1. Polynômes à une variable

Fonctions utiles : `degree`, `leading_coefficient`, `coefficients`, `expand`, `factor`, `gcd`, `quo`, `rem`.

Exercice 1.1 – Soient les polynômes $P_1 = x^6 + 2x^5 - 2x^4 + 2x^2 - 2x - 1 \quad \text{et } P_2 = x^5 + x^4 - 2x^3 + x^2 + x - 2$.

1. Déterminer le degré, le coefficient dominant et la liste des termes de $P = P_1P_2$.
2. Effectuer la division euclidienne de P_1 par P_2.
3. Calculer $Q = \text{pgcd}(P_1, P_2)$.
4. Factoriser P. Calculer $P(2)$.

Exercice 1.2 – Soit le polynôme $P = x^{11} + x^{10} + x^9 + 2x^8 + 2x^6 + 2x^4 + x^3 + x^2 + x$.

1. Factoriser P dans $\mathbb{Z}[x]$.
2. Factoriser P dans $\mathbb{Z}[i][x]$ et dans $\mathbb{Q}(i)[x]$.
3. Factoriser P dans $\mathbb{F}_2[x]$.
4. Factoriser P dans $\mathbb{F}_4[x]$.

Exercice 1.3 – Soit le polynôme $P = x^7 + x^5 + 2x^3 + 2x^2 + 3x + 2$.

1. Factoriser P dans $\mathbb{F}_2$ et $\mathbb{F}_7$.
2. En déduire une preuve de l'irréductibilité de P dans $\mathbb{Z}[x]$.
3. Vérifier l'irréductibilité de P avec Sage.

Exercice 1.4 – Soit p un nombre premier. Factoriser $x^p - x + c$ en facteurs irréductibles dans $\mathbb{F}_p[x]$ pour $0 \leq c < p$. Formuler une conjecture sur le type de factorisation de ces polynômes, et la prouver. **Suggestion:** observer que deux racines du polynôme diffèrent nécessairement d'un élément de $\mathbb{F}_p$; conclure en étudiant l'action du Frobenius sur les racines. **Note:** il est possible de se passer de la théorie de Galois, si on le souhaite.

Exercice 1.5 – Soit p un nombre premier. Factoriser le polynôme $x^{2p} + x^p + 1$ en facteurs irréductibles dans $\mathbb{Z}[x]$. Prouver que ces polynômes sont des produits de *polynômes cyclotomiques*.

2. Polynômes à plusieurs variables

À partir de maintenant, il est préférable de se servir des anneaux de polynômes de Sage, plutôt que des variables symboliques.

Exercice 2.1 – Soit le polynôme $P = xy^5 + 2y^4 + 3y^3x^3 + 4x^2y^2 + 5xy^2 + 6yx^3 + 7y$.

1. Donner le degré total de P.
2. Écrire P comme polynôme en x.

Exercice 2.2 – Transformer le polynôme $P = (x^2 + xy + x + y)(x + y)$ avec Sage sous les formes suivantes:

1. $x^3 + 2x^2y + xy^2 + x^2 + 2xy + y^2$;
2. $(x+1)(x+y)^2$;
3. $x^3 + (2y+1)x^2 + (y^2+2y)x + y^2$;
4. $(x+1)y^2 + (2x^2+2x)y + x^3 + x^2$.

3. Préliminaires sur les ordres admissibles

Exercice 3.1 –

1. Soit le polynôme $P = xy^5 + 2y^4 + 3y^3x^3 + 4x^2y^2 + 5xy^2 + 6yx^3 + 7y$.

   A. Ordonner P pour l'ordre lexicographique.
   B. Ordonner P pour l'ordre lexicographique gradué.

C. Ordonner P pour l'ordre lexicographique inverse gradué.
D. Montrer qu'en deux variables, l'ordre lexicographique gradué et l'ordre lexicographique inverse gradué coïncident.

2. Soit le polynôme $Q = xy^3zt + x^2yz^3t + x^2yz^2t + x^3z^2t^2$.

A. Ordonner Q à la main pour l'ordre lexicographique gradué.
B. Ordonner Q à la main pour l'ordre lexicographique inverse gradué.

Exercice 3.2 – Soit $\succ$ un ordre total compatible avec la multiplication. Montrer que $\succ$ est un ordre admissible si, et seulement si, pour tout monôme m non constant, $m \succ 1$.

Exercice 3.3 –

Montrer que l'ordre lexicographique est un ordre admissible. (voir aussi la proposition 4, p.55 du Cox, Little & O'Shea)

Exercice 3.4 –

1. Soient $g = x - y$, $h = x - y^2$ et $p = xy - x$ dans $\mathbb{Q}[x, y]$ muni de l'ordre lexicographique.

A. À quoi correspond la commande `p.reduce([g, h])` ?
B. À quoi correspond la commande `p.reduce([h, g])` ?
C. Montrer que p est dans l'idéal (g, h).

2. Soient $g = x^2y^2 - x$ et $h = xy^2 + y$.

A. À quoi correspond la commande `g.reduce([g, h])` ?
B. À quoi correspond la commande `h.reduce([g, h])` ?
C. Pleurer.

Exercice 3.5 –

Déterminer quel ordre monomial (`lex`, `deglex`, `degrevlex`) a été utilisé pour ordonner les termes des polynômes suivants :

1. $f(x, y, z) = 7x^2y^4z - 2xy^6 + x^2y^2$.
2. $f(x, y, z) = xy^3z + xy^2z^2 + x^2z^3$.
3. $f(x, y, z) = x^4y^5z + 2x^3y^2z - 4xy^2z^4$.

Exercice 3.6 –

Soient $f = x^7y^2 + x^3y^2 - y - 1$ et l'ensemble ordonné $F = \{f_1 = xy^2 - x, f_2 = x - y^3\}$.

1. Calculer $\overline{f}^F$ pour les ordres lexicographique et lexicographique gradué.
2. Effectuer les mêmes calculs en inversant l'ordre de F.

Exercice 3.7 –

1. Montrer que tout polynôme $f \in k[x, y, z]$ peut s'écrire sous la forme

$$f = h_1(y - x^2) + h_2(z - x^3) + r$$

avec $h_1, h_2 \in k[x, y, z]$ et $r \in k[x]$.

2. Trouver une écriture explicite de la forme $z^2 - x^4y = h_1(y - x^2) + h_2(z - x^3)$.

Exercice 3.8 - Dans cet exercice, nous verrons une façon de définir des ordres monomiaux sur $k[x_1, \ldots, x_n]$ qui généralise tous les ordres vus précédemment.

Soit M une matrice $m \times n$ à coefficients réels, et soient $w_1, \ldots, w_m$ ses vecteurs ligne. On définit la relation $<_M$ sur les monômes de la façon suivante. Soient x^α et x^β des monômes. On pose $x^\alpha <_M x^\beta$ si $w_1 \cdot \alpha < w_1 \cdot \beta$, ou si $w_1 \cdot \alpha = w_1 \cdot \beta$ et $w_2 \cdot \alpha < w_2 \cdot \beta$, ou s'il existe $i \in \{1, \ldots, n\}$ tel que $w_j \cdot \alpha = w_j \cdot \beta$ pour $1 \leq j \leq i - 1$ et $w_i \cdot \alpha < w_i \cdot \beta$.

1. Montrer que si $x^\alpha <_M x^\beta$ et $x^\gamma <_M x^\delta$, alors $x^{\alpha+\gamma} <_M x^{\beta+\delta}$.
2. Montrer que si M est la matrice identité, alors $<_M$ est l'ordre lexicographique avec $x_1 > x_2 > \ldots > x_n$.
3. On définit $\ker(M) = \{v \in \mathbb{R}^n, Mv = 0\}$. Supposons que $\ker(M) \cap \mathbb{Z}^n = \{0\}$. Montrer que $<_M$ définit un ordre total ; autrement dit :

A. si $x^\alpha <_M x^\beta$ et $x^\beta <_M x^\gamma$, alors $x^\alpha <_M x^\gamma$,
B. il est impossible d'avoir à la fois $x^\alpha <_M x^\beta$ et $x^\beta <_M x^\alpha$, et
C. si $\alpha \neq \beta$, alors soit $x^\alpha <_M x^\beta$, soit $x^\beta <_M x^\alpha$.

4. En plus de supposer que $\ker(M) \cap \mathbb{Z}^n = \{0\}$, on suppose maintenant que les coefficients de la première ligne w_1 sont positifs, et qu'au moins l'un d'eux est non nul. Montrer que $<_M$ est un *bon ordre*, c'est-à-dire que tout ensemble non vide de monômes possède un plus petit élément pour $<_M$.
5. Exprimer les ordres monomiaux vus en cours sous la forme $<_M$.

Pour aller plus loin : Lorenzo Robbiano a montré en 1985 que tous les ordres monomiaux s'écrivent comme $<_M$ pour une matrice M. Son article est très court et très lisible :

- Robbiano L. (1985) Term orderings on the polynomial ring. In: Caviness B.F. (eds) EUROCAL '85. EUROCAL 1985. Lecture Notes in Computer Science, vol 204. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-15984-3_321 .

4. Idéaux monomiaux

Fonction utiles : `lc`, `lm`, `lt`.

Soient $n > 0$ et k un corps, et considérons l'anneau $k[x_1, \ldots, x_n]$ muni d'un ordre monomial quelconque $<$. Nous utiliserons la notation suivante : si $\alpha \in \mathbb{N}^n$, alors $x^\alpha := \prod_{i=1}^n x_i^{\alpha_i}$.

Un idéal I de $k[x_1, \ldots, x_n]$ est un *idéal monomial* s'il existe un ensemble $A \subset \mathbb{N}^n$ tel que $I = \langle x^\alpha, \alpha \in A \rangle$.

Exercice 4.1 – Soit $I = \langle x^\alpha, \alpha \in A \rangle$ un idéal monomial et S l'ensemble des exposants qui apparaissent dans I. On considère un ordre monomial. Montrer que le plus petit élément de S appartient à A.

Exercice 4.2 –

Dans l'anneau $k[x_1, \ldots, x_n, y_1, \ldots, y_m]$, on considère l'ordre $\preccurlyeq$ défini par l'ordre lexicographique sur les x_i et par l'ordre degrevlex sur les y_j :

$$x^\alpha y^\beta \preccurlyeq x^\gamma y^\delta \Leftrightarrow x^\alpha \prec_{\text{lex}} x^\gamma \text{ ou } (x^\alpha = x^\gamma \text{ et } y^\beta \preccurlyeq_{\text{degrevlex}} y^\delta)$$

Montrer que $\preccurlyeq$ est un ordre monomial.

Exercice 4.3 – Soit l'idéal $I = \langle x^2 - 2xz + 5, xy^2 + yz^3, 3y^2 - 8z^3 \rangle$ de $\mathbb{Q}[x, y, z]$.

1. Donner une base de Gröbner G de I pour l'ordre lexicographique.
2. Même question pour l'ordre degrevlex.

Exercice 4.4 - Montrer que si $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_r} \rangle$ est un idéal monomial de $k[x_1, \ldots, x_n]$, alors $(x^{\alpha_1}, \ldots, x^{\alpha_r})$ est une base de Gröbner de I. Pour ce faire :

1. Montrer que si $x^\beta \in I$, alors x^β est divisible par l'un des x^{α_i}.
2. Montrer que si f est un élément de I, alors tous les monômes apparaissant dans f sont dans I.
3. En déduire que $\langle \mathrm{LT}(I) \rangle = I$, et conclure.

Exercice 4.5 - Dans cet exercice, nous démontrerons le *Lemme de Dickson*, qui est un cas particulier du théorème de la base de Hilbert pour les idéaux monomiaux.

- Lemme de Dickson : Si A est un sous-ensemble non vide de $\mathbb{N}^n$ et si $I = \langle x^\alpha, \alpha \in A \rangle$, alors il existe $\alpha_1, \ldots, \alpha_r \in A$ tels que $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_r} \rangle$.

La démonstration que nous présentons ci-dessous est une adaptation de l'orginiale de Dickson (1913).

Quelques notations : si $\alpha \in \mathbb{N}^n$, alors $\alpha + \mathbb{N}^n := \{\alpha + \beta, \beta \in \mathbb{N}^n\}$; de même, si $A \subset \mathbb{N}^n$, alors $A + \mathbb{N}^n := \{\alpha + \beta, \alpha \in A, \beta \in \mathbb{N}^n\}$.

1. *Illustration du cas* $n = 2$. On représente $\mathbb{N}^2$ comme l'ensemble des points entiers positifs du plan. Illustrer $A + \mathbb{N}^n$ si $A = \{(1,8), (3,5), (4,2)\}$, puis si $A = \{(x, y), y \geq 9 - x^2\}$. Dans le deuxième cas, décrire un sous-ensemble $\{\alpha_1, \ldots, \alpha_r\}$ de A tel que $A + \mathbb{N}^n = \{\alpha_1, \ldots, \alpha_r\} + \mathbb{N}^n$.
2. Nous allons maintenant montrer le lemme de Dickson par récurrence sur n. Montrer d'abord que l'énoncé du lemme est vrai pour $n = 1$.

