# Polynomial System Solving, a Survey

# (Draft)

### Note

These notes are an extended version of a draft I prepared for a course in a School on "Effective Methods in Algebraic Geometry", Torino, 1990. The aim of the course was to extend the algorithmic approach for solving univariate polynomial, to the case of systems of multivariate polynomial equations, containing only a finite number of solutions (the so-called $O$-dimensional systems); its main topics were

- the analysis of the equations of a $O$-dimensional ideal, by means of Gröbber basis techniques
- the discussion of the Trinks Algorithm which, by means of Gröbner bases, reduces the problem of solving a $O$-dimensional system to the problem of solving a sequence of univariate polynomials over algebraic extensions.

To this notes I have mainly added:

- a description of a different algorithm for solving $O$-dimensional systems based on eigenvalue computation, due to Auzinger-Stetter
- a set of examples based on Gröbner basis techniques, to support the theory presented.

The reader should be aware that there are many other approach on solving $O$-dimensional systems and which are not considered in these notes. A survey of Lazard [**L93**], while also omitting some important results, contains many more references of this note and an advanced discussion of the complexity of system solving.

### Introduction

### Recalls on Gröbner bases

Since Gröbner bases will be mainly used in this paper, let us introduce the notation and definition we need, refering the results to [**Mo**]

Let $\mathbf{T}$ be the commutative semigroup generated by $\{X_1, \ldots, X_n\}$ and let us assume that it is endowed with a well-ordering $<$, which is a semigroup ordering, i.e. it is compatible with the product:

$$\text{for each} \quad t, t_1, t_2 \in \mathbf{T}, \quad t_1 < t_2 \quad \text{implies} \quad t\, t_1 < t\, t_2$$

We consider also the polynomial ring $k[X_1, \ldots, X_n]$ which has an obvious $k$-vector space structure, for which $\mathbf{T}$ is a basis. In other words each element of $k[X_1, \ldots, X_n]$ has a unique representation as a linear combination of elements of $\mathbf{T}$. The well-ordering $<$ gives us something more: each element $f \in k[X_1, \ldots, X_n]$ has a unique *ordered* representation as a linear combination of elements of $\mathbf{T}$:

$$f = \sum_{i=1}^{s} c_i t_i : c_i \in k \setminus \{0\}, t_i \in \mathbf{T}, t_1 > \cdots > t_s$$

So to each non-zero element $f \in k[X_1, \ldots, X_n]$, we can associate $M(f) := t_1$, the *maximal term* of $f$, and $lc(f) := c_1$, the *leading coefficient* of $f$.

If $I \subset k[X_1, \ldots, X_n]$ is an ideal of $k[X_1, \ldots, X_n]$, the set

$$M(I) := \{M(f) \in \mathbf{T} : f \in I\} \subset \mathbf{T}$$

is a semigroup ideal of $\mathbf{T}$ and the set

$$O(I) := \mathbf{T} \setminus M(I)$$

is an *order ideal* of $\mathbf{T}$ i.e.

$$\text{for each} \quad m, t \in \mathbf{T}, mt \in O(I) \quad \text{implies} \quad t \in O(I)$$

The definitions given now are justified by the following

**Theorem 1** *The following holds:*
1) $k[X_1,\dots,X_n] = I \oplus Span_k(O(I))$
2) *There is a* $k$*-vector space isomorphism between* $k[X_1,\dots,X_n]/I$ *and* $Span_k(O(I))$
3) *for each* $f \in k[X_1,\dots,X_n]$ *there is a unique* $g := Can(f,I) \in Span_k(O(I))$ *s.t.* $f - g \in I$

*Moreover:*
a) $Can(f,I) = Can(g,I)$ *if and only if* $f - g \in I$
b) $Can(f,I) = 0$ *if and only if* $f \in I$ ▮

Remarking that each semigroup ideal in an ordered semigroup has a unique irredundant basis, we immediately obtain:

**Proposition 1** *If* $I \in k[X_1,\dots,X_n]$ *is an ideal, there is a unique set* $G \subset I$ *s.t.*
1) $\{M(g) : g \in G\}$ *is an irredundant basis of* $M(I)$
2) $lc(g) = 1$ *for each* $g \in G$
3) $g = M(g) - Can(M(g), I)$ *for each* $g \in G$.

$G$ *is called the reduced Gröbner basis of* $I$.

We can relax the notion above to introduce the following:

**Definition** *A set* $G \subset I$ *is called a Gröbner basis of* $I$ *if* $M(G) = M(I)$ *where* $M(G)$ *is the semigroup ideal generated by* $\{M(g) : g \in G\}$.

**Theorem 2** *The following conditions are equivalent:*
1) $G$ *is a Gröbner basis of* $I$
2) *for each* $f \in k[X_1,\dots,X_n]$:

$$f = Can(f,I) + \sum_{i=0}^{t} c_i l_i g_i \quad c_i \in k - \{0\},\ l_i \in \mathbf{T},\ g_i \in G$$

$$T(f) \geq l_1 T(g_1) > \dots > l_i T(g_i) > l_{i+1} T(g_{i+1}) > \dots$$

3) *for each* $f \in k[X_1,\dots,X_n]$, $f \in I$ *if and only if:*

$$f = \sum_{i=0}^{t} c_i l_i g_i \quad c_i \in k - \{0\},\ l_i \in \mathbf{T},\ g_i \in G$$

$$T(f) = l_1 T(g_1) > \dots > l_i T(g_i) > l_{i+1} T(g_{i+1}) > \dots$$

*Such a representation is called a Gröbner representation.* ▮

Since Gröbner bases are related to *term-orderings*, i.e. semigroup orderings on $\mathbf{T}$, let us recall those which are most commonly and will be quoted in this notes:
- the *lexicographical* ordering (*lex*) is defined by

$$t_1 := X_1^{e_1} \cdots X_n^{e_n} < X_1^{\eta_1} \cdots X_n^{\eta_n} =: t_2 \quad \text{if and only if there is} \quad j : e_i = \eta_i, i < j, e_j < \eta_j$$

(Remark that the ordering depends on the ordering $X_1 < \dots < X_n$ on the variables; to make clear this dependence we could speak of the "lex ordering s.t. $X_1 < \dots < X_n$")
- the *deg-rev-lex* ordering is defined by

$$t_1 := X_1^{e_1} \cdots X_n^{e_n} < X_1^{\eta_1} \cdots X_n^{\eta_n} =: t_2 \quad \text{if and only if either}$$

$$deg(t_1) < deg(t_2) \quad \text{or} \quad deg(t_1) = deg(t_2) \quad \text{and there is} \quad j : e_i = \eta_i, i < j, e_j > \eta_j$$

Application of Gröbner bases for elimination

Other applications of Gröbner bases will be quoted when will be nead; we just quote here a solution of the elimination problem, since we will need in several points.

Let $I \subset K[X_1, \ldots, X_n]$ be a 0-dimensional ideal. Denote $I_m := I \cap K[X_1, \ldots, X_m]$ for all $m \leq n$ (a "geometric" interpretation of this notion will be presented later).

Our general problem is, given $I$, to compute the ideal $I_m$. Let begin by introducing a class of orderings:

Denote by $\mathbf{T}(m)$ the free commutative subsemigroup of $\mathbf{T}$ generated by $X_1, \ldots, X_m$ and let us choose an ordering s.t. for each $i > m$, for each $t \in \mathbf{T}(m)$, $t < X_i$. For reasons which will become clear in the next theorem an order like that is called an *elimination ordering*, and even a $\{X_{m+1}, \ldots, X_n\}$-elimination ordering. Remark that the *lex* ordering is in this case for each $m$.

**Lemma 1** *Let $<$ be an elimination ordering and let $g \in K[X_1, \ldots, X_n]$. If $T(g) \in \mathbf{T}(m)$, then $g \in K[X_1, \ldots, X_m]$*

**Proof:** Since each term $t$ appearing in $g$ satisfies $t < T(g)$, obviously by the definition of an elimination ordering, $t \in \mathbf{T}(m)$ and so $g \in K[X_1, \ldots, X_m]$ ∎

**Corollary 1** *Let $G$ be a Gröbner basis of $I$ for an elimination ordering. Then $G \cap K[X_1, \ldots, X_m]$ is a Gröbner basis of $I_m = I \cap K[X_1, \ldots, X_m]$.* ∎

Since $\{X_{m+1}, \ldots, X_n\}$-elimination ordering are used to "eliminate" $X_i, i > m$" from $I$ allowing to compute $I \cap K[X_1, \ldots, X_m]$ the name is now explained and the Corollary 1 allows to solve the problem of computing $I_m$.

### Solving a System of Polynomial Equations

Let $K$ be a field with $\mathrm{char}(K) = 0$ and let $\mathcal{K}$ be its algebraic closure. Let $f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$, let

$$\mathcal{Z} := \mathcal{Z}(f_1, \ldots, f_s) := \{(x_1, \ldots, x_n) \in \mathcal{K}^n : f_i(x_1, \ldots, x_n) = 0\}$$

A subset $V \subset \mathcal{K}^n$ s.t. $V = \mathcal{Z}(f_1, \ldots, f_s)$ for some $f_1, \ldots, f_s$ is called an *algebraic variety.* If V is an algebraic variety, let

$$\mathcal{I}(V) := \{f \in K[X_1, \ldots, X_n] : f(a) = 0 \forall a \in V\}$$

Given this definitions, let us introduce the fundamental result of this Theory:

**Kronecker Theorem** *Let $f_1, \ldots, f_s \in K[X_1, \ldots, X_n], I = (f_1, \ldots, f_s), \mathcal{Z} := \mathcal{Z}(f_1, \ldots, f_s)$. Then $\mathcal{Z} = \emptyset$ if and only if $1 \in I$* ∎

Let $I$ denote the ideal generated by $(f_1, \ldots, f_s)$

**Lemma 2** $\forall f \in I, \forall (a_1, \ldots, a_n) \in \mathcal{Z}(f_1, \ldots, f_s), f(a_1, \ldots, a_n) = 0$

**Proof:** In fact $\exists g_i \in K[X_1, \ldots, X_n]$ s.t. $f = \sum_i g_i f_i$. ∎

Because of this, it is clear that if $(f_1, \ldots, f_s)$, $(g_1, \ldots, g_r)$ are basis of $I$, then

$$\mathcal{Z}(f_1, \ldots, f_s) = \mathcal{Z}(g_1, \ldots, g_r).$$

Because of this and of Lemma 2, it is natural to use the notation $\mathcal{Z}(J)$ to denote the zeroes of an ideal.

