MA^2 2011-2012
M2 Algèbre formelle

1 Fonctions MAPLE élémentaires

1.1 Polynômes à une variable

Fonctions utiles : **degree, lcoeff, op, tcoeff, coeff, coeffs, expand, sort, normal, factor, gcd, texteq, quo, rem, mod, RootOf, BezoutP, gcdex.**

1. Soient les polynômes :

$$P_1 = x^6 + 2x^5 - 2x^4 + 2x^2 - 2x - 1 \text{ et } P_2 = x^5 + x^4 - 2x^3 + x^2 + x - 2.$$

1.1 Déterminer le degré, le coefficient dominant et la liste des termes de $P = P_1 P_2$.
1.2 Calculer $Q = PGCD(P_1, P_2)$.
1.3 Factoriser P. Calculer $P(2)$.
1.4 Effectuer la division euclidienne de P_1 par P_2.

2. 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 ?

```
euclidepol:=proc(A,B,X)
local A0,A1,S0,S1,T0,T1,Q,U;
A0:=expand(A); A1:=expand(B);
S0:=1; S1:=0;
T0:=0; T1:=1;
while (A1 ¡¿ 0) do
Q:=quo(A0,A1,X);
U:=A1; A1:=expand(A0 - Q*A1); A0:=U;
U:=S1; S1:=expand(S0 - Q*S1); S0:=U;
U:=T1; T1:=expand(T0 - Q*T1); T0:=U;
```

```
end do;
return A0,S0,T0;
end proc;
```

3. Soit le polynôme

$$P = x^{11} + x^{10} + x^9 + 2x^8 + 2x^6 + 2x^4 + x^2 + x^3 + x.$$

3.1 Factoriser P dans $\mathbf{Z}[x]$.
3.2 Factoriser P dans $\mathbf{Z}[i][x]$.
3.3 Factoriser P dans $\mathbf{F}_2[x]$.
3.4 Factoriser P dans $\mathbf{F}_4[x]$.

4. Soit le polynôme

$$P = x^7 + x^5 + 2x^3 + 2x^2 + 3x + 2.$$

4.1 Factoriser P dans $\mathbf{F}_2$ et $\mathbf{F}_7$.
4.2 En déduire une preuve de l'irréductibilité de P dans $\mathbf{Z}[x]$.
4.3 Vérifier l'irréductibilité de P avec Maple.

5. Soit p un nombre premier. Factoriser $x^p - p$ en facteurs irréductibles dans $\mathbf{F}_p[x]$.

6* Soit p un nombre premier. Factoriser le polynôme $x^{2p} + x^p + 1$ en facteurs irréductibles dans $\mathbf{Z}[x]$.

1.2 Polynômes à plusieurs variables

Fonctions utiles : **plex, collect,tdeg**

1. Soit le polynôme $P = xy^5 + 2y^4 + 3y^3x^3 + 4x^2y^2 + 5x^12 + 6yx^3 + 7y$.
1.1 Donner le degré total de P.
1.2 Ecrire P comme polynôme en x.

2. Transformer le polynôme $P = (x^2 + xy + x + y)(x + y)$ avec Maple sous les formes suivantes:

2.1 $x^3 + 2x^2y + xy^2 + x^2 + 2xy + y^2$,

2.2 $(x + 1)(x + y)^2$,

2.3 $y^2 + (2y + y^2)x + (1 + 2y)x^2 + x^3$,

2.4 $x^3 + x^2 + (2x^2 + 2x)y + (x + 1)y^2$.

2 Ordres admissibles

2.1 Préliminaire sur les ordres admissibles

Fonction utiles : **with(Groebner), NormalForm, NormalForm,plex,grlex,tdeg**

1. Soit le polynôme

$$P = xy^5 + 2y^4 + 3y^3x^3 + 4x^2y^2 + 5x^12 + 6yx^3 + 7y.$$

1.1 Ordonner P dans l'ordre lexicographique.
1.2 Ordonner P par l'ordre lexicographique gradué.
1.2 Ordonner P par l'ordre lexicographique inverse gradué.

2. Montrer que l'ordre lexicographique est un ordre admissible.

3. Soient les polynômes

$$P_1 = x^2y^2 - x, P_2 = xy^3 + y \text{ et } P = x^3y^2 + 2xy^4.$$

3.1 Soit $F = [P_1, P_2]$, à quoi correspond la commande NormalForm(P,F,[x,y],plex) ?
3.2 Soit $F = [P_2, P_1]$, à quoi correspond la commande NormalForm(P,F,[x,y],plex) ?
3.3 Soit $F = [P_1, P_2]$, à quoi correspond la commande NormalForm(P,F,[x,y],tdeg) ?
3.4 Effectuer le même travail pour $P = x^2y^6$ et $F = [x^2y^2 - x^4, xy^3 - y^4]$.
3.5 Effectuer le même travail pour $P = x^2y^6 + z^5$ et $F = [x^2y^2 - z^4, xy^3 - y^4]$.

4. Déterminer quel ordre monomial (lex,grlex, grevlex) a été utilisé pour ordonner les termes des polynômes suivants : (a) $f(x, y, z) = 7x^2y^4z - 2xy^6 + x^2y^2$.
(b) $f(x, y, z) = xy^3z + xy^2z^2 + x^2z^3$.
(c) $f(x, y, z) = x^4y^5z + 2x^3y^2z - 4xy^2z^4$.

5. Soit $f = x^7y^2 + x^3y^2 - y - 1$ et l'ensemble ordonné $F = \{f_1 = xy^2 - x, f_2 = x - y^3\}$.
5.1 Calculer $\overline{f}^F$ pour les ordres lexicographique et lexicographique gradué.
5.2 Effectuer les mêmes calculs en inversant l'ordre de F.

6.

6.1 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 $r \in k[x]$.

6.2 trouver une écriture explicite de la forme

$$z^2 - x^4 y = h_1(y - x^2) + h_2(z - x^3).$$

2.2 Représentation matricielle des ordres admissibles.

1. Matrices de poids I

On étend l'ordre lexicographique $>_{lex}$ à $\mathbf{R}^n$ de la façon évidente. On définit une relation sur les monômes à n variables à partir d'une matrice A carrée réelle de taille n comme suit :

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} > x_1^{\beta_1} \cdots x_n^{\beta_n} \iff A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} >_{lex} A \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}.$$

1.1 Quelles conditions (nécessaires et suffisantes) doit vérifier A pour que l'ordre associé soit un ordre admissible ?

1.2 Donner successivement un exemple de matrice A tel que l'ordre associé soit l'ordre lex, tdeg, degrevlex, avec dans tous les cas $x_1 > \cdots > x_n$.

2. On s'intéresse à la construction d'ordres admissibles de $\mathbf{N}^n$.

Soient P et Q deux polynômes de $\mathbf{Z}[X]$. On dit que P est supérieur ou égal à Q (noté $P \geq Q$) si $P = Q$ ou si $P \neq Q$ et si le coefficient dominant de $P - Q$ est positif.

On dit que $P_1, \ldots, P_n \in \mathbf{Z}[X]$ sont rationnellement dépendants s'il existe $q_1, \ldots, q_n \in \mathbf{Q}$ non tous nuls tels que $q_1 P_1 + \cdots + q_n P_n$ soit le polynôme nul. Dans le cas contraire, on dit qu'ils sont rationnellement indépendants.

2.1 Soient $P_1, \ldots, P_n \in \mathbf{Z}[X]$ rationnellement indépendants. Dans $\mathbf{N}^n$, on définit $(a_i)_{1 \leq i \leq n} \geq (b_i)_{1 \leq i \leq n}$ si $\sum_{i=1}^{n} a_i P_i \geq \sum_{i=1}^{n} b_i P_i$. Montrer que c'est un ordre admissible de $\mathbf{N}^n$.

2.2 Déterminer $P_1, \ldots, P_n$ pour que l'ordre obtenu soit successivement l'ordre lexicographique,

l'ordre lexicographique gradué, lexicographique gradué inverse.

3* Matrices de poids II.

