 \underline{x}^{\alpha_1}$ = the leading term of f

Groeb 2

Def 2 Let $A = k[x_1, \dots, x_n]$, k = a field. Let $A^m = A^{\oplus m} = A e_1 \oplus \cdots \oplus A e_m$ a free A-module of rank m

(1) A monomial in A^m is an element of the form $X \cdot e_i$, $X = \underline{x}^\alpha$ a monomial in A, $1 \le i \le m$

(2) A term order on A^m is a linear order on the set of all monomials in A^m which satisfies (i) + (ii) below

(i) If $T = X e_i$ is a monomial in A^m and $Z \neq 1$ is a monomial in A, then $T < ZT$

(ii) If T, U are monomials in A^m, $T < U$, and Z is a monomial in A, then $ZT < ZU$

(3) For an element $f = a_1 T_1 + \cdots + a_n T_n$, $T_1 > T_2 > \cdots > T_n$, $a_1, \dots, a_n \in k$ (nonzero), T_i = monomial in A^m

(a) $lm(f) = T_1$

(b) $lc(f) = a_1$

(c) $lt(f) = a_1 T_1$

Example. Let $<$ be a term order on A. Have two term orders on A^m

(i) TOP (term over position) X, Y monomials in A

$X e_i <_{TOP} Y e_j \iff$ either $X < Y$, or $X = Y$ and $i < j$

$(\leadsto e_1 <_{TOP} e_2 <_{TOP} \cdots <_{TOP} e_m)$

(ii) POT (position over term)

$X e_i <_{POT} Y e_j \iff$ either $i < j$, or $i = j$ and $X < Y$

(again $e_1 <_{POT} e_2 <_{POT} \cdots <_{POT} e_m$)

Def 3 Let $x_1, \dots, x_n$ and $y_1, \dots, y_m$ be two sets of variables. Let $<_x$ be a term order on $\underline{x}^{\mathbb{N}^n}$, and let $<_y$ be a term order on $\underline{y}^{\mathbb{N}^m}$.

(a) An **elimination order** $<$ on $\underline{x}^{\mathbb{N}^n} \cdot \underline{y}^{\mathbb{N}^m}$ with the x-variables larger than the y-variables is a linear order on $\underline{x}^{\mathbb{N}^n} \cdot \underline{y}^{\mathbb{N}^m}$ such that

$\underline{y}^\beta > \underline{x}^\alpha \cdot \underline{y}^{\beta'} \Rightarrow \alpha = 0 \qquad \forall \alpha \in \mathbb{N}^n, \ \forall \beta, \beta' \in \mathbb{N}^m$

(b) The elimination order on $\underline{x}^{\mathbb{N}^n} \cdot \underline{y}^{\mathbb{N}^m}$ attached to $<_x$ and $<_y$ with the x-variables larger than the y-variables is defined by:

$\underline{x}^\alpha \underline{y}^\beta < \underline{x}^{\alpha'} \underline{y}^{\beta'} \iff$ either $\underline{x}^\alpha <_x \underline{x}^{\alpha'}$, or $\underline{x}^\alpha = \underline{x}^{\alpha'}$ and $\underline{y}^\beta <_y \underline{y}^{\beta'}$.

Remark: One uses an elimination order with the x-variables larger than the y-variables to "eliminate the x-variables" in elimination theory. This means: given an ideal $I \subseteq k[x_1, \dots, x_n; y_1, \dots, y_m]$, compute the ideal $I \cap k[y_1, \dots, y_m] \subseteq k[y_1, \dots, y_m]$.

Remark on term orders on A^m: Both the TOP and POT are compatible with the given term order $<_A$ on A, in the following sense:

$X <_A Y \Rightarrow X \cdot T < Y \cdot T \quad \forall X, Y \in \underline{x}^{\mathbb{N}^n}, \forall$ monomial T in A^m

Remark A property of $<_{revlex}$ on $\underline{x}^{\mathbb{N}^n}$

$\underline{x}^\alpha > \underline{x}^\beta$ and $\alpha_r + \alpha_{r+1} + \dots + \alpha_n \geq 1 \Rightarrow \beta_r + \dots + \beta_n \geq 1$ $\quad \forall \alpha = (\alpha_1, \dots \alpha_n) \in \mathbb{N}^n$, $\beta = (\beta_1, \dots, \beta_n)$ $\quad \forall r, 1 \leq r \leq n$

In other words, if $\underline{x}^\alpha > \underline{x}^\beta$ and $\underline{x}^\alpha \in (x_r, x_{r+1}, \dots, x_n) \cdot k[\underline{x}]$, then $\underline{x}^\beta \in (x_r, x_{r+1}, \dots x_n) k[\underline{x}]$

Lemma 2 Every term order on monomials in A^m is a well-ordering (on the set of all monomials of A^m)

Hint of a direct proof of Lemma 1: The semi-group $\mathbb{N}^n$ satisfies the following finiteness property: Let $S \subseteq \mathbb{N}^n$ be a subset of $\mathbb{N}^n$ such that $S + \mathbb{N}^n = S$. Then $\exists$ elements $s_1, \dots, s_r \in S$ s.t. $S = \bigcup_{i=1}^{r} (s_i + \mathbb{N}^n)$

Groeb 3a

Def: Let $x_1, \dots, x_n ; y_1, \dots, y_m$ be two groups variables. Let $A = k[y_1, \dots, y_m]$

$B = k[x_1, \dots, x_n ; y_1, \dots, y_m] = A[x_1, \dots, x_n]$

Let $F = Be_1 \oplus \cdots \oplus Be_\ell$

An elimination term order for F is a term order for (monomials in) F with the x-variables larger than the y-variable is a term order for F such that $\underline{y}^{\beta} e_i > \underline{x}^{\alpha} \underline{y}^{\beta'} e_j \Rightarrow \alpha = 0 \quad \forall \alpha \in \mathbb{N}^n, \forall \beta, \beta' \in \mathbb{N}^m, \forall i, j \in \{1, \dots, \ell\}$

Remark. Let $<$ be an elimination order on $\underline{x}^{\mathbb{N}^n} \underline{y}^{\mathbb{N}^m}$ with the x-variables larger than the y-variables. Then the TOP order $<_{TOP}$ for F is an elimination order for F with the x-variables larger than the y-variables