Supposons que le lemme est démontré pour $n - 1$ pour un certain $n > 1$. Montrons-le pour n. Soit α un élément quelconque de A.

1. Remarquer que si $A + \mathbb{N}^n = \alpha + \mathbb{N}^n$, alors la preuve du lemme est terminée.
2. Supposons que $A + \mathbb{N}^n \neq \alpha + \mathbb{N}^n$. Alors il existe $\beta \in A$ tel que $\beta_j < \alpha_j$ pour un certain $j \in \{1, \ldots, n\}$.

   Fixons $i \in \{1, \ldots, n\}$ et $c \in \mathbb{N}$ tels que $c < \alpha_i$. Soit $A_{i,c} := \{\beta \in A, \beta_i = c\}$.

   Montrer qu'il existe des éléments $\alpha_{i,c,1}, \ldots, \alpha_{i,c,m} \in A_{i,c}$ tels que pour tout $\gamma \in A_{i,c}$, on a que $x^\gamma \in \langle x^{\alpha_{i,c,1}}, \ldots, x^{\alpha_{i,c,m}} \rangle$.

   Pour ce faire, on pourra considérer $B_{i,c} = \{(\beta_1, \ldots, \beta_{i-1}, \beta_{i+1}, \ldots, \beta_n) \in \mathbb{N}^{n-1}, (\beta_1, \ldots, \beta_{i-1}, c, \beta_{i+1}, \ldots, \beta_n) \in A\}$ et appliquer l'hypothèse de récurrence à $B_{i,c}$.
3. Montrer qu'il n'y a qu'un nombre fini de choix possibles de i et c tels que $c < \alpha_i$. Conclure la démonstration du lemme de Dickson.

Le lemme de Dickson peut être utilisé pour démontrer le théorème de la base de Hilbert pour $k[x_1, \ldots, x_n]$.

1. Soit I un idéal de $k[x_1, \ldots, x_n]$.

   A. Montrer qu'on peut appliquer le lemme de Dickson à $\langle \mathrm{LT}(I) \rangle$. En déduire qu'il existe $f_1, \ldots, f_r \in I$ tels que $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_r) \rangle$.

   B. Montrer que si $f \in I$, alors l'algorithme de division de f par $f_1, \ldots, f_r$ donne un reste nul. Conclure.

5. Programmation Python/Sage

Exercice 5.1 – Que fait la procédure suivante ? Quels sont les arguments de la procédure ? Comment les variables sont elles initialisées ? Quelle est la condition d'arrêt de la boucle ? Que doit renvoyer la procédure ?

```
def euclidepol (A,B):
    A0 = A; A1 = B
    S0 = 1; S1 = 0
    T0 = 0; T1 = 1
    while A1 != 0:
        Q = A0//A1
        U = A1; A1 = A0 - Q*A1; A0 = U
        U = S1; S1 = S0 - Q*S1; S0 = U
        U = T1; T1 = T0 - Q*T1; T0 = U
    return (A0,S0,T0)
```

Exercice 5.2 – Écrire une fonction qui prend en entrée un corps k et un entier n et donne en sortie un polynôme aléatoire irréductible de $k[x]$ de degré n. **Consignes :** Ne vous servez pas de la méthode `.irreducible_element()`. Écrivez une boucle qui tire des polynômes au hasard jusqu'à en trouver un irréductible. Vous pouvez utiliser la méthode `.random_element()` des anneaux de polynômes pour tirer des polynômes au hasard.

Exercice 5.3 – Même question qu'à l'exercice précédent, mais cette fois-ci $k = \mathbb{F}_p$ est un corps premier, et vous donnerez en sortie le plus petit polynôme irréductible par l'ordre lexicographique (sur les coefficients).

Exercice 5.4 – Nous allons adopter une représentation distribuée creuse pour les polynômes : un monôme sera représenté par une liste à deux éléments. Le premier est le coefficient et le second la liste des exposants.

1. Écrire une fonction qui teste si un monôme m_1 est plus petit qu'un monôme m_2 pour l'ordre lexicographique.
2. Écrire une fonction qui, étant donnée une liste de monômes, renvoie son plus petit élément m.
3. Écrire une fonction qui, étant donnée une liste de monômes, énumère les monômes dans l'ordre croissant pour l'ordre lexicographique.
4. Écrire une fonction qui affiche un monome de la manière habituelle (par ex. `5 x^10 y^20`). Vous êtes libres de choisir la façon dont les noms des variables sont assignés (pour référence, `chr(97)` équivaut au caractère `'a'`).
5. (**avancé**) Transformer ces fonctions en une classe `Monome`, munie de deux champs, et au minimum des méthodes spéciales `__lt__`, `__repr__` et `__mul__`.

6. Calcul de bases de Gröbner

Exercice 6.1 –

Soit l'idéal I de $\mathbb{Q}[x,y]$ défini par

$$I = \langle x^2y^2 - x, xy^3 + y \rangle.$$

1. Donner une base de Gröbner de I pour l'ordre lexicographique.
2. Vérifier que les éléments obtenus appartiennent effectivement à I.
3. Soit $P = x^3y^2 + 2xy^4$. Calculer $\overline{P}^G$.

Exercice 6.2 – Dans $k[x,y,z]$, on choisit l'ordre degrevlex. Calculer une base de Gröbner de l'idéal $I = (xyz + z^3, y^2)$.

Exercice 6.3 – Soit G une base de Gröbner pour l'idéal $I \subset k[x_1,\dots,x_n]$ et supposons qu'il existe $P \neq Q \in G$ tels que $\mathrm{LT}(P)$ divise $\mathrm{LT}(Q)$. Montrer que $G \setminus \{Q\}$ est encore une base de Gröbner pour I.

Exercice 6.4 – Le polynôme $x^3 + 1$ est-il dans l'idéal engendré par $x + y + z$, $xy + yz + zx$ et $xyz + 1$?

Exercice 6.5 – Soit $I \in k[x_1,\dots,x_n]$ un idéal principal. Montrer que tout sous-ensemble fini contenant un générateur de I est une base de Gröbner pour I.

Exercice 6.6 –

Soit l'ideal

$$I = \left\langle z^5 - y^3t^2, x^2t - yz^2, x^2z^3 - y^4t, x^4z - y^5 \right\rangle$$

de $k[x,y,z,t]$.