On définit des ordres monomiaux en se donnant des matrices de poids. Ces ordres plus généraux permettent de retrouver tous les ordres déjà vus (voir exercice 1.). Étant donnee une matrice inversible $W = (w_{i,j})_{1 \leq i,j \leq n}$, le poids d'un monôme $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ est le vecteur colonne $W^t(\alpha_1, \ldots, \alpha_n)$. Deux monômes sont ensuite comparés en comparant lexicographiquement leurs poids respectifs. Autrement dit, pour comparer $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ et $X_1^{\beta_1} \cdots X_n^{\beta_n}$ on compare $w_{1,1}\alpha_1 + \cdots + w_{1,n}\alpha_n$ et $w_{1,1}\beta_1 + \cdots + w_{1,n}\beta_n$ si ces deux nombres sont différents, on statue sur l'ordre des monômes, sinon on continue avec $w_{2,1}\alpha_1 + \cdots + w_{2,n}\alpha_n$ et $w_{2,1}\beta_1 + \cdots + w_{2,n}\beta_n$ et ainsi de suite. La nature inversible de la matrice assure qu'on n'aura pas égalité jusquà la n-ième ligne.

3.1 Écrire une fonction qui prend en entrée un idéal et une permutation σ de $\{1, \ldots, n\}$, donnée sous forme de séquence Maple, calcule la matrice de poids correspondant à l'ordre $\mathrm{lex}(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$, puis retourne la base de Gröbner pour cet ordre.

3.2 Écrire une autre fonction qui itère sur l'ensemble des permutations des variables d'un système de polynômes pour calculer toutes les bases lexicographiques en n'affichant que les monômes de tête de chaque polynôme.

3 Bases de Gröbner

3.1 Idéaux monomiaux

Fonctions utiles : **LeadingCoefficient, LeadingMonomial, LeadingTerm**
1. Soit $I =< x^\alpha, \alpha \in A >$ 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.

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

$$x^\alpha y^\beta > x^\gamma y^\delta \Longleftrightarrow x^\alpha >_{lex} x^\gamma \text{ ou } x^\alpha = x^\gamma \text{ et } y^\beta >_{tdeg} y^\delta$$

Montrer que $>$ est un ordre monomial.

3.
3.1 Écrire une fonction qui teste si un monôme m_1 est plus petit qu'un monôme m_2 pour l'ordre lexicographique.
3.2 Écrire une fonction qui, étant donnée une séquence de monômes, renvoie son plus petit élément m.
3.3 Écrire une fonction qui énumère les monômes dans l'ordre croissant pour l'ordre lexicographique.

3.2 Calcul de bases de Gröbner

Fonctions utiles : **gbasis**

0. Soit l'idéal $I =< x^2 - 2xz + 5, xy^2 + yz^3, 3y^2 - 8z^3 >$ de $\mathbf{Q}[x, y, z]$.
0.1 Donner une base de Gröbner de I pour l'ordre lexicographique.
0.2 Donner une base de Gröbner de I pour l'ordre total.

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

$$I =< x^2y^2 - x, xy^3 + y > .$$

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

2. Dans $k[X_1, X_2, X_3]$, on choisit l'ordre lexicographique inverse. Calculer une base de Gröbner de l'idéal $I = (X_1X_2X_3 + X_3^3, X_2^2)$.

3. Soit G une base de Gröbner pour l'idéal $I \subset k[x_1, \dots, x_n]$ (avec l'ordre lexicographique) et suppose qu'il existe $p \neq q \in G$ tels que $LT(p)$ divise $LT(q)$. Montrer que $G_{\{}q\}$ est encore une base de Gröbner pour I.
4. Le polynôme $x^3 + 1$ est-il combinaison linéaire (sur $\mathbf{Q}[x, y, z]$) de $x + y + z, xy + yz + zx$ et $xyz + 1$?

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.

6. Soit l'ideal

$$I =< c^5 - b^3d^2, a^2d - bc^2, a^2c^3 - b^4d, a^4c - b^5 >$$

de $k[a, b, c, d]$.
6.1 Montrer que le système générateur de I est une base de gröbner pour l'ordre lexicographique avec $a > b > c > d$.
6.2 Trouver un ordre sur les variables tel que $< c^{11}, bc^2, b^3d^2, b^4d, b^5, a^2b^2d^3, a^4bd^4 >$ soit $< LT(I) >$.

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 $\mathbf{Q}[X, Y]$ engendré par $X - Y^2$ et $XY - X$.

8. Soit l'anneau A des polynômes à $2m$ indétermin'ees $(x_{ij})_{1 \leq i \leq 2, 1 \leq j \leq n}$,à coefficients dans

k.. Soit I l'idéal de A engendré par les $\binom{m}{2}$ polynômes $D_{k,\ell} = x_{1k}x_{2\ell} - x_{1\ell}x_{2k}$.
8.1 Pour $m = 3$, montrer que les $D_{k,\ell}$ forment une base de Gröbner universelle de I.
8.2 Pour $m \geq 3$, montrer que les $D_{k,\ell}$ forment une base de Gröbner universelle de I.

9* Soit V un sous-espace vectoriel de k^n de dimension $n - d < n$. Soit I son idéal annulateur dans $k[\underline{x}]$: l'idéal I est engendr{e par d formes linéaires indépendantes

$$I =< \sum_{j=1}^{n} a_{ij}x_j, 1 \leq i \leq n > .$$

On dit qu'une forme linéaire non nulle de I est un circuit si son ensemble de variables est minimal pour l'inclusion. 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.
9.1 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 $1 \leq k_1 < \cdots < k_{d_1} \leq n$.
9.2 En déduire qu'il y a au plus $\binom{n}{d-1}$ circuits.
9.3 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.

3.3 Critère de Buchberger

Fonction utile : **SPolynomial**

1. Soient les polynômes

$$P_1 = x^3y - 2x^2y^2 + x, P_2 = 3x^4 - y$$

de $\mathbf{Q}[x, y]$ avec l'ordre lexicographique.
1.1 Calculer $P = S(P_1, P_2)$.
1.2 Soit $I =< P_1, P_2 >$. La base (P_1, P_2) est-elle de Gröbner ?

2. Déterminer si les ensembles suivants sont des bases de Gröbner des idéaux qu'ils engendrent.
2.1 $\{x^2 - y, x^3 - z\}$ pour l'ordre lexicographique gradué.
2.2 $\{x^2 - y, x^3 - z\}$ pour l'ordre lexicographique avec $x < y < z$ puis $x > y > z$.
2.3 $\{xy^2 - xz + y, xy - z^2, x - yz^4\}$ avec l'ordre lexicographique.

3. La fonction $S(f, g)$ dépend-elle du choix de l'ordre monomial ?

4. Soit $I \subset k[x_1, \dots, x_n]$ un idéal et G une base de Gröbner de I.
4.1 Montrer que $\overline{f}^G = \overline{g}^G$ si et seulement si $f - g \in I$.
4.2 En déduire que $\overline{f+g}^G = \overline{f}^G + \overline{g}^G$.
4.3 En déduire que $\overline{fg}^G = \overline{\overline{f}^G\overline{g}^G}^G$.

3.4 Algorithme de Buchberger, Bases de Gröbner réduite

1. Déterminer une base de Gröbner des l'idéaux suivants :
1.1 $I =< x^2, xy + y^2 >$ de $k[x, y]$ avec l'ordre lexicographique,
1.2 $I =< y^2, xyz + z^3 >$ de $\mathbf{Q}[x, y, z]$ avec l'ordre lexicographique inverse gradué,
1.3 $I =< x^2y - 1, xy^2 - x >$ de $\mathbf{Q}[x, y]$ avec les ordres lexicographique et lexicographique gradué,

1.4 $I =< x - z^3, y - z^5 >$ de $\mathbf{Q}[x, y, z]$ avec les ordres lexicographique et lexicographique inverse gradué.

2. Montrer que pour tout $m \geq 1$, la base réduite de Gröbner de

$$I_m =< x^{m+1} - yz^{m-1}t, xy^{m-1} - z^m, x^m z - y^m t >\subset k[x, y, z, t]$$

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

3. Soit $2 \leq n' \leq n$.
3.1. 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 inverse, on désigne par I un idéal homogène non nul et par I' l'intersection $I' = I \cap (X_{n'}, \ldots, X_n)$.
3.2 Montrer que $LT(I') = LT(I) \cap (X_{n'}, \ldots, X_n)$.
3.3 Soit $f_1, \ldots, f_s$ une base de Gröbner de I formée de polynômes homogènes. Déduire des questions précédentes des générateurs de $LT(I')$. En déduire une base de Gröbner de I'.
3.4 Soit $f_1, \ldots, f_s$ une base de Gröbner réduite de I formée de polynômes homogènes. Donner une condition nécessaire et suffisante pour qu'on ait $I \cap (X_n) = X_n I$.

