	ANNEE UNIVERSITAIRE 2015/2016 **Examen première session** **Master 1** **Code UE : MSIN820, MSMA820** **Epreuve : Algèbre et calcul formel** **Date : 10/05/2016** **Heure : 9h00** **Durée : 3h** Documents autorisés : Feuilles d'exercices (énoncés). Epreuve de M. Jehanne	**Collège Sciences et technologies**

Exercice 1 [Bases de Gröbner]
1. On munit $\mathbb{Q}[t,x,y]$ de l'ordre monomial lexicographique $\prec = \prec_{\text{lex}}$ où $t \succ x \succ y$. Soient $f = x(t^4+1) - t$, $g = y(t^4+1) - t^3$ et $I = (f,g)$. La base de Gröbner réduite de I est égale à $\mathcal{B} = [b_1, b_2, b_3, b_4]$ où

$$\begin{cases} b_1 = t^2y - t + x \\ b_2 = tx - x^2 - y^2 \\ b_3 = ty^2 + x^3 + xy^2 - y \\ b_4 = x^4 + 2x^2y^2 - xy + y^4 \end{cases}$$

Comme l'ordre monomial utilisé est l'ordre lexicographique tel que $t \succ x \succ y$, un résultat du cours nous dit que $\mathcal{B} \cap \mathbb{Q}[x,y]$ est une base de Gröbner de l'idéal $I \cap \mathbb{Q}[x,y]$. On en déduit que $\mathbb{Q}[x,y] \cap I = b_4\mathbb{Q}[x,y]$. Le polynôme $P = b_4$ (considéré comme polynôme de $\mathbb{Q}[x,y]$ convient.
2. Montrons d'abord la première inclusion. Soit $(x,y) \in \mathcal{C}$. Alors il existe $t \in \mathbb{R}$ tel que $f(t,x,y) = g(t,x,y) = 0$. Comme I est l'idéal engendré par f et g, on en déduit que $h(t,x,y) = 0$ pour tout polynôme $h \in I$. En particulier, $b_4(t,x,y) = 0$, donc $P(x,y) = 0$ puisque $P = b_4$ ne dépend pas de t.

Montrons la seconde inclusion. Soit $(x,y) \in \mathbb{R}^2$ tel que $P(x,y) = 0$. Si $x = 0$, alors $y = 0$. Le point $(x,y) = (x(0), y(0))$ est donc le point de la courbe correspondant à $t = 0$. Si $x \neq 0$, posons $t = (x^2+y^2)/x$. Alors il est clair que $b_2(t,x,y) = 0$. On calcule $b_3(t,x,y) = (x^2y^2+y^4+x^2y^2-xy)/x = 0$ et $b_1(t,x,y) = (x^4y + y^5 + 2x^2y^3 - x^3 - xy^2 + x^3)/x^2 = 0$. Comme b_1, b_2, b_3, b_4 engendrent I, on en déduit que $f(t,x,y) = g(t,x,y) = 0$, donc que $(x,y) = (x(t), y(t)) \in \mathcal{C}$.

Exercice 2 [Factorisation en degrés distincts, Factorisation en degrés par intervalles]
1. Montrons la cotraposée. Si $f = f_1^2 f_2$ où f_1 est non inversible, alors $f' = 2f_1'f_1f_2 + f_1f_2'$, donc f_1 divise f' et f, donc f_1 divise $\text{pgcd}(f,f')$, qui est donc différent de 1.
2. Montrons par récurrence sur i que pour tout $i \in \mathbb{N} \setminus \{0\}$,

$$g_i = \prod_{Q \in \mathcal{E}_f(i)} Q \quad \text{et} \quad f_i = \prod_{Q \in \mathcal{E}_f([[i+1, \deg f]])} Q$$

c'est-à-dire que g_i est le produit des élément de $\text{Irr}(f)$ de degré i et f_i le produit des élément de $\text{Irr}(f)$ dont le degré est strictement supérieur à i.

Pour $i = 0$, c'est clair. Supposons cette propriété vraie pour $i-1$ et montrons là pour i. $g_i = \text{pgcd}(x^{p^i} - x, f_{i-1})$ est le produit des facteurs irréductibles unitaires de f_{i-1} dont le degré divise $i-1$. Comme f_i est le produit des facteurs irréductibles unitaires de f de degré strictement supérieur à $i-1$, c'est que g_i est le produit des facteurs irréductibles unitaires de f de degré i. Comme $f_i = f_{i-1}/g_i$, on enlève à f_{i-1} les facteurs irréductibles de degré i. