A Tutorial on Polynomial Ideals and Algebraic Varieties

Marc Moreno Maza

CS 9652a - Algorithms and software for symbolic solvers of polynomial systems

October 25, 2017

An overview of this tutorial

- **Main objective:** an introduction for non-experts.
- **Prerequisites:** some familiarity with linear algebra, univariate polynomials (division, Euclidean Algorithm, roots of a polynomial), polynomial rings (partial degree, ideal).
- **Outline:**
  - algebraic varieties,
  - term orders,
  - multivariate division,
  - leading term ideal,
  - Gröbner bases,
  - S-polynomials,
  - Buchberger's algorithm,

- Minimal Gröbner bases,
- Reduced Gröbner bases,
- elimination ideals,
- operation on ideals,
- Hilbert theorems of zeros,
- operation on algebraic varieties,
- constructible sets,
- Zariski topology,
- smoothness,
- multiplicity.

Some notations before we start the theory (I)

NOTATION. Throughout the talk, we consider a field $\mathbb{K}$ and an ordered set $X = x_1 < \cdots < x_n$ of n variables. Typically $\mathbb{K}$ will be

- a **finite field**, such as $\mathbb{Z}/p\mathbb{Z}$ for a prime p, or
- the field $\mathbb{Q}$ of **rational numbers**, or
- a field of **rational functions** over $\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{Q}$.

We will denote by $\overline{\mathbb{K}}$ an **algebraic closure** of $\mathbb{K}$.

https://en.wikipedia.org/wiki/Algebraic_closure

- $\overline{\mathbb{K}}$ is the smallest field containing $\mathbb{K}$ and over which any non-constant polynomial factorizes into factors of degree 1,
- For $\mathbb{K} = \mathbb{R}$, the field of *real numbers*, we can choose $\overline{\mathbb{K}} = \mathbb{C}$, the field of *complex numbers*.

We will also consider a field $\mathbb{L}$ extending $\mathbb{K}$ and contained in $\overline{\mathbb{K}}$. Hence, we have $\mathbb{K} \subset \mathbb{L} \subset \overline{\mathbb{K}}$. More on *field extensions* and *algebraic closures* in the next chapter.

Some notations before we start the theory (II)

NOTATION. We denote by $\mathbb{K}[x_1, \ldots, x_n]$ the ring of the polynomials with coefficients in $\mathbb{K}$ and variables in X. For $F \subset \mathbb{K}[x_1, \ldots, x_n]$, we write $\langle F \rangle$ and $\sqrt{\langle F \rangle}$ for the *ideal* generated by F in $\mathbb{K}[x_1, \ldots, x_n]$ and its *radical*, respectively. Thus, writing $F = \{g_1, \ldots, g_s\}$, by definition, for $f \in \mathbb{K}[x_1, \ldots, x_n]$ we have

- $f \in \langle F \rangle \iff (\exists q_1, \ldots, q_s \in \mathbb{K}[x_1, \ldots, x_n])\ f = q_1 g_1 + \cdots + q_s g_g,$
- $f \in \sqrt{\langle F \rangle} \iff (\exists e \in \mathbb{N})\ f^e \in \langle F \rangle.$

Observe that we have $\langle F \rangle \subseteq \sqrt{\langle F \rangle}$.

https://en.wikipedia.org/wiki/Ideal_(ring_theory)

https://en.wikipedia.org/wiki/Radical_of_an_ideal

EXAMPLE. *For* $F = \{xy^2 + 2y^2, x^4 - 2x^2 + 1\}$, *we have*

$$\sqrt{\langle F \rangle} = \langle x^2 - 1, y \rangle$$

NOTATION. For $1 \leq i \leq n$, we denote by $A^i(\mathbb{L})$ the affine space of dimension i over $\mathbb{L}$.

```
> with(PolynomialIdeals):
> g1 := x * y^2 + 2 * y^2;
                                    2      2
                           g1 := x y  + 2 y

> g2 := x^4 -2 *x^2 + 1;
                                 4      2
                          g2 := x  - 2 x  + 1

> J := <g1, g2>;
                         2      2   4      2
                   J := <x y  + 2 y , x  - 2 x  + 1>

> f := y^2;
                                       2
                               f := y

> f in J;
                                 true
```

```
> 1 in J;
                                    false

> gcdex(g2,(x+2),x,'s', 't');
                                      1

> s,t;
                              3         2
               1/9, -1/9 x  + 2/9 x  - 2/9 x + 4/9

> expand(s * g2 + t * (x +2) - 1);
                                      0

> ## Hence t is the inverse of (x+2) modulo g2
> g3 := t * (x +2) * y^2 + s * g2 * y^2:
> expand(g3);
                                       2
                                      y
```

Term orders (I)

NOTATION. We denote by M the **abelian monoid** generated by $x_1, \ldots, x_n$.

DEFINITION. A total order $\leq$ on M is a **term order** if the following two conditions hold

(i) for every $m \in \mathsf{M}$ we have $1_{\mathsf{M}} \leq m$

(ii) for every $m, m', m'' \in \mathsf{M}$ we have $m \leq m' \Rightarrow mm'' \leq m'm''$

NOTATION. For $f \in \mathbb{K}[x_1, \ldots, x_n]$ with $f \neq 0$, we denote by

- $\mathrm{lm}(f)$ the **leading monomial** of f, that is the largest $m \in \mathsf{M}$ occurring in f,
- $\mathrm{lc}(f)$ the **leading coefficient** of f, that is the coefficient of $\mathrm{lm}(f)$ in f,
- $\mathrm{lt}(f) = \mathrm{lc}(f)\mathrm{lm}(f)$ the **leading term** of f,
- $\mathrm{rd}(f)$ the **reductum** of f, that is $f - \mathrm{lt}(f)$.

PROPOSITION. For $f, g \in \mathbb{K}[x_1, \ldots, x_n]$, with $f \neq 0$ and $g \neq 0$, we have

$$\mathrm{lm}(fg) = \mathrm{lm}(f)\mathrm{lm}(g) \text{ and } \mathrm{lc}(fg) = \mathrm{lc}(f)\mathrm{lc}(g).$$

Term orders (II)

REMARK. Recall that the variables $x_1, \dots, x_n$ are ordered by

$$x_1 < \cdots < x_n.$$

Hence, we identify every monomial $m = x_n^{e_n} \cdots x_1^{e_1}$ with the tuple of non-negative integers $e = (e_n, \dots, e_1)$ often called the **exponent vector** of m.

It is convenient to denote by $|e|$ the sum $e_1 + \cdots + e_n$ which is the **total degree** of the monomial m. Finally, we define $\mathrm{rev}(e) = (e_1, \dots, e_n)$.

NOTATION. For $a = (a_n, \dots, a_1)$ and $b = (b_n, \dots, b_1)$ in $\mathbb{N}^n$ we define

$$a <_{lex} b \quad \Longleftrightarrow \quad (\exists i \in \{1, \dots, n\}) \text{ t.q. } \begin{cases} a_i < b_i \\ a_j = b_j \quad (\forall j > i) \end{cases}$$

and

$$a <_{deglex} b \quad \Longleftrightarrow \quad \begin{cases} |a| < |b| \text{ or} \\ |a| = |b| \text{ and } a <_{lex} b \end{cases}$$

and

$$a <_{degrevlex} b \quad \Longleftrightarrow \quad \begin{cases} |a| < |b| \text{ or} \\ |a| = |b| \text{ and } \operatorname{rev}(a) >_{lex} \operatorname{rev}(b) \end{cases} .$$

Moreover, we define

$$a \leq_{lex} b \quad \Longleftrightarrow \quad a <_{lex} b \;\text{ or }\; a = b$$

and

$$a \leq_{deglex} b \quad \Longleftrightarrow \quad a <_{deglex} b \;\text{ or }\; a = b$$

and

$$a \leq_{degrevlex} b \quad \Longleftrightarrow \quad a <_{degrevlex} b \;\text{ or }\; a = b.$$

PROPOSITION. The binary relations $\leq_{lex}$, $\leq_{deglex}$ and $\leq_{degrevlex}$ define term orders in $\mathbb{K}[x_1, \ldots, x_n]$.