4. Soit l'idéal $I =< y^4x + 3x^3 - y^4 - 3x^2, x^2y - 2x^2, 2y^4x - x^3 - 2y^4 + x^2 >$.
4.1 Montrer que $I \cap \mathbf{Q}[x] =< x^3 - x^2 >$. (On pourra utiliser l'exercice **3.**).
4.2 Montrer que $I \cap \mathbf{Q}[y] =< y^5 - 2y^4 >$.

5. 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.
5.1 On pose : $LT(f) = \lambda mm'$, $LT(g) = \mu mm''$, oú m est un monôme, m' et m'' sont deux monômes premiers entre eux, λ et μ sont deux scalaires. En utilisant la division du S-polynôme $S(f, g)$ par la suite f, g, montrer qu'il existe un polynôme g_1 dont $LT(g_1)$ n'est pas divisible par $LT(f)$ et tel que f divise $g_1 + \lambda m'$.
5.2 En déduire que $m = 1$.

5.3 En déduire que (f, g) est une base de Gröbner de I si et seulement si $LT(f)$ et $LT(g)$ sont premiers entre eux.
5.4 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'.
5.5 Donner une condition nécessaire et suffisante pour que (f, g) soit une base de Gröbner de I.

4 Variété affine et systèmes polynômiaux

Fonctions utiles : **solve,gsolve, msolve**

4.1 Rappels sur les résultants

1.
1.1 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 $x > y > z > t$.
1.2 En ̇eduire que $\sqrt{2}+\sqrt{5}$ est un nombre algébrique sur le corps des rationnels $\mathbf{Q}$, en exhibant un polynôme à une variable à coefficients rationnels dont il est racine.
1.3 Quel est le résultant de $(y-z)^2-2$ et y^2-5 par rapport à y ?
1.4 En déduire que $\mathbf{Q}(\sqrt{2},\sqrt{5}) = \mathbf{Q}(\sqrt{2}+\sqrt{5})$. Exprimer $\sqrt{2}$ et $\sqrt{5}$ en fonction de $\sqrt{2}+\sqrt{5}$.

2. Le degré (resp. le poids) du monôme non nul $ax_1^{\alpha_1}\cdots x_n^{\alpha_n}$ est $\sum \alpha_i$ (resp. $\sum i\alpha_i$). Le degré (resp. le poids) d'un polynôme est le maximum des degrés (resp. des poids) de ses monômes non nuls. Un polynôme $P \in k[x_1,\ldots,x_n]$ est dit symétrique si pour toute permutation

$$\sigma \in S_n, P(x_{\sigma(1)},\ldots,x_{\sigma(n)}) = P(x_1,\ldots,x_n).$$

Pour $1 \leq k \leq n$, on note $S_k = \sum_{1\leq i_1<\cdots<i_k} x_{i_1}\cdots x_{i_k}$ le k-ième polynôme symétrique élémentaire. **2.1** Si P est symétrique, montrer que le degré par rapport à n'importe quel variable est le même. Ce degré est appelé degré partiel de P.
2.2 Montrer que pour tout polynôme $P \in k[x_1,\ldots,x_n]$ symétrique de degré d, il existe un unique polynôme $F \in k[x_1,\ldots,x_n]$ tel que

$$P(x_1,\ldots,x_n) = F(S_1,\ldots,S_n)$$

où F est de poids d et de degré le degré partiel de P.

3. Déterminer à l'aide d'un résultant l'intersection des courbes de $\mathbf{R}^2$ définies par

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

4. On considère la courbe plane d'équation rationnelle

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

4.1 Donner une équation implicite de la courbe.
4.2 Expliciter l'exemple $x = t^2 + t + 1$, $y = (t^2 - 1)/(t^2 + 1)$.

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

6. Soient A et B deux polynômes de $K[X]$, où K est un corps.
6.1 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 ?)
6.2 Fabriquer un polynôme à coefficients entiers qui a $2^{1/2} + 7^{1/3}$ pour racine.

7. Soit K un corps infini, $P \in K[X_1, \dots, X_n]$ un polynôme non nul de degré d.
7.1 Montrer qu'il existe $(a_1, ..., a_{n-1})$ 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.
7.2 En utilisant un résultant en déduire le théorème des zéros de Hilbert.

4.2 Variétes affines

1. En utilisant Maple, donner les solutions des équations suivantes :
1.1 $x^3 - 1 = 0$,
1.2 $x^3 - 5ax^2 + x = 1$,
1.3 $x^7 - 2x^6 - 4x^5 - x^3 + x^2 + 6x + 4 = 0$.

2. En utilisant Maple, donner les solutions des systèmes d'équations suivants :
2.1 $\begin{cases} x^2 + y^2 = 25, \\ x^2 - 9 = y. \end{cases}$

2.2 $\begin{cases} x^2+y^2=1, \\ z=x-y, \\ z^2=x+y. \end{cases}$

2.3 $\begin{cases} cx+xy^2+xz^2=1, \\ cy+yx^2+yz^2=1, \\ cz+zx^2+zy^2=1. \end{cases}$ où c est un paramètre réel.

3. Résoudre l'équation suivante dans $\mathbf{Z}/7\mathbf{Z}$:

$$y^2=x^3-28.$$

4. On considère la surface S paramétrée par

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

ainsi que la courbe C tracée sur S et paramétrée par

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

4.1 Obtenir une équation implicite de S.
4.2 Obtenir des équations implicites de C.
4.3 Vérifier à l'aide de ces équations que $C \subset S$.

5. Soient les idéaux de $k[x,y]$:

$I=<x^2y+xy^2-2y; x^2+xy-x+y^2-2y; xy^2-x-y+y^3>$ et $J=<x-y2; xy-y; x^2-y>$

Montrer que $I=J$.

6. Soient les idéaux de $k[x,y]$:

$I=<x^2+xz; y+y^4+xz^2-3z; y+2x^2y^2+xz^2>$ et $J=<x^3+yz+xy; xyz+2y^2z^2-3x; x^3y-z^2>$

6.1 Montrer que $I \neq J$.
6.2 A-t-on $I \subset J$?
6.3 A-t-on $J \subset I$?

7. Soient a, b, c satisfaisant le système :

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

7.1 Montrer que $a^4 + b^4 + c^4 = 9$.
7.2 Montrer que $a^5 + b^5 + c^5 \neq 11$.
7.3 Que valent $a^5 + b^5 + c^5$ et $a^6 + b^6 + c^6$?

5 Résolution des systèmes d'équations polynômiales

5.1 Théorème d'élimination

1. Soit $I \subset k[x_1, \dots, x_n]$ un idéal.
1.1 Montrer que $I_\ell = I \cap k[x_{\ell+1}, \dots, x_n]$ est un idéal de $k[x_{\ell+1}, \dots, x_n]$.
1.2 Montrer que l'idéal $I_{\ell+1} \subset k[x_{\ell+2}, \dots, x_n]$ est le premier idéal d'élimination de $I_\ell \subset k[x_{\ell+1}, \dots, x_n]$.
1.3 En déduire comment appliquer le théorème d'élimination pour éliminer plusieurs variables.

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

3. Soit l'idéal I déterminé par les équations

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

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

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

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

5. Soient I et I' deux idéaux de $k[x_1, \ldots, x_n]$. Soit $J =< yI, (y-1)I' >\in k[\underline{x}, y]$. Montrer que $I \cap I'$ est l'idéal d'élimination $J_{\underline{x}}$.

6. Calculer l'intersection des idéaux

$$I =< x^2 - 2, x + y >, \ I' =< x^2 - 2, x - y >$$

dans $\mathbf{Q}[x, y]$.

7. Ecrire un algorithme qui détermine l'intersection de deux idéaux.

5.2 Rappel sur les idéaux

1.
Soit I un idéal non trivial de $k[x_1, \ldots, x_n]$ et $\{y_1, \ldots, y_r\} \subset \{x_1, \ldots, x_n\}$. L'ensemble des variables $\{y_1, \ldots, y_r\}$ est dit indépendant modulo I si $I \cap k[\underline{y}] = \{0\}$. La dimension de I est définie par $\dim I = \max\{|\{y_1, \ldots, y_r\}|,$ avec $\{y_1, \ldots, y_r\}$ indépendant modulo $I\}$.
1.1 Montrer qu'un idéal propre I est de dimension zéro si et seulement si il contient un polynôme non constant en chaque variable $\{x_1, \ldots, x_n\}$.
1.2 Soit I un idéal propre de $k[x_1, \ldots, x_n]$.
1.2.1 Si I est de dimension zéro, montrer que pour tout ordre admissible sur $k[x_1, \ldots, x_n]$ et pour toute base de Gröbner G de I, pour tout $1 \leq i \leq n$, il existe $g_i \in G$ avec $LM(g_i) = x_i^{\alpha_i}$ pour un $\alpha_i > 0$.
1.2.2 Supposons qu'il existe un ordre sur $k[x_1, \ldots, x_n]$ et une base de Gröbner G de I telle que pour tout $1 \leq i \leq n$, il existe $g_i \in G$ avec $LM(g_i) = x_i^{\alpha_i}$ pour un $\alpha_i > 0$. Montrer que $k[x_1, \ldots, x_n]/I$ est un k-espace vectoriel de dimension finie.
1.2.3 Si $k[x_1, \ldots, x_n]/I$ est un k-espace vectoriel de dimension finie, montrer que I est de dimension zéro.
1.2.4 En déduire que I est de dimension zéro si et seulement si $k[x_1, \ldots, x_n]/I$ est un k-espace vectoriel de dimension finie.