Only a weaker converse of Lemma 2 is true: for instance let consider $g = X^2 \in K[X]$, $I = (g)$, so $\mathcal{Z}(g) = \{0\}$; then $f =: X$ vanishes at 0 but is not in $I$; on the other side $f^2 \in I$. This example illustrates the following result:

**Hilbert'scher Nullstellensatz** *Let $f \in K[X_1, \ldots, X_n]$ be s.t. $f(a_1, \ldots, a_n) = 0$ $\forall (a_1, \ldots, a_n) \in \mathcal{Z}(J)$ then $\exists r$ s.t. $f^r \in J$.*

*In other words* $\mathcal{I}(\mathcal{Z}(J)) = \mathrm{Rad}(J)$

**Proof:** Consider the ideal $I := J + (1 - fT) \in K[X_1, \ldots, X_n, T]$; then $\mathcal{Z}(I) = \emptyset$; in fact assume $(x_1, \ldots, x_n, t) \in \mathcal{Z}(I)$;then $(x_1, \ldots, x_n) \in \mathcal{Z}(J)$, so that $f(x_1, \ldots, x_n) = 0$ and $1 - f(x_1, \ldots, x_n)t = 1 \neq 0$. By Kronecker theorem there are $g_i, h \in K[X_1, \ldots, X_n, T]$ s.t.

$$1 = h(1 - fT) + \sum g_i f_i$$

by substituting $T$ with $\frac{1}{f}$ and multiplying to get rid of denominators, we get the result ∎

Before stating another important result, we first need the following

**Lemma 3** *Let $L \supset K$ be a field extension. Let $f, f_1, \ldots, f_r \in K[X_1, \ldots, X_n]$. Let*

$$I := (f_1, \ldots, f_r) \subset K[X_1, \ldots, X_n]$$

$$J := (f_1, \ldots, f_r) \subset L[X_1, \ldots, X_n]$$

*Then $f \in I$ if and only if $f \in J$*

**Proof:** Let $f = \sum_i g_i f_i$ with $g_i \in L[X_1, \ldots, X_n]$. The coefficients of $g_i$ can be expressed linearly as a $K$-combination of a finite $K$-linear basis $\alpha_1 = 1, \alpha_2, \ldots, \alpha_t$ of $L$. So $f = \sum_{ij} g_{ij} f_i \alpha_j$ with $g_{ij} \in K[X_1, \ldots, X_n]$ and therefore $f = \sum_i g_{i1} f_i$. ∎

Using the same notation and the same argument of Lemma 3, it is easy to prove that

**Lemma 4** *Let $1 = \alpha_1, \alpha_2, \ldots, \alpha_t$ be a $K$-linear basis of $L$.*
*Let $g \in J$, $g = \sum_j g_j \alpha_j$ with $g_j \in K[X_1, \ldots, X_n]$. Then $g_1 \in I$.*

**Proof:** $\sum_j g_j \alpha_j = g = \sum_{ij} g_{ij} f_i \alpha_j$ implies $g_1 = \sum_{i1} g_{i1} f_i$. ∎

**Theorem 3** *Let $I$ be a non trivial ideal. The following are equivalent:*
*1) $\mathcal{Z}(I)$ is finite*
*2) $\forall i \exists p_i \in I \cap K[X_i]$*
*3) $K[X_1, \ldots, X_n]/I$ is a finite dimensional $K$-vector space.*
*4) $\forall i \exists d_i$ s.t. $X_i^{d_i} \in M(I)$ (w.r.t.* **any** *ordering).*

**Proof:**

1) $\Rightarrow$ 2) Let $\mathcal{Z}(I) = \{(a_{11}, \ldots, a_{1n}), \ldots, (a_{r1}, \ldots, a_{rn})\}$. Let $J = I\mathcal{K}[X_1, \ldots, X_n]$. Then $\mathcal{Z}(I) = \mathcal{Z}(J)$. Let $q_i(X_i) := (X_i - a_{1i}) \ldots (X_i - a_{ri}) \in \mathcal{K}[X_i]$. Then $q_i \in \mathrm{Rad}(J)$, so there is $s_i \in J \cap \mathcal{K}[X_i]$ and therefore (by Lemma 3) also $p_i \in I \cap K[X_i]$.

2) $\Rightarrow$ 1) If $(a_1, \ldots, a_n) \in Z(I)$, then $p_i(a_i) = 0$, which leaves only finitely many possibilities.

4) $\Rightarrow$ 3) The images of the terms $t \in \mathbf{T}$ s.t. $\deg_i(t) < d_i$ are a set of $K$-generators of $K[X_1, \ldots, X_n]/I$.

3) $\Rightarrow$ 2) The images of the powers of $X_i$ are linearly dependent.

2) $\Rightarrow$ 4) $M(p_i) \in M(I)$

**Example 1** Before discussing the results above, let us see three examples of ideal in $K[X, Y]$, let:

$$I_1 := (X^2 - 5X + 6, Y^2 - X)$$

$$I_2 := (X^3, X^2Y, XY^2, Y^3)$$

$$I_3 := (Y - X)$$

It is so easy, that you don't need this survey, to check that the solutions are:

$$\mathcal{Z}(I_1) = \{(2, \sqrt{2}), (2, -\sqrt{2}), (3, \sqrt{3}), (3, -\sqrt{3})\}$$

$$\mathcal{Z}(I_2) = \{(0, 0)\}$$

$$\mathcal{Z}(I_3) = \{(t, t) : t \in \mathcal{K}\}$$

and that conditions 2), 3) and 4) are satisfied only by $I_1, I_2$ and that, moreover denoting $A_i = K[X,Y]/I_i$ we have

$$dim(A_1) = 4 = \mathcal{Z}(I_1)$$

$$dim(A_2) = 6, \mathcal{Z}(I_2) = 1$$

$$dim(A_3) = +\infty, \mathcal{Z}(I_3) = +\infty$$

∎

**Remarks**

1) The theorems stated in this section allow to discriminate three different cases for the ideal $I \subset K[X_1, \ldots, X_n]$ and to do that by means of a Gröbner basis $G$ of $I$ w.r.t. **any** ordering
   * $\mathcal{Z}(I) = \emptyset$ which happens if and only if $1 \in I$, which is easily verified by checking whether $1 \in G$
   * $\mathcal{Z}$ is finite, which happens if and only if $K[X_1, \ldots, X_n]/I$ is a finite dimensional K-vector space, if and only if $\forall i$ there is a power of $X_i$ which is in $M(G) = M(I)$
   * $\mathcal{Z}$ is infinite, which happens if and only if $K[X_1, \ldots, X_n]/I$ is a infinite dimensional K-vector space, if and only if there is $i$ s.t. $\forall d\ X_i^d \notin M(G) = M(I)$
2) Ideal satisfying Theorem 3 are called 0-*dimensional*, in fact its solutions are just finitely many points. In fact the dimension of the variety $\mathcal{Z}(I)$, at least in the näif definition, can be translated to the ideal $I$ as follows:
   For an ideal $I \subset K[X_1, \ldots, X_n]$, $\dim(I)$, the *dimension* of $I$ is the maximal number of variables which are algebraically independent mod.$I$, i.e. $\dim(I) = d$ iff there are $d$ variables (w.l.o.g. after a permutation), $X_1, \ldots, X_d$ s.t.

$$I \cap K[X_1, \ldots, X_d] = (0)$$

$$I \cap K[X_1, \ldots, X_d, X_i] \neq (0) \quad \forall i > d$$

   They are usually called a *maximal set of independent variables.*
   Gröbner bases can be used to compute $\dim(I)$ and a maximal set of independent variables $X_{i_1}, \ldots, X_{i_d}$: in fact $\dim(I) = \dim(M(I) = \dim(\sqrt{M(I)})$ and a maximal set of indipendent variables for $\sqrt{M(I)}$ is such for $I$; the latter is computed by computing a maximal set of variables $X_{i_1}, \ldots, X_{i_d}$ such that no generators of $\sqrt{M(I)}$ depend only on this variables.
3) Let $I$ be 0-dimensional; the $K$-dimension of $K[X_1, \ldots, X_n]/I$ is called the *degree* of $I$, $\deg(I)$. Let $J = I\mathcal{K}[X_1, \ldots, X_n]$. A prime (maximal) ideal in $\mathcal{K}[X_1, \ldots, X_n]$ is the ideal of 1 point and has degree 1. By the Chinese Remainder Theorem, if $J$ is radical, $\deg(J)$ is therefore the cardinality of $\mathcal{Z}(J)$. If $J$ is primary (so $\text{card}(\mathcal{Z}(J) = 1)$ then by definition (but with a geometric meaning) $\deg(J)$ is called the *multiplicity* of $J$ (and of its single zero). Again by the Chinese Remainder Theorem, if $J$ is 0-dim., (so that its primaries are 0-dim too), $\deg(J)$ is therefore the numbers of zeroes of $J$, counted with multiplicity. Since a $K$-linear relation among terms gives rise to a $\mathcal{K}$-linear relation and conversely, $\deg(I) = \deg(J)$ and obviously $\text{card}(\mathcal{Z}(I) = \text{card}(\mathcal{Z}(J))$. So exactly as in the univariate case: *the degree is the number of zeroes counted with multiplicity.*
4) In the rest of this notes we will restrict ourselves to discuss how to solve a system of equation generating a 0-dimensional ideal.
5) We will see that solving a polynomial system of equations, consists to reduce the problem to solving a univariate polynomial equations. This means two things:
   1) we reduce the problem of solving a system of equations to solving one or more polynomial equations
   2) the theory is often obtained by extending it from the univariate polynomial case to the case of system of equations.
6) Both as an example to illustrate the last remark and because the following results will be used in this note to build examples, let us briefly discuss the notion of $\mathcal{K}$-conjugate zeroes. In the univariate case, if $\alpha_1 \in \mathcal{K}$ is a zero of the polynomial $f(X) \in K[X]$, then there is a unique irreducible factor $g(X) \in K[X]$ of $f(X)$, which is the minimal polynomial of $\alpha_1$. If we consider $g(X) \in \mathcal{K}[X]$ and factorize it on $\mathcal{K}$ we obtain linear factors

$$g(X) = (X - \alpha_1) \ldots (X - \alpha_s)$$

where the $\alpha_i$ are $\mathcal{K}$-conjugates of $\alpha_1$; moreover $g(X)$ is the generator of the ideal $J \cap K[X]$, where $J \subset \mathcal{K}[X[$ is the ideal generated by $(X - \alpha_1)$.
I apologize if I recalled this well-known result, which allowed me to recall the (perhaps not so) well-known generalization of it:
If $\mathbf{a} = (a_1, \ldots, a_n) \in \mathcal{Z}(I)$, where $I$ is a 0-dimensional ideal, then there is a unique 0-dimensional primary component $\mathbf{q}$ of $I$, whose prime is $Rad(\mathbf{q}) = \mathbf{p}$, and such that $\mathbf{a} \in \mathcal{Z}(\mathbf{p})$ . If we decompose $\mathbf{q}\mathcal{K}[X_1, \ldots, X_n]$ and $\mathbf{p}\mathcal{K}[X_1, \ldots, X_n]$ in primary decompositions, we obtain:

$$\mathbf{q}\mathcal{K}[X_1, \ldots, X_n] = \mathbf{q}_1 \cap \ldots \cap \mathbf{q}_s$$

$$\mathbf{p}\mathcal{K}[X_1, \ldots, X_n] = \mathbf{p}_1 \cap \ldots \cap \mathbf{p}_s$$

where:
- $\mathbf{q}_i$ is $\mathbf{p}_i$-prime
- $\mathbf{p}_i$ is linear: $\mathbf{p}_i = (X_1 - b_{1i}, \ldots, X_n - b_{ni})$
- denoting $\mathbf{b}_i = (b_{1i}, \ldots, b_{ni})$, one has $\mathcal{Z}(\mathbf{p}) = \{b_i : 1 \le i \le s\}$

so that $\mathbf{a}$ is one of the $\mathbf{b}_i$'s and the others are its $\mathcal{K}$-conjugates. What is more interesting for our examples is this other generalization:
- $\mathbf{p} = \mathbf{p}_1 \cap K[X_1, \ldots, X_n]$, $\mathbf{q} = \mathbf{q}_1 \cap K[X_1, \ldots, X_n]$

As we have discussed up to know and we will discuss later on, about applications of Gröbner bases to system solving, let us also discuss how to solve the following problem which we will need in order to present new examples:

**Problem** *Let $I \subset K[X_1, \ldots, X_n]$; let $P \subset K[Y_1, \ldots, Y_m]$ be a prime and let $\mathbf{K} := K[Y_1, \ldots, Y_m]/P = K[\alpha_1, \ldots, \alpha_m]$; let $\mathbf{b} \in \mathbf{K}^n \subset \mathcal{K}^n$ be an element in $\mathcal{Z}(I)$.*
*Let $\mathbf{q}_1 \subset \mathbf{K}[X_1, \ldots, X_n]$ be the primary component of $I$ with zero $\mathbf{b}$.*
*Then compute the primary component $\mathbf{q} \subset K[X_1, \ldots, X_n]$ of $I$ s.t. $\mathbf{b} \in \mathcal{Z}(\mathbf{q})$*

Assume that $P$ is generated by

$$f_1(Y_1, \ldots, Y_m), \ldots, f_r(Y_1, \ldots, Y_m)$$

and that $\mathbf{q}_1 \subset K(\alpha_1, \ldots, \alpha_m)[X_1, \ldots, X_n]$ is generated by

$$g_1(\alpha_1, \ldots, \alpha_m, X_1, \ldots, X_n), \ldots, g_s(\alpha_1, \ldots, \alpha_m, X_1, \ldots, X_n)$$

an easy solution is the following: let $J \subset K(Y_1, \ldots, Y_m, X_1, \ldots, X_n]$ be the ideal generated by

$$f_1(Y_1, \ldots, Y_m), \ldots, f_r(Y_1, \ldots, Y_m), g_1(Y_1, \ldots, Y_m, X_1, \ldots, X_n), \ldots, g_s(Y_1, \ldots, Y_m, X_1, \ldots, X_n)$$

then $\mathbf{q} = J \cap K[X_1, \ldots, X_n]$.