Term orders (III)

EXAMPLE. *Assume* $n = 2$ *and define* $x_1 = x$ *and* $x_2 = y$*. Then, we have*

$$1 <_{lex} x <_{lex} x^2 <_{lex} \cdots <_{lex} y <_{lex} xy <_{lex} x^2y <_{lex} \cdots <_{lex} y^2 <_{lex} \cdots$$

and

$$1 <_{deglex} x <_{deglex} y <_{deglex} x^2 <_{deglex} xy <_{deglex} y^2 <_{deglex} x^3 \cdots$$

For $n = 3$ *with* $x_1 = x$*,* $x_2 = y$ *and* $x_3 = z$ *we have*

$$y^3z \leq_{deglex} xyz^2 \ \text{ but } \ xyz^2 \leq_{degrevlex} y^3z.$$

PROPOSITION. Let $\leq$ be a term order for $\mathbb{K}[x_1, \ldots, x_n]$. Then for all monomials m, m', we have

$$m \mid m' \ \Rightarrow \ m \leq m'.$$

THEOREM. Let $\leq$ be a term order for $\mathbb{K}[x_1, \ldots, x_n]$. Then, for every non-empty set M of monomials of $\mathbb{K}[x_1, \ldots, x_n]$ there exists $m \in M$ such that we have

$$(\forall m' \in M) \ m \leq m'.$$

Multi-divisor division (I)

NOTATION. From now on, **we fix a term order $\leq$.**

DEFINITION. Let $f, g, h \in \mathbb{K}[x_1, \ldots, x_n]$ with $g \neq 0$. We say that f **reduces to** h **modulo** g in one step and we write

$$f \xrightarrow{g} h$$

if and only if $\mathrm{lm}(g)$ divides a non-zero term t of f and

$$h = f - \frac{t}{\mathrm{lc}(g)\mathrm{lm}(g)} g.$$

REMARK. When this holds, observe that we have

$$h = (f - t) - p \ \text{ with } \ p := \frac{t}{\mathrm{lm}(g)} \frac{\mathrm{rd}(g)}{\mathrm{lc}(g)}.$$

One can check that either $p = 0$ holds or that we have

$$\mathrm{lm}(p) < \mathrm{lm}(t).$$

Multi-divisor division (II)

DEFINITION. Let f, h, r and $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ with $f_i \neq 0$ for all $i = 1, \ldots, s$. Define $F = \{f_1, \ldots, f_s\}$. We say that f **reduces to** h **modulo** F and we write

$$f \xrightarrow{F}_{+} h$$

if and only if there exists a sequence of indices $i_1, i_2, \ldots, i_t$ and a sequence of polynomials $h_1, h_2, \ldots, h_{t-1}$ such that

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \cdots h_{t-1} \xrightarrow{f_{i_t}} r.$$

The polynomial r is called **reduced w.r.t.** F if

- either $r = 0$
- or no monomials in r is divisible by one of the $\mathrm{lm}(f_i)$, for $i = 1, \ldots, s$.

The polynomial r is called **a remainder of** f *w.r.t.* F if $f \xrightarrow{F}_{+} r$ and r is **reduced w.r.t.** F.

Multi-divisor division (III)

PROPOSITION. Let h, F be as in the previous definition, with $h \neq 0$, and let m be a monomial and $c \in \mathbb{K}$ with $c \neq 0$. Then, we have

$$cm \xrightarrow{F}_{+} h \implies \mathrm{lm}(h) < m.$$

PROPOSITION. Let f, F be as above. Then, we have

$$f \neq 0 \text{ and } f \xrightarrow{F}_{+} 0 \implies f \text{ not reduced w.r.t. } F.$$

PROPOSITION. Let f, F be as above. Then, we have

$$f \xrightarrow{F}_{+} 0 \Rightarrow f \in \langle F \rangle$$

Multi-divisor division (IV)

REMARK. Observe that the **univariate division** of f by g, with $g \notin \mathbb{K}$, in $\mathbb{K}[x]$ can be computed as follows:

$r := f$

$q := 0$

while $\mathrm{lm}(g) \mid \mathrm{lm}(r)$ **repeat**

Compute r' and q' such that

$$r \xrightarrow{g} r' \text{ and } r = q'g + r'$$

$r := r'$

$q := q + q'$

return (q, r)

Multi-divisor division (V)

DEFINITION. Let $f, g_1, \dots, g_s, q_1, \dots, q_s, r \in \mathbb{K}[x_1, \dots, x_n]$ such that $g_i \neq 0$ for all $i = 1, \dots, s$. Define $G = \{g_1, \dots, g_s\}$. We say that $(q_1, \dots, q_s)$ are the *quotients* and r the *remainder* in the *multivariate division* of f w.r.t. G if the following conditions hold

(i) $f = q_1 g_1 + \cdots + q_s g_s + r$,

(ii) r is reduced w.r.t. G,

(iii) $\max(\mathrm{lm}(q_1)\mathrm{lm}(g_1), \dots, \mathrm{lm}(q_s)\mathrm{lm}(g_s), \mathrm{lm}(r)) = \mathrm{lm}(f)$.

If this holds, then we write

$$\begin{array}{c|c|c|c} f & g_1 & \cdots & g_s \\ \hline r & q_1 & \cdots & q_s \end{array}.$$

Input: $f, g_1, \dots, g_s \in \mathbb{K}[x_1, \dots, x_n]$ such that $g_i \neq 0$ for all $i = 1, \dots, s$.

Output: $q_1, \dots, q_s, r \in \mathbb{K}[x_1, \dots, x_n]$ such that $\begin{array}{c|c|c|c} f & g_1 & \cdots & g_s \\ \hline r & q_1 & \cdots & q_s \end{array}.$

for $i := 1, \ldots, s$ **repeat** $q_i := 0$

$h := f$

$r := 0$

while $h \neq 0$ **repeat**

  $i := 1$

  while $i \leq s$ **repeat**

    if $\mathrm{lm}(g_i) \mid \mathrm{lm}(h)$ **then**

      $t := \dfrac{\mathrm{lt}(h)}{\mathrm{lt}(g_i)}$

      $q_i := q_i + t$

      $h := h - tg_i$

      $i := 1$

    else

      $i := i + 1$

  $r := r + \mathrm{lt}(h)$

  $h := h - \mathrm{lt}(h)$

return$(q_1, \ldots, q_s, r)$

Multi-divisor division (VI)

PROPOSITION. The previous algorithm terminates and is correct.

EXAMPLE. *With* $n = 1$, $x_1 = x$ *and* $\leq = \leq_{lex}$ *we consider* $g_1 = x^2$, $g_2 = x^2 - x$, $G = \{g_1, g_2\}$ *and* $f = x$. *Then, we have*

f	g_1	g_2
f	0	0

However f *is not reduced w.r.t.* $G = \{g_1, g_2\}$.

EXAMPLE. *With* $n = 2$, $x = x_1 < x_2 = y$ *and* $\leq = \leq_{deglex}$ *we consider* $g_1 = yx - y$, $g_2 = y^2 - x$, $G = \{g_1, g_2\}$ *and* $f = y^2 x$. *Then, we have*

f	g_1	g_2
x	y	1

EXAMPLE. *With* $n = 2$, $x = x_1 < x_2 = y$ *and* $\leq = \leq_{deglex}$ *we consider*

$f = y^2x - x$, $g_1 = yx - y$ and $g_2 = y^2 - x$. Then we have

f	g_1	g_2
0	y	1

However we have

f	g_2	g_1
$x^2 - x$	x	0

Leading term ideal

DEFINITION. For a subset S of $\mathbb{K}[x_1, \ldots, x_n]$, the **leading term ideal** of S is the ideal of $\mathbb{K}[x_1, \ldots, x_n]$ denoted by $\mathrm{lt}(S)$ and defined by

$$\mathrm{lt}(S) = \langle \mathrm{lt}(s) \ \mid \ s \in S \rangle.$$

PROPOSITION. Let S be a set of non-zero terms of $\mathbb{K}[x_1, \ldots, x_n]$ and let $\mathcal{I}$ be its leading term ideal. For every $f \in \mathbb{K}[x_1, \ldots, x_n]$ the following statements are equivalent

(i) $f \in \mathcal{I}$

(ii) for every term t of f there exists $s \in S$ such that s divides t.

Moreover, there exists a finite subset S_0 of S such that $\mathcal{I} = \langle S_0 \rangle$.

Gröbner bases (I)

DEFINITION. Let $\mathcal{I}$ be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$. A finite subset G of $\mathcal{I}$ is a **Gröbner basis of $\mathcal{I}$** if and only if

$$(\forall f \in \mathcal{I})\ (\exists g \in G)\ \ \mathrm{lm}(g)\ \ \text{divides}\ \mathrm{lm}(f).$$

A finite subset G of $\mathbb{K}[x_1, \ldots, x_n]$ is a **Gröbner basis** if it is a Gröbner basis for the ideal $\langle G \rangle$ it generates.

THEOREM. Let $\mathcal{I}$ be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$ and $G = \{g_1, \ldots, g_t\}$ be a finite subset of $\mathcal{I}$. Then, the following statements are equivalent

(i) G is a Gröbner basis for $\mathcal{I}$.

(ii) For every $f \in \mathbb{K}[x_1, \ldots, x_n]$ we have: $f \in \mathcal{I} \iff f \xrightarrow{G}_{+} 0$.