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

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

4. Ecrire un algorithme qui teste si un idéal est de dimension 0.

5. La procédure Maple suivante permet de trouver une base monomiale $B = \{x^\alpha | x^\alpha \notin < LT(I) >\}$ pour l'algèbre quotient $A = k[x_1, \ldots, x_n]/I$ lorsqu'elle est de dimension finie :

```
kbase:=proc(PList,VList,torder)
local B,C,G,v,t,l,m;
if finite(PList,VList) then
```

```
G:=gbasis(PList,VList,torder);
B:=[1];
for v in VList do
m:=degree(finduni(v,G,VList),v);
C:=B;
for t in C do
for l to m-1 do
t:= t*v;
if NormalForm(t,G,VList,torder)=t then
B:=[op(B),t];
fi;
od;
od;
od;
RETURN(B)
else
ERROR('A n'est pas de dimension finie')
fi
end:
```

5.1 Montrer que cette procédure calcule $\{x^\alpha | x^\alpha \notin < LT(I) >\}$ si A est de dimension finie.
5.2 Appliquer cette procédure à l'algèbre A définie par l'idéal $I =< x^2 + 3xy/2 + y^2/2 - 3x/2 - 3y/2, xy^2 - x, y^3 - y >$.
5.3 Vérifier par un calcul direct le résultat de la question 4.2.

6. A 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 $\varphi_g \circ \varphi_f = \mathrm{id}_{k^n}$, i.e.

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

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

6.1 On suppose que la base rduite G de Gröbner de I est de la forme

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

Montrer que φ_f est inversible.
6.2 On suppose dans cette question que φ_f est inversible d'inverse φ_g.
6.2.1 Montrer que l'ensemble $G = \{x_1 - g_1, \dots, x_n - g_n\}$ est un sous-ensemble réduit de I.
6.2.2 Montrer que $I \cap k[y_1, \dots, y_n] = \{0\}$.
6.2.3 En déduire que G est une base de Gröbner réduite de I.
6.2.4 Montrer que $g_i(f_1, \dots, g_n) = x_i$, $1 \leq i \leq n$.
6.3 Soit $f_1, \dots, f_n, g_1, \dots, g_n \in k[x_1, \dots, x_n]$ tels que $g_i(f_1, \dots, f_n) = x_i$, $1 \leq i \leq n$.
6.3.1 Montrer que $f_i(g_1, \dots, g_n) = x_i$, $1 \leq i \leq n$.
6.3.2 En déduire que $\varphi_g \circ \varphi_g = \mathrm{id}_{k^n}$ implique $\varphi_f \circ \varphi_g = \mathrm{id}_{k^n}$.

4.1.7 Question de Rodolphe

1. Le polynôme $P \in k[x_1, \dots, x_n]$ de degré d s'écrit $P = P_1 + P_2$ avec P_1 polynôme homogène de degré d (non nul) et P_2 polynôme de degré $< d$. Ainsi

$$P(x_1 + a_1 x_n, \dots, x_{n-1} + a_{n-1} x_n, x_n) = P_1(a_1, \dots, a_{n-1}, 1) x_n^d + Q$$

où Q est un polynôme de degré $< d$ en x_n. Comme k est infini et $P_1 \neq 0$, il existe $(a_1, \dots, a_{n-1}) \in k^{n-1}$ tel que $P_1(a_1, \dots, a_{n-1}, 1) = c \neq 0$.

2. Par récurrence sur le nombre de variables n. Si $n = 1$, $< f_1, \dots, f_m >=< g >\subset k[x_1]$. Si g est une constante non nulle, alors $< f_1, \dots, f_m >= 1$. Sinon g admet un zéro dans k qui est commun à tous les f_i.
Supposons le résultat vrai pour $n - 1 > 0$. On peut supposer que $f_i \neq 0$, $1 \leq i \leq m$. D'après la question **1.**, on peut supposer que le polynôme f_1 est unitaire en x_n. Soit

$$g(y, x_1, \dots, x_n) = f_2 + y f_3 + \cdots + y^{m-2} f_m.$$

Alors

$$Res(f_1, g, x_n) = a_k(x_1, \dots, x_{n-1}) y^k + \cdots + a_0(x_1, \dots, x_{n-1}) \in k[y, x_1, \dots, x_{n-1}].$$

Par conséquent, il existe $A, B \in k[y, x_1, \dots, x_n]$ tels que $Res(f_1, g, x_n) = Af_1 + Bg$. En identifiant les coefficients des y^i, on obtient $a_i(x_1, \dots, x_{n-1}) \in< f_1, \dots, f_m >$, $0 \leq i \leq k$. Si les $a_0, \dots, a_k$ ont un zéro commun $b \in k^{n-1}$, alors $Res(f_1, g, x_n)(y, b) = 0$. Comme f_1 est unitaire en x_n, son coefficient dominant en x_n ne s'annule jamais et donc $f_1(b, x_n)$ et $g(y, b, x_n)$ ont une racine commune dans k. Comme $f_1(b, x_n)$ n'a qu'un nombre fini de racines, il en existe une a qui est racine de $g(y, b, x_n)$ pour une infinité de $y \in k$. Donc $g(y, b, a) = 0$ et $f_2(b, a) = \cdots = f_m(b, a) = 0$. Donc (b, a) est racine commune aux $f_1, \dots, f_m$ ce qui est absurde.
Ainsi $a_0, \dots, a_k$ n'ont pas de zéro commun dans k^{n-1}. Par hypothèse de récurrence, $1 \in< a_0, \dots, a_k >$. Or $a_i \in< f_1, \dots, f_m >$, donc $1 \in< f_1, \dots, f_m >$.

6 Dimension d'une variété affine

Fonction utile : **HilbertPolynomial**

1. Soit I l'idéal de $k[x, y]$:

$$I =< x^3y, xy^2 > .$$

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

2. Soit I l'idéal de $k[x, y, z]$:

$$I =< x^3yz^5, xy^3z^2 > .$$

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

3. Soit I l'idéal de $k[x_1, \dots x_4]$:

$$I =< x_1x_3, x_1x_4^2, x_2x_3, x_2x_4^3 > .$$

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

4. Soit $I_1 \subset I_2$ des idéaux de $k[x_1, \dots, x_n]$.
4.1 Montrer que $C(< \mathrm{LT}(I_2) >) \subset C(< \mathrm{LT}(I_1) >)$.
4.2 Montrer que pour tout $s \geq 0$, ${}^aHF_{I_2}(s) \leq^a HF_{I_1}(s)$.
4.3 Montrer que $\deg^a HP_{I_2} \leq \deg^a HP_{I_1}$.

5. Soit k un corps algébriquement clos. Calculer la dimension des variétés affines définies par les idéaux suivants :
5.1 $I =< xz, xy - 1 >$,
5.2 $J =< zw - y^2, xy - z^3 >$.

6. On se donne des entiers $a_1, \dots, a_n$ strictement positifs et on considère l'idéal monomial $J = (X_1^{a_1}, \dots, X_n^{a_n})$. On se propose de calculer la fonction de Hilbert $h =^a HF_J$. On prolonge la fonction de Hilbert à $\mathbf{Z}$ par la valeur zéro sur les entiers négatifs.

6.1 Montrer qu'il existe un entier d_0 tel qu'on ait $h(d_0) \neq 0$ et $h(d) = 0$ pour tout $d > d_0$. Calculer d_0 et $h(d_0)$.
6.2 Montrer que pour tout $d \in \mathbb{Z}$ on a $h(d) = h(d_0 - d)$.
6.3 Calculer h quand $a_i = 2$ pour tout $i \in [1, n]$.
6.4 Calculer h quand $n = 2$, $a_1 \leq a_2$.

