université de BORDEAUX	**ANNEE UNIVERSITAIRE 2017/2018** **Examen première session** **Master 1** **Code UE : MSIN820, MSMA820** **Epreuve : Algèbre et calcul formel** **Date : 25/04/2018** **Heure : 8h00** **Durée : 3h** Documents autorisés : Feuilles d'exercices (énoncés). Epreuve de M. Jehanne – Corrigé	**Collège Sciences et technologies**

À la fin de l'épreuve, votre fichier "`votre_nom_Examen.sage`" est à envoyer à l'adresse : `arnaud.jehanne@u-bordeaux.fr`

Il est demandé de rédiger soigeusement et lisiblement. Tous les résultats doivent être justifiés.

Exercice 1 [Bases de Gröbner et systèmes polynomiaux]

Dans cet exercice, aucune programmation n'est demandée mais on pourra utiliser sage pour certains calculs. Dans ce cas, il vous est demandé d'écrire les commandes utilisées et les résultats obtenus sur votre fichier sage ou sws, ou sur votre copie.

Soient dans $\mathbb{Q}[X,Y]$ *les polynômes*

$$f_1 = 4X^2 + Y^2 - 16 \quad et \quad f_2 = XY + 2X - Y - 4$$

1. *Soit* I *l'idéal de* $\mathbb{Q}[X,Y]$ *engendré par* f_1 *et* f_2*. En utilisant la base de Gröbner réduite associée à un ordre monomial bien choisi, donner un générateur* g *de l'idéal* $I \cap \mathbb{Q}[Y]$*.*

On uitlise les commandes suivantes.

```
Qxy.<x,y>=PolynomialRing(QQ,order='lex')
f1=4*x^2+y^2-16
f2=x*y+2*x-y-4
I=Qxy.ideal([f1,f2])
G=I.groebner_basis()
```

Alors la base de Gröbner G a deux éléments $g_0 = x + 1/8y^3 + 1/4y^2 - 3/2y - 2$ et $g_1 = y^4 + 4y^3 - 8y^2 - 32y$. Comme l'ordre $\prec$ choisi est l'ordre lexicographique tel que $x \succ y$, on sait que $G \cap \mathbb{Q}[y]$ est une base de Gröbner de l'idéal $I \cap \mathbb{Q}[y]$ de $\mathbb{Q}[y]$. On en déduit que $I \cap \mathbb{Q}[y] = g_1\mathbb{Q}[y]$.

2. *En utilisant la base de Gröbner de la question précédente, calculer l'ensemble des solutions dans* $\mathbb{C}^2$ *du système d'équations* $f_1(x,y) = f_2(x,y) = 0$. Grâce à la commande `factor`, on voit que $g_1 = y(y+4)(y^2-8)$. Ainsi, si $P = (x,y)$ est solution du système, $y \in \{0, -4, 2\sqrt{2}, -2\sqrt{2}\}$. Pour chacune de ces valeurs, on trouve la valeur de x correspondante grâce à g_0. L'ensemble des solution est

$$\mathcal{S} = \{(2,0), (0,-4), (\sqrt{2}, 2\sqrt{2}), (-\sqrt{2}, -2\sqrt{2})\}.$$

3. *Donner une base du* $\mathbb{Q}$*-espace vectoriel* $\mathbb{Q}[X,Y]/I$. Les monômes standards pour G sont $1, Y, Y^2, Y^3$. Les classes de ces quatres éléments dans $\mathbb{Q}[X,Y]/I$ en constituent donc une base.

Exercice 2 [Racines de polynômes dans $\mathbb{Z}/p^n\mathbb{Z}$]

Soit p *un nombre premier.*

1. a) *Soit* P *un polynôme de* $\mathbb{F}_p[x]$*. Rappeler sans démonstration quel calcul de pgcd permet d'obtenir le produit des facteurs unitaires de degré* 1 *de* P*. Nous avons vu comment on peut alors factoriser le polynôme obtenu, ce qui permet de calculer toutes les racines de* P *dans* $\mathbb{F}_p$*. Nous ne le ferons pas ici.*

Il suffit de calculer $\text{pgcd}(P, x^p - x)$.

b) *Donner le résultat de ce pgcd dans le cas où $P = x^{10} - x + 1$ et $p = 11$ (on fera le calcul sur sage et on notera le résultat sur papier). En déduire que l'unique racine de ce polynôme P dans $\mathbb{F}_{11}$ est 2.*

Ici, ce calcul donne $x + 9$. Ce polynôme de $\mathbb{F}_{11}$ a pour racine 2.

Dans la suite de l'exercice, on considère un polynôme P de $\mathbb{Z}[x]$, et on s'intéresse aux racines de P dans $\mathbb{Z}/p^n\mathbb{Z}$, où n désigne un entier naturel non nul.

2. *Soit r un élément de $\mathbb{Z}$ tel que $P(r) \equiv 0 \mod p^n$. Que vaut $P(r) \mod p$?*

Comme p divise p^r et comme p^r divise $P(r)$, p divise $P(r)$ donc $P(r) \equiv 0 \mod p$.