Groeb 4

§2 The division algorithm

First, on $k[x_1, \cdots, x_n]$, with a given term order $<$

Description of the algorithm:

Input: $\vec{f} = (f_1, \cdots, f_s) \in k[x]^s$, $f_i \neq 0 \ \forall i$ and $f \in k[x]$

Output: $\vec{u} = (u_1, \cdots, u_s) \in k[x]^s$ and $r \in k[x]$ such that

- $f = u_1 f_1 + \cdots + u_s f_s + r$ $\quad r$ = remainder
- $\mathrm{Max}\left(lm(u_1) lm(f_1), \cdots, lm(u_s) lm(f_s), r \right) = lm(f)$
- r is <u>reduced</u> w.r.t. $\vec{f}$ in the sense that: or $r = a_1 x^{\alpha_1} + \cdots + a_m x^{\alpha_m}$ with $r \neq 0$, $\alpha_1 > \cdots > \alpha_m$ $a_i \neq 0 \ \forall i$

  and $lm(f_i) \nmid x^{\alpha_j} \quad \forall i = 1, \cdots, s, \ \forall j = 1, \cdots, m$

- Initialize: $u_1 = \cdots = u_s = 0$, $r := 0$, $h := f$ $\quad h$: variable to hold the polynomial to be divided by $\vec{f}$

Do ① unless $h = 0$

If $\exists i$ s.t. $lm(f_i) \mid lm(h)$, let $j = \min \{ i : lm(f_i) \mid lm(h) \}$ ← Variation here: Pick $j \in \{ i : lm(f_i) \mid lm(h) \}$

reassign values of $u_j \rightsquigarrow u_j + \dfrac{lt(h)}{lt(f_j)}$

$h \rightsquigarrow h - \dfrac{lt(h)}{lt(f_j)} f_j$; go back to ①

Otherwise $lp(f_j) \nmid lp(h) \quad \forall j = 1, \cdots, s$,

reassign $r \rightsquigarrow r + lt(h)$

$h \rightsquigarrow h - lt(h)$; go back to ①

(The effect is: test the next highest term of the old value of h)

Remark. 1) The output, $\vec{u}$ and $\vec{r}$, of the division algorithm generally depends on the order of the f_j's.

2) Will see: The output is independent of the order of the f_j's if $\{ f_j \}$ is a Groebner basis of the ideal $\sum_j f_j \, k[x_1, \cdots x_n)$

Notation: $f \xrightarrow{\vec{f}}_+ r$ "f is reduced to $\vec{r}$ after division by $\vec{f}$"

Groeb 5

§3 Groebner basis of ideals

Let $<$ be a term order on $A = k[x_1, \cdots x_n]$.

$\rightsquigarrow$ an increasing filtration of A by finite dim$^{\underline{l}}$ k-vector subspaces indexed by $\underline{x}^{\mathbb{N}^n}$: $\mathrm{Fil}_{\leq \underline{x}^\alpha} = \{0\} \cup \{f \in A \mid lm(f) \leq \underline{x}^\alpha\}$

Def^n 1 Let $I \subseteq k[x_1, \cdots, x_n]$ be an ideal, with the filtration $(I \cap \mathrm{Fil}_{\leq \underline{x}^\alpha})_{\alpha \in \mathbb{N}^n}$

Let $gr_{\leq}(I) := \bigoplus_{\alpha \in \mathbb{N}^n} (I \cap \mathrm{Fil}_{\leq \underline{x}^\alpha}) / (I \cap \mathrm{Fil}_{< \underline{x}^\alpha})$

↑ a graded ideal of $k[x_1, \cdots, x_n]$

Def^n 2 Let $G = \{g_1, \cdots, g_t\}$ be a finite subset of an ideal $I \subseteq k[\underline{x}]$ s.t. $g_i \neq 0 \ \forall i$.

We say that G is a Groebner basis of I if

(*) $\sum_i lm(g_i)\, k[\underline{x}] = gr_{\leq}(I)$. Equivalently, (**) $\forall f \in I$, $\exists\, i \in \{1, \cdots, t\}$ s.t. $lm(g_i) \mid lm(f)$.

(Exercise: Show that the two conditions are equivalent, and $I = \sum_{i=1}^t g_i\, k[\underline{x}]$.)

Theorem 3 Let $I \subseteq k[x_1, \cdots, x_n]$ be a non-zero ideal of $k[\underline{x}]$, and let $\vec{g} = (g_1, \cdots, g_t)$, $g_i \in I \ \forall i$. The following conditions are equivalent

(1) (**) $\forall f \in I$, $\exists\, i \in \{1, \cdots, t\}$ s.t. $lm(g_i) \mid lm(f)$

(2) $f \in I$ iff $f \xrightarrow{\vec{g}}_+ 0$ $\quad \forall f \in k[\underline{x}]$

(3) $f \in I$ iff $\exists\, h_1, \cdots, h_t \in k[\underline{x}]$ s.t. $f = \sum_{i=1}^t h_i g_i$ and $lm(f) = \max_{1 \leq i \leq t} (lm(h_i) \cdot lm(g_i))$ $\quad \forall f \in k[\underline{x}]$

(Note: We allow some (but not all) of the h_i's to be zero.)

(4) (*) $\sum_{i=1}^t lm(g_i) \cdot k[\underline{x}] = gr_{\leq}(I)$

(The equivalence of these conditions are not difficult.)

Groeb 6

Prop. Let $G = \{g_1, \dots, g_t\}$ be a finite set of non-zero elements of $k[x_1, \dots, x_n]$. Let $<$ be a term order on $x^{\mathbb{N}^n}$. Then G is a Groebner basis if and only if the remainder of division of f by G uniquely determined by f, $\forall f \in k[\underline{x}]$

i.e. in any expression $f = \sum_{i=1}^{t} h_i g_i + r$ with $lp(f) = Max(lp(h_i) \cdot lp(g_i), r)$ and r reduced w.r.t G

r is uniquely determined by f.

Pf. (a) Assume that G is a Groebner basis, and r_1, r_2 are two remainders

i.e. $f = \sum_i h_i g_i + r = \sum_i h_i' g_i + r'$ $\quad lp(f) = Max(lp(h_i)\, lp(g_i), r)$

and r, r' both reduced w.r.t. G $\quad = Max(lp(h_i)\, lp(g_i'), r')$

i.e. no term of r, r' is divisible by $lp(g_i)$ $\forall i$ ← This is the key

$\Rightarrow r - r' \in I = \sum_i g_i k[\underline{x}]$. If $r - r' \neq 0$, then $lp(r - r')$ is not divisible by $lp(g_i)$ $\forall i$ — contradiction.

