Université Paris 8 Année 2022–2023

Master Mathématiques et applications

Algorithmes arithmétiques II — Devoir à la maison

Transmis le 11 novembre 2022
mis à jour le 15 novembre 2022 (modif. mineures)

à rendre pour le **vendredi 23 décembre 2022**

Documents à fournir. Vous devez rendre, par email adressé `julien.lavauzelle@univ-paris8.fr` et jusqu'au vendredi 23 décembre 2022, une archive au format `.zip` contenant les documents ci-dessous :

1. un fichier édité sur ordinateur (pas de photos), au format `.pdf`, contenant vos réponses aux questions théoriques ;
2. vos fichiers de programmation pour les questions d'implantation.

Vous pouvez utiliser le langage de programmation de votre choix. Les logiciels de calcul formel comme `sage` ou `magma` sont fortement conseillés. Pour le logiciel `sage`, des fonctions utiles vous sont proposées en annexe.

Le **soin** et les **justifications** apportées à vos réponses seront évaluées. On notera également le soin apporté à l'implantation (commentaires, lisibilité, etc.).

Les chapitres 1 et 2 de la référence suivante :

David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms : An Introduction to Computational Algebraic Geometry and Commutative Algebra, 4th ed.* Springer, 2015

contiennent les preuves des résultats énoncés dans le sujet. Vous y trouverez également des exemples et explications complémentaires.

Une introduction aux bases de Gröbner

Présentation du sujet

Le sujet a pour objectif la découverte de la notion de **bases de Gröbner**, leur calcul effectif, et leur application à la résolution de systèmes polynomiaux.

Avant toute chose, introduisons quelques notations. Dans toute la suite, on considère un corps $\mathbb{F}$ sur lequel on peut opérer des calculs efficacement. On note $\mathbb{F}[x_1, \dots, x_n]$ l'anneau de polynômes à n variables $x_1, \dots, x_n$. On utilisera souvent la notation vectorielle $\boldsymbol{x}$ pour le n-uplet de variables $(x_1, \dots, x_n)$. En particulier, on notera $\mathbb{F}[\boldsymbol{x}] = \mathbb{F}[x_1, \dots, x_n]$ et $P(\boldsymbol{x}) = P(x_1, \dots, x_n)$ un élément de $\mathbb{F}[\boldsymbol{x}]$.

Tout polynôme $P(\boldsymbol{x}) \in \mathbb{F}[\boldsymbol{x}]$ peut alors s'écrire comme une somme finie

$$P(\boldsymbol{x}) = \sum_{(i_1,\dots,i_n)} p_{(i_1,\dots,i_n)} x_1^{i_1} \dots x_n^{i_n}, \quad \text{avec } p_{(i_1,\dots,i_n)} \neq 0,$$

que l'on écrira plus succinctement $P(\boldsymbol{x}) = \sum_{\boldsymbol{i}} p_{\boldsymbol{i}} \boldsymbol{x}^{\boldsymbol{i}}$. Observons ici que la notation $\boldsymbol{x}^{\boldsymbol{i}}$ représente le monôme $x_1^{i_1} \dots x_n^{i_n}$.

Le degré d'un monôme $\boldsymbol{x}^{\boldsymbol{i}}$ est simplement $\left\|\boldsymbol{x}^{\boldsymbol{i}}\right\|_1 := \sum_{j=1}^{n} i_j$. On définit alors le degré total d'un polynôme $P(\boldsymbol{x})$ comme le plus grand degré des monômes apparaissant dans $P(\boldsymbol{x})$.

Notation importante. Dans le cas de polynômes à deux ou trois variables, on notera souvent ces variables $x_1 = x$, $x_2 = y$ et $x_3 = z$.

1 Une première résolution d'un système polynomial

Essayons d'abord de comprendre à quel point un système polynomial peut être complexe à résoudre. Tout d'abord, considérons un cas favorable. Soit (E) le système suivant :

$$\begin{cases} 3\,x^4 + 2\,xy^2z + xy^2 + 2\,z^3 - 6\,x^2 + xy - y + 3 &= 0 \\ x^4 + xy^2z + z^3 - 2\,x^2 + 1 &= 0 \\ 2\,x^4 + 2\,xy^2z + xy^2 + 2\,z^3 - 4\,x^2 + xy - y + 2 &= 0 \end{cases}$$

Question 1.– Grâce à des combinaisons linéaires inversibles et à coefficients entiers des lignes de (E), essayer d'isoler une équation qui ne dépend que de la variable x.