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

8. Soit k un corps algébriquement clos et $I =< xy, wz >\in k[x, y, z]$.
8.1 Montrer que $I \cap k[x] = 0$ mais que $I \cap k[x, y]$ et $I \cap k[x, z]$ ne sont pas nuls.
8.2 Montrer que $I \cap k[y, z] = 0$ mais que $I \cap k[x, y, z] \neq 0$.
8.3 Quelle est la dimension de $V(I)$?

7 Caractéristique mixte

7.1 Bases de Gröbner sur les anneaux

1. Montrer que dans les anneaux suivants les équations linéaires sont résolubles :
$\mathbf{Z}$, $\mathbf{Z}_p$, $\mathbf{Q}[x_1, \dots, x_n]$ et $\mathbf{Z}[i]$.

2. Soit $R = \mathbf{Z}$, $f = xy - 1$ et $F = \{7x + 1, 11x^3 - 2y^2 + 1, 3y - 5\}$. Trouver un polynôme minimal pour F tel que $f \to^F r$.

3. Programmer un algorithme d'entrée et de sortie suivantes :
Input : $f, f_1, \dots, f_s \in A$ avec $f_i \neq 0, 1 \leq i \leq s$.
Output : $h_1, \dots, h_s, r$ avec $f = h_1 f_1 + \cdots + h_s f_s + r$ avec
$\mathrm{LP}(f) = \max(\max_{1 \leq i \leq s}(\mathrm{LP}(h_i)\,\mathrm{LP}(f_i)), \mathrm{LP}(r))$
et r est minimal pour F.

4. Si G est une base de Gröbner, $f \in < G >$ avec $f \to^G r$ et r minimal alors $r = 0$.

5. Soit $R = W_4(\mathbf{F}_4)$.
5.1 Écrire un isomorphisme de R dans $\mathbf{Z}/2^4\mathbf{Z}$.
5.2 Notons $a = (a_0, a_1, a_2, a_3), b = (b_0, b_1, b_2, b_3) \in R$. Écrire $S_0(a, b), S_1(a, b), S_2(a, b), S_3(a, b)$.
5.3 Écrire $P_0(a, b)$, $P_1(a, b)$, $P_2(a, b)$, $P_3(a, b)$.

6. Montrer que l'ensemble $F = \{3x^2y - x, 2z^2 - x\} \subset \mathbf{Z}[x, y, z]$ est une base de Gröbner pour l'ordre deglex $x > y > z$ mais n'est pas une base de Gröbner pour l'ordre lex où $x > y > z$.

7. Lemme de Hensel
Soit $f(x_1, \dots, x_n) \in \mathbf{Z}[x_1, \dots, x_n]$ et $\underline{a} \in \mathbf{Z}^n$ tels qu'il existe $m \geq 0$ avec

$$f(\underline{a}) \equiv 0 \mod p^{2m+1}$$

et il existe i avec

$$\frac{\partial f}{\partial X_i}(\underline{a}) \not\equiv 0 \mod p^{m+1}.$$

7.1 Montrer qu'il existe $\underline{a}_{2m+2} \in \mathbf{Z}^n$ tel que $\underline{a}_{2m+2} \equiv \underline{a} \mod p^{m+1}$ et $f(\underline{a}_{2m+2} \equiv 0 \mod p^{2m+2}$.

7.2 Montrer qu'il existe $\underline{a}_{2m+3} \in \mathbf{Z}^n$ tel que $\underline{a}_{2m+2} \equiv \underline{a}_{2m+3} \mod p^{m+2}$ et $f(\underline{a}_{2m+3} \equiv 0 \mod p^{2m+3}$.

7.3 En suivant ce procédé, construire une suite de Cauchy $(\underline{a}_{2m+k})_k$ de $\mathbf{Z}_p^n$.

7.4 En déduire qu'il existe $\underline{b} \in \mathbf{Z}_p^n$ tel que $f(\underline{b}) = 0$ et $\underline{b} \equiv \underline{a} \mod p^{m+1}$.

7.2 Attaque algébrique de NTRU à l'aide des vecteurs de Witt

Soit N un nombre premier, q une puissance de 2 et $p = 2 + X$ des paramètres publics. La clé secrète est formée par $F, g \in \mathbf{F}_2[X]$ deux polynômes de degré $N-1$. On pose $f = 1 + p * F$ où $*$ est la multiplication dans $\mathbf{Z}/q\mathbf{Z}(X]/(X^N - 1)$.
La clé publique est alors $h = p * f^{-1} * g$ où f^{-1} est l'inverse de f dans $\mathbf{Z}/q\mathbf{Z}[X]/(X^N - 1)$. Cet inverse existe en général. Les calculs d'inverse ou de multiplication $*$ se font en temps polynomial.
L'objet de ce problème est l'algébrisation de la recherche de la clé secrète F.
1. Posons

$$g = \sum_{i=0}^{N-1} g_i X^i \text{ où } g_i \in \mathbf{F}_2, F = \sum_{i=0}^{N-1} F_i X^i \text{ où } F_i \in \mathbf{F}_2, \quad h = \sum_{i=0}^{N-1} h_i X^i$$

où $h_i \in W_4(\mathbf{F}_2)$ connu s'écrit $h_i = [h_{i0}, h_{i1}, h_{i2}, h_{i3}]$. Les inconnues sont les g_i et les F_i.
1.1 Écrire $f = \sum_{i=0}^{N-1} f_i X^i \in W_4(\mathbf{F}_2)[X]$ en fonction des F_i.
1.2 Écrire $p * g$ en fonction des g_i.
1.3 Écrire $f * h$ en fonction des f_i, g_j.
2. On va écrire la somme de s termes de $W_4(\mathbf{F}_2)$.
2.1 Écrire $S_0(a_1, \ldots, a_s)$, $S_1(a_1, \ldots, a_s)$.
2.2 Écrire $S_2(a_1, \ldots, a_s)$.
2.3 Écrire $S_3(a_1, \ldots, a_s)$.

8 Caractéristique $p > 0$

8.1 Théorie des codes algébriques

1. Soit $\mathbf{F}_4 = \mathbf{F}_2[\alpha]/ < \alpha^2 + \alpha + 1 >$ et C le code linéaire de $\mathbf{F}_4^5$ défini par la matrice génératrice

$$G = \begin{pmatrix} \alpha & 0\alpha + 1 & 1 & 0 & \\ 1 & 1 & \alpha & 0 & 1 \end{pmatrix}.$$

Déterminer l'ensemble C.

2. Montrer que la distance de Hamming est une distance.

3. Soit C un code linéaire. Montrer que la distance minimum d de C est égale au minimum $\min_{x \in C - \{0\}} |\{i, x_i \not\emptyset\}|$. (Indication : $x - y \in C$ si $x, y \in C$).

4. Les codes de Hamming
Une famille de vecteurs $S \subset \mathbf{F}_q^m$ est dite maximale si chaque couple d'éléments distincts de S est linéairement indépendant et si S est maximale pour l'inclusion pour les ensemble ayant cette propriété. Si les colonnes d'une matrice de vérification d'un code linéaire C forme une famille maximale, le code est dit code de Hamming.
4.1 Quel est le cardinal d'une famille maximale dans $\mathbf{F}_q^m$?
4.2 Quelle est la dimension k d'un code définie par une matrice de vérification maximale ?
4.3 Ecrire une matrice de v{erification maximale pour $q = 3$ et $k = 2$.
4.4 Montrer que la distance minimale d'un code de Hamming est 3.

5. Comment déterminer sous Maple la matrice de vérification d'un code de matrice génératrice donnée G ?

6. Code cyclique de dimension 1.
Soient $r \in \mathbf{N}^*$ et $k = \mathbf{F}_q$ avec $q = 2^r$.

6.1 Quel est le code linéaire du codage défini par la matrice de $M_{4\times 2}(\mathbf{F}_2)$: $\begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 0 \end{pmatrix}$?

Montrer que C est cyclique. Trouver un générateur de C.

6.2 Montrer qu'il existe $\alpha \in k$ tel que $k = \mathbf{F}_2[\alpha]$.
Pour $k < q$, soient

$$L = \{\, P \in k[X] \mid \deg P \leq k-1 \,\}$$

$$C = \{\, (f(1), f(\alpha), \ldots, f(\alpha^{q-2})) \in k^{q-1} \mid f \in L \,\}.$$

Montrer que C est un code linéaire (dit de Reed-Salomon).