(b) Assume that the remainder of division of f by G is unique determined by f $\forall f \neq 0$;

write $f \xrightarrow[G]{}_+ r$ for "f reduces to r"

Claim: This assumption implies: $\forall c \in k$ $\forall$ monomial $\underline{x}^\alpha$, $\forall g_i$, $g - c\underline{x}^\alpha g_i \xrightarrow[G]{}_+ r$ if $g \xrightarrow[G]{}_+ r$.

It is easy to see that (b) follows from the claim, $\because$ every element $f \in I$ $f \neq 0$

can be written as $f = \sum_{i=1}^{t} \sum_a \underline{x}^{\alpha_{i,a}} \cdot g_i$ (finite sum), so $f \xrightarrow[G]{}_+ 0$ $\forall f \in I$, $f \neq 0$.

It remains to prove the claim.

Separate two cases: (a) The monomial $\underline{x}^\alpha \cdot lm(g_i)$ appears in a term of f

(b) The monomial $\underline{x}^\alpha\, lm(g_i)$ does not appear in any term of f

Let's illustrate the argument in case (b):

Then do: $g - c \cdot \underline{x}^\alpha \cdot g_i \xrightarrow{g_i} (g - c \cdot \underline{x}^\alpha \cdot g_i) + c \cdot \underline{x}^\alpha \cdot g_i$ ✓

Groeb 7

§4 Buchberger's algorithm

k = a field

Def 1 For $0 \neq f, g \in k[x_1, \cdots, x_n]$, define $S(f,g) \in k[x_1, \cdots, x_n]$ by

$$S(f,g) = \frac{LCM(lm(f), lm(g))}{lt(f)} \cdot f - \frac{LCM(lm(f), lm(g))}{lt(g)} g.$$

Called the S-polynomial of f and g.

Theorem 2 (Buchberger) Let $G = \{g_1, \cdots, g_t\}$ be a finite set of non-zero elements of $k[x_1 \cdots x_n]$. Then G is Groebner basis of $\sum_i g_i k[x_1, \cdots, x_n]$ iff

$$S(g_i, g_j) \xrightarrow{G}_+ 0 \qquad \forall_{i \neq j}$$

Lemma Let $f_1, \cdots, f_s \in k[x_1 \cdots x_n]$ be non-zero polynomials s.t. $lm(f_i) = \underline{x}^{\alpha} \ \forall_{i=1 \cdots s}$.
Suppose that $c_1, \cdots, c_s \in k$ s.t. $f \overset{def}{=} \sum_{i=1}^{s} c_i f_i$ has $lm(f) < \underline{x}^{\alpha}$.
i.e. $\sum_{i=1}^{s} c_i \cdot lc(f_i) = 0$. Then $f \in \sum_{i=1}^{s-1} k \cdot S(f_i, f_{i+1})$

pf: Let $a_i = lc(f_i)$

$$f = c_1 f_1 + \cdots + c_s f_s$$
$$= c_1 a_1 \left(\frac{f_1}{a_1}\right) + \cdots + c_s a_s \left(\frac{f_s}{a_s}\right)$$
$$= c_1 a_1 \left(\frac{f_1}{a_1} - \frac{f_2}{a_2}\right) + (c_1 a_1 + c_2 a_2)\left(\frac{f_2}{a_2} - \frac{f_3}{a_3}\right) + \cdots + (c_1 a_1 + \cdots + c_i f_i)\left(\frac{f_i}{a_i} - \frac{f_{i+1}}{a_{i+1}}\right)$$
$$+ \cdots + (c_1 a_1 + \cdots + c_{s-1} a_{s-1})\left(\frac{f_{s-1}}{a_{s-1}} - \frac{f_s}{a_s}\right) + \underbrace{(c_1 a_1 + \cdots + c_s a_s)}_{=0} \frac{f_s}{a_s}$$
$$= \sum_{i=1}^{s-1} \left(\sum_{j=1}^{i} c_j a_j\right) \cdot S(f_i, f_{i+1}) \qquad \text{q.e.d.}$$

Proof of Thm 2 "only if" is trivial, $\because S(g_i, g_j) \in \sum_{\ell=1}^{t} g_\ell k[x_1 \cdots, x_n]$

Given $f \in I = \sum_{i=1}^{t} g_i k[\underline{x}]$

"if": Pick $h_1, \cdots, h_t \in k[\underline{x}]$ s.t. $f = \sum_{i=1}^{t} h_i g_i$ and

$$\underline{x}^{\alpha} := \max_{1 \leq i \leq t} \left(lm(h_i) \cdot lp(g_i)\right) \leq \max_{1 \leq i \leq t} \left(lm(h_i') \cdot lm(g_i)\right) \quad \forall h_1', \cdots, h_t' \in k[\underline{x}] \text{ s.t. } f = \sum_{i=1}^{t} h_i' \cdot g_i$$

Claim: $\underline{x}^{\alpha} = lp(f)$ (Claim $\Rightarrow f \xrightarrow{G}_+ 0 \ \forall f \in I$, so G is a Groebner basis)

Suppose that $\underline{x}^{\alpha} > lp(f)$. Will find a better representation of f with a smaller $\underline{x}^{\alpha}$.

Let $S = \{ i \mid lm(h_i) \cdot lm(g_i) = \underline{x}^{\alpha} \}$

Consider $g := \sum_{i \in S} lt(h_i) \cdot g_i = \sum_{i \in S} lc(h_i) \cdot lm(h_i) \cdot g_i$

Lemma $\Rightarrow g \in \sum_{i,j \in S} k \cdot S(lm(h_i) g_i, lm(h_j) \cdot g_j)$

$$S(lm(h_i)\cdot g_i,\ lm(h_j)g_j) = \frac{\underline{x}^\alpha}{lt(lm(h_i)\cdot g_i)}\, lm(h_i)\cdot g_i - \frac{\underline{x}^\alpha}{lt(lm(h_j)\cdot g_j)}\, lm(h_i)\cdot g_i$$
$$= \frac{\underline{x}^\alpha}{lt(g_i)}\, g_i - \frac{\underline{x}^\alpha}{lt(g_j)}\cdot g_j = \frac{\underline{x}^\alpha}{LCM(lm(g_i), lm(g_j))}\cdot S(g_i, g_j)$$

Since $S(g_i,g_j) \xrightarrow{G}_+ 0$, it follows that $\frac{\underline{x}^\alpha}{LCM(lm(g_i), lm(g_j))}\cdot S(g_i,g_j) \xrightarrow{G}_+ 0$

$\exists\, h_{i,j,\mu} \in k[x_1,\dots,x_n] \quad \mu=1,\dots,t$ s.t.