1. Montrer que le système générateur de I est une base de Gröbner pour l'ordre lexicographique avec $x > y > z > t$.
2. Trouver un ordre sur les variables tel que $\left\langle z^{11}, yz^2, y^3t^2, y^4t, y^5, x^2y^2t^3, x^4yt^4 \right\rangle$ soit $\langle \mathrm{LT}(I) \rangle$.

Exercice 6.7 – On se place dans un anneau $R = k[x_1,\dots,x_n]$ où k est un corps commutatif. Soit I un idéal de R non nul. Une base de Gröbner universelle est un ensemble qui est une base de Gröbner de I pour tous les ordres admissibles de R. Calculer une base de Gröbner universelle de l'idéal de $\mathbb{Q}[x,y]$ engendré par $x - y^2$ et $xy - x$.

Exercice 6.8 –

Soit l'anneau A des polynômes à $2m$ indéterminées $(x_{ij})_{1\le i\le 2, 1\le j\le m}$, à coefficients dans k. Soit I l'idéal de A engendré par les $\binom{m}{2}$ polynômes $D_{k,\ell} = x_{1k}x_{2\ell} - x_{1\ell}x_{2k}$, pour $1 \le k < \ell \le m$.

1. Pour $m = 3$, montrer que les $D_{k,\ell}$ forment une base de Gröbner universelle de I.
2. Pour $m > 3$, montrer que les $D_{k,\ell}$ forment une base de Gröbner universelle de I.

Exercice 6.9 –

Soit V un sous-espace vectoriel de k^n de dimension $n-d<n$. Soit I son idéal annulateur dans $k\boxed{x}$: l'idéal I est engendré par d formes linéaires indépendantes

$$I=\left\langle \sum_{j=1}^{n} a_{ij}x_j\ ,\ 1\leq i\leq d\right\rangle .$$

Soit $A=(a_{ij})$ la matrice $d\times n$ dont les coefficients sont les a_{ij} définis ci-dessus. On dit qu'une forme linéaire non nulle L dans I est un circuit si l'ensemble des variables apparaîssant dans toute écriture de L est minimal pour l'inclusion.

Pour $j_i,\ldots,j_d$ des entiers entre 1 et n, on définit $D_{j_1,\ldots,j_d}$ comme étant le déterminant de la matrice dont les colonnes sont les colonnes $j_1,\ldots,j_d$ de A. On dit qu'un d-sous-ensemble $J=\{j_1,\ldots,j_d\}\subset\{1,\ldots,n\}$ est une base, si le déterminant D_J de la matrice $(a_{ij})_{i,j\in\{j_1,\ldots,j_d\}}$ associée est non nul.

1. Montrer que les circuits sont précisément les formes linéaires non nulles

$$D_{k_1,\ldots,k_{d-1},1}x_1+D_{k_1,\ldots,k_{d-1},2}x_2+\cdots+D_{k_1,\ldots,n}x_n$$

   où $1\leq k_1<\cdots<k_{d_1}\leq n$.
2. En déduire qu'il y a au plus $\binom{n}{d-1}$ circuits.
3. Soit I' un idéal engendré par des formes linéaires. Montrer que l'ensemble des circuits dans I' est une base de Gröbner universelle de I'.

7. Critère de Buchberger

Exercice 7.1 – Soient les polynômes $P_1=x^3y-2x^2y^2+x$ et $P_2=3x^4-y$ de $\mathbb{Q}[x,y]$ avec l'ordre lexicographique.

1. Calculer $P=\mathrm{Syz}(P_1,P_2)$.
2. Soit $I=\langle P_1,P_2\rangle$. La base (P_1,P_2) est-elle de Gröbner ?

Exercice 7.2 – Déterminer si les ensembles suivants sont des bases de Gröbner des idéaux qu'ils engendrent.

1. $\{x^2-y,x^3-z\}$ pour l'ordre lexicographique gradué.
2. $\{x^2-y,x^3-z\}$ pour l'ordre lexicographique avec $x<y<z$ puis $x>y>z$.
3. $\{xy^2-xz+y,xy-z^2,x-yz^4\}$ avec l'ordre lexicographique.

Exercice 7.3 – La fonction $\mathrm{Syz}(f,g)$ dépend-elle du choix de l'ordre monomial ?

Exercice 7.4 – Soit $I\subset k[x_1,\ldots,x_n]$ un idéal et $G=\{g_1,\ldots,g_m\}$ une base de Gröbner de I.

1. Montrer que $\overline{f_1}^G=\overline{f_2}^G$ si, et seulement si, $f_1-f_2\in I$.
2. En déduire que $\overline{f_1+f_2}^G=\overline{f_1}^G+\overline{f_2}^G$.
3. En déduire que $\overline{f_1f_2}^G=\overline{\overline{f_1}^G\,\overline{f_2}^G}^G$.

8. Algorithme de Buchberger, Bases de Gröbner réduite

Exercice 8.1 – Déterminer une base de Gröbner des idéaux suivants :

1. $I=\langle x^2,xy+y^2\rangle$ de $k[x,y]$ pour l'ordre lexicographique.
2. $I=\langle y^2,xyz+z^3\rangle$ de $\mathbb{Q}[x,y,z]$ pour l'ordre lexicographique inverse gradué.
3. $I=\langle x^2y-1,xy^2-x\rangle$ de $\mathbb{Q}[x,y]$ pour les ordres lexicographique et lexicographique gradué.
4. $I=\langle x-z^3,y-z^5\rangle$ de $\mathbb{Q}[x,y,z]$ pour les ordres lexicographique et lexicographique inverse gradué.

Exercice 8.2 – Montrer que pour tout $m\geq 1$, la base de Gröbner réduite de

$$I_m=\langle x^{m+1}-yz^{m-1}t,xy^{m-1}-z^m,x^mz-y^mt\rangle\subset k[x,y,z,t]$$

pour l'ordre lexicographique inverse gradué contient $f_m=z^{m^2+1}-y^{m^2}t$. En déduire la base de Gröbner réduite de I_m.

Exercice 8.3 –

Soient $2\leq n'\leq n$.