Question 2.– Résoudre cette équation en x, puis substituer la variable x par le ou les valeurs obtenues dans les autres équations, et itérer le procédé sur y et z pour obtenir l'ensemble des solutions du système.

On observe que dans ce cas de figure, on a pu résoudre le système en imitant la résolution d'un système **linéaire**, c'est-à-dire par combinaisons linéaires de lignes et substitutions.

Cependant, ce n'est pas toujours possible. Prenons l'exemple suivant :

$$\begin{cases} x^2 + y^2 - 1 &= 0 \\ xy - \frac{1}{2} = 0 \end{cases}$$

En utilisant simplement des combinaisons linéaires de ces équations à coefficients réels, il est impossible d'isoler une équation en x ou en y. Néanmoins, on va réussir à le faire en choisissant des polynômes $f(x, y)$ comme coefficients de ces combinaisons linéaires.

Notons $P_1(x,y) = x^2 + y^2 - 1$ et $P_2(x,y) = xy - 1$ les polynômes correspondant aux deux équations. Alors on a

$$x^2 \cdot P_1(x,y) - (xy + \tfrac{1}{2}) \cdot P_2(x,y) = x^4 + x^2y^2 - x^2 - x^2y^2 + \tfrac{1}{4} = x^4 - x^2 + \tfrac{1}{4}$$

Puis, on peut trouver les solutions $x = \pm\frac{\sqrt{2}}{2}$ de cette équation à une variable, et en déduire les deux solutions du système : $\{\pm(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2})\}$.

Dans la suite du devoir, nous allons chercher à comprendre comment trouver calculatoirement les polynômes x^2 et $xy + \frac{1}{2}$ qui permettent cette simplification, puis à résoudre des systèmes polynomiaux plus complexes. Pour cela, on va d'abord introduire un peu de théorie.

2 Ordres monomiaux et division polynomiale

2.1 Ordres monomiaux

Dans la partie précédente, on a entraperçu l'importance de la **division polynomiale** et de la **réduction** de polynômes pour résoudre un système d'équations polynomiales. Les opérations effectuées s'apparentaient grossièrement à une division euclidienne de polynômes, où par des sommes et multiplications de polynômes, on veut extraire un reste qui est « plus petit » que les dividendes.

Ces notions reposent donc sur une relation d'ordre sur les polynômes : de manière informelle, on a cherché à faire décroître le degré (en x, en y, ...) des polynômes engagés dans les équations.

On sait que dans l'anneau des polynômes à une variable, il existe une manière simple de comparer deux monômes. Il suffit de comparer leur exposant grâce à la relation d'ordre naturelle de $\mathbb{N}$. Cela permet ensuite de comparer deux polynômes, en comparant leur termes de plus grand degré.

Dans le cas de polynômes multivariés, l'analogie est plus compliquée. En effet, il n'existe pas d'ordre canonique sur $\mathbb{N}^n$. On a donc besoin de définir de quelle type de relation d'ordre on souhaite munir $\mathbb{F}[\boldsymbol{x}]$.

Définition 2.1

Une relation d'ordre monomiale est une relation d'ordre totale $\succ$ sur les n-uplets d'entiers naturels, vérifiant les propriétés supplémentaires suivantes :

- *Si $\boldsymbol{u} \succ \boldsymbol{v}$, alors pour tout $\boldsymbol{w} \in \mathbb{N}^n$, $\boldsymbol{u} + \boldsymbol{w} \succ \boldsymbol{v} + \boldsymbol{w}$.*
- *[« bien ordonné »] Tout sous-ensemble non-vide de $\mathbb{N}^n$ admet un plus petit élément pour $\succ$.*

On définit également $\boldsymbol{u} \succeq \boldsymbol{v} \iff (\boldsymbol{u} \succ \boldsymbol{v}$ ou $\boldsymbol{u} = \boldsymbol{v})$.

Ce type de relation s'étend naturellement aux monômes, en posant $\boldsymbol{x^i} \succ \boldsymbol{x^j} \iff \boldsymbol{i} \succ \boldsymbol{j}$.