$\Rightarrow \forall i,j \in S,\ S(lm(h_i)g_i,\ lm(h_j)g_j) = \sum_{\mu=1}^{t} h_{i,j,\mu}\cdot g_\mu$ with $lm(h_{i,j,\mu})\cdot lm(g_\mu) < \underline{x}^\alpha$

$\therefore lm(S(g_i,g_j)) < LCM(lm(g_i), lm(g_j))$

This gives us another expression

$$f = \sum_{i,j\in S}\sum_{\mu} c_{i,j,\mu}\cdot h_{i,j,\mu}\cdot g_\mu + \sum_{i\notin S} h_i\cdot g_i \qquad c_{i,j,\mu}\in k$$

s.t. $\quad Max\left(\left\{lm(h_{i,j,\mu})\, lm(g_\mu) \;\middle|\; \substack{i,j\in S \\ 1\le\mu\le t}\right\} \cup \left\{ lm(h_i)\, lm(g_i) \;\middle|\; i\notin S\right\}\right) < x^\alpha$

This is a contradiction. QED

Buchberger's theorem gives an effective criterion on whether a given set of generators of an ideal $I \subseteq k[x_1,\dots,x_n]$ is a Groebner basis. It also leads to an algorithm for constructing a Groebner basis of a given ideal I, starting with a set of generators of I:

Begin with a set $\{f_1,\dots,f_s\}$ of generators of an ideal $I \subseteq k[\underline{x}]$ and a term order of $\underline{x}^{\mathbb{N}^n}$

Compute $S(f_i,f_j)$ and $S(f_i,f_j) \xrightarrow{\vec{f}}_+ r_{ij}$

$\vec{f} = (f_1,\dots,f_s)$

If $r_{ij} = 0 \quad \forall i\neq j$, $(f_1,\dots,f_s)$ is a Groebner basis

Otherwise, expand $f_1,\dots,f_s$ include the first non-zero r_{ij} one encounters. and repeat this.

Prop: The above algorithm stops eventually:

At the i-th run we get a finite set of generators G_n. If G_n is not a Groebner basis, we get an element $r_n \in I$, reduced w.r.t. G_n. So $lm(r_n) \notin \sum_{f\in G_n} lm(f)\cdot k[\underline{x}] = J_n$ Thus $J_n \subsetneq J_{n+1}$. Such an ascending chain must stop. QED.

§5

Uniqueness of reduced Groebner basis

(analog of: row reduced echelon form in linear algebra)

Def 1. a) A Groebner basis $G=\{g_1,\dots,g_t\}$ for an ideal $I \in k[x_1,\dots,x_n]$ is minimal if $lc(g_i)=1$ $\forall i=1,\dots t$ and $lt(g_i) \nmid lt(g_j)$ $\forall i \neq j$

b) A Groebner basis $G=\{g_1,\dots,g_t\}$ of I is reduced if $lc(g_i)=1$ $\forall i=1,\dots,t$ and $lt(g_i)$ does not divid any term of g_j $\forall i \neq j$.

(Clearly every reduced Groebner basis is minimal)

Prop 2. Let $G=\{g_1,\dots,g_t\}$ and $G'=\{g'_1,\dots,g'_s\}$ be Groebner basis of the same ideal $I \leq k[x_1,\dots,x_n]$. Then $s=t$, and $\exists!\ \sigma \in S_t$ s.t. $lt(g_i) = lt(g'_{\sigma(i)})$ $\forall i=1,\dots,t$

(Exer. Note that $\{lt(g_1),\dots,lt(g_t)\}$ is the set of extremal points of $\{\alpha \in \mathbb{N}^n \mid x^\alpha \in gr_\leq(I)\}$

Theorem 3 Fix a term order on $x^{\mathbb{N}^n}$. Every non-zero ideal I of $k[x_1,\dots,x_n]$ has a unique reduced Groebner basis

Pf: Existence easy.

Uniquess: Let $\{g_1,\dots,g_t\}$ and $\{g'_1,\dots,g'_t\}$ be minimal Groebner bases of I s.t. $lt(g_i)=lt(g'_i)$ $\forall i=1,\dots t$

Show: $g_1=g'_1$. If $g_1-g'_1 \neq 0$, $lm(g_1-g'_1)$ is divisible by $lm(g_i)$ for some i. But $i \notin \{2,3,\dots t\}$ by assumption, so $lm''(g'_i)$

$lm(g_1) \mid lm(g_1-g'_1)$, hence $lm(g_1)=lm(g'_1) < lm(g_1-g'_1)$, a contradiction. q.e.d

Groeb 10

§6. Generalization to free modules of finite rank over $k[x_1,\cdots,x_n]$, k = a field

Division algorithm on A^m, $A = k[x_1,\cdots,x_n]$, w.r.t. a term order $<$ on A^n

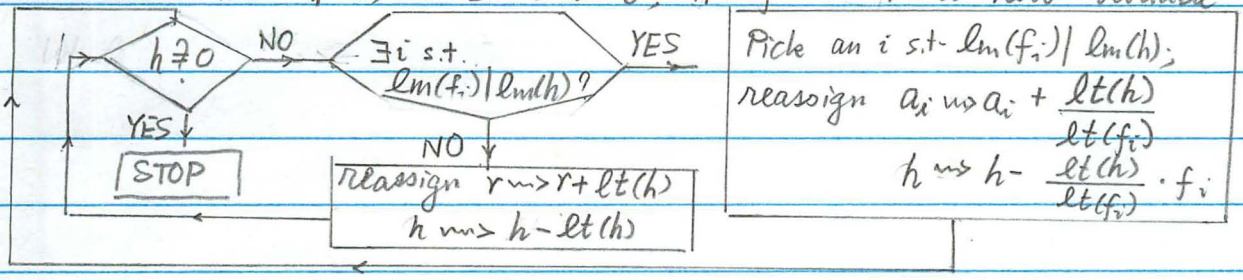
Input: $f, f_1, \cdots, f_s \in A^m$ $\quad f_i \neq 0$ for $i=1,\cdots,s$