(iii) For every $f \in \mathbb{K}[x_1, \ldots, x_n]$, the polynomial f belongs to $\mathcal{I}$ if and only if there exists $q_1, \ldots, q_t \in \mathbb{K}[x_1, \ldots, x_n]$ such that $f = q_1 g_1 + \cdots q_t g_t$ and $\max(\mathrm{lm}(q_1)\mathrm{lm}(g_1), \ldots, \mathrm{lm}(q_s)\mathrm{lm}(g_s)) = \mathrm{lm}(f)$.

(iv) $\mathrm{lt}(G) = \mathrm{lt}(\mathcal{I})$.

Gröbner bases (II)

COROLLARY. Let $\mathcal{I}$ be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$ and $G = \{g_1, \ldots, g_t\}$ be a finite subset of $\mathcal{I}$. If G is a Gröbner basis of $\mathcal{I}$, then we have $\mathcal{I} = \langle g_1, \ldots, g_t \rangle$.

PROOF ▷ Clearly $\langle g_1, \ldots, g_t \rangle \subseteq \mathcal{I}$ holds. For the reverse inclusion, let $f \in \mathcal{I}$. With the previous theorem we have $f \xrightarrow{G}_+ 0$, which implies $f \in \langle g_1, \ldots, g_t \rangle$. ◁

THEOREM. Every ideal of $\mathbb{K}[x_1, \ldots, x_n]$ admits a Gröbner basis.

PROOF ▷ Let $\mathcal{I}$ be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$. The leading term ideal $\mathrm{lt}(\mathcal{I})$ is generated by a finite subset S_G of $\mathrm{lt}(\mathcal{I})$. Hence S_G is of the form $\{\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t)\}$ where $g_1, \ldots, g_t$ are polynomials of $\mathcal{I}$. We define $G = \{g_1, \ldots, g_t\}$ such that we have $\mathrm{lt}(\mathcal{I}) = \mathrm{lt}(G)$. With the previous theorem we deduce that G is a Gröbner basis for $\mathcal{I}$. ◁

THEOREM. Let $G = \{g_1, \ldots, g_t\}$ be a set of non-zero polynomials of $\mathbb{K}[x_1, \ldots, x_n]$. Then, the set G is a Gröbner basis if and only if for all $f \in \mathbb{K}[x_1, \ldots, x_n]$ all remainders of a multivariate division of f w.r.t. G are equal.

S-polynomials (I)

<u>REMARK.</u> *Let $f, f_1, \ldots, f_s$ be non-zero polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. We define $F = \{f_1, \ldots, f_s\}$. For performing the multivariate division of f w.r.t F, one needs to order the polynomials in F. We know that the result of this division may depend on this order. For one order, we may first reduce a term t in f by a polynomial f_i and for another order, we may first reduce t by a polynomial f_j, with $j \neq i$. In the first case we obtain the polynomial*

$$h_i = f - \frac{t}{\mathrm{lt}(f_i)} f_i$$

and in the second case we obtain the polynomial

$$h_j = f - \frac{t}{\mathrm{lt}(f_j)} f_j.$$

The ambiguity *that is introduced is*

$$h_j - h_i = \frac{t}{\mathrm{lt}(f_i)} f_i - \frac{t}{\mathrm{lt}(f_j)} f_j.$$

This leads to the notion of a S-polynomial

S-polynomials (II)

DEFINITION. Let $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ be two non-zero polynomials and let L be the least common multiple of $\mathrm{lm}(f)$ and $\mathrm{lm}(g)$. The polynomial

$$S(f,g) = \frac{L}{\mathrm{lt}(f)} f - \frac{L}{\mathrm{lt}(g)} g$$

is called **the S-polynomial** of f and g.

EXAMPLE. *With $n = 2$, $x = x_1 < x_2 = y$ and $\leq = \leq_{deglex}$ we consider $f_1 = yx - y$, $f_2 = y^2 - x$, $F = \{f_1, f_2\}$ and $f = y^2x$. We have*

$$f \xrightarrow{f_1} f - yf_1 = y^2 \text{ and } f \xrightarrow{f_2} f - xf_2 = x^2.$$

The ambiguity *introduced is*

$$S(f_1, f_2) = yf_1 - xf_2 = -y^2 + x^2.$$

Also note that

$$S(f_1, f_2) \in \langle f_1, f_2 \rangle.$$

Moreover, the polynomial $S(f_1, f_2)$ *is not reduced w.r.t.* F *and we have*

$$S(f_1, f_2) \xrightarrow{f_2} x^2 - x.$$

The polynomial $f_4 = x^2 - x$ *is reduced w.r.t.* F *without being null. Observe that we have*

$$f \xrightarrow{f_1} y^2 \xrightarrow{f_2} x \ \text{ and } \ f \xrightarrow{f_2} x^2 \xrightarrow{f_4} x.$$

Hence, adding f_4 *to* F *allows the two reductions to converge toward the same result.*

Buchberger's algorithm (I)

<u>THEOREM.</u>[Buchberger] Let $G = \{g_1, \ldots, g_t\}$ be a set of non-zero polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. Then, the set G is a Gröbner basis if and only if for all $i \neq j$ we have

$$S(g_i, g_j) \xrightarrow{G}_+ 0.$$

<u>EXAMPLE.</u> *With $n = 2$, $x = x_1 < x_2 = y$ and $\leq = \leq_{deglex}$ we consider $f_1 = xy - x$ and $f_2 = x^2 - y$. We define $F = \{f_1, f_2\}$. Then we have*

$$S(f_1, f_2) = xf_1 - yf_2 = y^2 - x^2 \xrightarrow{f_2} y^2 - y$$

Since $f_3 = y^2 - y$ is reduced w.r.t. F, the set F is not a Gröbner basis. So, let us define $F' = F \cup \{f_3\}$. Now we have

$$S(f_1, f_2) \xrightarrow{F'}_+ 0.$$

Then we have

$$S(f_1, f_3) = yf_1 - xf_3 = y(xy - x) - x(y^2 - y) = 0.$$

and

$$S(f_2, f_3) = y^2(x^2 - y) - x^2(y^2 - y) = -y^3 + yx^2 \xrightarrow{f_3} yx^2 - y^2 \xrightarrow{f_2} 0.$$

Thus, Buchberger's Theorem shows that F' is a Gröbner basis.

Buchberger's algorithm (II)

Input: $F = \{f_1, \ldots, f_s\} \subseteq \mathbb{K}[x_1, \ldots, x_n]$ with $f_i \neq 0$ for all $i = 1, \ldots, s$.

Output: $G = \{g_1, \ldots, g_t\} \subseteq \mathbb{K}[x_1, \ldots, x_n]$ a Gröbner basis of $\langle F \rangle$.

$G_0 := F$
$P := \{(f_i, f_j) \mid 1 \leq i < j \leq s\}$
$i := 1$
while $P \neq \emptyset$ **repeat**
  Choose $(f, g) \in P$
  $P := P \setminus \{(f, g)\}$
  Compute h_i the remainder of $S(f, g)$ w.r.t. G_{i-1}
  if $h_i \neq 0$ **then**
    $P := P \cup \{(g, h_i) \mid g \in G_{i-1}\}$
    $G_i := G_{i-1} \cup \{h_i\}$
    $i := i + 1$
return(G_{i-1})

Buchberger's algorithm (III)

THEOREM. Buchberger's algorithm terminates and is correct.

PROOF ▷ The previous algorithm constructs a sequence of sets

$$G_0 \subseteq G_1 \subseteq \cdots \subseteq G_i \subseteq G_{i+1} \subseteq \cdots$$

together with a sequence of non-zero polynomials $h_1, \ldots, h_i, h_{i+1}, \ldots$ such that h_i is reduced w.r.t. G_{i-1}. Hence, no term in h_i is divisible by $\mathrm{lm}(g)$ for any g in G_{i-1}. Thus we have

$$\mathrm{lt}(h_i) \notin \mathrm{lt}(G_{i-1})$$

Therefore, we have

$$\mathrm{lt}(G_{i-1}) \subseteq \mathrm{lt}(G_i) \;\text{ but }\; \mathrm{lt}(G_{i-1}) \neq \mathrm{lt}(G_i)$$

It follows, that the $\mathrm{lt}(G_i)$'s form a strictly ascending chain of ideals. Since $\mathbb{K}[x_1, \ldots, x_n]$ is Noetherian, this chain must be ultimately constant. This implies that the algorithm must terminate. The proof of the correctness of the algorithm follows from Buchberger's Theorem. ◁

Buchberger's algorithm (IV)