Exemple 2.2

L'ordre lexicographique $\succ_{\text{lex}}$ est défini par $\boldsymbol{u} \succ_{\text{lex}} \boldsymbol{v}$ si et seulement si la première entrée non-nulle en partant de la gauche de $\boldsymbol{u} - \boldsymbol{v}$ est strictement positive. Par exemple, $(1,1,4) \succ_{\text{lex}} (0,8,7)$ et $(1,1,4) \succ_{\text{lex}} (1,1,2)$.

Comme expliqué précédemment, l'ordre lexicographique s'étend aux monômes. En particulier, pour n variables $(x_1, \ldots, x_n)$ on a :

$$x_1 \succ_{\text{lex}} x_2 \succ_{\text{lex}} \cdots \succ_{\text{lex}} x_n.$$

Une autre caractérisation d'un ordre monomial est donnée par le lemme suivant.

Lemme 2.3

Un ordre $\succ$ sur des monômes est bien ordonné (voir Définition 2.1) si et seulement toute suite strictement décroissante

$$\boldsymbol{u}_0 \succ \boldsymbol{u}_1 \succ \cdots \succ \cdots \succ \boldsymbol{u}_k \succ \dots$$

est finie.

Notons que l'ordre naturel sur $\mathbb{N}$ est bien ordonné.

Définition 2.4

*L'ordre lexicogaphique renversé gradué (*graded reversed lexicographic order*), noté $\succ_{\text{grevlex}}$, est défini par :*

$$\boldsymbol{u} \succ_{\text{grevlex}} \boldsymbol{v} \iff \begin{cases} \|\boldsymbol{u}\|_1 > \|\boldsymbol{v}\|_1 \\ \text{ou} \\ \|\boldsymbol{u}\|_1 = \|\boldsymbol{v}\|_1 \quad \text{et} \quad \text{la première entrée non-nulle en partant de la droite} \\ \qquad\qquad \text{de } \boldsymbol{u} - \boldsymbol{v} \text{ est strictement négative} \end{cases}$$

Question 3.– Classer dans l'ordre décroissant, pour $\succ_{\text{lex}}$ et pour $\succ_{\text{grevlex}}$, les monômes suivants :

$$\{x,\ x^2y,\ y^9,\ xyz,\ yz^4,\ xz,\ xy,\ x^2z\}\,.$$

Question 4.– Démontrer que l'ordre lexicographique est un ordre monomial. On pourra utiliser le Lemme 2.3.

2.2 Division polynomiale

Grâce à la relation d'ordre définie dans la section précédente, on peut maintenant spécifier des monômes et des coefficients maximaux d'un polynôme (relativement à cet ordre).

Définition 2.5

Soit $P(\boldsymbol{x}) = \sum_{\boldsymbol{i}} p_{\boldsymbol{i}} \boldsymbol{x}^{\boldsymbol{i}} \in \mathbb{F}[\boldsymbol{x}]$ et $\succ$ un ordre monomial. On définit :

- *le multidegré de P comme* $\text{mdeg}(P) := \max\{\boldsymbol{i} \in \mathbb{N}^n \mid p_{\boldsymbol{i}} \neq 0\}$ *(où le maximum est pris selon $\succ$),*
- *le coefficient de tête (*leading coefficient*) de P comme* $\text{LC}(P) := p_{\text{mdeg}(P)} \in \mathbb{F} \setminus \{0\}$,
- *le monôme de tête (*leading monomial*) de P comme* $\text{LM}(P) := \boldsymbol{x}^{\text{mdeg}(P)}$,
- *le terme de tête (*leading term*) de P comme* $\text{LT}(P) := \text{LC}(P) \cdot \text{LM}(P) = p_{\text{mdeg}(P)} \boldsymbol{x}^{\text{mdeg}(P)}$,

Par exemple, le polynôme $P(\boldsymbol{x}) = 3x_1x_2^2 + 2x_3^4 - 6x_1^2x_2x_3$ admet, pour l'ordre lexicographique, comme multidegré $\text{mdeg}(P) = (2,1,1)$, comme coefficient de tête $\text{LC}(P) = -6$, comme monôme de tête $\text{LM}(P) = x_1^2x_2x_3$ et comme terme de tête $\text{LT}(P) = -6x_1^2x_2x_3$.