In fact if $\phi : K(Y_1, \ldots, Y_m, X_1, \ldots, X_n] \to \mathbf{K}[X_1, \ldots, X_n]$ is the morphism s.t. $\phi(Y_i) = \alpha_i$, then $J = \phi(\mathbf{q}_1)^{-1}$, $\phi(J) = \mathbf{q}_1$ so that $\mathbf{q} = \mathbf{q}_1 \cap K[X_1, \ldots, X_n] = J \cap K[X_1, \ldots, X_n]$

**Example 2** To give an easy example to convince the reader of this result, let us just consider the case of univariate polynomials. Let

$$f(X) = (X^2 - 2)^2 (X^2 - 3)^2$$

we choose $\mathbf{b} = \sqrt{2}$; then we take the ideal $P$ generated by $X^2 - 2$ to compute in $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[X]/P$; the primary component $\mathbf{q}_1$ of $I$ with zero $\mathbf{b}$ is of course the ideal generated by $(X - \sqrt{2})^2 = X^2 - 2\sqrt{2}X + 2)$.

Then we set $I = (Y^2 - 2, X^2 - 2YX + 2)$. A lex G-basis of $I$ is: $\{Y + 1/4X^3 - 3/2X, X^4 - 4X^2 + 4\}$ so correctly $I \cap K[X] = X^4 - 4X^2 + 4 = (X^2 - 2)^2$ ▮

**Exercise 1** Using Gröbner basis computes the prime $\mathbf{p}$ and primary $\mathbf{q}$ ideals in $\mathbb{Q}[X, Y]$ which
- $\mathbf{p}$ is s.t. $\mathbf{a} := (\sqrt{2} + \sqrt{3}, \sqrt{2}\sqrt{3}) \in \mathcal{Z}(\mathbf{p})$
- Denoting

$$\mathbf{q}_0 = \{(X - \sqrt{2} - \sqrt{3})^2, (Y - \sqrt{2}\sqrt{3})^2, (X - \sqrt{2} - \sqrt{3})(Y - \sqrt{2}\sqrt{3})\}$$

$\mathbf{q}$ has $\mathbf{q}_0$ as its primary component at $\mathbf{a}$

Moreover we want to compute the G-bases under the lex ordering with $Y < X$

In practice any computer algebra includes Gröbner basis computation, at least with a lex termordering and it also allows to apply a change of coordinates to a polynomial ring; all of this is what one needs to solve all the examples in this notes related to Gröbner basis and the reader is encouraged to try to solve these exercises with the computer algebra of his own choice.

Of course it is sufficient to compute over the ring $\mathbf{K} = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ i.e. $\mathbb{Q}[U,T]/P$, where $P = (U^2 - 2, T^2 - 3]$.

To obtain $\mathbf{p}$ we have of course to compute $\mathbf{p}_1 \cap \mathbb{Q}[X,Y]$, where $\mathbf{p}_1 = (X - \sqrt{2} - \sqrt{3}, Y - \sqrt{2}\sqrt{3}) \subset \mathbf{K}[X,Y]$. So we have

$$J = (U^2 - 2, T^2 - 3, X - U - T, Y - UT) \subset K[X,Y,U,T]$$

A lex Gröbner basis of $J$ under the ordering $Y < X < T < U$ is

$$\{T + XY - 3X, X^2 - 2Y - 5, U - XY + 2X, Y^2 - 6\}$$

so that

$$\mathbf{p} = \{X^2 - 2Y - 5, Y^2 - 6\}$$

and it is easy to verify that $\mathbf{a}$ is a zero of $\mathbf{p}$

As for the computation of $\mathbf{q}$, it is easy that

$$\begin{aligned}\mathbf{q}_0 =& \{(X - \sqrt{2} - \sqrt{3})^2, (Y - \sqrt{2}\sqrt{3})^2, (X - \sqrt{2} - \sqrt{3})(Y - \sqrt{2}\sqrt{3})\} = \\ =& \{2\sqrt{6} - 2\sqrt{3}X - 2\sqrt{2}X + X^2 + 5 - \sqrt{6}X - \sqrt{3}Y + 2\sqrt{3} - \sqrt{2}Y + 3\sqrt{2} + XY - 2\sqrt{6}Y + Y^2 + 6\}\end{aligned}$$

Therefore we have

$$J = \{U^2 - 2, T^2 - 3, 2TU - 2TX - 2UX + X^2 + 5, -TUX - TY + 2T - UY + 3U + XY, -2TUY + Y^2 + 6\}$$

A lex Gröbner basis of $J \subset K[X,Y,U,T]$ under the ordering $Y < X < T < U$ is

$$\begin{aligned}&\{T - 11/2X^3Y + 27/2X^3 + 13/6XY^3 + 11/2XY^2 - 23/2XY - 75/2X, X^4 - 4X^2Y - 10X^2 + 4Y^2 + 20Y + 25, \\ &\quad U + 9/2X^3Y - 11X^3 - 7/4XY^3 - 9/2XY^2 + 9XY + 30X, X^2Y^2 - 6X^2 - 2Y^3 - 5Y^2 + 12Y + 30, Y^4 - 12Y^2 + 36\}\end{aligned}$$

so that

$$\mathbf{q} = \{X^4 - 4X^2Y - 10X^2 + 4Y^2 + 20Y + 25, X^2Y^2 - 6X^2 - 2Y^3 - 5Y^2 + 12Y + 30, Y^4 - 12Y^2 + 36\}$$

## Structure theorem for 0-dimensional ideal

### Basissatze for 0-dimensional prime and primary ideal

In this section we will discuss some results mainly due to Gianni, which describe the structure of Gröbner bases for a 0-dimensional ideal. Some of this structure results have been used to improve system solving (and some of them are used in that section).

Let us begin by fixing notations to use throughout this section. Let $I$ be a 0-dimensional ideal in $K[X_1, \ldots, X_n]$. Denote

$I_i := I \cap K[X_1, \ldots, X_i]$

$A_i := K[X_1, \ldots, X_i]/I_i$

$\pi_i : K[X_1, \ldots, X_i] \to A_i$ the canonical projection and its polynomial extensions

$\pi = \pi_n : K[X_1, \ldots, X_n] \to K[X_1, \ldots, X_i]/I$

First of all, let's try to analize what informations on the lex Gröbner basis $G$ can be deduced by the fact that $I$ is 0-dimensional. Since $\forall i \exists d_i$ s.t. $X_i^{d_i} \in M(G)$, there is a polynomial $f_i \in K[X_1, \ldots, X_i] \setminus K[X_1, \ldots, X_{i-1}]$, monic s.t. $M(f_i) = X_i^{d_i}$. Moreover if $h \in G$, , $h \neq f_i$, then thanks to reduction, one has $\deg_k(h) < \deg_k(f_k), \forall k$.

We can therefore write

$$G = \{f_1, \ldots, f_n\} \cup \{h_{ij}\}$$

with $f_i \in K[X_1, \ldots, X_i] \setminus K[X_1, \ldots, X_{i-1}]$ monic, $h_{ij} \in K[X_1, \ldots, X_i] \setminus K[X_1, \ldots, X_{i-1}]$, $\deg_k(h) < \deg_k(f_k), \forall k \leq i$.

Once fixed the notation, let us begin by recalling a classical result by Gröbner (the references to G-basis are of course spurious), which is probably the pattern of the successive results.

**Nulldimensional Primbasissatz** *The following conditions are equivalent:*

*1) $I$ is prime*

*2) $\forall i \exists f_i \in K[X_1, \ldots, X_i] \setminus K[X_1, \ldots, X_{i-1}]$ s.t.*

*i) $\forall i, I_i = (f_1, \ldots, f_i)$*

*ii) $I = (f_1, \ldots, f_n)$*

*iii) $\forall i, f_i$ is monic in $X_i$*

*iv) $\forall i, \pi_{i-1}(f_i) \in A_{i-1}[X_i]$ is irreducible over the field $A_{i-1}$.*

*Moreover:*

*a) if $m_i := \deg(f_i)$, $m := m_1 \ldots m_n$, then $deg(I) = m$*

*b) $(f_1, \ldots, f_n)$ is a reduced lex G-basis of $I$*

*As a consequence:*

*c) each 0-dimensional prime ideal is maximal*

**Proof:**

Assume 2). By construction, inductively, each $A_i$ is a simple algebraic field extension of $A_{i-1}$ of degree $m_i$. Therefore each $I_i$ (and so also $I$) is maximal and so prime. This proves 2) $\Rightarrow$ 1) and c).

Ad b): $M(f_i)$ and $M(f_j)$ are relatively prime $\forall i, j, i \neq j$.

Ad 1) $\Rightarrow$ 2) Since I is prime and 0-dimensional, $I_1 = I \cap K[X_1] \neq (0)$ is prime, so it is generated by a monic irreducible polynomial $f_1$. So inductively, we can assume to have found $f_1, \ldots, f_{i-1}$ satisfying iii) and iv) and generating the prime ideal $I_{i-1}$. Since $I \cap K[X_i] \neq (0)$, $\pi_{i-1}(I_i) \neq (0)$ and is prime, so there is a monic polynomial $f_i \in K[X_1, \ldots, X_i] - K[X_1, \ldots, X_{i-1}]$ s.t. $\pi_{i-1}(f_i)$ is a generator of $\pi_{i-1}(I_i)$ and so it is irreducible. Also $I_i = (f_1, \ldots, f_i)$.

Ad a): we have a tower of finite algebraic simple extensions $K = A_0 \subset A_1 \subset \cdots \subset A_n$. ▮

**Corollary 2** *$I$ is prime if and only if*

*1) its reduced lex G-basis is $(f_1, \ldots, f_n)$*

*2) $\forall i, \pi_{i-1}(f_i) \in A_{i-1}[X_i]$ is irreducible* ▮

**Nulldimensional Primärbasissatz** *The following conditions are equivalent:*

*1) $I$ is primary*

*2) $\forall i, \exists f_i, g_i, h_{ij} \in K[X_1, \ldots, X_i] - K[X_1, \ldots, X_{i-1}]$, s.t. denoting*

*$J_i := (g_1, \ldots, g_i) \subset K[X_1, \ldots, X_i]$,*

*$\rho_i : K[X_1, \ldots, X_i] \to B_i := K[X_1, \ldots, X_i]/J_i$ the canonical projection and its polynomial extensions:*

*the following holds*

*i) $\forall i, f_i, g_i$ are monic in $X_i$*

*ii) $\forall i, (g_1, \ldots, g_i)$ is a primbasis of the prime ideal $J_i$*

*iii) $\rho_{i-1}(f_i)$ is a power of the irreducible polynomial $\rho_{i-1}(g_i)$*

*iv) $\deg_i(h_{ij}) < \deg_i(f_i), \rho_{i-1}(h_{ij}) = 0$*

*v) $I_i = (f_1, \ldots, f_i, \{h_{kj} : k \leq i\})$*

*Moreover:*

*a) if $h \in I_i, \deg_i(h) < \deg_i(f_i)$, then $\rho_{i-1}(h) = 0$*

*b) $J_i = \mathrm{Rad}(I_i)$*

Assume 2). Since a 0-dimensional ideal is primary if and only if its radical is prime, we have to prove that the prime ideals $J_i$ are the radicals of the ideals $I_i$. Inductively one has: $I_1 = (f_1), J_1 = (g_1), f_1 = g_1^r$ so $J_1 = \mathrm{Rad}(I_1)$.