<u>EXAMPLE.</u> *With* $n = 2$, $x = x_1 < x_2 = y$ *and* $\leq\, = \,\leq_{lex}$ *we consider* $f_1 = y + x^2 - 1$ *and* $f_2 = y^2 + x - 1$. *We define* $F = \{f_1, f_2\}$. *Following Buchberger's Algorithm, let us compute a Gröbner basis of* F *for the* $\leq_{lex}$ *ordering induced by* $y > x$. *We set* $G_0 = F$. *Then, we compute*

$$S(f_1, f_2) = yx^2 - y - x + 1 \xrightarrow{f_1} -x^4 + 2x^2 - x \xrightarrow{f_2} -x^4 + 2x^2 - x.$$

So, we define

$$h_1 = -x^4 + 2x^2 - x \text{ and } G_1 = \{f_1, f_2, h_1\}.$$

Then, we compute

$$S(f_1, h_1) = -2yx^2 + yx - x^6 + x^4 \xrightarrow{G_1} 0$$

and

$$S(f_2, h_1) = -2y^2x^2 + y^2x - x^5 + x^4 \xrightarrow{G_1} 0$$

Hence G_1 *is a Gröbner basis of the ideal generated by* F *for the lexicographical* *ordering induced by $y > x$. Now observe that*

$$f_2 = (y + 3x^2 + 1)f_1 - h_1$$

which shows that f_2 is in the ideal generated by f_1 and h_1. Therefore $\{f_1, h_1\}$ is a set of generators of the ideal generated by F.

Minimal Gröbner bases

PROPOSITION. Let $G = \{g_1, \dots g_t\}$ be a Gröbner basis for an ideal non-trivial $\mathcal{I}$ of $\mathbb{K}[x_1, \dots, x_n]$. If $\mathrm{lc}(g_2)$ divides $\mathrm{lc}(g_1)$ then $\{g_2, \dots g_t\}$ is also a Gröbner basis of $\mathcal{I}$.

PROOF $\triangleright$ A consequence of the definition of a Gröbner basis. $\triangleleft$

DEFINITION. A Gröbner basis $G = \{g_1, \dots g_t\}$ of $\mathbb{K}[x_1, \dots, x_n]$ is called **minimal** if the following conditions hold

- for all $i = 1, \dots, t$ the leading coefficient $\mathrm{lc}(g_i)$ of g_i is 1,
- for all $1 \leq i < j \leq t$ the leading monomial $\mathrm{lm}(g_i)$ does not divide the leading monomial $\mathrm{lm}(g_j)$.

PROPOSITION. Every non-trivial ideal $\mathcal{I}$ of $\mathbb{K}[x_1, \dots, x_n]$ admits a minimal Gröbner basis.

PROPOSITION. Let $G = \{g_1, \dots g_t\}$ and $H = \{h_1, \dots, h_s\}$ be two minimal Gröbner bases for the same non-trivial ideal $\mathcal{I}$ of $\mathbb{K}[x_1, \dots, x_n]$ for the same term order. Then, $s = t$ and after re-indexing the elements of H, if necessary, we have $\mathrm{lm}(g_i) = \mathrm{lm}(h_i)$ for all $i = 1, \dots, t$.

Reduced Gröbner bases (I)

<u>DEFINITION.</u> A Gröbner basis $G = \{g_1, \ldots g_t\}$ of $\mathbb{K}[x_1, \ldots, x_n]$ is called **reduced** if the following conditions hold

- for all $i = 1, \ldots, t$ the leading coefficient $\mathrm{lc}(g_i)$ of g_i is 1,
- for all $1 \leq i < j \leq t$ no monomials of g_j can be divided by the leading monomial $\mathrm{lm}(g_i)$.

Input: $G = \{g_1, \ldots, g_t\} \subseteq \mathbb{K}[x_1, \ldots, x_n]$ a minimal Gröbner basis of a non-trivial ideal $\mathcal{I}$.

Output: a reduced Gröbner basis of $\mathcal{I}$.

$H_1 := \{g_2, \ldots g_t\}$
for $i := 1 \cdots t$ **repeat**
  Compute h_i the remainder of g_i w.r.t. H_i
  $H_{i+1} := \{h_i\} \cup H_i \setminus \{g_{i+1}\}$
return(H_{t+1})

Reduced Gröbner bases (II)

PROPOSITION. The previous algorithm terminates and is correct.

THEOREM.[Buchberger] Every non-trivial ideal $\mathcal{I}$ of $\mathbb{K}[x_1, \ldots, x_n]$ admits a unique reduced Gröbner basis.

THEOREM. Let F be a finite set of non-zero polynomials of $\mathbb{K}[x_1, \ldots, x_n]$ and let G be a reduced Gröbner basis of $\langle F \rangle$. Then $\langle F \rangle = \mathbb{K}[x_1, \ldots, x_n]$ if and only if $G = \{1\}$.

PROOF $\triangleright$ The condition is clearly sufficient. Let us prove that it is necessary. Let us assume that $\langle F \rangle = \mathbb{K}[x_1, \ldots, x_n]$. Then $1 \in \langle F \rangle$. The only polynomial f such that $\mathrm{lc}(f) = 1$ and $\mathrm{lm}(f)$ divides 1 is 1 itself. Therefore, $1 \in G$. But the leading monomial of 1 divides any monomial. Hence, we have $G = \{1\}$. $\triangleleft$

Elimination ideals

DEFINITION. Let $\mathcal{I}$ be a non-trivial ideal of $\mathbb{K}[x_1, \ldots, x_n]$ and let $0 \leq k < n$ be an integer. The k-th *elimination ideal* of $\mathcal{I}$ is the ideal $\mathcal{I}_k = \mathcal{I} \cap \mathbb{K}[x_1, \ldots, x_{n-k}]$.

DEFINITION. Let $0 \leq k < n$ be an integer. A term order $<$ is said of *k-elimination* if for every monomial Y of $\mathbb{K}[x_1, \ldots, x_n]$ with a positive degree w.r.t. at least one of the variables $x_{n-k+1}, \ldots, x_n$ and for every monomial X of $\mathbb{K}[x_1, \ldots, x_{n-k}]$ we have $X < Y$.

EXAMPLE. *The lexicographical ordering induced by $x_1 < \cdots < x_n$ is of k-elimination for every $0 \leq k < n$.*

THEOREM.[Elimination Theorem] Let $0 < k < n$ be an integer and let $<$ be a term order of k-elimination. Let $\mathcal{I}$ be a non-trivial ideal and let $\mathcal{I}_k$ be its k-th elimination ideal of $\mathcal{I}$. Let G be a Gröbner basis of $\mathcal{I}$ for $<$. Then, the set $G_k = G \cap \mathbb{K}[x_1, \ldots, x_{n-k}]$ is a Gröbner basis of $\mathcal{I}_k$ for $<$.

PROOF $\triangleright$ See Chapter 3 in (Cox, Little, O'Shea, 1992). $\triangleleft$

```
 J := <y + x^2 -1, y^2 + x -1>;
                                      2           2
                               J := <y  + x - 1, x  + y - 1>
> EliminationIdeal(J,{x});
                                        4      2
                                      <x  - 2 x  + x>
> EliminationIdeal(J,{y});
                                        4      2
                                      <y  - 2 y  + y>
 J := <y + x^2 -1, y^3 + x -1>;
                                      2           3
                               J := <x  + y - 1, y  + x - 1>
> EliminationIdeal(J,{x});
                                      6      4      2
                                  <x  - 3 x  + 3 x  - x>
> J := <y^2 + y + x, z^2 + z*y + 1>;
                                     2                  2
                              J := <y  + x + y, y z + z  + 1>
> EliminationIdeal(J,{x});
                                             <0>
```

Intersection of ideals (I)

<u>LEMMA.</u> Let $\mathcal{I}$ be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$ and let t an extra variable. Let $\{f_1, \ldots, f_s\}$ and $\{g_1, \ldots, g_r\}$ be two sets of generators of $\mathcal{I}$. Then we have the following properties.

- The sets $\{tf_1, \ldots, tf_s\}$ and $\{tg_1, \ldots, tg_r\}$ generate the same ideal in $\mathbb{K}[x_1, \ldots, x_n, t]$ denoted $t\mathcal{I}$.
- For every polynomial $h(x_1, \ldots, x_n, t) \in t\mathcal{I}$ and for every element $a \in \mathbb{K}$, we have $h(x_1, \ldots, x_n, a) \in \mathcal{I}$.