Theorème 2.6 (*Division sur les polynômes à plusieurs variables*)

Soit $\succ$ un ordre monomial et $P_1, \dots, P_s$ des polynômes de $\mathbb{F}[\boldsymbol{x}]$. Alors, tout $F \in \mathbb{F}[\boldsymbol{x}]$ peut être écrit comme

$$F = Q_1P_1 + \cdots + Q_sP_s + R$$

avec $Q_i \in \mathbb{F}[\boldsymbol{x}]$ et le **reste** *$R \in \mathbb{F}[\boldsymbol{x}]$ qui est :*

- *ou bien nul ;*
- *ou bien égal à une combinaison linéaire de monômes qui ne sont pas divisibles par l'un des $\text{LT}(P_1), \dots, \text{LT}(P_s)$.*

Algorithme 1 : Algorithme de division polynomiale.

Entrée : Un polynôme P à diviser et un ensemble de diviseurs $\mathcal{G} = \{G_1, \ldots, G_k\}$
Sortie : Une liste de quotients $\mathcal{Q} = \{Q_1, \ldots, Q_k\}$ et un reste R tels que $P = \sum_{i=1}^{k} Q_i G_i + R$ et tel qu'aucun terme de R n'est divisible par l'un des $\mathrm{LT}(G_i)$.

$F \leftarrow P$
$Q_1 \leftarrow 0, \ldots, Q_k \leftarrow 0$
$R \leftarrow 0$
Tant que $F \neq 0$ **faire**
    $i \leftarrow 1$
    `test_division` $\leftarrow$ `False`
    Tant que $i \leq k$ *et* `test_division` $=$ `False` **faire**
        Si $\mathrm{LT}(G_i)$ *divise* $\mathrm{LT}(F)$
            $Q_i \leftarrow Q_i + \mathrm{LT}(F)/\mathrm{LT}(G_i)$
            $F \leftarrow F - G_i \cdot \mathrm{LT}(F)/\mathrm{LT}(G_i)$
            `test_division` $\leftarrow$ `True`
        Sinon
            $i \leftarrow i + 1$
    Si `test_division` $=$ `False`
        $R \leftarrow R + \mathrm{LT}(F)$
        $F \leftarrow F - \mathrm{LT}(F)$
Retourner $(Q_1, \ldots, Q_k)$ et R

De ce théorème, on peut déduire l'algorithme de division polynomiale décrit dans l'Algorithme 1.

Question 5.– Exécuter à la main l'algorithme de division polynomiale (Algorithme 1), sur les instances suivantes :
1. $P = xy^3 + x$, $\mathcal{G} = [G_1, G_2]$ avec $G_1 = y^2 + x$ et $G_2 = xy$, en utilisant l'ordre $\succ_{\text{lex}}$
2. $P = xy^3 + x$, $\mathcal{G} = [G_2, G_1]$ en utilisant l'ordre $\succ_{\text{lex}}$ (on a simplement inversé l'ordre des polynômes)
3. $P = xy^3 + x$, $\mathcal{G} = [G_1, G_2]$ en utilisant l'ordre $\succ_{\text{grevlex}}$ (on changé d'ordre)

Que remarquez-vous ? Commentez, notamment en comparant au cas d'une variable.

Question 6.– Implanter l'algorithme de division polynomiale (Algorithme 1), puis proposer une fonction de test de validité et un jeu de tests.

Dans la suite, si $\mathcal{G} = (G_1, \ldots, G_k)$ est une séquence de polynômes et P est un polynôme, on note $\overline{P}^{\mathcal{G}}$ le reste de la division de P par $\mathcal{G}$.

3 Bases de Gröbner

Dans l'anneau de polynômes à une variable $\mathbb{F}[x]$, il est facile de tester l'appartenance d'un polynôme $P(x)$ à un idéal I engendré par des générateurs $G_1(x), \ldots, G_k(x)$. Simplement, on effectue la division euclidienne par les $G_i(x)$ et on teste si le dernier reste vaut 0.

Au vu de la section précédente, la division polynomiale n'est pas satisfaisante, puisque les résultats (notamment le calcul du reste) dépendent à la fois de l'ordre des diviseurs et de l'ordre monomial choisi. En particulier, on ne peut pas tester l'appartenance à un idéal.