Also, by iii), $f_i - g_i^r = p$ where $p \in J_{i-1}K[X_1, \ldots, X_i]$ and so for some $s$, $p^s \in I_{i-1}K[X_1, \ldots, X_i]$; therefore $g_i^{rs} = p^s + uf_i \in I_i$. So $J_i \subset \mathrm{Rad}(I_i)$ and by maximality, $J_i = \mathrm{Rad}(I_i)$. This proves 2) $\Rightarrow$ 1) and b).

Ad a): let $h \in I_i$, $\deg_i(h) < \deg_i(f_i)$, and let $h = pf_i + \sum p_j h_{ij} + u$, with $u \in I_{i-1}K[X_1, \ldots, X_i]$. Then

$$\rho_{i-1}(h) = \rho_{i-1}(p)\rho_{i-1}(f_i) + \sum \rho_{i-1}(p_j)\rho_{i-1}(h_{ij}) = \rho_{i-1}(p)\rho_{i-1}(f_i)$$

giving a contradiction on degrees unless $\rho_{i-1}(h) = 0$.

Let us prove 1) $\Rightarrow$ 2) Since $I$ is primary, each $I_i$ is primary. For $i = 1$, the statement 2) states the existence of polynomials $f_1$ and $g_1$, with $g_1$ irreducible and $f_1$ a power of it, s.t. $I_1 = (f_1)$, which is clearly true.

So assume to have proved 2) for $i-1$. $\rho_{i-1}(I_i) \subset B_{i-1}[X_i]$ so it is generated by a power of an irreducible monic polynomial. So there are $f_i, g_i \in K[X_1, \ldots, X_i]$ satisfying i) and iii).

$J_i = (g_1, \ldots, g_i)$ is then prime by the Primbasissatz. There are now polynomials

$$p_1, \ldots, p_s \in K[X_1, \ldots, X_i] - K[X_1, \ldots, X_{i-1}]$$

s.t. $I_i = I_{i-1} + (f_i, p_1, \ldots, p_s)$. By pseudodivision by $f_i$ we can assume $\deg_i(p_j) < \deg_i(f_i)$, so that by the argument on degree sketched above, $\rho_{i-1}(p_j) = 0$. ▮

**Corollary 3** *$I$ is primary if and only if its reduced lex G-basis satisfies:*
- *$\forall i$ there is $g_i$ monic s.t. $\rho_{i-1}(g_i)$ is irreducible and $\rho_{i-1}(f_i)$ is a power of it*
- *$\forall i, j, \rho_{i-1}(h_{ij}) = 0$* ▮

**Exercise 2** Verify the two Primbasissätze on the examples of Exercise 1, where clearly $\mathbf{p}$ is prime of $\mathbf{q}$

We have:

$$\mathbf{p} = \{X^2 - 2Y - 5, Y^2 - 6\}$$

$$\mathbf{q} = \{X^4 - 4X^2Y - 10X^2 + 4Y^2 + 20Y + 25, X^2Y^2 - 6X^2 - 2Y^3 - 5Y^2 + 12Y + 30, Y^4 - 12Y^2 + 36\}$$

It is easy to verify that $f_1 = Y^2 - 6 \in \mathbb{Q}[Y]$ and $f_2 = X^2 - 2\sqrt{6} - 5 \in (\mathbb{Q}[\sqrt{6}])[X]$ (where $K[\sqrt{6} = k[Y]/f_1[Y])$ are irreducible.

It is also easy to verify that

$$Y^4 - 12Y^2 + 36 = (Y^2 - 6)^2$$

$$X^4 - 4X^2Y - 10X^2 + 4Y^2 + 20Y + 25 = (X^2 - 2Y - 5)^2$$

and denoting $\rho_1 : \mathbb{Q}[X, Y] \to (\mathbb{Q}[\sqrt{6}])[X]$, the morphism s.t. $\rho_1(Y) = \sqrt{6}$ one has

$$\rho_1(X^2Y^2 - 6X^2 - 2Y^3 - 5Y^2 + 12Y + 30) = 0$$

So the example satisfies both Primbasissätze ▮

### Shape Lemma and structures for 0-dimensional ideal in generic positions

Let us consider a 0-dimensional ideal $I$, which has therefore only finitely many solutions. As we consider for instance the Primbasissatz we realize that the first coordinate can only partially discriminate the zeros, and the next coordinates are needed to discriminate them. This happens because projecting the points on the line $X_1 = 0$ causes that different points have the same projection.

On the other side, if the zeros are projected over a "generic" line, then the projections in general are separate

As we will see in the next paragraphs, the fact that different points are projected to the same point on the line $X_1 = 0$, creates problems in the two polynomial system algorithms we describe; on the other side both algorithms are improved if one chooses a generic line as first coordinate. It is therefore interesting to analize the properties of Gröbner bases when generic coordinates are chosen.

In particular one obtains the so called "Shape Lemmata" ([**G-M**]) which essentially reduce the problem of solving polynomial systems, to the problem of solving a single polynomial.

To make this approach more precise let us say that $I$ is in *generic position* if the first coordinates of the points of $\mathcal{Z}(I)$ are different each other.

Given a 0-dimensional $I$ there exists a homogeneous linear change of coordinates $L$:

$$L(X_1) := c_1X_1 + \sum_{j=2}^{n} c_jX_j, \quad c_j \in K$$
$$L(X_j) := X_jj > 1$$

such that $L(I)$ is in generic position. More exactly there exists a subvectorspace of $n$-tuples $(c_1,\dots,c_n)$ s.t. $L(I)$ is not a generic position. A change of coordinates which put $I$ in generic position will be called a *generic changement*

With this definition we are going to study the structure of a Gröbner basis of a 0-dimensional ideal in generic position and we will see that the structural theorems show that a generic change will essentially "reduce" a 0-dimensional ideal to a univariate polynomial; in particular prime, primary, radical ideals are so "reduced" to irreducible, irreducible power, squarefree polynomials.

**Nulldimensional Allgemeine Primbasissatz** *For a O-dimensional ideal $I$ in generic position the following conditions are equivalent:*
*1) $I$ is prime*
*2) $\exists f_1 \in K[X_1], \forall i > 1\ \exists g_i \in K[X_1]$ s.t.*
*i) $f_1$ is monic and irreducible*
*ii) $\forall i > 1, \deg(g_i) < \deg(f_1)$*
*iii) $I = (f_1, X_2 - g_2(X_1), \dots, X_n - g_n(X_1))$*

**Proof:**
$2) \Rightarrow 1)$ $K[X_1,\dots,X_n]/I \simeq K[X_1]/f_1$

$1) \Rightarrow 2)$ Let $f_1$ be the monic generator of $I \cap K[X_1]$, which is a prime ideal, so that $f_1$ is irreducible. Let $d := \deg(f)$. The roots of $f_1$ are the first coordinates of the zeroes of $I$, so $\dim_K(K[X_1]/f_1) = \dim_K(K[X_1,\dots,X_n]/I)$. Since $\pi(1),\dots,\pi(X_1^{d-1})$ are linearly independent in $K[X_1,\dots,X_n]/I$ and so a basis, therefore for each $i : \pi(X_i) = \sum_{j=0}^{d-1} c_{ij}\pi(X_1^j)$. Let $g_i := \sum c_{ij}X_1^j$. Then $X_i - g_i(X_1) \in I$. Since $(f_1, X_2 - g_2(X_1), \dots, X_n - g_n(X_1)) \subset I$, by a $K$-dim. count one has $I = (f_1, X_2 - g_2(X_1), \dots, X_n - g_n(X_1))$
∎

**Corollary 4** *$I$ is prime if and only if*
*1) its reduced lex G-basis is $(f_1, X_2 - g_2(X_1), \dots, X_n - g_n(X_1))$*
*2) $f_1$ is irreducible.* ∎

**Nulldimensional Allgemeine Radikalbasissatz** *For a O-dimensional ideal in generic position the following conditions are equivalent:*
*1) $I$ is radical*
*2) $\exists f_1 \in K[X_1], \forall i > 1\ \exists g_i \in K[X_1]$ s.t.*
*i) $f_1$ is monic and squarefree*
*ii) $\forall i > 1, \deg(g_i) < \deg(f_1)$*
*iii) $I = (f_1, X_2 - g_2(X_1), \dots, X_n - g_n(X_1))$*

**Proof:**
$2) \Rightarrow 1)$ $K[X_1,\dots,X_n]/I \simeq K[X_1]/f_1$

$1) \Rightarrow 2)$ Let $f_1$ be the monic generator of $I \cap K[X_1]$, which is a radical ideal, so that $f_1$ is squarefree. Let $d := \deg(f)$. The roots of $f_1$ are the first coordinates of the zeroes of $I$, so $dim_K(K[X_1]/f_1) = \dim_K(K[X_1,\dots,X_n]/I)$. Since $\pi(1),\dots,\pi(X_1^{d-1})$ are linearly independent in $K[X_1,\dots,X_n]/I$ and so a basis,therefore for each $i : \pi(X_i) = \sum_{j=0}^{d-1} c_{ij}\pi(X_1^j)$. Let $g_i := \sum c_{ij}X_1^j$. Then $X_i - g_i(X_1) \in I$. Since $(f_1, X_2 - g_2(X_1), \dots, X_n - g_n(X_1)) \subset I$, by a $K$-dim. count one has $I = (f_1, X_2 - g_2(X_1), \dots, X_n - g_n(X_1))$
∎

**Corollary 5** *I is radical if and only if*
*1) its reduced lex G-basis is* $(f_1, X_2 - g_2(X_1), \ldots, X_n - g_n(X_1))$
*2)* $f_1$ *is squarefree* ∎

**Exercise 3** To verify the Allgemeine Radikalbasissatz it could be useful to test on an example of a 0-dimensional ideal with many points. A tricky way is just to consider the ideal $I = (X^2+X, Y^2+Y, Z^2+Z) \in \mathbb{Q}[X,Y,Z]$. It is very easy to write down its 8 points. It is much more difficult to find a line s.t. the projections on it of the 8 points are different. Just as a first example let $L(X) = X+Y+Z, L(Y) = Y, L(Z) = Z$; a Gröbner basis computation $G$ of $L(I)$ returns a basis s.t.

$$G \cap Q[X] = X^4 - 6X^3 + 11X^2 - 6X$$

so that the 8 points project over just 4 of them (which ones?) If you think what are the 8 points, it is clear that a good change of coordinate is $L(X) = X + 2Y + 4Z, L(Y) = Y, L(Z) = Z$. A Gröbner basis of L(I) is:

$$f_1(X) = X^8 - 28X^7 + 322X^6 - 1960X^5 + 6769X^4 - 13132X^3 + 13068X^2 - 5040X$$

$$Y - 1/630X^7 + 7/180X^6 - 13/36X^5 + 14/9X^4 - 539/180X^3 + 343/180X^2 - 1/7X$$

$$Z + 1/252X^7 - 7/72X^6 + 337/360X^5 - 161/36X^4 + 791/72X^3 - 931/72X^2 + 2341/420X$$

satisfying the Shape Lemma statement.