1. Soient $r\geq 1$ un entier et $J=(m_1,\ldots,m_r)$ un idéal monomial de $k[X_1,\ldots,X_n]$. Donner des générateurs de l'idéal $J\cap(X_{n'},\ldots,X_n)$. Dans la suite on fixe sur $k[X_1,\ldots,X_n]$ l'ordre lexicographique, on désigne par I un idéal homogène non nul et par I' l'intersection $I'=I\cap(X_{n'},\ldots,X_n)$.
2. Montrer que $\mathrm{LT}(I')=\mathrm{LT}(I)\cap(X_{n'},\ldots,X_n)$.
3. Soit $(f_1,\ldots,f_s)$ une base de Gröbner de I formée de polynômes homogènes. Déduire des questions précédentes des générateurs de $\mathrm{LT}(I')$. En déduire une base de Gröbner de I'.
4. Soit $(f_1,\ldots,f_s)$ une base de Gröbner réduite de I formée de polynômes homogènes. Donner une condition nécessaire et suffisante pour que l'on ait $I\cap(X_n)=X_nI$.

Exercice 8.4 – Soient f et g deux polynômes non nuls sans facteur commun et I l'idéal qu'ils engendrent. On suppose que (f,g) est une base de Gröbner de I.

1. On pose : $\mathrm{LT}(f) = \lambda m m'$, $\mathrm{LT}(g) = \mu m m''$, où m est un monôme, m' et m'' sont deux monômes premiers entre eux et λ et μ deux scalaires. En utilisant la division du S-polynôme $\mathrm{Syz}(f,g)$ par la suite (f,g), montrer qu'il existe un polynôme g_1 dont $\mathrm{LT}(g_1)$ n'est pas divisible par $\mathrm{LT}(f)$ et tel que f divise $g_1 + \lambda m'$.
2. En déduire que $m = 1$.
3. En déduire que (f,g) est une base de Gröbner de I si, et seulement si, $\mathrm{LT}(f)$ et $\mathrm{LT}(g)$ sont premiers entre eux.
4. On pose $f = hf'$, $g = hg'$, où f' et g' n'ont pas de facteur commun. Montrer que (f,g) est une base de Gröbner de I si, et seulement si, (f', g') est une base de Gröbner de l'idéal I' engendré par f' et g'.
5. Donner une condition nécessaire et suffisante pour que (f,g) soit une base de Gröbner de I.

Exercice 8.5 - Soit $k[x_1, \ldots, x_n]$ muni d'un ordre monomial $<$ tel que $x_1 > \ldots > x_n$. Soient $\ell_1, \ldots, \ell_m \in k[x_1, \ldots, x_n]$ des polynômes de degré 1. Montrer que la base de Gröbner réduite de $I = \langle \ell_1, \ldots, \ell_m \rangle$ ne contient que des polynômes de degré 1. (On pourra considérer la réduction du système d'équations linéaires défini par les $\ell_1, \ldots, \ell_m$ et utiliser l'unicité de la base de Gröbner réduite.) Montrer que l'énoncé n'est plus vrai avec des polynômes de degré 2.

9. Résultants et élimination

Exercice 9.1 – Soit l'idéal $I = \left\langle y^4x + 3x^3 - y^4 - 3x^2, x^2y - 2x^2, 2y^4x - x^3 - 2y^4 + x^2 \right\rangle$.

1. Montrer que $I \cap \mathbb{Q}[x] = \left\langle x^3 - x^2 \right\rangle$.
2. Montrer que $I \cap \mathbb{Q}[y] = \left\langle y^5 - 2y^4 \right\rangle$.

Exercice 9.2 –

1. Calculer une base de Gröbner réduite de l'idéal engendré par $(x + y - z; x^2 - 2t^2; y^2 - 5t^2)$ pour l'ordre lexicographique induit par $x > y > z > t$.
2. En déduire que $\sqrt{2} + \sqrt{5}$ est un nombre algébrique sur le corps des rationnels $\mathbb{Q}$, en exhibant un polynôme à une variable à coefficients rationnels dont il est racine.
3. Quel est le résultant de $(y - z)^2 - 2$ et $y^2 - 5$ par rapport à y ?
4. En déduire que $\mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}(\sqrt{2} + \sqrt{5})$. Exprimer $\sqrt{2}$ et $\sqrt{5}$ en fonction de $\sqrt{2} + \sqrt{5}$.

Exercice 9.3 – Soient A et B deux polynômes de $K[X]$, où K est un corps.

1. Fabriquer un polynôme dont les racines sont les sommes d'une racine de A et d'une racine de B. (Quels sont les Y tels que le système $A(X) = B(Y - X) = 0$ ait une solution ?)
2. Fabriquer un polynôme à coefficients entiers qui a $2^{1/2} + 7^{1/3}$ pour racine.

Exercice 9.4 – Déterminer à l'aide d'un résultant l'intersection des courbes de $\mathbb{R}^2$ définies par

$$f(X,Y) = X^4 + Y^4 - 1,\ g(X,Y) = X^5Y^2 - 4X^3Y^3 + X^2Y^5 - 1.$$

Exercice 9.5 –

On considère la courbe plane d'équation rationnelle

$$\left\{ \left(x = a(t)/b(t), y = c(t)/d(t) \right) \in \mathbb{R}^2, t \in \mathbb{R} \right\}.$$

1. Comment trouver une équation implicite de la courbe ?
2. On considère la paramétrisation rationnelle

$$\begin{cases} x = \dfrac{u^2}{v} \\ y = \dfrac{v^2}{u} \\ z = u \end{cases}$$

   Vérifier que les points (x,y,z) sont sur la surface $x^2y = z^3$.

3. Soit I l'idéal $\left\langle vx - u^2, uy - v^2, z - u \right\rangle$. Calculer $I_2 = I \cap \mathbb{R}[x,y,z]$.
4. Impliciter l'exemple $x = t^2 + t + 1$, $y = (t^2 - 1)/(t^2 + 1)$.

Exercice 9.6 – Donner l'aire d'un triangle en fonction des longueurs a, b, c de ses trois côtés.

Exercice 9.7 – Soit K un corps infini, $P \in K[X_1, \ldots, X_n]$ un polynôme non nul de degré d.

1. Montrer qu'il existe $(a_1, \ldots, a_{n-1})$ dans K^{n-1} tel que le polynôme $P(X_1 + a_1X_n, \cdots, X_{n-1} + a_{n-1}X_n, X_n)$ soit de la forme $cX_n^d + Q$, où c est un élément non nul de K et Q un polynôme de degré $< d$ par rapport à X_n.
2. En utilisant un résultant en déduire le théorème des zéros de Hilbert.

10. Variétés affines

Exercice 10.1 – En utilisant Sage, donner les solutions des équations suivantes :

1. $x^3 - 1 = 0$.
2. $x^3 - 5ax^2 + x = 1$.

3. $x^7-2x^6-4x^5-x^3+x^2+6x+4=0$.