Ceci est dû au fait que dans notre algorithme de division polynomiale, on « oublie » les termes d'ordre inférieur. Plutôt que de modifier l'algorithme, nous allons voir comment calculer un autre ensemble de générateurs $G'_1, \ldots, G'_s$ du même idéal I, pour lequel l'algorithme de division polynomiale donnera un résultat unique et indépendant de l'ordre des générateurs. Ce nouvel ensemble de générateurs sera appelé **base de Gröbner**.

3.1 Définitions et propriétés des bases de Gröbner

Soit I un idéal non-nul de $\mathbb{F}[\boldsymbol{x}]$. On peut alors définir l'ensemble des termes de têtes de I comme

$$\mathrm{LT}(I) = \{\mathrm{LT}(P) \mid P \in I\},$$

puis l'idéal engendré par ces termes de têtes comme $\langle \mathrm{LT}(I) \rangle$. Si $P_1, \ldots P_k$ forment un système de générateurs de I, alors on a bien entendu $\langle \mathrm{LT}(P_1), \ldots, \mathrm{LT}(P_k) \rangle \subseteq \langle \mathrm{LT}(I) \rangle$, mais hélas, l'inclusion réciproque n'est pas vraie.

Question 7.– Donner un contre-exemple à l'inclusion réciproque.

Définition 3.1

Soit $\succ$ un ordre monomial sur $\mathbb{F}[\boldsymbol{x}]$ et I un idéal non-nul de $\mathbb{F}[\boldsymbol{x}]$. Soit $G_1, \ldots, G_k$ des polynômes de I. On dit que $\mathcal{G} = \{G_1, \ldots, G_k\}$ est une base de Gröbner de I si

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(G_1), \ldots, \mathrm{LT}(G_k) \rangle .$$

Autrement dit, un ensemble de polynômes $G_1, \ldots, G_k$ générant un idéal I est une base de Grönbner de I si les termes de tête de ces polynômes engendrent tous les termes de tête de l'idéal.

Theorème 3.2 (*Théorème de la base de Hilbert*)

Tout idéal non-nul de $\mathbb{F}[\boldsymbol{x}]$ admet un ensemble fini de générateurs.

Corollaire 3.3

Tout idéal non-nul de $\mathbb{F}[\boldsymbol{x}]$ admet une base de Gröbner.

Question 8.– Soit I l'idéal engendré par $\mathcal{G} = \{x + y^2, xy\}$ que l'on a introduit à la **Question 5**. Démontrer que $\mathcal{G}' = \{x + y^2, y^3\}$ est une base de Gröbner de cet idéal I, pour l'ordre lexigographique. Pour cela, on calculera explicitement $\langle \mathrm{LT}(I) \rangle$.

Comme annoncé précédemment, si $\mathcal{G}$ est une base de Gröbner, alors l'algorithme de division appliqué sur $\mathcal{G}$ retourne un reste unique et indépendant de l'ordre des polynômes dans la base.

Proposition 3.4

Soit I un idéal de $\mathbb{F}[\boldsymbol{x}]$ et $\mathcal{G} = \{G_1, \ldots, G_s\}$ une base de Gröbner de I. Pour tout $P \in \mathbb{F}[\boldsymbol{x}]$, il existe un unique $R \in \mathbb{F}[\boldsymbol{x}]$ tel que :

1. *R s'écrit $R = P - G$ où $G = \sum_i Q_i G_i \in I$;*
2. *aucun des termes de R n'est divisible par l'un des $\mathrm{LT}(G_i)$.*

De plus, cet élément R est obtenu par exécution de l'Algorithme 1.

Attention, le résultat de la division polynomiale dépend toujours de l'ordre monomial $\succ$ choisi !

3.2 Calcul d'une base de Gröbner

Nous allons maintenant chercher à calculer une base de Gröbner à partir des générateurs d'un idéal I. Pour cela, l'idée va être de créer de nouveaux polynômes de l'idéal, dont les termes de tête apparaissent comme termes de tête d'éléments de I. Cette création se fera par l'intermédiaire de combinaisons simples appelées S-polynômes.

Définition 3.5

Soient P et Q deux polynômes non-nuls de $\mathbb{F}[\boldsymbol{x}]$. Notons $\boldsymbol{u} = \mathrm{mdeg}(P)$ et $\boldsymbol{v} = \mathrm{mdeg}(Q)$.