<u>PROPOSITION.</u> Let $\mathcal{I}$ and $\mathcal{J}$ be two ideals of $\mathbb{K}[x_1, \ldots, x_n]$. Let t be an extra variable. Then we have

$$\mathcal{I} \cap \mathcal{J} = \langle t\mathcal{I} + (1-t)\mathcal{J} \rangle \cap \mathbb{K}[x_1, \ldots, x_n] \tag{1}$$

Intersection of ideals (II)

PROOF $\triangleright$ Let $f \in \mathbb{K}[x_1, \ldots, x_n]$. First assume that $f \in \mathcal{I} \cap \mathcal{J}$ holds. Then, clearly tf and $(1-t)f$ belong to $t\mathcal{I}$ and $(1-t)\mathcal{J}$ respectively. Hence, f belongs to the sum of these ideals. Since f belongs to $\mathbb{K}[x_1, \ldots, x_n]$, we have $f \in \langle t\mathcal{I} + (1-t)\mathcal{J} \rangle \cap \mathbb{K}[x_1, \ldots, x_n]$. Conversely, assume that this latter relation holds. Then there exists $g(x_1, \ldots, x_n, t) \in t\mathcal{I}$ and $h(x_1, \ldots, x_n, t) \in (1-t)\mathcal{J}$ such that

$$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n, t) + h(x_1, \ldots, x_n, t)$$

Since every polynomial in $t\mathcal{I}$ is a multiple of t we must have by specializing t to 0

$$f(x_1, \ldots, x_n) = h(x_1, \ldots, x_n, 0)$$

which shows that f belongs to $\mathcal{J}$. Similarly, by specializing t to 1 we obtain

$$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n, 1)$$

which shows that f belongs to $\mathcal{I}$. Therefore, we have $f \in \mathcal{I} \cap \mathcal{J}$. $\triangleleft$

Intersection of ideals (III)

Input: $\mathcal{I}$ and $\mathcal{J}$ ideals of $\mathbb{K}[x_1, \ldots, x_n]$ generated by $\{f_1, \ldots, f_s\}$ and $\{g_1, \ldots, g_r\}$ respectively.

Output: A Gröbner basis of $\mathcal{I} \cap \mathcal{J}$.

Let t be an extra variable

$F := \{tf_1, \ldots, tf_s, (1-t)g_1, \ldots, (1-t)g_r\}$

Let $<$ be a term order in $\mathbb{K}[x_1, \ldots, x_n, t]$ such that every monomial involving t is greater than every monomial of degree zero w.r.t. t

Compute G a Gröbner basis of F w.r.t. $<$

return $G \cap \mathbb{K}[x_1, \ldots, x_n]$

```
> J := <y^2 + 1>; K := <x^2 -2>;
                                   2
                             J := <y  + 1>

                                   2
                             K := <x  - 2>

> Intersect(J, K);
                          2  2    2      2
                        <x  y  + x  - 2 y  - 2>

> J := <y^2 - 1>; K := <y^2 - 2*y + 1>;
                                   2
                             J := <y  - 1>
                                2
                          K := <y  - 2 y + 1>
> Intersect(J, K);
                             3    2
                           <y  - y  - y + 1>
```

```
> J := <x*(x-1), y^2*(y-2)>;
```

$$J := \langle x\,(x - 1),\ y^2\,(y - 2)\rangle$$

```
> K := <(x-1)^2*y^3>;
```

$$K := \langle (x - 1)^2\, y^3\rangle$$

```
> L := Intersect(J, K);
```

$$\langle x^3\, y^3 - 2\, x^2\, y^3 + x\, y^3,\ x^2\, y^4 - 2\, x^2\, y^3 - 2\, x\, y^4 + 4\, x\, y^3 + y^4 - 2\, y^3\rangle$$

```
> map(factor, Generators(L));
```

$$\{x\, y^3\, (x - 1)^2,\ y^3\, (x - 1)^2\, (y - 2)\}$$

Quotient of ideals (I)

DEFINITION. Let $\mathcal{I}, \mathcal{J}$ be ideals of $\mathbb{K}[x_1, \ldots, x_n]$ and X be a non-empty subset of $\mathbb{K}[x_1, \ldots, x_n]$.

- The *sum* of $\mathcal{I}$ and $\mathcal{J}$ is denoted by $\mathcal{I} + \mathcal{J}$ and defined by

$$\mathcal{I} + \mathcal{J} \;=\; \{a + b \mid (a, b) \in \mathcal{I} \times \mathcal{J}\}.$$

- The *product* $\mathcal{I}$ and $\mathcal{J}$ is denoted by $\mathcal{I}\mathcal{J}$ and defined by

$$\mathcal{I}\mathcal{J} \;=\; \{ab \mid (a, b) \in \mathcal{I} \times \mathcal{J}\}.$$

- The *quotient* of $\mathcal{I}$ by X is denoted by $\mathcal{I} : X$ and defined by

$$\mathcal{I} : X \;=\; \{a \in \mathbb{A} \mid (\forall x \in X)\, ax \in \mathcal{I}\}.$$

Quotient of ideals (II)

<u>PROPOSITION.</u> Let $\mathcal{I}, \mathcal{J}, \mathcal{K}$ be ideals of $\mathbb{K}[x_1, \ldots, x_n]$ and X be a non-empty subset of $\mathbb{K}[x_1, \ldots, x_n]$. Then, the following properties hold.

(1) $\mathcal{I} \cap \mathcal{J}$ and $\mathcal{I}\mathcal{J}$ are ideals of $\mathbb{K}[x_1, \ldots, x_n]$.

(2) If $\mathcal{I} + \mathcal{J}$ is not $\mathbb{K}[x_1, \ldots, x_n]$, then it is an ideal of $\mathbb{K}[x_1, \ldots, x_n]$.

(3) If $\mathcal{I} : X$ is not $\mathbb{K}[x_1, \ldots, x_n]$, then it is an ideal of $\mathbb{K}[x_1, \ldots, x_n]$.

(4) We have $\mathcal{I}\mathcal{J} \subseteq \mathcal{I} \cap \mathcal{J}$.

(5) We have $\mathcal{J}(\mathcal{I} : \mathcal{J}) \subseteq \mathcal{I} \subseteq \mathcal{I} : \mathcal{J}$.

(6) We have $\mathcal{I} : (\mathcal{J} + \mathcal{K}) = \mathcal{I} : \mathcal{J} + \mathcal{I} : \mathcal{K}$.

(7) We have $(\mathcal{I} : \mathcal{J}) : \mathcal{K} = \mathcal{I} : (\mathcal{J}\mathcal{K}) = (\mathcal{I} : \mathcal{K}) : \mathcal{J}$.

(8) We have $(\mathcal{I} \cap \mathcal{J}) : \mathcal{K} = (\mathcal{I} : \mathcal{K}) \cap (\mathcal{J} : \mathcal{K})$.

Quotient of ideals (III)

PROPOSITION. Let $f_1, \ldots, f_s, g$ be polynomials of $\mathbb{K}[x_1, \ldots, x_n]$ and let $\mathcal{I}$ be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$. Then we have

$$\mathcal{I} \cap \langle g \rangle = \langle f_1, \ldots, f_s \rangle \;\Rightarrow\; \mathcal{I} : \langle g \rangle = \langle f_1/g, \ldots, f_s/g \rangle. \tag{2}$$

PROOF $\triangleright$ We assume that $\{f_1, \ldots, f_s\}$ generates $\mathcal{I} \cap \langle g \rangle$. Observe that for $1 \leq i \leq s$ the polynomial f_i is a multiple of g. So we can consider the ideal $\mathcal{J}$ of $\mathbb{K}[x_1, \ldots, x_n]$ generated by $\{f_1/g, \ldots, f_s/g\}$. Now, let $f \in \mathcal{J}$. For every $p \in \langle g \rangle$ we have $fp \in \langle f_1, \ldots, f_s \rangle$, that is $f \in \mathcal{I} : \langle g \rangle$. Conversely, let $f \in \mathcal{I} : \langle g \rangle$. Then, $fg \in \mathcal{I} \cap \langle g \rangle$ holds. Hence, there exists $q_1, \ldots, q_s \in \mathbb{K}[x_1, \ldots, x_n]$ such that $fg = \sum_{i=1}^{i=s} q_i f_i$. Since every f_i is a multiple of g, this latter equality shows that f lies in $\mathcal{J}$. $\triangleleft$

Quotient of ideals (IV)

Input: $\mathcal{I}$ and $\mathcal{J}$ ideals of $\mathbb{K}[x_1, \ldots, x_n]$ generated by $\{f_1, \ldots, f_s\}$ and $\{g_1, \ldots, g_r\}$ respectively.

Output: A Gröbner basis of the quotient ideal $\mathcal{I} : \mathcal{J}$.