Exercice 10.2 – En utilisant Sage, donner les solutions des systèmes d'équations suivants :

1. $\begin{cases} x^2+y^2=25, \\ x^2-9=y. \end{cases}$.
2. $\begin{cases} x^2+y^2=1, \\ z=x-y, \\ z^2=x+y. \end{cases}$.
3. $\begin{cases} cx+xy^2+xz^2=1, \\ cy+yx^2+yz^2=1, \\ cz+zx^2+zy^2=1. \end{cases}$ où c est un paramètre réel.

Exercice 10.3 – Résoudre l'équation suivante dans $\mathbb{Z}/7\mathbb{Z}$: $y^2=x^3-28$.

Exercice 10.4 – On considère la surface S paramétrée par

$$\begin{cases} x=(2+\cos u)\cos t, \\ y=(2+\cos u)\sin t, \\ z=\sin u \end{cases}$$

et la courbe C tracée sur S et paramétrée par

$$\begin{cases} x=(2+\cos 2s)\cos 3s, \\ y=(2+\cos 2s)\sin 3s, \\ z=\sin 2s. \end{cases}$$

1. Obtenir une équation implicite de S.
2. Obtenir des équations implicites de C.
3. Vérifier à l'aide de ces équations que $C\subset S$.

Exercice 10.5 – Soient les idéaux de $k[x,y]$:

$$\begin{aligned} I &= \langle x^2y+xy^2-2y; x^2+xy-x+y^2-2y; xy^2-x-y+y^3\rangle \text{ et} \\ J &= \langle x-y^2; xy-y; x^2-y\rangle . \end{aligned}$$

Montrer que $I=J$.

Exercice 10.6 – Soient les idéaux de $k[x,y,z]$:

$$\begin{aligned} I &= \langle x^2+xz; y+y^4+xz^2-3z; y+2x^2y^2+xz^2\rangle \text{ et} \\ J &= \langle x^3+yz+xy; xyz+2y^2z^2-3x; x^3y-z^2\rangle . \end{aligned}$$

1. Montrer que $I\neq J$.
2. A-t-on $I\subset J$?
3. A-t-on $J\subset I$?

Exercice 10.7 – Soient a,b,c satisfaisant le système :

$$\begin{cases} a+b+c &= 3 \\ a^2+b^2+c^2 &= 5 \\ a^3+b^3+c^3 &= 7 \end{cases}$$

1. Montrer que $a^4+b^4+c^4=9$.
2. Montrer que $a^5+b^5+c^5\neq 11$.
3. Que valent $a^5+b^5+c^5$ et $a^6+b^6+c^6$?

Exercice 10.8 – (Sagebook, exercice 36) Soit J un idéal de dimension zéro de $\mathbb{Q}[x,y]$. Soit χ_x le polynôme caractéristique de l'application linéaire

$$\begin{aligned} m_x : \mathbb{Q}[x,y]/J &\to \mathbb{Q}[x,y]/J \\ p+J &\mapsto xp+J \end{aligned}$$

Calculer χ_x dans le cas $J=\langle x^2+y^2-1, 4x^2y^2-1\rangle$. Montrer que toute racine de χ_x est l'abscisse d'un point de la variété $V_{\mathbb{C}}(J)$.

11. Théorème d'élimination

Exercice 11.1 – Soit $I\subseteq k[x_1,\dots,x_n]$ un idéal.

1. Montrer que $I_\ell=I\cap k[x_{\ell+1},\dots,x_n]$ est un idéal de $k[x_{\ell+1},\dots,x_n]$.
2. Montrer que l'idéal $I_{\ell+1}\subseteq k[x_{\ell+2},\dots,x_n]$ est le premier idéal d'élimination de $I_\ell\subseteq k[x_{\ell+1},\dots,x_n]$.
3. En déduire comment appliquer le théorème d'élimination pour éliminer plusieurs variables.

Exercice 11.2 – Soient le système d'équations

$$\begin{cases} x^2+2y^2 & =3 \\ x^2+xy+y^2 & =3 \end{cases}$$

et I l'idéal engendré par ces équations.

1. Déterminer des bases de $I \cap k[x]$, et de $I \cap k[y]$.
2. En déduire l'ensemble des solutions de ce système.

Exercice 11.3 – Soit I l'idéal déterminé par les équations

$$x^2+y^2+z^2=4,\ x^2+2y^2=5,\ xz=1.$$

1. Calculer les idéaux I_1 et I_2.
2. Combien le système associé admet-il de solutions $(x,y,z) \in \mathbb{Q}^3$?
3. Combien le système associé admet-il de solutions $(x,y,z) \in \mathbb{C}^3$?

Exercice 11.4 –

Utiliser le théorème d'élimination pour résoudre le système suivant dans $\mathbb{R}^3$ puis dans $\mathbb{C}^3$:

$$\begin{cases} x^2+2y^2-y-2z & =0 \\ x^2-8y^2+10z-1 & =0 \\ x^2-7xy & =0. \end{cases}$$

Exercice 11.5 –

Soit $f=x^4y^2+x^2y^4-x^2y^2 \in \mathbb{Q}[x,y]$. On cherche à calculer les valeurs critiques de f vu comme fonction polynomiale de $\mathbb{R}^2$ dans $\mathbb{R}$.

1. Soit J l'ideal $\left\langle \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y} \right\rangle$. Quelle est la dimension de J ? Peut-on calculer simplement les points critiques de f ?
2. En considérant l'idéal $\left\langle \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, f-t \right\rangle \subset \mathbb{Q}[x,y,t]$, trouver un polynôme de $\mathbb{Q}[t]$ dont l'ensemble des racines contient les valeurs critiques de f.

Exercice 11.6 –

Soient I et J deux idéaux de $k[x_1,\dots,x_n]$. Soit $\langle tI+(t-1)J \rangle \in k[t,x_1,\dots,x_n]$. Montrer que $I \cap J = \langle tI+(t-1)J \rangle \cap k[x_1,\dots,x_n]$.

Exercice 11.7 –

Calculer, dans $\mathbb{Q}[x,y]$, l'intersection des idéaux

$$I=\langle x^2-2, x+y \rangle,\ J=\langle x^2-2, x-y \rangle.$$

Exercice 11.8 –

Écrire un algorithme qui détermine l'intersection de deux idéaux.