Of course the zeroes of $f_1(X)$ are $\{0,1,2,3,4,5,6,7\}$. Just to verify how one can use the Shape lemma results to solve equations, let us denote $g_2(X), g_3(X)$ the polynomials such that $G = \{f_1, Y - g_2, Z - g_3)\}$; we have (check it with your computer algebra system)

| $X$ | $Y = g_2(X)$ | $Z = g_3(X)$ | $X - 2Y - 4Z$ |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 1 |
| 2 | 1 | 0 | 0 |
| 3 | 1 | 0 | 1 |
| 4 | 0 | 1 | 0 |
| 5 | 0 | 1 | 1 |
| 6 | 1 | 1 | 0 |
| 7 | 1 | 1 | 1 |

∎

**Nulldimensional Allgemeine Primärbasissatz** *For an ideal in generic position the following conditions are equivalent:*
*1)* $I$ *is primary*
*2)* $\forall i, \exists f_i, g_i, h_{ij} \in K[X_1, \ldots, X_i] - K[X_1, \ldots, X_{i-1}]$ *s.t. denoting*
$J_i := (g_1, \ldots, g_i) \subset K[X_1, \ldots, X_i]$
$\rho_i : K[X_1, \ldots, X_i] \to B_i := K[X_1, \ldots, X_i]/J_i$ *the canonical projection and its polynomial extensions:*
*i)* $\forall i, f_i, g_i$ *are monic in* $X_i$
*ii)* $g_1$ *is irreducible*
*iii)* $\forall i > 1, g_i$ *is linear in* $X_i$
*iv)* $\rho_{i-1}(f_i)$ *is a power of* $\rho_{i-1}(g_i)$
*v)* $\deg_i(h_{ij}) < \deg_i(f_i), \rho_{i-1}(h_{ij}) = 0$
*vi)* $I_i = (f_1, \ldots, f_i, \{h_{kj} : k \le i\})$

**Proof:** One can use the proof of the Primärbasissatz, remarking that $(g_1, \ldots, g_n) = \mathrm{Rad}(I)$ is a prime in generic position. ∎

**Exercise 4** It is now the time to test the Primbasissats and Primärbasissatz on the example of $\mathbf{p}$ and $\mathbf{q}$.

$$\mathbf{p} = \{X^2 - 2Y - 5, Y^2 - 6\}$$

$$\mathbf{q} = \{X^4 - 4X^2Y - 10X^2 + 4Y^2 + 20Y + 25, X^2Y^2 - 6X^2 - 2Y^3 - 5Y^2 + 12Y + 30, Y^4 - 12Y^2 + 36\}$$

Remark that since $\mathbf{p}$ has the root $(+\sqrt{2} + \sqrt{3}, \sqrt{6})$ its other 3 roots are

$$(+\sqrt{2} - \sqrt{3}, -\sqrt{6}), (-\sqrt{2} + \sqrt{3}, -\sqrt{6}), (\sqrt{2} - \sqrt{3}, +\sqrt{6}).$$

Since the 4 roots are distinguished by their $X$ coordinate, there is not even need to apply a change of coordinates, since it is sufficient to compute a lex basis over $\mathbb{Q}(X, Y)$ with $X < Y$.

We obtain the following bases:

$$\mathbf{p} = \{Y - 1/2X^2 + 5/2, X^4 - 10X^2 + 1\}$$

$$\begin{aligned}\mathbf{q} =& \{Y^2 - YX^2 + 5Y + 1/4X^4 - 5/2X^2 + 25/4, \\ & YX^4 - 10YX^2 + Y - 1/2X^6 + 15/2X^4 - 51/2X^2 + 5/2, X^8 - 20X^6 + 102X^4 - 20X^2 + 1\}\end{aligned}$$

About the last result, remark that:

$$X^8 - 20X^6 + 102X^4 - 20X^2 + 1 = (X^4 - 10X^2 + 1)^2$$

$$YX^4 - 10YX^2 + Y - 1/2X^6 + 15/2X^4 - 51/2X^2 + 5/2 = (X^4 - 10X^2 + 1)(Y - 1/2X^2 + 5/2)$$

$$Y^2 - YX^2 + 5Y + 1/4X^4 - 5/2X^2 + 25/4 = (Y - 1/2X^2 + 5/2)^2$$

▮

**Solving a System of 0-dimensional ideal: Auzinger-Stetter system algorithm**

Let $I = (f_1, \ldots, f_n) \subset K[X_1, \ldots, X_n]$ be a 0-dimensional ideal, and let it be also a radical ideal (so it has only simple zeros). Then the algebra $A := K[X_1, \ldots, X_n]/I$ has the set $O(I)$ as a $K$-linear basis; multiplication in $A$ by an element $g \in Span_K(O(I))$ is a linear morphism; let $M_g$ be the matrix representing it w.r.t. the basis $O(I)$. Let us moreover denote $\mathcal{Z}(I) = \{\alpha^{(1)}, \ldots, \alpha^{(s)}\}$, where $\alpha^{(i)} = (\alpha_1^{(i)}, \ldots, \alpha_n^{(i)})$. Let also $O(I) = \{1, t_2, \ldots, t_s\}$. Under this notation, the following holds [**A-S**]:

**Auzinger-Stetter Theorem** *The eigenvalues of $M_g^T$ are $\lambda_1 := g(\alpha^{(1)}), \ldots, \lambda_s := g(\alpha^{(s)})$.*

*Moreover, if all of them are distinct (which happens if the zeroes of $I$ are all simple and $g$ is sufficiently generic), then the eigenspace corresponding to $\lambda_j$ is generated by $(1, t_2(\alpha^{(j)}), \ldots, t_s(\alpha^{(j)}))$.*

**Proof:** Let us write $M_g^T = (m_{\lambda\rho})$ so that it holds

$$gt_\lambda = \sum_\rho m_{\lambda\rho} t_\rho \quad \forall\lambda$$

Evaluating it at $\alpha^{(j)}$ we obtain:

$$g(\alpha^{(j)}) t_\lambda(\alpha^{(j)}) = \sum_\rho m_{\lambda\rho} t_\rho(\alpha^{(j)}) \quad \forall\lambda$$

so that denoting

$$V(\alpha^{(j)}) = \left(1, t_2(\alpha^{(j)}), \ldots, t_s(\alpha^{(j)})\right)$$

we have

$$g(\alpha^{(j)}) V(\alpha^{(j)}) = M_g^T V(\alpha^{(j)})$$

▮

**Exercise 5** Compute the solutions of the ideal $I = \{X^2 - X, XY, Y^2 - Y\} \subset K[X, Y]$ trying $g = X$, $g = Y$, $g = X + 2Y$

Of course $O(I) = \{1, X, Y\}$ so that the matrix $M_X^T$ is

$$M_X^T = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

which therefore has a double eigenvalue 0 with eigenspace $\{(a, 0, b) : a, b \in \mathcal{K}\}$ from which the zeroes cannot be read off; and a simple eigenvalue 1 with eigenspace generated by $(1, 1, 0)$, from which we get the zero $(1, 0)$.

In the same way the matrix $M_Y^T$ is

$$M_Y^T = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

which therefore has again a double eigenvalue 0 with eigenspace $\{(a, b, 0) : a, b \in \mathcal{K}\}$ from which the zeroes cannot be again read off; and a simple eigenvalue 1 with eigenspace generated by $(1, 0, 1)$, from which we get the zero $(0, 1)$.

For $g = X + 2Y$ we have $M_g^T$ is

$$M_g^T = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

which has eigenvalues $0, 1, 2$ and the corresponding eigenspaces are generated by $(1, 0, 0)$, $(1, 1, 0)$, $(1, 0, 1)$ respectively, i.e. the eigenspaces are generated by $(1, X, Y)$ evaluated at $(0, 0), (1, 0), (0, 1)$ so that the three zeroes can be read off immediately.

Remark therefore that, even if the ideal has simple zeros they can be computed only if for some polynomials $g$ the matrix $M_g^T$ is such that its characteristic polynomial has simple roots. This means in particular that the projection is good only on a generic line or, equivalently, on a coordinate after a generic changement of coordinates ▮

**Exercise 6** Let apply the Auzinger-Stetter Algorithm to find the solutions of the example $\mathbf{p}$.

Since

$$\mathbf{p} = \{X^2 - 2Y - 5, Y^2 - 6\}$$

we have

$$O(\mathbf{p}) = \{1, X, Y, XY\}$$

so that

$$M_X^T = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 5 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \\ 12 & 5 & 0 & 0 \end{pmatrix}$$

whose determinant is $T^4 - 10T^2 + 1$;checking the exercise 4, you will see that the solutions of the determinant are in fact $\pm\sqrt{2} \pm \sqrt{3}$ to which you get the vectors:

$$\begin{array}{rl} \sqrt{2} + \sqrt{3} & (1, \sqrt{2} + \sqrt{3}, \sqrt{6}, 3\sqrt{2} + 2\sqrt{3}) \\ \sqrt{2} - \sqrt{3} & (1, \sqrt{2} - \sqrt{3}, -\sqrt{6}, 3\sqrt{2} - 2\sqrt{3}) \\ -\sqrt{2} + \sqrt{3} & (1, -\sqrt{2} + \sqrt{3}, -\sqrt{6}, -3\sqrt{2} + 2\sqrt{3}) \\ -\sqrt{2} - \sqrt{3} & (1, -\sqrt{2} - \sqrt{3}, +\sqrt{6}, -3\sqrt{2} - 2\sqrt{3}) \end{array}$$

**Exercise 7** Trying to check what happens applying the Auzinger-Stetter Algorithm to the example of $\mathbf{q}$ which has 4 roots of multiplicity 3 and requires to study a 12x12 matrix, it is to difficult. Since it is however interesting to understand what happens for multiple roots, let us study the following primaries of the point $(1,1)$ with multiplicity 3:

$$I_1 := ((X-1)^2, (X-1)(Y-1), (Y-1)^2) \quad O(I_1 := \{1, X, Y\}$$
$$I_2 := ((X-1)^3, Y-1) \quad ,O(I_1 := \{1, X, X^2\}$$
$$I_3 := (X-1, (Y-1)^3) \quad O(I_1 := \{1, Y, Y^2\}$$

$$M := M_X^T(I_1) = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 2 & 0 \\ -1 & 1 & 1 \end{pmatrix}$$

has only the eigenvalue $\lambda = 1$ with multiplicity 3. A Jordan solution returns the three vectors

$$v_1 = (1,1,1), v_2 = (0,1,0), v_3 = (0,0,1)$$

which satisfy

$$Mv_1 = \lambda v_1, Mv_2 = \lambda v_2 + v_1, Mv_3 = \lambda v_3$$

$$M := M_X^T(I_2) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -3 & 3 \end{pmatrix}$$

has only the eigenvalue $\lambda = 1$ with multiplicity 3. A Jordan solution returns the three vectors

$$v_1 = (1,1,1), v_2 = (0,1,2), v_3 = (0,0,1)$$

which satisfy

$$Mv_1 = \lambda v_1, Mv_2 = \lambda v_2 + v_1, Mv_3 = \lambda v_3 + v_2$$

$$M := M_X^T(I_3) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

has only the eigenvalue $\lambda = 1$ with multiplicity 3 and a dimension 3 for the eigenvalue space.

The relations between primary ideals at a multiple points and the Jordan systems of a matrix, which are just sketched in these examples, are discussed in [**S-M**]

### Solving a System of 0-dimensional ideal: Trinks system algorithm

#### Trinks algorithm

Another well-known algorithm ([**T**])to solve systems of equations for 0-dimensional ideal is a classical application of Gröbner basis.