Let H_1 be a Gröbner basis of $\mathcal{I} \cap \langle g_1 \rangle$.
$Q := \{h/g_1 \mid h \in H\}$
for $i = 2 \cdots r$ **repeat**
  Let H_i be a Gröbner basis of $\mathcal{I} \cap \langle g_i \rangle$.
  $H_i^* := \{h/g_i \mid h \in H_i\}$
  Replace Q by a Gröbner basis of $\langle Q \rangle \cap \langle H_i^* \rangle$
return Q

```
> J := <x^3-1, y^2-3>;

                              3        2
                        J := <x  - 1, y  - 3>

> K := <x^2-z>;

                                  2
                            K := <x  - z>

> S := Add(J, K);

                          3        2        2
                    S := <x  - 1, y  - 3, x  - z>

> Quotient(J, <x^2+x+1>);

                                   2
                           <x - 1, y  - 3>
```

Saturation of an ideal (I)

DEFINITION. Let $\mathcal{I}$ be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$ and h be a non-zero element of $\mathbb{K}[x_1, \ldots, x_n]$.

The *saturated ideal* of $\mathcal{I}$ by h is denoted by $\mathcal{I} : h^\infty$ and defined by

$$\mathcal{I} : h^\infty \;=\; \{f \in \mathbb{K}[x_1, \ldots, x_n] \;|\; (\exists e \in \mathbb{N})\; h^e f \in \mathcal{I}\}.$$

PROPOSITION. Let $\mathcal{I}$ and h be as above. Then, $\mathcal{I} : h^\infty$ is an ideal. Moreover, there exists an integer N such that $\mathcal{I} : h^\infty = \mathcal{I} : h^N$.

Saturation of an ideal (II)

PROPOSITION. Let $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$ be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$ and let $h \in \mathbb{K}[x_1, \ldots, x_n]$ be a non-zero polynomial. Let y be an extra variable. The we have

$$\mathcal{I} : h^\infty = \langle f_1, \ldots, f_s, 1 - yh \rangle \cap \mathbb{K}[x_1, \ldots, x_n]. \quad (3)$$

PROOF $\triangleright$ Let $g \in \mathcal{I} : h^\infty$. Then, there exists $e \in \mathbb{N}$ and polynomials $q_1, \ldots, q_s \in \mathbb{K}[x_1, \ldots, x_n]$ such that

$$h^e g = q_1 f_1 + \cdots q_s f_s.$$

Now observe that

$$\begin{array}{rcl} g & = & y^e h^e g + (1 - y^e h^e) g \\ & = & \sum_i q_i f_i y^e + (1 - yh)(1 + yh + \cdots + y^{e-1} h^{e-1}) g \end{array}$$

Since g belongs to $\mathbb{K}[x_1, \ldots, x_n]$ we have

$g \in \langle f_1, \ldots, f_s, 1 - yh \rangle \cap \mathbb{K}[x_1, \ldots, x_n]$. Conversely, assume that this g belongs to this latter ideal. Then, there exist polynomials $q_1, \ldots, q_s, q_0 \in \mathbb{K}[x_1, \ldots, x_n][y]$ such that

$$g = \sum_i q_i f_i + q_0(1 - yh)$$

holds. Let e be the highest degree w.r.t. y among the polynomials $q_1, \ldots, q_s, q_0$ Then replacing y with $1/h$ and multiplying this equality by h^e, we obtain $h^e g \in \mathcal{I}$. $\lhd$

Saturation of an ideal (III)

Input: h a polynomial of $\mathbb{K}[x_1, \ldots, x_n]$ and $\mathcal{I}$ an ideal of $\mathbb{K}[x_1, \ldots, x_n]$ generated by $\{f_1, \ldots, f_s\}$.

Output: A Gröbner basis of the saturated ideal $\mathcal{I} : h^\infty$.

Let y be an extra variable.
Let $<$ be a term order in $\mathbb{K}[x_1, \ldots, x_n, y]$ such that every monomial involving y is greater than every monomial of degree zero w.r.t. y
F := $\{f_1, \ldots, f_s, 1 - yh\}$
Compute G a Gröbner basis of F w.r.t. $<$
return $G \cap \mathbb{K}[x_1, \ldots, x_n]$

```
> J := <x^2, (y-1)^2*(y+1)>;
```

$$J := \langle x^2,\ (y - 1)^2\ (y + 1)\rangle$$

```
> Saturate(J, y-1);
```

$$\langle x^2,\ y + 1\rangle$$

```
> K := <x^3*y^2 + x*y^2, x^3*y + x^3*y^3>;
```

$$K := \langle x^3\ y^2 + x\ y^2,\ x^3\ y^3 + x^3\ y\rangle$$

```
> Saturate(K, x);
```

$$\langle y^3 + y,\ x^2\ y + y\rangle$$

```
q1 := Quotient(K, x);
```

$$q1 := \langle -x^2 y + y^3 ,\ x^2 y^2 + y^2 ,\ x^4 y + x^2 y \rangle$$

```
> q2 := Quotient(q1, x);
```

$$q2 := \langle -x^2 y + y^3 ,\ x^2 y^2 + y^2 ,\ x^3 y + x y \rangle$$

```
> q3 := Quotient(q2, x);
```

$$q3 := \langle y^3 + y,\ x^2 y + y \rangle$$

```
> Saturate(q3, y);
```

$$\langle x^2 + 1,\ y^2 + 1 \rangle$$

Algebraic varieties (I)

DEFINITION. For $f_1, \dots, f_s \in \mathbb{K}[x_1, \dots, x_n]$, we define

$$V_{\mathbb{L}}(f_1, \dots, f_s) = \{\zeta \in A^n(\mathbb{L}) \mid f_1(\zeta) = \cdots = f_s(\zeta) = 0\}.$$

More generally, for $F \subset \mathbb{K}[x_1, \dots, x_n]$, the **zero set** of F in $A^n(\mathbb{L})$ is defined by

$$V_{\mathbb{L}}(F) = \{\zeta \in A^n(\mathbb{L}) \mid (\forall f \in F)\ f(\zeta) = 0\}.$$

A subset $\mathcal{V}$ of $A^n(\mathbb{L})$ is an **(affine) algebraic variety** over $\mathbb{K}$ if there exists $F \subset \mathbb{K}[x_1, \dots, x_n]$ such that $\mathcal{V} = V_{\mathbb{L}}(F)$.

PROPOSITION. For $F \subset \mathbb{K}[x_1, \dots, x_n]$, we have

$$V_{\mathbb{L}}(F) = V_{\mathbb{L}}(\langle F \rangle).$$

COROLLARY. For $f_1, \dots, f_s, g_1, \dots, g_t \in \mathbb{K}[x_1, \dots, x_n]$, we have

$$\langle f_1, \dots, f_s \rangle = \langle g_1, \dots, g_t \rangle \ \Rightarrow\ V_{\mathbb{L}}(f_1, \dots, f_s) = V_{\mathbb{L}}(g_1, \dots, g_t).$$

Algebraic varieties (II)

DEFINITION. Let $\mathcal{V}$ be any subset of $A^n(\mathbb{L})$. (Hence, $\mathcal{V}$ may not be an algebraic variety.) The **ideal over** $\mathbb{K}$ of $\mathcal{V}$ is defined by

$$I_{\mathbb{K}}(\mathcal{V}) = \{f \in \mathbb{K}[x_1, \ldots, x_n] \mid (\forall \zeta \in \mathcal{V}) f(\zeta) = 0\}.$$

PROPOSITION. Let $\mathcal{I}, \mathcal{J}$ be ideals of $\mathbb{K}[x_1, \ldots, x_n]$ and let $\mathcal{V}, \mathcal{W} \subset A^n(\mathbb{L})$ be algebraic varieties over $\mathbb{K}$. Then we have

(i) $\mathcal{I} \subseteq \mathcal{J} \ \Rightarrow \ V_{\mathbb{L}}(\mathcal{J}) \subseteq V_{\mathbb{L}}(\mathcal{I})$,

(ii) $\mathcal{V} \subseteq \mathcal{W} \iff I_{\mathbb{K}}(\mathcal{W}) \subseteq I_{\mathbb{K}}(\mathcal{V})$,

(iii) $V_{\mathbb{L}}(I_{\mathbb{K}}(\mathcal{V})) = \mathcal{V}$,

(iv) $I_{\mathbb{K}}(V_{\mathbb{L}}(\mathcal{I})) \supseteq \mathcal{I}$,

(v) $V_{\mathbb{L}}(\mathcal{I}) \cap V_{\mathbb{L}}(\mathcal{J}) = V_{\mathbb{L}}(\mathcal{I} + \mathcal{J})$

(vi) $V_{\mathbb{L}}(\mathcal{I}) \cup V_{\mathbb{L}}(\mathcal{J}) = V_{\mathbb{L}}(\mathcal{I} \cap \mathcal{J}) = V_{\mathbb{L}}(\mathcal{I}.\mathcal{J})$.