Output: $a_1,\cdots,a_s \in A$, $r \in A^m$ with $f = a_1 f_1 + \cdots + a_s f_s + r$

and • r: reduced w.r.t. $\{f_1,\cdots,f_s\}$, i.e. either $r=0$ or $r\neq 0$ and no term of r is divisible by $lm(f_i)$ $\forall i=1,\cdots,s$

• $\max\left(lm(a_i f_i)_{1\le i\le s}, lm(r)\right) = lm(f)$

Initialization: $a_1=0,\cdots,a_s=0$, $r=0$, $h=f$ $\quad h$: a new variable



- The above division algorithm allows "some randomness" in the step which involves picking an element of $\{i : lm(f_i) \mid lm(h)\}$
- When the algorithm stops, the values in the registers $a_1,\cdots,a_s, r$ are the required output. Notation: $f \xrightarrow{\{f_1,\cdots,f_s\}}_+ r$

Def^n 1 Let $0 \neq M \subseteq A^m$ be an A-submodule. A subset $G=\{g_1,\cdots,g_t\} \subseteq M$ with $g_i \neq 0$ $\forall i=1,\cdots,t$ is a Groebner basis of M w.r.t. a given term order $<$ on A^m if $\forall f \in A^m$, $\exists\ i \in \{1,\cdots,t\}$ s.t. $lm(g_i) \mid lm(f)$.

Thm 2 Let $0 \neq M \subseteq A^m$ be an A-submodule, and $G=\{g_1,\cdots,g_t\}$ $g_i \neq 0$ $\forall i$, $<$: a term order on A^m

The following are equivalent

(i) G is a Groebner basis of M

(ii) $f \in M \iff f \xrightarrow{G}_+ 0$ $\quad (0 \neq f \in M)$

(iii) $f \in M \iff \exists\ h_1,\cdots,h_t \in A$ s.t. $f = h_1 g_1 + \cdots + h_t g_t$ and $lm(f) = \max_{1\le i\le t}\left(lm(h_i)\cdot lm(g_i)\right)$

(iv) $\forall\ 0 \neq f \in A^m$, if $f \xrightarrow{G}_+ r_1$ and $f \xrightarrow{G}_+ r_2$ and r_1, r_2 are reduced mod G, then $r_1 = r_2$

(v) $\sum A \cdot lm(g_i) = gr_<(M)$

Groeb 11

Def 3 For $f, g \in A^m$, $f \neq 0$, $g \neq 0$, define $S(f,g) \in A^m$ by

$$S(f,g) = \frac{LCM(lm(f), lm(g))}{lt(f)} f - \frac{LCM(lm(f), lm(g))}{lt(g)} g$$

Note: If $lm(f) = X^{\alpha} \cdot e_i$, $lm(g) = X^{\beta} \cdot e_j$ and $i \neq j$, then $LCM(lm(f), lm(g)) = 0$ by definition, and $S(f,g) = 0$

Theorem 4 Let M be a non-zero A-submodule of A^m, $G = \{g_1, \dots g_k\} \subseteq M$. $g_i \neq 0 \ \forall i$

Then G is a Groebner basis of M iff

$$S(g_i, g_j) \xrightarrow[+]{G} 0 \qquad \forall i, j \text{ with } i \neq j$$

Algorithm to enhance a set of generators of M to a Groebner basis: At each stage, compute $S(f_i, f_j) \xrightarrow[+]{G} r_{ij}$. Whenever one get a non-zero remainder r_{ij}, add r_{ij} to the set of generators and repeat. After a finite number of steps, all remainders are zero, and we have a Groebner basis of M.

Groeb 12

§7. First Applications of Groebner bases

(1) The ideal membership problem: determine where a given element $f \in k[x_1,\dots x_n]$ lies in an ideal I, I defined by a set of generators.
First compute a Groebner basis of I using Buchberger's algorithm, then perform a division to see whether $f \xrightarrow{G}_+ 0$

(2) Solve polynomial equations: Given $f_1,\dots,f_m \in k[x_1,\dots x_n]$, say $m \geq n$
Find common zeros of $\sum_i f_i k[x]$
Use $<_{lex}$ with $x_1 > x_2 > \dots > x_n$
Key: $<_{lex}$ is an elimination order
$\rightsquigarrow$ Let $G = \{g_1,\dots,g_t\}$ be a Groebner basis of $\sum_i f_i k[x_1,\dots,x_n] = I$
Then $G \cap k[x_n]$ is a Groebner basis of $I \cap k[x_n]$
$G \cap k[x_{n-1}, x_n]$ is a Groebner basis of $I \cap k[x_{n-1}, x_n]$
$G \cap k[x_i, x_{i+1},\dots,x_n]$ is a Groebner basis of $I \cap k[x_i, x_{i+1},\dots,x_n]$

(3) Elimination: $I = (f_1,\dots,f_\ell) \subseteq k[x_1,\dots,x_n;y_1,\dots,y_m]$
$<$: an elimination order on $x^{\mathbb{N}^n} \cdot y^{\mathbb{N}^m}$ with the x-variables larger than the y-var.
Let $G = \{g_1,\dots,g_t\}$ be a Groebner basis for I
$\rightsquigarrow$ $G \cap k[y_1,\dots,y_m]$ is a Groebner basis for $I \cap k[y_1,\dots,y_m]$
("eliminate the x-variables")

(4) Intersection of ideals
Lemma: Let $I, J \subseteq k[x_1,\dots,x_n]$ be ideals. Let w be a new variable.
Then $I \cap J = \left(w \cdot I \cdot k[x_1,\dots,x_n,w] + (1-w) \cdot J \cdot k[x_1,\dots,x_n,w]\right) \cap k[x_1,\dots,x_n]$
(Exer.)
This Lemma + elimination gives a method to compute $I \cap J$

(5) Compute the $\overset{gcd}{lcm}$ of two non-zero elements $f, g \in k[x_1, \dots, x_n]$

