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	**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

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

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 $I \cap \mathbb{Q}[Y]$.

2. En utilisant la base de Gröbner de la question précédente, calculer l'ensemble des solutions dans $\mathbb{C}^2$ du système d'équations $f_1(x,y) = f_2(x,y) = 0$.

3. Donner une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[X,Y]/I$.

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.

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.

Soit n un entier naturel non nul. Dans la suite de l'exercice, on considère un polynôme P de $\mathbb{Z}[x]$, et on s'intéresse aux racines de P modulo p^n, c'est-à-dire aux entiers r tels que $P(r) \equiv 0 \mod p^n$.

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

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

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

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

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 $2^i \geq n$.

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 tels que $P(r) \equiv 0 \mod p$ et $P'(r) \not\equiv 0 \mod p$, et qui en sortie rend un entier r' congru à r modulo p tel que $P(r') \equiv 0 \mod p^n$. On s'efforcera d'optimiser la complexité de cette fonction.

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

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.

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.

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

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 $1 = T^m f^m + (1 - T^m f^m)$).

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 $T = 1/f(X)$).

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 $G_f = \{1\}$.

Quelques commandes.

— Pour définir l'anneau `Qxy`$= \mathbb{Q}[x, y]$:

```
Qxy.<x,y>=PolynomialRing(QQ,order='ordre choisi')
```

où l'ordre choisi $\prec$ est l'un des ordres suivants vérifiant $x \succ y$.

`'degrevlex'` (ordre par défaut) - ordre lexicographique gradué inverse

`'lex'` - ordre lexicographique

`'deglex'` - ordre lexicographique gradué

— Pour définir l'idéal I de $\mathbb{Q}[x, y]$ engendré par une liste l de polynômes : `I=Qxy.ideal(l)`. Sa base de Gröbner peut être calculée grâce à la commande `I.groebner_basis()`.

— On peut définir l'anneau `kx`$= \mathbb{F}_p[x]$ en posant `kx.<x>=PolynomialRing(GF(p))`.

— De même, `Zx`$= \mathbb{Z}[x]$ peut être défini par la commande `Zx.<x>=PolynomialRing(ZZ)`.

— Si P est un polynôme, on peut calculer sa dérivée par la commande `diff(P,x)`.

— Soient n et k des entiers tels que la classe de k modulo n est inversible. On peut calculer l'inverse $c \in \mathbb{Z}/n\mathbb{Z}$ de cette classe par la commande

```
c=mod(k,n)^(-1)
```

— Pour définir un représentant r dans $\mathbb{Z}$ d'un élément c de $\mathbb{Z}/n\mathbb{Z}$: `r=c.lift()`.