Zariski topology (I)

REMARK. *Let $\mathcal{E}$ be a non-empty set. We recall that a* topology *of $\mathcal{E}$ is a collection $\mathcal{T}$ of subsets of $\mathcal{E}$ satisfying the following axioms*

(O_1) $\mathcal{E} \in \mathcal{T}$,

(O_2) *the intersection of two elements of $\mathcal{T}$ is an element of $\mathcal{T}$,*

(O_3) *any union (finite or not) of elements of $\mathcal{T}$ is an element of $\mathcal{T}$.*

The elements of $\mathcal{T}$ are called the open sets *of the topology. Their complements are called the* closed sets *of the topology and satisfy the following properties*

(C_1) $\emptyset$ *is a closed set.*

(C_2) *the union of two closed sets is a closed set,*

(C_3) *any intersection (finite or not) of closed sets is a closed set.*

Observe that a topology may be given by its closed sets rather than its open sets. Therefore, the properties of $(C_1), (C_2), (C_3)$ can be viewed as axiomx for a topology given by its closed sets.

Zariski topology (II)

<u>REMARK.</u> *A subset* X *of* $\mathcal{E}$ *may be* approximated *by a closed set, precisely the intersection of all the closed sets containing* X, *which is called the* closure *of* X *w.r.t. the topology and which is denoted by* $\overline{X}$. *The map* $X \longmapsto \overline{X}$ *satisfies the following properties for every subsets* X, Y *of* $\mathcal{E}$

(F_1) $X \subseteq \overline{X}$

(F_2) $\overline{\overline{X}} = \overline{X}$

(F_3) $X \subseteq Y \implies \overline{X} \subseteq \overline{Y}$

(F_4) $X \subseteq \overline{Y} \iff \overline{X} \subseteq \overline{Y}$

(F_5) $\overline{X \cup Y} = \overline{X} \cup \overline{Y}$

(F_6) $X \subseteq Y \implies \overline{Y} = \overline{X} \cup \overline{Y \setminus X}$

Zariski topology (III)

PROPOSITION. The set of the affine varieties over $\mathbb{K}$ of $A^n(\mathbb{L})$ are the closed sets of a topology called *Zariski topology*.

PROPOSITION. Let $\mathcal{W}$ be a subset of $A^n(\mathbb{L})$. The affine variety $V_{\mathbb{L}}(I_{\mathbb{K}}(W))$ is the intersection of all varieties V containing $\mathcal{W}$. Therefore, it is denoted $\overline{\mathcal{W}}$ and called the *Zariski closuer* of $\mathcal{W}$.

Zariski topology (IV)

Hilbert theorems of zeros (I)

LEMMA. Let $\mathbb{L}$ be an infinite field and let $p \in \mathbb{L}[x_1, \ldots, x_k]$. Then we have

$$p \neq 0 \quad \Rightarrow \quad (\exists (a_1, \ldots, a_n) \in \mathbb{L}^n)\; p(a_1, \ldots, a_n) \neq 0.$$

THEOREM.[Weak Theorem of Zeros] Let $\mathbb{L}$ be an algebraically closed field of which $\mathbb{K}$ is a sub-field and let F be a subset of $\mathbb{K}[x_1, \ldots, x_n]$. Then we have

$$V_{\mathbb{L}}(\langle F \rangle) = \emptyset \quad \Rightarrow \quad \langle F \rangle = \mathbb{K}[x_1, \ldots, x_n].$$

Hilbert theorems of zeros (II)

LEMMA. Let $f_1, \ldots, f_s, h$ be polynomials of $\mathbb{K}[x_1, \ldots, x_n]$ and let y be an extra variable. Then we have

$$\langle f_1, \ldots, f_s, 1 - yh \rangle = \mathbb{K}[x_1, \ldots, x_n, y] \;\Rightarrow\; h \in \sqrt{\langle f_1, \ldots, f_s \rangle}$$

where $\langle f_1, \ldots, f_s, 1 - yh \rangle$ and $\langle f_1, \ldots, f_s \rangle$ denote respectively the ideals generated by $\{f_1, \ldots, f_s, 1 - yh\}$ in $\mathbb{K}[x_1, \ldots, x_n, y]$ and $\{f_1, \ldots, f_s\}$ in $\mathbb{K}[x_1, \ldots, x_n] = \mathbb{K}[x_1, \ldots, x_n]$.

Hilbert theorems of zeros (III)

PROOF $\triangleright$ Let us assume that $\langle f_1, \ldots, f_s, 1 - yh \rangle$ generates $\mathbb{K}[x_1, \ldots, x_n, y]$. Then there exists $p_1, \ldots, p_s, q \in \mathbb{K}[x_1, \ldots, x_n, y]$ such that

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, y) f_i + q(x_1, \ldots, x_n, y)(1 - yh)$$

Substituting $1/h$ to y we obtain

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, 1/h) f_i.$$

Let e be the maximum degree in y among the polynomials $p_1, \ldots, p_s$. By multiplying the previous equality by h^e we obtain

$$h^e = \sum_{i=1}^{s} q_i f_i.$$

where $q_i = h^e p_i(x_1, \ldots, x_n, 1/h)$ is a polynomial of $\mathbb{K}[x_1, \ldots, x_n]$ for $1 \leq i \leq s$. This shows that h belongs to the radical of the ideal generated by $f_1, \ldots, f_s$ in $\mathbb{K}[x_1, \ldots, x_n]$. $\triangleleft$

Hilbert theorems of zeros (IV)

<u>THEOREM.</u>[Theorem of Zeros] Let $\mathbb{L}$ be an algebraically closed field of which $\mathbb{K}$ is a sub-field. Let $F = \{f_1, \ldots, f_s\}$ be a subset of $\mathbb{K}[x_1, \ldots, x_n]$ and let $h \in \mathbb{K}[x_1, \ldots, x_n]$. Then we have

$$h \in I_{\mathbb{K}}(V_{\mathbb{L}}(F)) \iff (\exists e \in \mathbb{N})\ h^e \in \langle F \rangle.$$

Hilbert theorems of zeros (V)

PROOF $\triangleright$ The condition (right-hand part of the equivalence) is clearly sufficient. Let us prove it is necessary. So, let us assume that $h \in I_{\mathbb{K}}(V_{\mathbb{L}}(F))$. Let y be an extra variable and consider $\mathcal{J}$ the subset of $\mathbb{K}[x_1, \ldots, x_n, y]$ generated by $\langle f_1, \ldots, f_s, 1 - yh\rangle$. Let $a = (a_1, \ldots, a_n, a_{n+1}) \in \mathbb{L}^{n+1}$ be a point. We distinguish two cases.

- If $(a_1, \ldots, a_n) \in V_{\mathbb{L}}(F)$ then $(a_1, \ldots, a_n) \in V_{\mathbb{L}}(h)$ and $a \notin V_{\mathbb{L}}(\mathcal{J})$.
- If $(a_1, \ldots, a_n) \notin V_{\mathbb{L}}(F)$ then clearly $a \notin V_{\mathbb{L}}(\mathcal{J})$.

Therefore $a \notin V_{\mathbb{L}}(\mathcal{J})$ in any case. By virtue of Theorem **??** we have $\mathcal{J} = \mathbb{K}[x_1, \ldots, x_n, y]$. Then, from Lemma 60 we obtain $h \in \sqrt{\langle f_1, \ldots, f_s\rangle}$ which completes the proof. $\triangleleft$

Hilbert theorems of zeros (VI)

<u>THEOREM.</u>[Strong Theorem of Zeros] Let $\mathbb{L}$ be a field of which $\mathbb{K}$ is a sub-field. Let F be a subset of $\mathbb{K}[x_1, \ldots, x_n]$ and let V be the affine variety of F over $\mathbb{L}$. Then we have

$$\sqrt{I_{\mathbb{K}}(V)} = I_{\mathbb{K}}(V). \tag{4}$$

In addition, if $\mathbb{L}$ is an algebraically closed field, then we have

$$I_{\mathbb{K}}(V_{\mathbb{L}}(\langle F \rangle)) = \sqrt{\langle F \rangle}. \tag{5}$$

Hilbert theorems of zeros (VII)

PROOF ▷ Relation (4) is a consequence of the fact that $\mathbb{K}[x_1, \ldots, x_n]$ is an integral domain. The details are left to the reader | To Do. | Let us prove Relation (5. Let $f \in \sqrt{\langle F \rangle}$. There exists $e \in \mathbb{N}$ such that $f^e \in \langle F \rangle$. Hence, f^e, and thus f, belong to $I_{\mathbb{K}}(V_{\mathbb{L}}(\langle F \rangle))$. Conversely, let $f \in I_{\mathbb{K}}(V_{\mathbb{L}}(\langle F \rangle))$. By definition, the polynomial f vanishes at every point of $V_{\mathbb{L}}(\langle F \rangle)$. Hence, by virtue of Theorem **??** there exits an integer e such that $f^e \in \langle F \rangle$, that is $f \in \sqrt{\langle F \rangle}$. ◁