6.3 Montrer qu'un codage linéaire

$$E : k^k \longrightarrow R = k[X]/ < X^{q-1} - 1 >$$

est cyclique si et seulement si les polynômes de $C = E(k^k) \subseteq \{\, f \in k[X] \mid \deg f < q-2\}$ ont un ensemble commun de $q-k-1$ zéros.

6.4 En déduire que le code de Reed-Salomon est cyclique.

Idée pour l'examen
7.p.368 Introduction to Maple
3 et 4 gb-td1.pdf
report.pdf à partir de la page 27
1. Soit $f, g \in \mathbf{C}[x, y]$. Montrer que $V(f, g)$ est infini si et seulement si f et g ont un facteur commun non constant.

Université de Versailles – St Quentin **2010–2011**
MA^2 — Master Algèbre Appliquée 11/10/2010
M2 Algèbre formelle 2 heures

Partiel

Tous documents et appareils électroniques interdits, sauf :
polycopié du cours, ordinateur sous Maple.

1. Soit

$$f_1 = y^5 - x^{15}y^2,\ f_2 = x^{40} \text{ et } f = x^2y^4 + 3y.$$

Montrer que $f \in \sqrt{< f_1, f_2 >}$. Déterminer le plus petit $e > 0$ tel que $f^e \in < f_1, f_2 >$.

2. En utilisant uniquement la fonction gbasis de Maple, déterminer l'ensemble des solutions dans $\mathbf{Q}^3$ du système

$$\begin{cases} x^2 + yz + x = 0 \\ z^2 + xy + z = 0 \\ y^2 + zx + y = 0. \end{cases}$$

Problème. On considère le système (*)

$$\begin{cases} a_{11}\sigma_1 + a_{12}\sigma_2 + \cdots + a_{1m}\sigma_m = b_1 \\ a_{21}\sigma_1 + a_{22}\sigma_2 + \cdots + a_{2m}\sigma_m = b_2 \\ \cdots \\ a_{n1}\sigma_1 + a_{n2}\sigma_2 + \cdots + a_{nm}\sigma_m = b_n \end{cases}$$

où $a_{ij} \in \mathbf{Z}, b_i \in \mathbf{Z}$, $1 \leq i \leq n, 1 \leq j \leq m$. On cherche une solution $(\sigma_1, \ldots, \sigma_m) \in \mathbf{N}^m$ qui minimise la fonction coût

$$c(\sigma_1, \ldots, \sigma_m) = \sum_{j=1}^{m} c_j\sigma_j,$$

où $c_j \in \mathbf{R}$, $1 \leq i \leq m$.

1. On suppose dans cette question que les a_{ij} et b_j sont positifs. On considère l'application polynômiale ϕ définie par

$$\phi : k[y_1, \ldots, y_m] \to k[x_1, \ldots, x_n],\ \phi(y_j) = x_1^{a_{1j}} x_2^{a_{2j}} \cdots x_n^{a_{nj}},\ 1 \leq j \leq m.$$

1.1 Montrer que le système (*) admet une solution $(\sigma_1, \dots, \sigma_m) \in \mathbf{N}^m$ si et seulement si $x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}$ est l'image par ϕ d'un produit de puissances $y_1^{\sigma_1} y_2^{\sigma_2} \cdots y_m^{\sigma_m} \in k[y_1, \dots, y_m]$.
1.2 Si $x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n} = \phi(y_1^{\sigma_1} y_2^{\sigma_2} \cdots y_m^{\sigma_m})$, montrer que $(\sigma_1, \dots, \sigma_m)$ est solution de (*).
1.3 Si $x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}$ est l'image par ϕ d'un élément de $k[y_1, \dots, y_m]$, montrer que c'est l'image d'un monôme $y_1^{\sigma_1} y_2^{\sigma_2} \cdots y_m^{\sigma_m}$.
1.4 En déduire un algorithme pour déterminer si le système (*) a une solution.
1.5 Appliquer l'algorithme de la question 1.4 au système suivant :

$$\begin{cases} 3\sigma_1 + 2\sigma_2 + \sigma_3 + \sigma_4 = 10 \\ 4\sigma_1 + \sigma_2 + \sigma_3 = 5 \end{cases}$$

2. On revient à présent au cas $a_{ij} \in \mathbf{Z}$ et $b_j \in \mathbf{Z}$. L'idée est d'ajouter une variable w et de travailler dans l'anneau $k[x_1, \dots, x_n, w]/I$ où $I =< x_1 x_2 \cdots x_n w - 1 >$ en modifiant le système d'équations pour se ramener à la situation de la question **1.**.
2.1 Montrer que l'on peut choisir $a'_{ij}, \alpha_j \in \mathbf{N}$ de telle façon que pour tout $1 \leq j \leq m$,

$$(a_{1j}, a_{2j}, \dots, a_{nj}) = (a'_{1j}, a'_{2j}, \dots, a'_{nj}) + \alpha_j(-1, \dots, -1)$$

et on peut choisir $b'_1, \dots, b'_n, \beta \in \mathbf{N}$ tels que

$$(b_1, b_2, \dots, b_n) = (b'_1, b'_2, \dots, b'_n) + \beta(-1, -1, \dots, -1).$$

2.2 On considère l'homomorphisme d'algèbre

$$\phi : k[y_1, \dots, y_m] \to k[x_1, \dots, x_n, w]/I, \quad y_j \mapsto x_1^{a'_{1j}} x_2^{a'_{2j}} \cdots x_n^{a'_{nj}} w^{\alpha_j} + I$$

Montrer qu'il existe une solution $(\sigma_1, \dots, \sigma_m) \in \mathbf{N}^m$ du système (*) si et seulement si $x_1^{b'_1} \cdots x_n^{b'_n} w^\beta + I$ est dans l'image sous ϕ d'un produit de puissances de $k[y_1, \dots y_m]$.
2.3 Si $x_1^{b'_1} \cdots x_n^{b'_n} w^\beta + I$ est dans l'image de ϕ, montrer qu'il est l'image d'un produit de puissances $y_1^{\sigma_1} \cdots y_m^{\sigma_m} \in k[y_1, \dots, y_m]$.
2.4 Résoudre dans $\mathbf{N}^4$ le système (**)

$$\begin{cases} 3\sigma_1 - 2\sigma_2 + \sigma_3 - \sigma_4 = -1 \\ 4\sigma_1 + \sigma_2 - \sigma_3 = 5 \end{cases}$$

3. Un ordre $<_c$ sur les variables $y_1, \dots, y_m$ est dit compatible avec la fonction coût si

$$\left.\begin{array}{c} \phi(y_1^{\sigma_1} y_2^{\sigma_2} \cdots y_m^{\sigma_m}) = \phi(y_1^{\sigma'_1} y_2^{\sigma_2} \cdots y_m^{\sigma'_m}) \\ \text{et} \\ c(\sigma_1, \dots, \sigma_m) < c(\sigma'_1, \dots, \sigma'_m) \end{array}\right\} \Longrightarrow y_1^{\sigma_1} y_2^{\sigma_2} \cdots y_m^{\sigma_m} <_c y_1^{\sigma'_1} y_2^{\sigma'_2} \cdots y_m^{\sigma'_m}.$$

3.1 Soit G une base de Gröbner pour

$$K =< x_1 x_2 \cdots x_n w - 1, y_j - x_1^{a'_{1j}} x_2^{a'_{2j}} \cdots x_n^{a'_{nj}} w^{\alpha_j}, 1 \leq j \leq m >$$

pour un ordre compatible avec la fonction coût et tel que $x > w > y$. Si $\overline{x_1^{b'_1} \cdots x_n^{b'_n} w^{\beta}}^G = y_1^{\sigma_1} \cdots y_m^{\sigma_n}$, montrer que $(\sigma_1, \dots, \sigma_m)$ est une solution de (*) qui minimise le coût.
3.2 On considère le système (**) avec la fonction coût

$$c(\sigma_1, \dots, \sigma_4) = 1000\sigma_1 + \sigma_2 + \sigma_3 + 100\sigma_4$$

Trouver un ordre compatible avec la fonction coût et tel que $x > w > y$. En déduire une solution de (**) qui minimise le coût.