(Recall that $k[x_1, \dots, x_n]$ is a UFD)

$lcm(f,g) \cdot k[x_1, \dots, x_n] = f\,k[x_1, \dots, x_n] \cap g\,k[x_1, \dots, x_n]$

$gcd(f,g) = f \cdot g \,/\, lcm(f,g)$

(6) Compute $(I : J)$, $I, J \neq 0$ ideals of $k[x_1, \dots, x_n]$

Let $J = \sum_{i=1}^{\ell} f_i \cdot k[x_1, \dots, x_n]$ $\quad f_i \neq 0 \ \forall_i$

(a) $(I : J) = \bigcap_{i=1}^{\ell} (I : f_i)$

(b) $(I : f_i) = \frac{1}{f_i} \cdot (I \cap f_i)$

(7) Find an explicit k-basis of $k[x_1, \dots, x_n]/I$, $\quad I = \sum_{i=1}^{\ell} f_i\, k[x_1, \dots, x_n]$

or more generally, find an explicit k-basis of $k[x_1, \dots, x_n]^{\oplus m}/M$,

where M is a $k[x_1, \dots, x_n]$-submodule of $k[x_1, \dots, x_n]^{\oplus m}$.

Let $<$ be a term order on $k[x_1, \dots, x_n]^{\oplus m}$, and let $G = \{g_1, \dots, g_t\}$ be a reduced Groebner basis of M. Then the image in $k[x_1, \dots, x_n]^{\oplus m}/M$ of

$$\left\{ \pm x^{\alpha} \cdot e_i \;\middle|\; \pm x^{\alpha} \cdot e_i \text{ is not divisible by } lm(g_j) \ \forall_{j=1,\dots,t} \right\}$$

is a k-basis of $k[x_1, \dots, x_n]^{\oplus m}/M$

(8) Compute $\ker\left(\psi : k[y_1, \dots, y_m] \to k[z_1, \dots z_n]\right)$ $\quad \psi$: a k-linear ring homom.

Let $f_i \overset{def}{=} \psi(y_i)$, $\quad i = 1, \dots, m$

Consider the ideal $\sum_{i=1}^{m} (y_i - f_i(x_1, \dots, x_n))\, k[x_1, \dots, x_n; y_1, \dots, y_m] =: J$

Then $\ker(\psi) = J \cap k[y_1, \dots, y_m]$

Groeb 14

§8 Syzygies (= linear relations)

Def 1 Let M be a (left) R-module and let $u_1, \cdots, u_n \in M$ be elements of M. Define the relation module, or the syzygy module $Syz(u_1, \cdots, u_n)$ by

$$Syz(u_1, \cdots, u_n) = \{ (a_1, \cdots, a_n) \in R^n \mid \sum_{i=1}^n a_i u_i = 0 \},$$

i.e. $$0 \to Syz(u_1, \cdots, u_n) \to R^n \longrightarrow M$$
$$(a_1, \cdots a_n) \mapsto \sum_{i=1}^n a_i u_i$$

Lemma 2 Let M be an R-module, let P and Q be projective R-modules. Let $p: P \twoheadrightarrow M$ and $q: Q \twoheadrightarrow M$ be R-linear surjections, $R := Ker(p)$, $S := Ker(Q)$. Let $f: P \to Q$ and $g: Q \to P$ be R-linear maps st. $p = q \circ f$ and $q = p \circ g$

$$\begin{array}{ccccc} S & \hookrightarrow & Q & \overset{q}{\twoheadrightarrow} & M \\ & & f \uparrow \downarrow g & & \| \\ R & \hookrightarrow & P & \underset{p}{\twoheadrightarrow} & M \end{array}$$

Then: $R = Im(id_P - g \circ f) + g(S)$

Rmk: In the case P, Q are both free modules of finite rank, Lemma 2 tells us how to express the syzygy module module R of a set $(u_1, \cdots, u_s)$ of generators of M in terms of the syszgy module S of another set $(v_1, \cdots, v_t)$ of generators of M

Pf of Lemma 2 $p = q \circ f = p \circ g f$ $\rightsquigarrow Im(id_P - g \circ f) \subseteq R$, clearly $g(S) \subseteq R$

$q = p \circ g = q \circ f \circ g$

$x \in R \Rightarrow f(x) \in S \Rightarrow x = \underbrace{x - g(f(x))}_{\in Im(id_P - g \circ f)} + \underbrace{g(f(x))}_{\in g(S)}$

q.e.d.

Prop 3 Let $Y_1, \cdots, Y_s$ be non-zero monomials in $A^m = k[X_1, \cdots, X_n]^m$

$Syz(Y_1, \cdots, Y_s) \subseteq A\vec{v}_1 \oplus \cdots \oplus A\vec{v}_s = A^s$

Then $$Syz(Y_1, \cdots, Y_s) = \sum_{0 \le i < j \le s} A \cdot \left(\frac{lcm(Y_i, Y_j)}{Y_i} \vec{v}_i - \frac{lcm(Y_i, Y_j)}{Y_j} \right)$$

Pf. $Syz(Y_1, \cdots, Y_s)$ = A-span of monomials in $Syz(Y_1, \cdots, Y_s) \subseteq A\vec{v}_1 \oplus \cdots \oplus A\vec{v}_s = A^s$ because $Y_1, \cdots, Y_s$ are monomials in A^m

Groeb 15

Let $h_1, \dots, h_s$ be terms in A s.t. $h_1 Y_1 + \dots + h_s Y_s = 0$, i.e. $\sum_j h_j \vec{v}_j \in Syz(Y_1, \dots, Y_s)$

Must show: $\sum_j h_j \vec{v}_j \in \sum_{i,j} A\left(\frac{lcm(Y_i, Y_j)}{Y_i}\vec{v}_i - \frac{lcm(Y_i, Y_j)}{Y_j}\vec{v}_j\right)$

$\forall i = 1, \dots, n$, let $S_i = \{ j \mid Y_j \in A \cdot \vec{e}_i \}$. $\rightsquigarrow \sum_{j \in S_i} h_j Y_j = 0$ Write $Y_j = z_j \cdot e_i$, $z_j \in A$ $\forall j \in S_i$