Let $I \subset K[X_1, \ldots, X_n]$ be a 0-dimensional ideal. Denote $I_m := I \cap K[X_1, \ldots, X_m]$ for all $m \leq n$.

One has that $\mathcal{Z}(I_m) \subset \mathcal{K}^m$ is the projection of $\mathcal{Z}(I)$ over the first $m$ coordinates, i.e.:

$$\mathcal{Z}(I_m) = \{(x_1, \ldots, x_m) \subset \mathcal{K}^m : \exists x_{m+1}, \ldots, x_n \in \mathcal{K} : (x_1, \ldots, x_n) \in \mathcal{Z}(I)\}$$

(more exactly, it is the *closure* of the projection of $\mathcal{Z}(I)$). As a consequence:

**Trinks Theorem** *Let $(a_1, \ldots, a_{n-1}) \in \mathcal{K}^{n-1}$ be a zero of $I_{n-1}$, i.e. $(a_1, \ldots, a_{n-1}) \in \mathcal{Z}(I_{n-1})$. Let $\pi : K[X_1, \ldots, X_n] \to \mathcal{K}[X_n]$ be the morphism s.t. $\pi(f) = f(a_1, \ldots, a_{n-1}, X_n)$. Let $J := \pi(I) \subset \mathcal{K}[X_n]$. Then:*

*$a \in \mathcal{K}$ is a zero of $J$ iff $(a_1, \ldots, a_{n-1}, a)$ is a zero of $I$.*

**Proof:** Assume $(a_1, \ldots, a_{n-1}, a)$ is a zero of $I$ and let $h \in J$; let $g \in I$ be s.t. $h = \pi(g)$, so that $h(X_n) = g(a_1, \ldots, a_{n-1}, X_n)$; then $h(a) = g(a_1, \ldots, a_{n-1}, a) = 0$. Conversely, assume $a$ is a zero of $J$ and let $g \in I$, $h(X_n) = \pi(g) = g(a_1, \ldots, a_{n-1}, X_n)$. Then $g(a_1, \ldots, a_{n-1}, a) = h(a) = 0$. ▮

**Remarks**

1) Trinks Algorithm is of course based on induction: it essentially computes $\mathcal{Z}(I_m)$ in terms of the computation of $\mathcal{Z}(I_{m-1})$ and of course on the ability of solving univariate polynomials (in fact, $J$ is of course generated by a single polynomial).
2) The problem of solving a system of equations is so reduced by the Trink Algorithm to compute the zeroes of a univariate polynomial over a finite algebraic extension of K by explicitly given algebraic numbers. This will be done in some computational model for algebraic numbers. E.g. one could be interested just in the real roots and compute them either symbolically (by Sturm sequences) or numerically (but the resulting algorithm is unstable: for a numerical approach it is better to use Macaulay resultants). For the complex solutions one could either
   - use the classical computational method in which the roots are computed by giving the irreducible factors of a polynomial.
   - or the Duval method.
3) In order to apply an inductive Trinks Algorithm we need of course to be able to compute
   i) $I_m \; \forall m < n$
   ii) if $(a_1, \ldots, a_{m-1})$ is a zero of $I_{m-1}$, and using the notation of the Theorem, $\pi : K[X_1, \ldots, X_m] \to \mathcal{K}[X_m]$ be the morphism s.t. $\pi(f) = f(a_1, \ldots, a_{m-1}, X_m)$, we need to compute a univariate generator in $\mathcal{K}[X_m]$ of the ideal $J = \pi(I_m) \subset \mathcal{K}[X_m]$. Gröbner basis can be used for these problems:

   In fact problem i) is an elimination problem, which was already discussed in Corollary 1. An obvious solution of problem ii) (another one will be discussed later) consists of course in computing the set

$$H := \{\pi(g) : g \in G_m \setminus G_{m-1}\}$$

   and then computing the GCD of $H$ in $\mathcal{K}[X_m]$, which gives a generator of the ideal $J$.

### Trinks Algorithm

On the basis of the notes of this section, we can finally present the original Trinks Algorithm. There have been suggestions how to improve it, and we will discuss this argument, after presenting some further results on solving system of equations.

$Z :=$ **Solve**$(f_1, \ldots, f_r)$
  **where**
    $f_1, \ldots, f_r \in K[X_1, \ldots, X_n]$
    $I$ is the ideal generated by $(f_1, \ldots, f_r)$
    $Z = \{a : a \in \mathcal{Z}(I)\}$
  **Compute** *any* Gröbner basis of $(f_1, \ldots, f_r)$
  **If** $I$ is 0-dimensional **then**
    **Compute** the reduced lex G-basis $G$ of $(f_1, \ldots, f_r)$
    **Let** $p(X_1)$ be the unique element in $G \cap [X_1]$
    $Z_1 := \{a \in \mathcal{K} : p(a) = 0\}$
    **For** $i = 2 \ldots n$ **do**
      $Z_i := \emptyset$
      **For all** $(a_1, \ldots, a_{i-1}) \in Z_{i-1}$ **do**
        $H := \{g(a_1, \ldots, a_{i-1}, X_i) : g \in G_i \setminus G_{i-1}\}$
        $p := \mathrm{GCD}(H)$
        $Z := \{a \in \mathcal{K} : p(a) = 0\}$
        $Z_i := Z_i \cap \{(a_1, \ldots, a_{i-1}, a) : a \in Z\}$
  $Z := Z_n$

**Remarks**

- Checking if $I$ is 0-dimensional, or better if there are only finitely many solutions, can be done by the previously computed Gröbner basis.

- the statement

  **Compute** *any* Gröbner basis of $(f_1, \ldots, f_r)$

  in the presence of the next request of computing a *lex* G-basis is to be justified: a lex Gröbner basis is of course needed to compute $G_i \forall i$. Of course the lex Gröbner basis could be computed in the first step where it was required to compute *any* basis. The reasons for this are in the introduction of the FGLM algorithm: it can be faster to compute first a Gröbner basis (say for the deg-rev-lex) and use it to obtain the lex basis via the FGLM algorithm, than to compute the lex basis directly. The introduction of the FGLM algorithm in the Triks one will be discussed in the next section.

**Exercise 8** Apply the Trink algorithm to the same example $I = (X^2 - X, XY, Y^2 - Y) \subset K[X, Y]$

Clearly $I \cup K[X] = \{X^2 - X\}$, so that we get the solutions $x = 0, x = 1$; substituting $x = 0$ in $I$ we get the ideal $\{Y^2 - Y\}$ giving the solutions $y = 0, y = 1$; substituting $x = 1$ in $I$ we get the ideal $(Y, Y^2 - Y) = (Y)$ giving the solution $y = 0$.

So we have again the three solutions $(0,0), (0,1), (1,0)$ ▮

**Exercise 9** The example above shows that projection on the line $X = 0$ doesn't separate the points by their coordinates, so that it requires solving non linear polynomial. Since in a previous chapter we discussed about generic changement of coordinates, let's see their effect.

Let $L : K[X, Y] \to K[X, Y]$ be the change of coordinate $L(X) = X + 2Y, L(Y) = Y$. Let $I = \{X^2 - X, XY, Y^2 - Y\}$. Compute the lex Gröbner basis of $J = L(I)$ and apply the Trinks Algorithm to it.

One has $J = \{X^2 + 4XY + 4Y^2 - X - 2Y, XY + 2Y^2, Y^2 - Y\}$ and a Gröbner basis computation gives $G = \{X^3 + X^2 - 2X, Y - 1/6X^2 + 1/6X\}$. ¿From $X^3 + X^2 - 2X$ we get the solutions $x = 0, 1, -2$ so that plugging the solutions in the linear polynomial $Y - 1/6X^2 + 1/6X$ one gets the three solutions $(0,0), (1,0), (-2,1)$. Since these are the solutions of $L(I)$, applying to them the change of coordinate $L^{-1}$, which is $L^{-1}(a, b) = (a - 2b, b)$ we get again the solutions $(0,0), (1,0), (0,1)$ of $J$ ▮

**Exercise 10** Let us now apply the Trinks algorithm to compute the zeros of $\mathbf{p}, \mathbf{q}$

Since

$$\mathbf{p} = \{X^2 - 2Y - 5, Y^2 - 6\}$$

the solutions of $Y^2 - 6$ are $y = \pm\sqrt{6}$; so by plugging the solutions into $X^2 - 2Y - 5$ we have to solve the solutions $X^2 - 2\sqrt{6} - 5$ which returns the solutions $x = \pm\sqrt{2} \mp \sqrt{3}$ and $X^2 + 2\sqrt{6} - 5$ which returns the solutions $x = \pm\sqrt{2} \pm \sqrt{3}$

Let us apply Trinks algorithm to

$$\mathbf{q} = \{X^4 - 4X^2Y - 10X^2 + 4Y^2 + 20Y + 25, X^2Y^2 - 6X^2 - 2Y^3 - 5Y^2 + 12Y + 30, Y^4 - 12Y^2 + 36\}$$

of course since $Y^4 - 12Y^2 + 36 = (Y^2 - 6)^2$ we obtain $y = \pm\sqrt{6}$; naturally for $f(X, Y) = X^2Y^2 - 6X^2 - 2Y^3 - 5Y^2 + 12Y + 30$ we have $f(X, \pm\sqrt{6}) = 0$, while the equations

$$X^4 \mp 4\sqrt{6}X^2 - 10X^2 \pm 24 + 20\sqrt{6} + 25 = (X^2 \pm 2\sqrt{6} - 5)^2$$

which are solved as above. ▮

## Improvements to Trinks algorithm

### Splitting by polynomial factorization

**Lemma 5** *Let $I := J + (fg)$. Then*

$$\mathrm{Rad}(I) = \mathrm{Rad}(J + (f)) \cap \mathrm{Rad}(J + (g)), \quad \mathcal{Z}(I) = \mathcal{Z}(J + (f)) \cup Z(J + (g))$$

**Proof:** Let $a \in \mathcal{K}^n, a \in \mathcal{Z}(I)$. Then $h(a) = 0 \forall h \in J$ and $f(a)g(a) = 0$. Therefore either $f(a) = 0$ and $a \in \mathcal{Z}(J + (f))$ or $g(a) = 0$ and $a \in \mathcal{Z}(J + (g))$.

Conversely if $a \in \mathcal{Z}(J + (f))$, then $h(a) = 0 \forall h \in J$ and $f(a)g(a) = 0$, so $a \in \mathcal{Z}(I)$. ▮

For large systems where the solutions are expected to come into many different conjugate sets (e.g. in chemical applications), one could factorize the polynomials appearing during the G-basis computation and split the problem according to the result above; i.e. each time a polynomial is factorized as $fg$, the G-basis computation is restarted on $(I, f)$ and on $(I, g)$ separately **[MMN]**.

### Improvement by the Gianni-Kalkbrenner theorem

Let us recall the problem ii) related to the Trinks Algorithm.

Let us assume $I$ has finitely many solutions and $G$ is its reduced Gröbner basis w.r.t. *lex*, so that $G_m := G \cap K[X_1, \ldots, X_m]$ is a Gröbner basis of $I_m = I \cap K[X_1, \ldots, X_m]$; let $(a_1, \ldots, a_{m-1})$ is a zero of $I_{m-1}$, and let $\pi : K[X_1, \ldots, X_m] \to \mathcal{K}[X_m]$ be the morphism s.t. $\pi(f) = f(a_1, \ldots, a_{m-1}, X_m)$ and let $J = \pi(I_m) \subset \mathcal{K}[X_m]$.

The problem is to compute the polynomial in $\mathcal{K}[X_m]$ which generates $J$. We present here a proposed improvement by Gianni and Kalkbrenner.