Université de Versailles – St Quentin **2010–2011**
MA^2 — Master Algèbre Appliquée **.**
M2 Algèbre formelle **.**

Devoir pour le 4 novembre

2. Soient $p \leq n$ deux entiers positifs, et $X = (x_{ij})_{1\leq i\leq p, 1\leq j\leq n}$ une $(p * n)$-matrice à coefficients des indéterminéees. Si k est un corps, on considère l'idéal I_{pn} de $k[x_{11}, ..., x_{pn}]$ engendré par les $(p * p)$-mineurs de la matrice X.
2.1. On considère le cas particulier $p = 2, n = 3$, et on note $I = I_{23}$. On choisit pour ordonner les monômes de $R = k[x_{11}, x_{12}, x_{13}, x_{21}, x_{22}, x_{23}]$ l'ordre lexicographique induit par $x_{11} < x_{22} < x_{12} < x_{23} < x_{13} < x_{21}$ le monôme dominant étant le plus petit. Calculer une base standard de I.
2.2. Soit K un idéal homogène dun anneau de polynômes A. On appelle paramètre un élément a de A tel que $\dim A/(K + a) = \dim A/K1$. Montrer qu'un élément non diviseur de zéro de A/K est un paramètre.
Montrer que x_{21} est un paramètre non diviseur de zéro dans R/I, et x_{13} un paramètre non diviseur de zéro dans $R/(I + x_{21})$. Comparer les dimensions et les degrés des ensembles algébriques projectifs définis par I, $I + (x_{21})$ et $J = I + (x_{21}, x_{13})$ dans $\mathbf{P}^5_k$. Est que x_{23} est un paramètre pour R/J ?
2.3. On considère le changement de variables $x_{22} \leftarrow x_{22} + x_{11}$, $x_{23} \leftarrow x_{23} + x_{12}$. Calculer une base standard de J, toujours pour le même ordre. Montrer que x_{23} est un paramètre non diviseur de zéro dans R/J, et x_{22} un paramètre non diviseur de zéro dans $R/(J+x_{23})$. Donner la dimension et le degré de $I_{23} = I$.
2.4 Calculer directement sur la base standard de I la fonction de Hilbert et sa régularité. Vérifier la dimension et le degré du sous-ensemble algébrique défini dans $\mathbf{P}^5_k$ par I_{23}.
2.5* Généraliser à p et n quelconques.

Université de Versailles – St Quentin **2011–2012**
MA^2 — Master Algèbre Appliquée 25/11/2011
M2 Algèbre formelle 3 heures

Examen

Tous documents et appareils électroniques interdits, sauf :
polycopié du cours, ordinateur sous Sage.

1. Soit I l'idéal de $k[x, y, z]$:

$$I =< x^4y^2z^3, xy^3z^2 > .$$

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

2. On considère la surface S paramétrée par

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

ainsi que la courbe C tracée sur S et paramétrée par

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

2.1 Obtenir une équation implicite de S.
2.2 Obtenir des équations implicites de C.
2.3 Vérifier à l'aide de ces équations que $C \subset S$.

3. Soit k un corps fini q éléments. Soit $n_1, \dots, n_m \in \mathbf{N}$ et R un k-espace vectoriel de dimension $n_1 \cdots n_m$.
3.1 Montrer que

$$R \simeq k[X_1, ..., X_m]/ < X^{n_1} - 1, \dots, X^{n_m} - 1 > .$$

On appelle code cyclique en dimension m tout idéal I de R. Pour $f \in k[X_1, \dots, X_n]$, notons $[f]$ sa classe dans R. À l'idéal $I =< [f_1], \dots, [f_s] >$ de R on associe l'idéal $J =< f_1, \dots, f_s, X^{n_1} - 1, \dots, X^{n_m} - 1 >$ de $k[X_1, \dots, X_m]$. On fixe sur $k[X_1, \dots, X_m]$ un ordre admissible quelconque. Soit $G = \{g_1, ..., g_t\}$ une base de Gröbner de J.
3.2 Caractériser $\dim_k k[X_1, \dots, X_n]/J$ en fonction de $< LT(J) >$.
3.3 Caractériser $\dim_k I$ en fonction de $< LT(J) >$.

4. A 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 $\varphi_g \circ \varphi_f = \mathrm{id}_{k^n}$, i.e.

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

Soit $I =< y_1 - f_1, \dots, y_n - f_n >\subset k[x_1, \dots, x_n, y_1, \dots, y_n]$ muni de l'ordre lexicographique.
4.1 On suppose que la base rduite G de Gröbner de I est de la forme

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

Montrer que φ_f est inversible.
4.2 On suppose dans cette question que φ_f est inversible d'inverse φ_g.
4.2.1 Montrer que l'ensemble $G = \{x_1 - g_1, \dots, x_n - g_n\}$ est un sous-ensemble réduit de I.
4.2.2 Montrer que $I \cap k[y_1, \dots, y_n] = \{0\}$.
4.2.3 En déduire que G est une base de Gröbner réduite de I.
4.2.4 Montrer que $g_i(f_1, \dots, g_n) = x_i$, $1 \leq i \leq n$.
4.3 Soit $f_1, \dots, f_n, g_1, \dots, g_n \in k[x_1, \dots, x_n]$ tels que $g_i(f_1, \dots, f_n) = x_i$, $1 \leq i \leq n$.
4.3.1 Montrer que $f_i(g_1, \dots, g_n) = x_i$, $1 \leq i \leq n$.
4.3.2 En déduire que $\varphi_g \circ \varphi_g = \mathrm{id}_{k^n}$ implique $\varphi_f \circ \varphi_g = \mathrm{id}_{k^n}$.

Université de Versailles – St Quentin **2010–2011**
MA^2 — Master Algèbre Appliquée 6/12/2010
M2 Algèbre formelle 3 heures

Examen

Tous documents et appareils électroniques interdits, sauf :
polycopié du cours, ordinateur sous Maple.

1. Soit k un corps de caractéristique $p > 0$ et I un idéal de l'anneau $R = k[x_1, \dots, x_n]$ muni d'un ordre admissible. On note $I^{[p]}$ l'idéal engendré par les puissances p-ième de tous les éléments de I. On suppose que $\{f_1, \dots, f_m\}$ est une base de Gröbner de I. Déterminer une base de Gröbner de $I^{[p]}$.

2. Soit k un corps algébriquement clos. Soit A une k-algèbre. Une décomposition de Stanley de A est une représentation sous la forme d'une somme directe de k-espaces vectoriels :

$$A = \oplus_{\alpha \in F} \mathbf{x}^\alpha k[\mathbf{X}_\alpha]$$

où F est un sous-ensemble fini de $\mathbf{N}^n$, $\alpha = (\alpha_1, \dots, \alpha_n)$, $\mathbf{X}_\alpha$ est un sous-ensemble de $\{x_1, \dots, x_n\}$ et $\mathbf{x}^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$.

2.1 Soit $A = k[x, y, z]/(xy, yz, xz)$. Montrer que $k[y] \oplus xk[x] \oplus zk[z]$ est une décomposition de Stanley de A.

2.2 Soit $A = k[x_1, \dots, x_n]/I$ une k-algèbre admettant la décomposition de Stanley $A = \oplus_{\alpha \in F} \mathbf{x}^\alpha k[\mathbf{X}_\alpha]$. Pour $\alpha \in F$, on note $|\alpha| = \sum_{i=1}^n \alpha_i$. Enfin $d = \max_{\alpha \in F} |\mathbf{X}_\alpha|$ où $|\mathbf{X}_\alpha|$ est le cardinal de $\mathbf{X}_\alpha$.

2.2.1 Calculer la série de Hilbert de $V(I)$.

2.2.2 Quelle est la dimension de $V(I)$?

2.3 On suppose que $A = k[x_1, \dots, x_n]/I$ avec I idéal monomial. L'objet de cette question est de montrer que A admet une décomposition de Stanley.

2.3.1 Si $n = 1$, montrer que A admet une décomposition de Stanley.

2.3.2 Si $n \geq 2$, montrer que I est engendré par une famille finie d'éléments de la forme $\{m_1 x_n^{d_1}, \dots, m_l x_n^{d_l}\}$ avec $m_1, \dots, m_l \in k[x_1, \dots, x_{n-1}]$ et $0 \leq d_1 \leq d_2 \leq \cdots \leq d_l$.

2.3.3 En déduire que A admet une décomposition de Stanley.

3. Soit l'idéal $I =< (u-1)x + y^2, uy + u >\in k[x, y, u]$ muni de l'ordre lexicographique $x > y > u$.
3.1 Montrer que $G = \{ux - x + y^2, uy + u, xy + x - y^3 - y^2\}$ est une base de Gröbner de I.
3.2 Soit $V = V(I)$. Quelle est la projection de V par $\pi_2 : \mathbf{C}^3 \to \mathbf{C}, (x, y, u) \mapsto u$?
3.3 On évalue G en $u = 1$, la famille $G_1 = \{y^2, y + 1, xy + x - y^3 - y^2\}$ obtenue est-elle une base de Gröbner dans $k[x, y]$?
3.4 Si on évalue G en $u = b \neq 0, 1$, la famille G_b est-elle une base de Gröbner dans $k[x, y]$?