Suffices to show:

$$\sum_{j \in S_i} h_j \vec{v}_j \in \sum_{j, j' \in S_i} A\left(\frac{lcm(Y_j, Y_{j'})}{Y_j}\vec{v}_j - \frac{lcm(Y_j, Y_{j'})}{Y_{j'}}\vec{v}_{j'}\right)$$

Write $S_i = \{ j_1, j_2, \dots, j_a \}$ (distinct), $h_{j_\mu} = c_\mu \cdot X_\mu$ $c_\mu \in k$, X_μ: monomial in A, $z_{j_\mu} = d_\mu W_\mu$

May assume $\begin{cases} c_a \neq 0 \\ X_\mu \cdot W_\mu = X, \ \forall \mu = 1, \dots, a \end{cases}$ (Otherwise, decompose S_i into a disjoint union of subsets)

Know: $c_1 d_1 + \dots + c_a d_a = 0$

$$\rightsquigarrow \sum_{j \in S_i} h_j \vec{v}_j = c_1 X_1 \vec{v}_{\mu_1} + \dots + c_a X_a \vec{v}_{\mu_a}$$

$$= c_1 d_1 \frac{X}{d_1 W_1}\vec{v}_{\mu_1} + \dots + c_a d_a \frac{X}{d_a W_a}\vec{v}_{\mu_a}$$

Write as a telescoping sum

$$= c_1 d_1 \frac{X}{lcm(W_1, W_2)} \cdot \left(\frac{lcm(W_1, W_2)}{d_1 W_1}\vec{v}_{\mu_1} - \frac{lcm(W_1, W_2)}{d_2 W_2}\vec{v}_{\mu_2}\right)$$

$$+ (c_1 d_1 + c_2 d_2) \frac{X}{lcm(W_2, W_3)}\left(\frac{lcm(W_2, W_3)}{d_2 W_2}\vec{v}_{\mu_2} - \frac{lcm(W_2, W_3)}{d_3 W_3}\vec{v}_{\mu_3}\right)$$

$$+ \dots$$

$$+ (c_1 d_1 + \dots + c_{a-1} d_{a-1}) \frac{X}{lcm(W_{a-1}, W_a)}\left(\frac{lcm(W_{a-1}, W_a)}{d_{a-1} W_{a-1}}\vec{v}_{a-1} - \frac{lcm(W_{a-1}, W_a)}{d_a W_a}\vec{v}_a\right)$$

$$+ \underbrace{(c_1 d_1 + \dots + c_a d_a)}_{0} \frac{X}{c_a d_a}$$

QED.

Note: This proof is similar to the Lemma in §2, before Buchberger's theorem.

Groeb 16

Theorem 4 Let $(g_1, \cdots, g_t)$ be a finite sequence of non-zero elements in A^m which is a Groebner basis of $\sum_{j=1}^{t} A g_j$ w.r.t a term order $<$ on $A^{\oplus m}$.

Define, for each $i \neq j$,

$$S(g_i, g_j) := \frac{lcm\left(lm(g_i), lm(g_j)\right)}{lm(g_i)} g_i - \frac{lcm\left(lm(g_i), lm(g_j)\right)}{lm(g_j)} g_j$$

and write $S(g_i, g_j)$ as

$$S(g_i, g_j) = \sum_{\nu=1}^{t} h_{ij\nu}\, g_\nu \qquad h_{ij\nu} \in A$$

$$\max_{\nu} \left(lm(h_{ij\nu}) \cdot lm(g_\nu)\right) = lm\, S(g_i, g_j)$$

Then

$$(*) \qquad Syz(g_1, \cdots, g_t) = \sum_{i,j} A \cdot \left(\frac{lcm\left(lm(g_i), lm(g_j)\right)}{lm(g_i)} \vec{v}_i - \frac{lcm\left(lm(g_i), lm(g_j)\right)}{lm(g_j)} \vec{v}_j - \sum_{\nu=1}^{t} h_{ij\nu} \vec{v}_\nu \right)$$

$$\| \qquad\qquad S(g_i, g_j) \in A\vec{v}_1 + \cdots + A\vec{v}_t$$

Pf: Suppose that $Syz(g_1, \cdots g_t) \neq$ r.h.s. of $(*)$

Let $X = \operatorname{Min}_{\sum_j u_j \vec{v}_j \in Syz(g_1, \cdots g_t) \setminus \text{rhs of } (*)} \left(\max_{1 \le j \le t} \left(lm(u_j) \cdot lm(g_j) \right) \right)$, a monomial in $A\vec{v}_1 + \cdots + A\vec{v}_t$

$\rightsquigarrow$ Have $u_1 \vec{v}_1 + \cdots + u_t \vec{v}_t \in Syz(g_1, \cdots, g_t) \setminus$ rhs of $(*)$

s.t. $\max_{1 \le j \le t} \left(lm(u_j)\, lm(g_j) \right) = X$

Will produce an element $u_1' \vec{v}_1 + \cdots + u_t' \vec{v}_t \equiv u_1 \vec{v}_1 + \cdots + u_t \vec{v}_t \pmod{\text{rhs of } *}$

with $\max_{1 \le j \le t} \left(lm(u_j') \cdot lm(g_j) \right) < X$, which is a contradiction.

Define

- $S := \left\{ j \in \{1, 2, \cdots t\} \;\middle|\; lm(u_j)\, lm(g_j) = X \right\}$
- $w_j = \begin{cases} u_j & \text{if } j \notin S \\ u_j - lt(u_j) & \text{if } j \in S \end{cases}$

Have: $\sum_{j \in S} lt(w_j) \cdot lm(g_j) = 0$, i.e. $\sum_{j \in S} lt(w_j) \vec{v}_j \in Syz\left(lm(g_1), \cdots, lm(g_t)\right)$

Prop 3 $\Rightarrow$ $\exists\ (a_{ij})_{i,j \in S}$ s.t. $\sum_{j \in S} lt(w_j) \vec{v}_j = \sum_{i,j \in S} a_{ij} \left(\frac{lcm(lm(g_i), lm(g_j))}{lm(g_i)} \vec{v}_i - \frac{lcm\left(lm(g_i), lm(g_j)\right)}{lm(g_j)} \vec{v}_j \right)$

a_{ij} = a term in A

$lm(a_{ij}) \cdot lcm\left(lm(g_i), lm(g_j)\right) = X$

if $a_{ij} \cdot lcm\left(lm(g_i), lm(g_j)\right) \neq 0$

$$\Rightarrow \sum_{j=1}^{t} u_j \vec{v}_j - \sum_{i,j \in S} a_{ij}\, s(g_i, g_j) \in Syz(g_1, \cdots, g_t)$$

$$\| \quad \vdots$$

$$\sum_{j=1}^{t} u_j' \vec{v}_j \quad \text{and} \quad \max_{1 \le j \le t} \left(lm(u_j') \cdot lm(g_j) \right) < X. \qquad \text{QED}$$