12. Rappel sur les idéaux

Exercice 12.1 –

Soit I un idéal non trivial de $k[x_1,\dots,x_n]$ et soit $\{y_1,\dots,y_r\} \subseteq \{x_1,\dots,x_n\}$. L'ensemble des variables $\{y_1,\dots,y_r\}$ est dit *indépendant modulo* I si $I \cap k[\underline{y}] = \{0\}$. La dimension de I est définie par

$$\dim I = \max\{|\{y_1,\dots,y_r\}|,\ \text{avec } \{y_1,\dots,y_r\} \text{ algebriquement independants modulo } I\}.$$

1. Montrer qu'un idéal propre I est de dimension zéro si, et seulement si, il contient un polynôme non constant en chaque variable $\{x_1,\dots,x_n\}$.

Soit I un idéal propre de $k[x_1,\dots,x_n]$.

2. Si I est de dimension zéro, montrer que pour tout ordre admissible sur $k[x_1,\dots,x_n]$ et pour toute base de Gröbner G de I, pour tout $1 \le i \le n$, il existe $g_i \in G$ avec $\mathrm{LM}(g_i)=x_i^{\alpha_i}$ pour un $\alpha_i \ge 0$.
3. Supposons qu'il existe un ordre sur $k[x_1,\dots,x_n]$ et une base de Gröbner G de I telle que pour tout $1 \le i \le n$, il existe $g_i \in G$ avec $\mathrm{LM}(g_i)=x_i^{\alpha_i}$ pour un $\alpha_i > 0$. Montrer que $k[x_1,\dots,x_n]/I$ est un k-espace vectoriel de dimension finie.
4. Si $k[x_1,\dots,x_n]/I$ est un k-espace vectoriel de dimension finie, montrer que I est de dimension zéro.
5. En déduire que I est de dimension zéro si, et seulement si, $k[x_1,\dots,x_n]/I$ est un k-espace vectoriel de dimension finie.
6. Montrer que I est de dimension zéro si et seulement si la variété $V(I)$ ne contient qu'un nombre fini de points.

Exercice 12.2 –

Soit I l'idéal de $\mathbb{Q}[x,y]$ engendré par y^2+x^2 et x^2-2. Montrer que I est un idéal de dimension zéro.

Exercice 12.3 –

Quelle est la dimension de l'idéal I de $\mathbb{Q}[x_1,x_2,x_3]$ engendré par $x_1x_3+x_3, x_2x_3+x_3$?

Exercice 12.4 –

Écrire un algorithme qui teste si un idéal est de dimension 0.

Exercice 12.5 –

À un n-uplet $f=(f_1,\dots,f_n)\in k[x_1,\dots,x_n]^n$ on associe une application

$$\varphi_f\;:\;k^n\to k^n$$
$$a=(a_1,\dots,a_n)\mapsto(f_1(a),\dots,f_n(a))\,.$$

On dit que φ_f est inversible s'il existe $g=(g_1,\dots,g_n)\in k[x_1,\dots,x_n]^n$ tels que $\varphi_g\circ\varphi_f=\mathrm{Id}_{k^n}$, c.-à-d. si

$$g_i(f_1,\dots,f_n)=x_i,\;1\le i\le n.$$

Soit $I=\langle y_1-f_1,\dots,y_n-f_n\rangle\subseteq k[x_1,\dots,x_n,y_1,\dots,y_n]$ muni de l'ordre lexicographique.

1. On suppose que la base de Gröbner réduite G de I est de la forme

$$G=\{x_1-g_1,\dots,x_n-g_n\}.$$

   Montrer que φ_f est inversible.

2. On suppose dans cette question que φ_f est inversible d'inverse φ_g.
   A. Montrer que l'ensemble $G=\{x_1-g_1,\dots,x_n-g_n\}$ est un sous-ensemble réduit de I.
   B. Montrer que $I\cap k[y_1,\dots,y_n]=\{0\}$.
   C. En déduire que G est une base de Gröbner réduite de I.
   D. Montrer que $g_i(f_1,\dots,f_n)=x_i$, $1\le i\le n$.
3. Soit $f_1,\dots,f_n,g_1,\dots,g_n\in k[x_1,\dots,x_n]$ tels que $g_i(f_1,\dots,f_n)=x_i$, $1\le i\le n$.
   A. Montrer que $f_i(g_1,\dots,g_n)=x_i$, $1\le i\le n$.
   B. En déduire que $\varphi_g\circ\varphi_f=\mathrm{Id}_{k^n}$ implique $\varphi_f\circ\varphi_g=\mathrm{Id}_{k^n}$.

13. Dimension d'un idéal

Exercice 13.1 –

Soit $I\subset k\left[x_1,\dots,x_n\right]$ un idéal monomial tel que $\dim\mathbb{V}\left(I\right)=n-1$.

1. Montrer que les monômes de n'importe quel ensemble de générateurs de I ont un facteur commun non constant.
2. On écrit $\mathbb{V}\left(I\right)=V_1\cup\ldots\cup V_p$, où les V_i sont des sous-espaces de coordonnées tels que $V_i\nsubseteq V_j$ pour $i\ne j$. On suppose de plus qu'un seul des V_i est de dimension $n-1$.
   A. Quelle est la valeur maximale que peut prendre p ?
   B. Donner un exemple où ce p maximum est atteint.

Exercice 13.2 –

Soit I un idéal monomial de $k\left[x_1,\dots,x_n\right]$.

1. Si $\mathbb{V}\left(I\right)$ est de dimension 0, que peut être $\mathbb{V}\left(I\right)$?
2. Montrer que $\mathbb{V}\left(I\right)$ est de dimension 0 si et seulement si pour tout $i\in\{1,\dots,n\}$, il existe $\ell_i\ge1$ tel que $x_i^{\ell_i}\in I$.

Exercice 13.3 –

Soit I l'idéal de $k[x,y]$:

$$I=\left\langle x^3y,xy^2\right\rangle.$$

Calculer la fonction de Hilbert ${}^aHF_I(s)$ de plusieurs façons différentes avec et sans Sage.

Exercice 13.4 –

Soit I l'idéal de $k[x,y,z]$:

$$I=\left\langle x^3yz^5,xy^3z^2\right\rangle.$$

Calculer la fonction de Hilbert ${}^aHF_I(s)$.

Exercice 13.5 –

Soit I l'idéal de $k[x_1,\dots x_4]$:

$$I=\left\langle x_1x_3,x_1x_4^2,x_2x_3,x_2x_4^3\right\rangle.$$

Calculer la fonction de Hilbert ${}^aHF_I(s)$.

Exercice 13.6 –

Soient $I_1\subset I_2$ des idéaux de $k[x_1,\dots,x_n]$.