Radical membership (I)

THEOREM. Let $f_1, \ldots, f_s, h$ be polynomials of $\mathbb{K}[x_1, \ldots, x_n]$ and let y be an extra variable. Let $\mathcal{I}$ be the ideal generated by $f_1, \ldots, f_s$ in $\mathbb{K}[x_1, \ldots, x_n]$. Then we have

$$h \in \sqrt{\mathcal{I}} \iff \langle f_1, \ldots, f_s, 1 - yh \rangle = \mathbb{K}[x_1, \ldots, x_n, y] \tag{6}$$

PROOF ▷ Lemma 60 states that the condition is sufficient. Let us prove that it is necessary. Let e be a positive integer such that $h^e \in \mathcal{I}$. We write

$$1 - y^e h^e = (1 - yh)(1 + yh + \cdots + y^{e-1}h^{e-1}) \in \mathcal{J} \tag{7}$$

Let $\mathcal{J}$ be the subset of $\mathbb{K}[x_1, \ldots, x_n, y]$ generated by $f_1, \ldots, f_s, 1 - yh$. (Thus $\mathcal{J}$ is either an ideal or the entire ring). Relation (7) shows that $1 - y^e h^e$ belongs to the ideal generated by $1 - yh$ in $\mathbb{K}[x_1, \ldots, x_n, y]$. Since $h^e \in \mathcal{I}$, the polynomial $y^e h^e$ lies in the ideal generated by $f_1, \ldots, f_s$ in $\mathbb{K}[x_1, \ldots, x_n, y]$. Therefore $1 = 1 - y^e h^e + y^e h^e$ belongs to $\mathcal{J}$. ◁

Radical membership (II)

Input: $f_1, \ldots, f_s, h$ be polynomials of $\mathbb{K}[x_1, \ldots, x_n]$ and y be an extra variable.

Output: $true$ if and only if h belongs to $\sqrt{\langle f_1, \ldots, f_s \rangle}$.

Choose any term order $<$ for the monomials of $\mathbb{K}[x_1, \ldots, x_n, y]$

Compute a Gröbner basis G of $f_1, \ldots, f_s, 1 - yh$ w.r.t.$<$

return $G \cap \mathbb{K} \neq \emptyset$

Operation on algebraic varieties

The tangent space at a point (I)

NOTATION. Let $V \subset A^n(\mathbb{L})$ be a variety over $\mathbb{K}$ and let $f_1, \dots, f_r \in \mathbb{K}[x_1, \dots, x_n]$ be such that $I_{\mathbb{K}}(V) = \langle f_1, \dots, f_r \rangle$.

Consider a point $p \in V$. We choose our coordinate system so that p is the origin.

We consider an arbitrary line ℓ through p and a point $q = (a_1, \dots, a_n)$, that is

$$\ell = \{(ta_1, \dots, ta_n) \mid t \in \mathbb{L}\}.$$

The intersection $V \cap \ell$ is described by the system of equations in $\mathbb{L}[t]$

$$f_1(ta_1, \dots, ta_n) = \cdots = f_r(ta_1, \dots, ta_n) = 0$$

DEFINITION. We say that the line ℓ is **tangent to** p **at order** n if $t = 0$ is a zero of order $n + 1$ of the above system.

We say that the line ℓ **tangent to** p if it is tangent to V at order one.

The tangent space at a point (II)

DEFINITION. The **tangent space** T_pV of V at p is the union of all points lying on lines tangent to V at p.

In the degenerate case where p is an isolated point of V, the tangent space of V at p is the zero-dimensional vector space consisting only of the point p.

PROPOSITION. The above definition is independent of the choice of generators of $I_{\mathbb{K}}(V)$.

EXAMPLE. *Consider the* **parabola** $V \subset A^2(\mathbb{L})$ *defined by* $y = x^2$ *with* $x < y$. *The expression* $ta_2 - t^2a_1 = 0$ *shows that*

$$T_pV = \{(a_1, 0) \mid a_1 \in \mathbb{L}\}.$$

EXAMPLE. *Consider the* **nodal curve** $V \subset A^2(\mathbb{L})$ *defined by* $y^2 = x^2 + x^3$ *with* $x < y$. *The expression* $t^2a_2^2 - t^2a_1^2 - t^3a_1^3 = 0$ *shows that* $T_pV = A^2(\mathbb{L})$.

EXAMPLE. *Consider the* **cusp** $V \subset A^2(\mathbb{L})$ *defined by* $y^2 = x^3$ *with* $x < y$. *The expression* $t^2a_2^2 - t^3a_1^3 = 0$ *shows that* $T_pV = A^2(\mathbb{L})$.

The tangent space at a point (III)

DEFINITION. The **differential** of $f \in \mathbb{L}[x_1, \ldots, x_n]$ at an arbitrary point $p = (p_1, \ldots, p_n) \in A^n(\mathbb{L})$, denoted by $dF|_p$, is the **linear part of the Taylor expansion of** f around p, that is

$$df|_p(x - p) = \sum_{j=1}^{j=n} \frac{\partial f}{\partial x_j}(p)(x_j - p_j).$$

Observe that $dF|_p$ is a linear form from $A^n(\mathbb{L})$ to $\mathbb{L}$.

THEOREM. Recall $V \subset A^n(\mathbb{L})$ is a variety over $\mathbb{K}$ and $f_1, \ldots, f_r \in \mathbb{K}[x_1, \ldots, x_n]$ are such that $I_{\mathbb{K}}(V) = \langle f_1, \ldots, f_r \rangle$. Let p a point of V. Then, the tangent space T_pV of V at p is the linear variety defined by

$$T_pV = V_{\mathbb{K}}(df_1|_p(x - p), \ldots, df_1|_r(x - p)).$$

Moreover, the tangent space T_pV is independent of the choice of generators of $I_{\mathbb{K}}(V)$.

The tangent space at a point (IV)

COROLLARY. Let $V(f) \subset A^n(\mathbb{L})$, for $f \in \mathbb{K}[x_1, \ldots, x_n]$, be an **hypersurface** and let $p \in V(f)$ be a point. Then, the dimension of the tangent space T_pV is given by

$$\dim(T_pV) = \begin{cases} n-1 & \text{if} \quad \text{at least one} \frac{\partial f}{\partial x_j}(p) \neq 0 \\ n & \text{if} \quad \text{all} \frac{\partial f}{\partial x_j}(p) = 0 \end{cases}$$

EXAMPLE. *Continuing the* **parabola** *example, we define* $f(x,y) = y - x^2$ *such that, for* $p = (p_1, p_2) \in A^2(\mathbb{L})$*, we have*

$$T_pV = V_{\mathbb{K}}(-2p_1(x - p_1) + 1\,(y - p_2))$$

We observe $\dim(T_pV) = 1$ *for all* p.

EXAMPLE. *Continuing the* **nodal curve** *example, we define* $f(x,y) = y^2 - x^2 - x^3$ *such that, for* $p = (p_1, p_2) \in A^2(\mathbb{L})$*, we have*

$$T_pV = V_{\mathbb{K}}(-(2p_1 + 3p_1^2)(x - p_1) + 2p_2(y - p_2))$$

We observe $\dim(T_pV)$ *is* 2 *for* $p = (0,0)$ *and* 1 *otherwise.*

Smoothness (I)

DEFINITION. Let $V \subset A^n(\mathbb{L})$ be a variety over $\mathbb{K}$ and let $p \in V$ be a point. The **dimension of** V at p, denoted by $\dim_p V$, is the maximum dimension of an irreducible variety V' over $\mathbb{K}$ such that

$$\{p\} \subseteq V' \subseteq V.$$

The point is said **smooth** if we have

$$\dim_p V = \dim(T_p V).$$

DEFINITION. For $f_1, \ldots, f_r \in \mathbb{L}[x_1, \ldots, x_n]$ and $p \in A^n(\mathbb{L})$, the **Jacobian matrix** of $f_1, \ldots, f_r$ at p is the $r \times n$ matrix denoted by $\mathrm{Jac}(f_1, \ldots, f_r)(p)$ whose (i, j)-element is $\frac{\partial f_i}{\partial x_j}(p)$.

THEOREM.[Jacobian Criterion] Let $f_1, \ldots, f_r \in \mathbb{K}[x_1, \ldots, x_n]$ be polynomials and let $p \in V(f_1, \ldots, f_r)$ be a point. **Assume that $\mathbb{K}$ has characteristic 0.** If $\mathrm{Jac}(f_1, \ldots, f_r)(p)$ has rank r, then

- the point p is **smooth** and,
- lies in a unique irreducible component of V of dimension $n - r$.

Smoothness (II)

Multiplicity