Étudions maintenant la réciproque. Soit r un entier tel que $P(r) \equiv 0 \mod p$. Dans les questions suivantes, on suppose pour simplifier que $\text{pgcd}\,(P'(r), p) = 1$ et on cherche à calculer un entier r' tel que $r' \equiv r \mod p$ et $P(r') \equiv 0 \mod p^n$.

3. *Soient x, t, k, i dans $\mathbb{Z}$ tels que $k > 0$ et $i \geq 0$. Montrer que $(x + tp^k)^i \equiv x^i + itp^k x^{i-1} \mod p^{2k}$. En déduire que*

$$P(x + tp^k) \equiv P(x) + tp^k P'(x) \mod p^{2k}.$$

On utilise la formule du binôme.

$$\begin{aligned}(x + tp^k)^i &= \sum_{j=0}^{i} \binom{i}{j} x^{i-j} t^j p^{jk} \\ &\equiv x^i + itp^k x^{i-1} \mod p^{2k}\end{aligned}$$

puisque $p^{jk} \equiv 0 \mod p^{2k}$ dès que $j \geq 2$. On note $P = \sum_{i=0}^{m} a_i x^i$. Alors

$$\begin{aligned}P(x + tp^k) &= \sum_{i=0}^{m} a_i (x + tp^k)^i \\ &\equiv a_0 + \sum_{i=1}^{m} a_i (x^i + itp^k x^{i-1}) \mod p^{2k} \\ &\equiv + \sum_{i=0}^{m} a_i x^i + tp^k \sum_{i=1}^{m} a_i i x^{i-1} \mod p^{2k} \\ &\equiv P(x) + tp^k P'(x) \mod p^{2k}.\end{aligned}$$

4. *On suppose avoir trouvé un entier r_k qui vérifie $r_k \equiv r \mod p$ et $P(r_k) \equiv 0 \mod p^k$ (donc p^k divise $P(r_k)$). Justifier pourquoi la classe de $P'(r_k)$ dans $\mathbb{Z}/p^k\mathbb{Z}$ est inversible. En déduire qu'il existe un entier t_k unique modulo p^k, tel que*

$$\frac{P(r_k)}{p^k} + t_k P'(r_k) \equiv 0 \mod p^k.$$

Comme $P'(r_k) \equiv P'(r) \mod p$, cet entier est premier à p, il est donc aussi premier à p^k, ce qui signifie que sa classe dans $\mathbb{Z}/p^k\mathbb{Z}$ est inversible. Soit alors a un entier tel que $aP'(r_k) \equiv 1 \mod p^k$. $\frac{P(r_k)}{p^k} + t_k P'(r_k) \equiv 0 \mod p^k$. si et seulement si

$$t_k \equiv -a\frac{P(r_k)}{p^k} \mod p^k.$$

Cela prouve le résultat.

5. *Soit alors $r_{2k} = r_k + t_k p^k$. Montrer que $r_{2k} \equiv r \mod p$ et $P(r_{2k}) \equiv 0 \mod p^{2k}$. Ainsi, à partir de $r_1 = r$, on calcule r_2, puis r_4, r_8, ... On peut s'arrêter dès que l'on a calculé r_{2^i} où $2^i \geq n$.*

Comme $r_{2k} = r_k + t_k p^k$, et comme $k > 0$, $r_{2k} \equiv r_k \mod p$. Comme $r_k \equiv r \mod p$, on obtient aussi : $r_{2k} \equiv r \mod p$.

$$\begin{aligned} P(r_{2k}) &= P(r_k + t_k p^k) \\ &\equiv P(r_k) + t_k p^k P'(r_k) \mod p^{2k} \\ &\equiv p^k \left(\frac{P(r_k)}{p^k} + t_k P'(r_k) \right) \mod p^{2k} \\ &\equiv 0 \mod p^{2k} \end{aligned}$$

car p^k divise $\dfrac{P(r_k)}{p^k} + t_k P'(r_k)$ d'après la question 4.

6. *En utilisant l'algorithme que suggèrent les questions précédentes, écrire sur machine une fonction* `Relevement` *qui en entrée prend un nombre premier p, un entier naturel non nul n, un polynôme P de $\mathbb{Z}[x]$ et un entier r tel que $P(r) \equiv 0 \mod 0$ et $P'(r) \not\equiv 0 \mod p$, et qui en sortie rend un entier s congru à r modulo p tel que $P(s) \equiv 0 \mod p^n$. On s'efforcera d'optimiser la complexité de cette fonction.*

7. *En utilisant cette fonction, calculer l'unique racine de $x^{10} - x + 1$ modulo 11^7.*

On trouve 2924528.

Exercice 3 [Radical d'un idéal dans un anneau de polynômes]

Soit K un corps. On note $K[X] = K[X_1, \ldots, X_n]$ et $X = (X_1, \ldots, X_n)$. Soit I un idéal de $K[X]$, on appelle radical de I l'ensemble

$$\sqrt{I} = \{f \in K[X] \ : \ \exists m \in \mathbb{N} \setminus \{0\} \text{ vérifiant } f^m \in I\}.$$

On rappelle que $\mathcal{I}$ est un idéal de $K[X]$ si $\mathcal{I}$ est un sous-groupe de $K[X]$ et si pour tout $f \in K[X]$ et tout $j \in \mathcal{I}$, $jf \in \mathcal{I}$.