4. Montrer que le système

$$\begin{cases} t^2 + x^2 + y^2 + z^2 = 0 \\ t^2 + 2x^2 - xy - z^2 = 0 \\ t + y^3 - z^3 = 0 \end{cases}$$

à une infinité de solutions dans $\mathbf{C}^4$.

5. Soit I un idéal de dimension 0 de $\mathbf{C}[x_1, \dots, x_n]$, i.e. tel que $A = \mathbf{C}[x_1, \dots, x_n]/I$ est un $\mathbf{C}$-espace vectoriel de dimension finie.
5.1 Montrer que $V(I)$ est un ensemble fini de $\mathbf{C}^n$. On note $V(I) = \{p_1, \dots, p_m\}$.
5.2 Montrer que l'application

$$\varphi : A \to \mathbf{C}^m, [f] \mapsto (f(p_1), \dots, f(p_m))$$

est une application linéaire bien définie.
5.3 Montrer que $\dim_{\mathbf{C}} A \geq m$.
5.4 Si I est radiciel ($I = \sqrt{I}$) montrer que $\dim_{\mathbf{C}} A = m$.
5.5 Si $\dim_{\mathbf{C}} A = m$, montrer que I est radiciel.

A. Les polynômes orthogonaux de Tchebychev sont définis comme les uniques polynômes réalisant l'égalité

$$T_n(\cos\theta) = \cos n\theta$$

pour tout entier naturel $n \in \mathbf{N}$. Ainsi, $T_0(x) = 1, T_1(x) = x, T_2(x) = 2x^2 - 1$, etc... Il sagit dans cet exercice d'étudier les relations fonctionnelles linéaires vérifiées par les $T_n(x)$. On introduit donc le corps des fractions rationnelles $\mathbf{Q}(n, x)$ muni de son décalage avant en n, noté σ, et de sa dérivation usuelle par rapport à x, notée δ. L'algèbre de Ore $\mathbf{Q}(n, x)[S, D; \sigma, id, 0, \delta]$ sera notée A. Dans cette algèbre,

$$S_n = (n+1)S \text{ et } Dx = xD + 1$$

On note I l'idéal annulateur de l'application T qui a (n, x) associe $T_n(x)$:

$$I = \{L \in A : L \cdot T = 0\}.$$

On rappelle les formules de trigonométrie

$$\cos(x)^2 + \sin(x)^2 = 1 \text{ et } \cos(a+b) = \cos a \cos b - \sin a \sin b.$$

1. (a) Calculer $\cos(n+1)x$ et en déduire $P_1 = (1-x^2)D + nS - nx \in I$.
(b) Calculer $\cos(n+1)x + \cos(n-1)x$ et en déduire $P_2 = S^2 - 2xS + 1 \in I$.
2. Soit $>$ l'ordre monomial lexicographique de A pour lequel $D > S$.
(a) Écrire par ordre croissant les 6 monômes en S et D de degré au plus 2.
(b) Calculer les restes des divisions de $S^2, S^3, DetSD$ par $\{P_1, P_2\}$.
3. (a) Que vaut le S-polynôme de P_1 et P_2 ?
(b) Montrer que $\{P_1, P_2\}$ est une base de Gröbner pour l'ordre introduit précédemment.
On admet qu'il n'existe aucune fraction rationnelle $R(n, x)$ telle que pour tout $n \in N$,

$$\frac{\cos(n+1)\theta}{\cos n\theta} = R(n, \cos\theta).$$

4. Montrer que I est l'idéal à gauche engendré par P_1 et P_2.
On rappelle que si R est le reste de la division de $U \in A$ par la base de Gröbner $\{P_1, P_2\}$ et si $V \in A$, alors VU et VR ont même reste par division par cette même base de Gröbner.
5. On désire maintenant calculer un polynôme annulateur de T purement différentiel.

(a) Quelle est la dimension sur $\mathbf{Q}(n, x)$ de l'espace vectoriel quotient A/I ?
(b) En déduire l'existence dun polynôme $D^2 + a(n, x)D + b(n, x)$ qui annule T.
Les fractions rationnelles a et b de la question précédente ont des dénominateurs qui rendent pénible un calcul direct à la main. Les questions qui suivent proposent un autre calcul plus facile.
6. (a) Calculer les restes des divisions de 1 et $(1-x^2)D$ par $\{P_1, P_2\}$. En déduire les reste des divisions de $(1-x^2)SD$ et $(1-x^2)D(1-x^2)D$ par $\{P_1, P_2\}$.
(b) En déduire que $P_3 = (1x^2)D^2xD + n^2$ est dans I.
7. (a) Considérer le S-polynôme de P_1 et P_3 pour montrer sans aucun calcul que $\{P_1, P_3\}$ est une base de Gröbner pour l'ordre lexicographique pour lequel S est plus grand que D.
(b) Montrer que $\{P_1, P_2\}$ et $\{P_1, P_3\}$ engendrent le même idéal. Conclure.

Université de Versailles – St Quentin **2010–2011**
MA^2 — Master Algèbre Appliquée 21/3/2011
M2 Algèbre formelle 3 heures

Examen session 2

Tous documents et appareils électroniques interdits, sauf :
polycopié du cours, ordinateur sous Maple.

1. Soit le polynôme
$$P = x^7 + x^5 + 2x^3 + 2x^2 + 3x + 2.$$

1.1 Prouver l'irréductibilité de P dans $\mathbf{Z}[x]$.
1.2 Vérifier l'irréductibilité de P avec Maple.
1.3 Factoriser P dans $\mathbf{F}_{16}[x]$.

2. Soit $I \subset k[x_1, \dots, x_n]$ un idéal et G une base de Gröbner de I.
2.1 Montrer que $\overline{f}^G = \overline{g}^G$ si et seulement si $f - g \in I$.
2.2 Montrer que $\overline{f+g}^G = \overline{f}^G + \overline{g}^G$.
2.3 Montrer que $\overline{fg}^G = \overline{\overline{f}^G \overline{g}^G}^G$.

3. 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.
3.1 On pose : $LT(f) = \lambda m m'$, $LT(g) = \mu m m''$, oú m est un monôme, m' et m'' sont deux monômes premiers entre eux, λ et μ sont deux scalaires. En utilisant la division du S-polynôme $S(f, g)$ par la suite f, g, montrer qu'il existe un polynôme g_1 dont $LT(g_1)$ n'est pas divisible par $LT(f)$ et tel que f divise $g_1 + \lambda m'$.
3.2 En déduire que $m = 1$.
3.3 En déduire que (f, g) est une base de Gröbner de I si et seulement si $LT(f)$ et $LT(g)$ sont premiers entre eux.
3.4 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'.
3.5 Donner une condition nécessaire et suffisante pour que (f, g) soit une base de Gröbner

de I.

Soit K un corps infini, $P \in K[X_1, \dots, X_n]$ un polynôme non nul de degré d.
4.1 Montrer qu'il existe $(a_1, \dots, a_{n-1})$ 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.
4.2 En utilisant un résultant en déduire le théorème des zéros de Hilbert.

5. Soit k un corps fini q éléments. Soit $n_1, \dots, n_m \in \mathbf{N}$ et R un k-espace vectoriel de dimension $n_1 \cdots n_m$.
5.1 Montrer que

$$R \simeq k[X_1, ..., X_m]/ < X^{n_1} - 1, \dots, X^{n_m} - 1 > .$$

On appelle code cyclique en dimension m tout idéal I de R. Pour $f \in k[X_1, \dots, X_n]$, notons $[f]$ sa classe dans R. À l'idéal $I =< [f_1], \dots, [f_s] >$ de R on associe l'idéal $J =< f_1, \dots, f_s, X^{n_1} - 1, \dots, X^{n_m} - 1 >$ de $k[X_1, \dots, X_m]$. On fixe sur $k[X_1, \dots, X_m]$ un ordre admissible quelconque. Soit $G = \{g_1, ..., g_t\}$ une base de Gröbner de J.
5.2 Caractériser $\dim_k k[X_1, \dots, X_n]/J$ en fonction de $< LT(J) >$.
5.3 Caractériser $\dim_k I$ en fonction de $< LT(J) >$.

6. Soit I l'idéal de $k[x, y, z]$:

$$I =< x^4y^2z^3, xy^3z^2 > .$$

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