How to compute the syzygy module $Syz(u_1, \cdots, u_s)$ of a set $(u_1, \cdots, u_s)$ of generators $u_1, \cdots, u_s$ of a submodule $M \subseteq A^m$, $A = k[x_1, \cdots, x_n]$:

1) Expand the given set of generators $u_1, \cdots, u_s$ to a Groebner basis $(g_1, \cdots, g_t)$ of M w.r.t. a chosen term order on A^m (Buchberger's algorithm)
2) By Theorem 4, the process of computing $(g_1, \cdots, g_t)$ during the execution of the Buchberger's algorithm also furnishes a set of generators of $Syz(g_1, \cdots, g_t)$
3) Use Lemma 2 to get a set of generators of $Syz(u_1, \cdots, u_s)$.

Remark: Here we need to find $(a_{ij}) \in M_{s \times t}(A)$ such that $g_j = \sum_{i=1}^{s} a_{ij} u_i$, which one obtains by tracking the computation of the Groebner basis $(g_1, \cdots, g_t)$.

§9 Applications of syzygies

(1) Compute the intersection of two ideals $I, J \leq k[x_1, \dots, x_n] = A$

Let $I = \sum_{i=1}^{s} f_i A$, $J = \sum_{j=1}^{s} g_j A$.

Consider the Syzygy module $Syz\left(\begin{bmatrix}1\\1\end{bmatrix}, \begin{bmatrix}f_1\\0\end{bmatrix}, \dots, \begin{bmatrix}f_s\\0\end{bmatrix}, \begin{bmatrix}0\\g_1\end{bmatrix}, \dots, \begin{bmatrix}0\\g_t\end{bmatrix}\right)$ of $u_i \in A^2 \ \forall i$, where the vectors are $u_0, u_1, \dots, u_s, u_{s+1}, \dots, u_{s+t}$ respectively.

Let $\left(\sum_{\mu=0}^{s+t} h_{\ell\mu} \vec{v}_\mu\right)_{1\leq \ell \leq r}$ be a set of generators of $Syz(u_0, u_1, \dots u_s, u_{s+1}, \dots, u_{s+t})$

Then $I \cap J = \sum_{\ell=1}^{r} h_{\ell 0} A$

($h_{\ell 0}$ = the first coord of the syzygy $h_{\ell 0}\vec{v_0} + h_{\ell 1}\vec{v_1} + \dots + h_{\ell, s+t}\vec{v}_{s+t}$)

(2) Compute the intersection $M \cap N$ of two A-submodules of A^m, $A = k[x_1, \dots, x_n]$

(3) Let $I = f_1 A + f_2 A + f_3 A$, $J = g_1 A + g_2 A$, compute $(I : J)$ "ideal quotient"

Consider $Syz\left(\begin{bmatrix}f_1\\f_2\\f_3\end{bmatrix}, \begin{bmatrix}g_1\\0\\0\end{bmatrix}, \begin{bmatrix}g_2\\0\\0\end{bmatrix}, \begin{bmatrix}0\\g_1\\0\end{bmatrix}, \begin{bmatrix}0\\g_2\\0\end{bmatrix}, \begin{bmatrix}0\\0\\g_1\end{bmatrix}, \begin{bmatrix}0\\0\\g_2\end{bmatrix}\right)$ $\quad A = k[x_1, \dots, x_n]$

(the vectors being $u_0, u_1, u_2, u_3, u_4, u_5, u_6$)

The ideal of A generated by the first coordinates $(h_{\ell 0})_{1\leq \ell\leq r}$ of a set $\left(\sum_{\mu=0}^{6} h_{\ell\mu}\vec{v}_\mu\right)_{1\leq\ell\leq r}$ of generators of $Syz(u_0, u_1, \dots, u_6)$ is equal to $(I : J)$.

(4) Let $M \leq A^m$ be an A-submodule of A^m, compute $Ann_A(A/M)$

(5) Let M, N be finitely generated A-modules, $A = k[x_1, \dots, x_n]$.

Compute (a) A free resolution of M

(b) $Ext_A^i(M, N)$, $Tor_i^A(M, N)$

Groeb 19

Hilbert syzygy theorem:

Let M be a finitely generated graded A-module, $A = k[x_1, \dots, x_n]$, k = a field.
There exists a finite *minimal* resolution

$$0 \to F_s \xrightarrow{\partial_s} \cdots \longrightarrow F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\partial_0} M \to 0 \qquad \text{with} \quad s \leq n$$

F_i = finite free graded A-module

That this resolution is minimal means:

$$\forall\, i \text{ with } 0 \leq i \leq s-1, \quad \dim_k \left(\operatorname{Im}(\partial_i) \Big/ (x_1, \dots, x_n) \cdot \operatorname{Im}(\partial_i) \right) = \operatorname{rank}_A(F_i)$$

$\dim_k$ = minimal number of generators of $\operatorname{Im}(\partial_i)$

Corollary Let M be a finite A-module, $A = k[x_1, \dots x_n]$, k = a field.
There exists a finite free resolution

$$0 \to F_s \xrightarrow{\partial_s} \cdots \longrightarrow F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\partial_0} M \to 0 \qquad \text{with} \quad s \leq n+1$$

$$\left(M \cong \tilde{M} \otimes_{k[x_0, x_1, \dots, x_n]} k[x_0, x_1, \dots x_n]/(1-x_0) \right)$$

Remark 1) It is a deep result that every finitely generated projective $k[x_1, \dots, x_n]$ is free (Serre's conjecture, Theorem of Quillen – Suslin).
(k a field)

$\Rightarrow$ Every finite A-module admits a finite free resolution of length $\leq n$.

2) There is a *constructive* proof of the above result, using method involving Groebner basis. See Theorem 3.10.4, p. 197 of "An Introduction to Gröbner Bases" by Adams and Loustaunau