- *Si l'on note $\boldsymbol{w} = (w_1, \ldots, w_n)$ avec $w_i = \max(u_i, v_i)$, alors le monôme $\boldsymbol{x}^{\boldsymbol{w}}$ est appelé ppcm de $\mathrm{LM}(P)$ et de $\mathrm{LM}(Q)$. On le note $\mathrm{ppcm}(\mathrm{LM}(P), \mathrm{LM}(Q))$.*
- *Avec les notations précédentes, le S-polynôme de P et Q est défini comme :*

$$S(P,Q) \coloneqq \frac{\boldsymbol{x}^{\boldsymbol{w}}}{\mathrm{LT}(P)} P - \frac{\boldsymbol{x}^{\boldsymbol{w}}}{\mathrm{LT}(Q)} Q \in \mathbb{F}[\boldsymbol{x}]\,.$$

Les S-polynômes permettent également de tester si une séquence de polynômes forme une base de Gröbner de l'idéal qu'ils engendrent :

Theorème 3.6 (*Critère de Buchberger*)

Soit $\mathcal{G} = (G_1, \ldots, G_k)$ une séquence de polynômes et $I = \langle G_1, \ldots, G_k \rangle$. Alors, G est une base de Gröbner de I si et seulement si

$$\forall i \neq j,\ \overline{S(G_1, G_j)}^{\mathcal{G}} = 0\,.$$

Muni de ce critère, on peut déduire l'Algorithme 2 qui calcule une base de Gröbner d'un idéal décrit par un ensemble de générateurs quelconques.

Algorithme 2 : Algorithme de Buchberger

Entrée : $(G_1, \ldots, G_k)$ des polynômes engendrant un idéal I
Sortie : Une base de Gröbner de I

```
G ← (G_1, ..., G_k)
Faire
    G' ← G
    Pour tout paire d'éléments distincts G'_i, G'_j de G' faire
        Calculer P_{i,j} ← S(G'_i, G'_j)^{G'}
        Si P_{i,j} ≠ 0
            Ajouter P_{i,j} à G
tant que G' = G;
Retourner G
```

Question 9.– Implanter une fonction de calcul du S-polynôme de deux polynômes P et Q.

Question 10.– Implanter l'algorithme de Buchberger (Algorithme 2).

L'algorithme de Buchberger (Algorithme 2) construit une base de Gröbner très redondante : beaucoup de polynômes peuvent en être éliminés tout en conservant les propriétés d'une base de Gröbner. Réduire une base de Gröbner nous sera ensuite utile pour résoudre des systèmes polynomiaux.

Pour un idéal I donné, il existe une unique base de Gröbner de taille minimale, aux coefficients dominants des polynômes près. Cette base de Gröbner est appelée **base réduite**. Elle est caractérisée précisément de la sorte :

Définition 3.7

Soit $\mathcal{G} = \{G_1, \ldots, G_s\}$ une base de Gröbner d'un idéal I. On dit que $\mathcal{G}$ est réduite si :

1. $\mathrm{LC}(G_i) = 1$ *pour tout* $i = 1, \ldots, s$;
2. *pour tout* $i \in \{1, \ldots, s\}$, *aucun monôme de* G_i *n'appartient à* $\langle \{\mathrm{LT}(G_j) \mid j \neq i\} \rangle$.

Un algorithme assez naïf permet de réduire une base de Gröbner

Algorithme 3 : Réduction d'une base de Gröbner.

Entrée : $\mathcal{G} = \{G_1, \ldots, G_k\}$ une base de Gröbner de I
Sortie : La base de Gröbner réduite de I

$\mathcal{G}' \leftarrow \varnothing$
Tant que $\mathcal{G} \neq \varnothing$ **faire**
  $P \leftarrow \min_{\succ} \mathcal{G}$
  Ajouter P à $\mathcal{G}'$
  $\mathcal{G} \leftarrow \{G \in \mathcal{G} \mid \mathrm{LM}(P) \text{ ne divise pas } \mathrm{LM}(G)\}$
$\mathcal{G}'' \leftarrow \varnothing$
Pour tout $G \in \mathcal{G}'$ **faire**
  Ajouter $\overline{G}^{\mathcal{G}' \setminus \{G\}}$ à $\mathcal{G}''$
Retourner $\mathcal{G}''$

Question 11.– Implanter l'algorithme de réduction de base de Gröbner (Algorithme 3).