1. Montrer que $C(\langle\mathrm{LT}(I_2)\rangle)\subset C(\langle\mathrm{LT}(I_1)\rangle)$.
2. Montrer que pour tout $s\ge0$, ${}^aHF_{I_2}(s)\le{}^aHF_{I_1}(s)$.
3. Montrer que $\deg^a HP_{I_2}\le\deg^a HP_{I_1}$.

Exercice 13.7 –

Soit k un corps algébriquement clos. Calculer la dimension des variétés affines définies par les idéaux suivants :

1. $I = \langle xz, xy-1 \rangle$.
2. $J = \left\langle zw-y^2, xy-z^3 \right\rangle$.

Exercice 13.8 –

Montrer qu'un point $p=(a_1,\ldots,a_n) \in k^n$ est une variété affine de dimension zéro.

Exercice 13.9 –

Soit k un corps algébriquement clos et $I = \langle xy, xz \rangle \in k[x,y,z]$.

1. Montrer que $I \cap k[x] = 0$ mais que $I \cap k[x,y]$ et $I \cap k[x,z]$ ne sont pas nuls.
2. Montrer que $I \cap k[y,z] = 0$ mais que $I \cap k[x,y,z] \neq 0$.
3. Quelle est la dimension de $V(I)$?

14. Cônes et éventails de Gröbner

Exercice 14.1 -

Pour chacun des idéaux suivants, représenter l'éventail de Gröbner.

1. I = $\langle x^2+y^2-1, x+2y \rangle$ (l'éventail contient deux cônes maximaux).
2. I = $\langle x^3-y, x+y^3+1 \rangle$ (l'éventail contient trois cônes maximaux).
3. I = $\langle y^2-x^2, z-y^4 \rangle$ (l'éventail contient quatre cônes maximaux ; représenter son intersection avec le plan $x+y+z=1$).
4. I = $\langle y-x^2, z-x^3 \rangle$ (l'éventail contient six cônes maximaux ; représenter son intersection avec le plan $x+y+z=1$).

Exercice 14.2 -

Soit G une base de Gröbner marquée pour un ordre matriciel $<_M$, et soit w la première ligne (non nulle) de M. Soit w' un vecteur dans le cône de Gröbner C_G. Pour tout $f \in k[x_1,\ldots,x_n]$, on définit $\mathrm{in}_{w'}(f)$ comme étant la somme des termes de f de w'-poids maximal.

Montrer que l'ensemble $\mathrm{in}_{w'}(G)$ est une base de Gröbner de l'idéal $\langle \mathrm{in}_{w'}(G) \rangle$ pour l'ordre $<_M$. Observer que $\langle \mathrm{in}_{w'}(G) \rangle$ est un idéal monomial si w' se trouve dans l'intérieur du cône C_G.

Exercice 14.3 -

Pour chacun des idéaux de l'exercice 14.1, effectuer une marche de Gröbner pour convertir la base de Gröbner marquée pour l'ordre lex avec $x>y>z$ en celle pour l'ordre lexicographique avec $z>y>x$.

15. Polynômes symétriques et théorie des invariants

Exercice 15.1 -

c Montrer que l'anneau des polynômes C_3-invariants est égal à

$K[x_1,x_2,x_3]^{C_3} = K[\sigma_1,\sigma_2,\sigma_3, x_1x_2^2+x_2x_3^2+x_3x_1^2, x_1^2x_2+x_2^2x_3+x_3^2x_1]$,

où les σ_i sont les polynômes symétriques élémentaires.

Exercice 15.2 -

Soit K un corps de caractéristique nulle. Soit G le sous-groupe de $GL_2(K)$ engendré par $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

1. Montrer que G est un groupe cyclique d'ordre 4.
2. Montrer que $K[x_1,x_2]^G = K[x_1^2+x_2^2, x_1^3x_2-x_1x_2^3, x_1^2x_2^2]$.
3. Exprimer le polynôme G-invariant $-x_1^8x_2^8+x_1^8x_2^4-2x_1^6x_2^6+x_1^4x_2^8+x_1^9x_2+2x_1^7x_2^3-2x_1^3x_2^7-x_1x_2^9$ en termes des générateurs trouvés à la question précédente.

Exercice 15.3 -

Soit K un corps de caractéristique nulle contenant une racine cubique primitive de l'unité ζ (autrement dit, $\zeta^3=1$, mais ζ et ζ^2 sont différents de 1). Soit G le sous-groupe de $GL_3(K)$ engendré par $\begin{pmatrix} \zeta & 0 & 0 \\ 0 & \zeta & 0 \\ 0 & 0 & \zeta \end{pmatrix}$.

1. Montrer que $K[x_1,x_2,x_3]^G = K[x_1^3,x_2^3,x_3^3,x_1x_2^2,x_1^2x_2,x_1x_3^2,x_1^2x_3,x_2x_3^2,x_2^2x_3,x_1x_2x_3]$.
2. Calculer l'idéal dea relations entre les générateurs trouvés à la question précédente.

Exercice 15.4 -

(Discriminants.) Soit $n \geq 2$ un entier, et soit S_n le groupe symétrique. Considérons le polynôme $f = \prod_{1 \leq i < j \leq n}(x_i-x_j)^2$.

1. Montrer que f est un polynôme symétrique à coefficients entiers.
2. En déduire qu'il existe un polynôme $\Delta \in \mathbb{Z}[y_1,\ldots,y_n]$ tel que $f = \Delta(\sigma_1,\ldots,\sigma_n)$, où les σ_i sont les fonctions symétriques élémentaires. Le polynôme Δ est appelé le discriminant d'ordre n.
3. Montrer que, pour $n=2$, on a $\Delta = y_1^2-4y_2$. Montrer que pour $n=3$, on a $\Delta = y_1^2y_2^2-4y_2^3-4y_1^3y_3-27y_3^2+18y_1y_2y_3$.

4. Soit T une autre variable, et considérons le polynôme $\prod_{i=1}^{n}(T-x_i)$. Montrer que ce polynôme est égal à $T^n-\sigma_1T^{n-1}+\sigma_2T^{n-2}-\ldots+(-1)^n\sigma_n$.
5. Soit maintenant $p\in K[T]$ un polynôme de degré n et de coefficient directeur 1. Écrivons $p=T^n+\sum_{i=0}^{n-1}(-1)^ia_iT^{n-i}$. On appelle discriminant de p l'élément de K défini par $\Delta_p:=\Delta(a_1,\ldots,a_n)$. Supposons enfin que p est scindé dans K. Montrer que p admet une racine multiple si et seulement si $\Delta_p=0$.