1. *Montrer que $\sqrt{I}$ est un idéal de $K[X]$ contenant I.*

Soit $f \in I$, alors $f = f^1 \in \sqrt{I}$, donc $I \subset \sqrt{I}$. En particulier, $\sqrt{I} \neq \emptyset$. Soient f et g deux éléments de $\sqrt{I}$. Il existe donc des entiers positifs m et m' tels que $f^m \in I$ et $g^{m'} \in I$. Soit $\lambda \in K$. Pour montrer que $f - g \in \sqrt{I}$, on utilise la formule du binôme

$$(f-g)^{m+m'} = \sum_{k=0}^{m+m'} (-1)^k \binom{m+m'}{k} f^{m+m'-k} g^k.$$

Si $k \geq m'$, alors $g^k \in I$ et si $k < m'$, $m + m' - k > m$ et donc $f^{m+m'-k} \in I$. On en déduit que tous les termes de la somme sont dans I. Ainsi, $(f-g)^{m+m'} \in I$ donc $f - g \in \sqrt{I}$.

Reste à voir que $\sqrt{I}$ est absorbant. Soit $h \in K[X]$. $(fh)^m = f^m h^m \in I$ puisque $f^m \in I$. On en déduit que $hf \in \sqrt{I}$.

2. *Soient $f_1, \ldots, f_s$ des polynômes de $K[X]$ et $I =< f_1, \ldots, f_s >$ l'idéal engendré par ces polynômes. À tout $f \in K[X]$ on associe l'idéal J_f de l'anneau $K[X_1, \ldots, X_n, T]$ suivant.*

$$J_f =< f_1(X) \ldots, f_s(X), 1 - Tf(X) >\in K[X_1, \ldots, X_n, T].$$

Dans cette question, on montre l'équivalence : $f \in \sqrt{I} \iff 1 \in J_f$.

a) Montrer que si $f \in \sqrt{I}$, alors $1 \in J_f$ (on pourra utiliser l'identité $1 = T^m f^m + (1 - T^m f^m)$).

Soit $f \in \sqrt{I}$, et soit m un entier strictement positif tel que $f^m \in I$. Comme $f^m \in I$ et $I \subset J_f$, $f^m \in J_f$. De plus,

$$1 - T^m f^m = (1 - Tf) \sum_{i=0}^{m-1} (Tf)^i,$$

donc $1 - T^m f^m \in J_f$. On déduit de l'égalité $1 = T^m f^m + (1 - T^m f^m)$ que $1 \in J_f$.

b) Montrer la réciproque (on pourra utiliser une identité de la forme

$$1 = q_1(X,T)f_1(X) + \cdots + q_s(X,T)f_s(X) + q_{s+1}(X,T)(1 - Tf(X))$$

et l'évaluer en $T = 1/f(X)$).

On suppose que $1 \in J_f$. Alors il existe $q_1(X,T), \ldots, q_s(X,T), q_{s+1}(X,T) \in K(X,T)$ tels que

$$1 = q_1(X,T)f_1(X) + \cdots + q_s(X,T)f_s(X).$$

En évaluant en $T = \dfrac{1}{f(X)}$, on trouve

$$1 = q_1\left(X, \frac{1}{f(X)}\right) f_1(X) + \cdots + q_s\left(X, \frac{1}{f(X)}\right) f_s(X).$$

Soit $d = \max\{\deg_T q_i(X,T) \ : \ i \in [[1,s]]\}$ En multipliant l'inégalité précédente par $f(X)^d$, on obtient que

$$f(X)^d = f(X)^d q_1\left(X, \frac{1}{f(X)}\right) f_1(X) + \cdots + f(X)^d q_s\left(X, \frac{1}{f(X)}\right) f_s(X),$$

où les $f(X)^d q_i\left(X, \dfrac{1}{f(X)}\right)$ sont des polynômes de $K[X]$. On en déduit que $f^d \in I$, donc que $f \in \sqrt{I}$.

3. *Soient $f \in K[X]$ et G_f la base de Gröbner réduite de J_f pour un ordre monomial donné. Montrer que $f \in \sqrt{I}$ si et seulement si $G_f = \{1\}$.*

D'après la question précédente, $f \in \sqrt{I}$ si et seulement si $1 \in J_f$. Bien sûr, $1 \in J_f$ si et seulement si $J_f = K[X,T]$.

Si $G_f = \{1\}$, il est clair que $1 \in J_f$. Réciproquement, si $1 \in J_f$, alors $< \mathrm{lt}(1) >=< 1 >=< K[X,T] >=< \mathrm{lt}(K[X,T]) >$, donc $\{1\}$ est une base de Gröbner de $K[X,T]$. Comme cette base est de cardinal 1, elle est réduite. C'est donc l'unique base de Gröbner réduite de $K[X,T]$.