Question 12.– En utilisant vos implantations, calculer une base de Gröbner **réduite** pour les idéaux suivants :

1. $I = \langle y^2 + x, xy \rangle$, c'est-à-dire l'idéal de la **Question 5**, avec l'ordre $\succ_{\mathrm{lex}}$
2. $I = \langle y^2 + x, xy \rangle$, c'est-à-dire l'idéal de la **Question 5**, avec l'ordre $\succ_{\mathrm{grevlex}}$
3. $I = \langle x^2 + y^2 - 1, xy - \frac{1}{2} \rangle$, c'est-à-dire l'idéal du système polynomial de la Section 1, avec l'ordre $\succ_{\mathrm{lex}}$
4. **[plus difficile]** I est l'ensemble ds polynômes à 3 variables qui s'annulent en l'origine $O = (0, 0, 0)$ et dont le gradient s'annule également en O (avec l'ordre $\succ_{\mathrm{lex}}$).

4 Résolution d'un système d'équations polynomiales

Considérons un système de k équations polynomiales de la forme

$$\begin{cases} G_1(\boldsymbol{x}) &= 0 \\ & \vdots \\ G_k(\boldsymbol{x}) &= 0 \end{cases}$$

Pour résoudre le système, l'idée est de s'intéresser à l'idéal $I = \langle G_1, \ldots, G_k \rangle$, d'en calculer une base de Gröbner réduite, et d'espérer aboutir à un nouveau système pour lequel on puisse éliminer/substituer des variables.

Pour cela, on va considérer l'ordre lexicographique $\succ_{\text{lex}}$. En effet, si $\mathcal{G}$ est une base de Gröbner réduite de I, alors on peut s'attendre à ce que le plus petit polynôme de $\mathcal{G}$ ne dépende que de x_n (la dernière variable dans l'ordre lexicographique). Il suffira ensuite de résoudre cette dernière équation à 1 variable (on sait le faire, au moins numériquement), puis d'itérer le procédé avec les autres variables $x_{n-1}, \ldots, x_1$.

Question 13.– En adoptant la stratégie ci-dessus,

1. retrouver les deux solutions réelles du système

$$\begin{cases} x^2 + y^2 - 1 &= 0 \\ xy - \frac{1}{2} = 0 \end{cases}$$

2. calculer la valeur exacte des points d'intesections réels de ces trois surfaces de l'espace à trois dimensions :
   - le plan d'équation $x + y = z + 1$,
   - la sphère de rayon 1,
   - la surface cublique de Clebsch, d'équation $x^3 + y^3 + z^3 + 1 = (x + y + z + 1)^3$
3. **[plus difficile]** déterminer l'ensemble des parallelépidèdes rectangles (aussi appelés pavés droits) dont le volume vaut 24, l'aire vaut 52 et la grande diagonale 29.

Vos solutions devront être apportées par l'exécution de votre code.

Fonctions utiles en sage

Pour déclarer un anneau de polynômes à 3 variables x, y, z sur $\mathbb{Q}$ dans sage, lui associer l'ordre lexicographique, puis en extraire les variables, on peut suivre les étapes suivantes.

```
sage: RING = PolynomialRing(QQ, 3, "x,y,z", order="lex")
sage: RING
Multivariate Polynomial Ring in x, y, z over Rational Field
sage: x,y,z = RING.gens()
sage: 3*z*x - y**2*x + x**2
x^2 - x*y^2 + 3*x*z
```

Remarque : dans le code ci-dessus, `sage:` représente l'invite de commande du logiciel. À ne pas recopier !

Pour obtenir l'ordre $\succ_{\text{grevlex}}$, remplacer `order="lex"` par `order="degrevlex"`.

commande/code	description
`P.lm()`	monôme de tête de `P`
`P.lt()`	terme de tête de `P`
`P.lc()`	coefficient de tête de `P`
`P.degrees()`	multidegré de `P`
`P.divides(Q)`	teste si `P` divise `Q`
`P // Q`	division de `P` par `Q` (conseil : n'utiliser que lorsque `Q` divise `P`)
`P.monomials()`	liste des monômes (sans coefficient) de `P`

TABLE 1 – Manipulation des polynômes multivariés. On suppose que `P` et `Q` sont des polynômes.

Références

[CLO15] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms : An Introduction to Computational Algebraic Geometry and Commutative Algebra, 4th ed.* Springer, 2015.