We need some notation: let us also consider the elements of $G_m$ as univariate polynomials in $X_m$ with coefficients in $K[X_1, \ldots, X_{m-1}]$ and denote the leading coefficient of $g \in G_m$ by $lp(g) \in K[X_1, \ldots, X_{m-1}]$, i.e.

$$g = lp(g)(X_1, \ldots, X_{m-1})X_m^d + h_{d-1}(X_1, \ldots, X_{m-1})X_m^{d-1} + \cdots + h_0(X_1, \ldots, X_{m-1})$$

An improvement has been proposed by Gianni **[G]** and Kalkbrenner **[K]**.

**Lemma 6** *There is $g \in I_m$ s.t. $\pi(g)$ generates $J$ and $\pi(lp(g)) \neq 0$, i.e. $\deg_m(g) = \deg(\pi(g))$*

**Proof:** First assume that $I$ is primary. Then by the Nulldimensional Primärbasissatz, $\pi(I)$ is generated by the image of the monic polynomial in the lex G-basis of $I$; so the result is obvious. In the general case let $I = \cap_j I_j = \prod_j I_j$ be an irredundant primary decomposition (Recall that if $I, J$ are 0-dimensional primary ideals belonging to different primes then $I \cap J = IJ$ by the Chinese Remainder Theorem).

For each $I_j$ there is $g_j \in I_j$ s.t. $\pi(g_j)$ generates $\pi(I_j)$ and $\pi(lp(g_j)) \neq 0$. Let $g := \prod_j g_j$. Then $\pi(lp(g)) = \prod_j \pi(lp(g_j)) \neq 0$. Moreover $\pi(g)$ generates $\prod_j \pi(I_j) = \pi(\prod_j I_j) = \pi(I)$.

**Lemma 7** *$\pi(G_m)$ is a G-basis for $\pi(I_m)$*

**Proof:** For $g \in K[X_1, \ldots, X_m]$ denote $L(g) := Lp(g)X_n^r, r = deg_n(g)$. Denote $L(I) := (L(g) : g \in I)$ Remark that if $g \in I_{m-1}$ then $L(g) = g, \pi(L(g)) = 0$; therefore $\pi(L(I)) = \pi(L(G)) \subset M(\pi(G)) \subset M(\pi(I))$. Let now $g$ be as in the previous Lemma 6 and let $r := deg_m(g) = deg(\pi(g))$, let $g = \sum_i h_i g_i$ be a G-representation, let $J := \{i : deg_m(h_i g_i) = deg_m(g)\}$, then: $lp(g) = \sum_J lp(h_i)lp(g_i)$. Since $\pi(lp(g)) \neq 0$, there is $i$ s.t. $\pi(lp(g_i)) \neq 0$. So $M(\pi(I)) = (X_n^r) \subset \pi(L(I))$ and therefore $M(\pi(G)) = M(\pi(I))$.

**Theorem 4** *Let $g \in G_m \setminus G_{m-1}$ be a polynomial of minimal $X_m$-degree in $G$ s.t. $\pi(lp(g)) \neq 0$. Then $\pi(I_m) = (\pi(g))$.*

**Proof:** Remark that the proof of the previous Lemma, guarantees that there is an element $h \in G_m \setminus G_{m-1}$ s.t. $\pi(h)$ generates $\pi(I_m)$ and moreover $\pi(lp(h)) \neq 0$. Clearly if $f \in G_m \setminus G_{m-1}$ s.t. $\pi(lp(f)) \neq 0$, then $M(\pi(f)) \in M(\pi(I_m))$, so $M(\pi(h))$ divides $M(\pi(f))$, which means that $X_m$-degree of $f$ is greater than that of $h$. Therefore $h \in G_m \setminus G_{m-1}$ is the only polynomial of minimal $X_m$-degree in $G$ s.t. $\pi(lp(h)) \neq 0$.▮

As a consequence of the Gianni-Kalkbrenner result, the following lines of the Trinks algorithm

$H := \{g(a_1, \ldots, a_{i-1}, X_i) : g \in G_i \setminus G_{i-1}\}$
$p := \text{GCD}(H)$
$Z := \{a \in \mathcal{K} : p(a) = 0\}$

can be substituted by the simpler:

**Choose** the least element $p$ in $G$ (according to increasing maximal term) s.t. $p \in G_i \setminus G_{i-1}\}$ and $lp(q)((a_1, \ldots, a_{i-1}) = 0$
$Z := \{a \in K : p(a) = 0\}$

so that we obtain this version of the algorithm:

$Z := \mathbf{Solve}(f_1, \ldots, f_r)$
**where**
$f_1, \ldots, f_r \in K[X_1, \ldots, X_n]$
$I$ is the ideal generated by $(f_1, \ldots, f_r)$
$Z = \{a : a \in \mathcal{Z}(I)\}$
**Compute** *any* Gröbner basis of $(f_1, \ldots, f_r)$
**If** $I$ is 0-dimensional **then**
**Compute** the reduced lex G-basis $G$ of $(f_1, \ldots, f_r)$
**Sort** $G$ by increasing maximal terms
$p_i := Min(g \in G : g \in K[X_1, \ldots X_i])$
$Z_1 := \{a \in \mathcal{K} : p_1(a) = 0\}$
**For** $i = 2 \ldots n$ **do**
$Z_i := \emptyset$
**For all** $(a_1, \ldots, a_{i-1}) \in Z_{i-1}$ **do**
$q := p_j$
**While** $lp(q)((a_1, \ldots, a_{i-1}) = 0$ **do**
$q := \mathbf{Next}(q, G)$
$Z := \{a \in \mathcal{K} : q(a) = 0\}$
$Z_i := Z_i \cap \{(a_1, \ldots, a_{i-1}, a) : a \in Z\}$
$Z := Z_n$

### Using the FGLM algorithm

Practical analysis of Buchberger Algorithm have shown that usually to compute a G-basis for deg-rev-lex is much faster than for lex. However deg-rev-lex is useless for elimination, which can be instead computed by means of lex ordering: in fact in the Trinks algorithm, the lex G-basis is used to have in **one** computation all elimination ideals $I_j := I \cap K[X_1, \ldots, X_j]$

A more recent algorithm (FGLM) was suggested which given a Gröbner basis $G_1$ of a 0-dim. ideal $I \subset K[X_1, \ldots, X_n]$ with respect to a term-ordering $<_1$ and given a different term-ordering $<_2$, allows to compute, by linear algebra methods, a Gröbner basis $G_2$ of $I \subset K[X_1, \ldots, X_n]$ with respect to $<_2$.

The suggestion of [**FGLM**] was then to apply the algorithm to obtain the lex G-basis given the deg-rev-lex one.

Experiments shown that usually the faster way to compute a lex G-bases is by computing the deg-rev-lex G-basis and applying FGLM. The FGLM idea has been modified and improved by suggestion of Faugere [**F**]and Traverso et al. [**GMRT**]

Either using FGLM of other similar ideas, it is possible to use **any** Gröbner basis of $I$ to compute its reduced lex Gröbner basis and in such a way that it is sorted by increasing maximal terms. Using it we obtain the following variant.

$Z := \mathbf{Solve}(f_1, \ldots, f_r)$
**where**
$f_1, \ldots, f_r \in K[X_1, \ldots, X_n]$
$I$ is the ideal generated by $(f_1, \ldots, f_r)$
$Z = \{a : a \in \mathcal{Z}(I)\}$
**Compute** *any* Gröbner basis of $(f_1, \ldots, f_r)$
**If** $I$ is 0-dimensional **then**
**Compute** the reduced lex G-basis $G$ of $(f_1, \ldots, f_r)$ by some FGLM convesion algorithm, such that $G$ is sorted by increasing maximal terms.
$p_i := Min(g \in G : g \in K[X_1, \ldots X_i])$
$Z_1 := \{a \in \mathcal{K} : p_1(a) = 0\}$
**For** $i = 2 \ldots n$ **do**
$Z_i := \emptyset$
**For all** $(a_1, \ldots, a_{i-1}) \in Z_{i-1}$ **do**
$q := p_j$

$$
\begin{array}{l}
\quad\quad \textbf{While } lp(q)((a_1,\ldots,a_{i-1}) = 0 \textbf{ do} \\
\quad\quad\quad q := \textbf{Next}(q, G) \\
\quad\quad Z := \{a \in \mathcal{K} : q(a) = 0\} \\
\quad\quad Z_i := Z_i \cap \{(a_1,\ldots,a_{i-1},a) : a \in Z\} \\
Z := Z_n
\end{array}
$$

### An algorithm for computing the radical of a 0-dimensional ideal

The computation of zeroes of a 0-dimensional ideal $I$ can be obviously reduced to the computation of zeros of its radical, $\mathrm{Rad}(I)$; if this ideal is in generic position, the structure theorem can then be used: computing the zeroes just requires factoring a univariate squarefree polynomial. Let us discuss an algorithm by Gianni **[G-M]** to compute the radical of a 0-dimensional ideal.

**Lemma 8** *Let $I, J \subset K[Y_1,\ldots,Y_m]$ be zero-dimensional ideals s.t. $I + J = (1)$. Let*

$$I' := (I, X - p'(Y_1,\ldots,Y_m)) \subset K[Y_1,\ldots,Y_m,X]$$

$$J' := (J, X - p"(Y_1,\ldots,Y_m)) \subset K[Y_1,\ldots,Y_m,X]$$

*Then there is a polynomial $q \in K[Y_1,\ldots,Y_m]$, s.t. $I' \cap J' = (I \cap J, X - q)$.*

**Proof:** By the Chinese Remainder Theorem, there is a polynomial $q \in K[Y_1,\ldots,Y_m]$, unique $\mathrm{mod} I \cap J$, s.t. $q - p' \in I, q - p" \in J$. Hence $X - q \in I' \cap J'$, and, since it is linear in X, it is the generator of $I' \cap J'$ mod $.I \cap J$. ▮

**Lemma 9** *Let $I$ be a 0-dimensional ideal; let $G$ be its reduced lex Gröbner basis. Let $\{g\} = G \cap K[X_1]$. Let $c \in K$ and let $L_c$ be the linear change of coordinates:*

$$
\begin{aligned}
L_c(X_1) :=& X_1 + cX_n \\
L_c(X_i) :=& X_i
\end{aligned}
$$

*If $g$ is squarefree, then for almost all choices of $c$, $X_n \in M(L_c(I))$.*

**Proof:** Let

$$(a_{11},\ldots,a_{1n}),\ldots,(a_{d1},\ldots,a_{dn})$$

be the distinct zeros of $I$. Since $g$ is squarefree, $a_{i1} \neq a_{j1}$ if $i \neq j$. Then the zeros of $L_c(I)$ are

$$(b_{11},a_{12},\ldots,a_{1n}),\ldots,(b_{d1},a_{d2},\ldots,a_{dn})$$

with $b_{i1} = a_{i1} + ca_{in}$ and for almost of choices of $c$, one still has $b_{i1} \neq b_{j1}$ if $i \neq j$.

Let $J := L_c(I)\mathcal{K}[X_1,\ldots,X_n]$, $J = \cap_{i=1}^d J_i$ the primary decomposition, where each $J_i$ has the single zero $(b_{i1},a_{i2},\ldots,a_{in})$ with some multiplicity. Let $J' := J \cap k[X_1,\ldots,X_{n-1}]$, $J'_i := J_i \cap \mathcal{K}[X_1,\ldots,X_{n-1}]$. If $i \neq j$, since $b_{i1} \neq b_{j1}$, $J'_i$ and $J'_j$ are relatively prime. Also $J_i = J'_i + (cX_n + X_1 - a_{i1})$. So there is a polynomial $h \in \mathcal{K}[X_1,\ldots,X_{n-1}]$ s.t. $J = (\cap J'_i, X_n - h) = (J', X_n - h)$. Since $J$ is generated by polynomials in $K[X_1,\ldots,X_n]$, $h \in K[X_1,\ldots,X_n]$. ▮

**Example 3** To support this statement let us show some examples. We start with the very symple example $I = (X, Y^2)$ and we choose the linear change of coordinates $L(X) = X + Y), L(Y) = Y$; we obtain then $J = L(I) = (X + Y, Y^2) = (X^2, X + Y)$; as in the theorem we have also $J' = (X^2), J = (J', X + Y)$

And now let us consider the effect to an ideal with several multiple roots, like $I = (X^3 + X, Y^2 + 2XY + X^2)$, with roots $(-1,-1),(0,0),(1,1)$; applying $L(X) = X + Y), L(Y) = Y$ we obtain

$$
\begin{aligned}
J = L(I) =& (Y^3 + 3Y^2X + 3YX^2 - Y + X^3 - X, 4Y^2 + 4YX + X^2) \\
=& (Y + 3/64X^5 - 5/16X^3 + X, X^6 - 8X^4 + 16X^2)
\end{aligned}
$$

where $X^6 - 8X^4 + 16X^2 = (X^3 - 4X)^2$

Clearly $I$ is the intersection of the three ideals

$$I_1 = (X+1, Y^2 - 2Y + 1)$$
$$I_2 = (X, Y^2)$$
$$I_3 = (X-1, Y^2 + 2Y + 1)$$

and $J$ is the intersection of

$$J_1 = L(I_1) = (Y + X + 1, Y^2 - 2Y + 1) = (Y + X + 1, X^2 + 4X + 4)$$
$$J_2 = L(I_2) = (Y + X, Y^2) = (Y + X, X^2)$$
$$J_3 = L(I_3) = (Y + X - 1, Y^2 + 2Y + 1) = (Y + X - 1, X^2 - 4X + 4)$$

and finally it is easy to verify that

$$\begin{aligned} 3/64X^5 - 5/16X^3 + X &= X + 1 \bmod X^2 + 4X + 4 \\ &= X \bmod X^2 \\ &= X - 1 \bmod X^2 - 4X + 4 \end{aligned}$$

▮

**Theorem 5** *Let $I$ be a 0-dimensional ideal; let $G$ be its reduced lex Gröbner basis. Let $g = G \cap K[X_1]$ and let $i$ be the least index s.t. for $j > i, X_j \in M(I)$. Then:*

1) *If $g$ is not squarefree, let $g'$ be a squarefree polynomial with the same roots of $g$; then $I' := (G \cup \{g'\})$ is s.t. $I \subset I'$, $I \neq I'$ and $\mathrm{Rad}(I) = \mathrm{Rad}(I')$.*
2) *if $g$ is squarefree, and $i = 1$, then $I$ is radical*
3) *if $g$ is squarefree and $i > 1$, let $c \in K$ and let $L_c$ be the linear change of coordinates:*

$$L_c(X_1) := X_1 + cX_i$$
$$L_c(X_j) := X_j$$

*Then for almost all choices of $c$, for $j \geq i, X_j \in M(L_c(I))$ (the univariate polynomial in the reduced Gröbner basis of $L_c(I)$ is not necessarily squarefree).*

**Proof:**

1) Clearly $g' \notin I$ so $I \subset I', I \neq I'$ and $\mathrm{Rad}(I) \subset \mathrm{Rad}(I')$. Since $g'$ has the same roots as $g$, $g' \in \mathrm{Rad}(I)$ so $\mathrm{Rad}(I') = \mathrm{Rad}(I)$.
2) It follows from the Nulldimensional Allgemeine Radikalbasissatz
3) By assumption there are polynomials $g_j(X_1), j = i+1 \dots n$ s.t. $G = \{X_j - g_j(X_1) : j = i+1 \dots n\} \cup G'$, $G' := G \cap K[X_1, \dots, X_i]$. Then, for almost all choices of $c$, $X_i \in M(L_c(I))$. Since $X_j - g_j(cX_i + X_1) \in L_c(I)$ for $j = i+1 \dots n$, the thesis follows. ▮

The following algorithm then computes the radical of a zero-dimensional ideal; at its termination it return an ideal $J$ and numbers $c_i \in K$, $2 \leq i \leq n$ such that $J$ is radical and in generic position and $J = rad(L(I))$ where

$$L(X_1) = X_1 + \sum c_i X_i$$
$$L(X_i) = X_i$$

$J := I$
**For** $i = 2 \dots n$ **do**
  $c_i := 0$
**Compute** $G$ the reduced lex G-basis of $J$
**Repeat**
  **Let** $g$ be s.t. $\{g\} = G \cap K[X_1]$

**If** $g$ is not squarefree then
  $h :=$ **SQFR**$(g)$
  $J := (G \cup \{h\})$
  **Compute** $G$ the reduced lex G-basis of $J$
**Let** $i$ the least index s.t. for $j > i, X_j \in M(J)$
**If** $i > 1$ **then**
  **choose random** $c \in K$
  $c_i := c_i + c$
  $J := L_c(J)$
  **Compute** $G$ the reduced lex G-basis of $J$
**Until** $g$ is squarefree and $i = 1$

**Exercise 11** As an example, let us apply the Gianni algorithm to the ideal

$$\begin{aligned}\mathbf{q} =&\{X^4 - 4X^2Y - 10X^2 + 4Y^2 + 20Y + 25,\\ &X^2Y^2 - 6X^2 - 2Y^3 - 5Y^2 + 12Y + 30, Y^4 - 12Y^2 + 36\} \subset \mathbb{Q}[Y, X]\end{aligned}$$

Since of course $Y^4 - 12Y^2 + 36 = (Y^2 - 6)^2$,we have to compute the lex G-basis of

$$\begin{aligned}&\{X^4 - 4X^2Y - 10X^2 + 4Y^2 + 20Y + 25, X^2Y^2 - 6X^2 - 2Y^3 - 5Y^2 + 12Y + 30,\\ &Y^4 - 12Y^2 + 36, Y^2 - 6\}\end{aligned}$$

we still use the ordering $Y < X$ which gives us

$$I = \{X^4 - 4X^2Y - 10X^2 + 20Y + 49, Y^2 - 6\}$$

we then perform the change of coordinate

$$L(Y) = Y + X, L(X) = X$$

and we compute the Gröbner basis of $L(J)$ which gives

$$X + 11/384Y^7 - 13/384Y^6 - 157/128Y^5 - 165/128Y^4 + 1835/128Y^3 + 5587/128Y^2 + 15587/384Y + 3419/384$$

$$Y^8 - 44Y^6 - 96Y^5 + 438Y^4 + 2112Y^3 + 3316Y^2 + 2208Y + 529$$

Finally since:

$$Y^8 - 44Y^6 - 96Y^5 + 438Y^4 + 2112Y^3 + 3316Y^2 + 2208Y + 529 = (Y^4 - 22Y^2 - 48Y - 23)^2$$

the radical of $\mathbf{q}$ is then

$$X + 11/384Y^7 - 13/384Y^6 - 157/128Y^5 - 165/128Y^4 + 1835/128Y^3 + 5587/128Y^2 + 15587/384Y + 3419/384$$

$$Y^4 - 22Y^2 - 48Y - 23$$

whose Gröbner basis is

$$\{Y^4 - 22Y^2 - 48Y - 23, X + 1/4Y^3 - 1/4Y^2 - 19/4Y - 25/4\}.$$

It is easy to verify that the basis above is in fact the G-basis of $L(\mathbf{p})$ ▮

### Lazard's triangular systems

The notion of *triangular system* was introduced by Lazard [**L92**].

Let say that a triangular system $\{f_1, \ldots, f_n\} \subset K[X_1, \ldots, X_n]$ is such that:

-) $\forall i$ $f_i$ is a monic polynomial in $Xi$ with coefficients over $K[X_1, \ldots, X_{i-1}]$

i.e.

$$\begin{Bmatrix} f_1(X_1) = X_1^{d_1} + \sum_{i=0}^{d_1+1} g_{1i} X_1^i \\ f_2(X_1, X_2) = X_2^{d_2} + \sum_{i=0}^{d_2+1} g_{2i}(X_1) X_2^i \\ \dots \\ f_n(X_1, \dots, X_n) = X_n^{d_n} + \sum_{i=0}^{d_n+1} g_{ni}(X_1, \dots, X_{n-1} X_n^i \end{Bmatrix}$$

Given a triangular system it is obvious how to solve it and Trinks algorithm already explain how to do it: you first solve the system $f_1(X_1) = 0$ and you plug in the solution $X_1 = a_1$ in the other polynomials and then solve the system $f_2(a_1, X_2) = 0$, etc. What is even more interesting is that $\{f_1, \dots, f_n\}$ is a Gröbner basis and is the system of equations discussed by many Basissätze.

Lazard ([**L92**]) not only introduced the idea of triangular system but proposed algorithms which solved the following problem

**Problem** *Given a 0-dim. ideal $I \subset K[X_1, \dots, X_n]$, returns sets of triangular systems*

$$\{f_1^{(1)}, \dots, f_n^{(1)}\}, \dots \{f_1^{(s)}, \dots, f_n^{(s)}\}$$

*so that*

$$\mathcal{Z}(I) = \cup_s \mathcal{Z}(f_1^{(s)}, \dots, f_n^{(s)})$$

The same problem is also discussed by Möller [**M**].

## References


[**A-S**] W. Auzinger, J. Stetter, *An elimination algorithm for the computation of all zeros of a system of multivariate polynomial equations*, Int. Ser. Num. Math. **86** (1988), 11 – 30

[**F**] J.C. Faugère, Resolutions des systems d'equations algebriques, , *Ph. D. Thesis*, Univ. Paris 6 (1994)

[**FGLM**] J.C. Faugère, P. Gianni, D. Lazard, T. Mora, Efficient change of ordering for zero-dimensional Gröbner bases, *J. Symb. Comp.*, to appear

[**G-M**] P. Gianni, T. Mora, *Algebraic solution of systems of polynomial equation using Gröbner bases*, Proc. AAECC 5, LNCS **356** (1989), 247–257

[**GMRT**] P. Gianni, T. Mora, L. Robbiano, C. Traverso, Hilbert functions and Buchberger algorithm, *Preprint*

[**L92**] D. Lazard, *Solving zero-dimensional algebraic systems*, J. Symb. Comp. **136** (1992), 117–131

[**L93**] D. Lazard, *Systems of algebraic equations (algorithms and complexity)*, in D. Eisenbud, L. Robbiano Eds. *Computational Algebraic Geometry and Commutative Algebra*, D. Eisenbud, L. Robbiano Eds., Cambridge (1993), 106–150

[**MMN**] H.Melenk, H.M. Möller, W. Neun *On Groebner bases computation on a supercomputer using Reduce* (1988), Preprint

[**Mö**] H.M. Möller, *On decomposing systems of polynomial equations with finite many solutions*, AAECC **4** 217–230 (1993)

[**Mo**] T. Mora, *An introduction to commutative and non-commutative Gröbner bases*, Theor. Comp. Sci., to appear

[**S-M**] H. Stetter, M. Möller, *Multivariate Polynomial Equations With Multipli Zeros Solved by Matrix Eigenproblems*, to appear

[**Tr**] W. Trinks, *Über Buchbergers Verfahren, Systeme für algebraischen Gleighungen zu lösen*, J. Number Th. **10** (1978), 475–488

[**G**] P. Gianni, *Properties of Gröbner bases under specialization*, Proc. EUROCAL '87, Lect. N. Comp. Sci. **378** (1989), 293–297

[**K**] M. Kalkbrener, *Solving systems of polynomial equations by using Gróbner bases*, Proc. EUROCAL '87, Lect. N. Comp. Sci. **378** (1989), 282–293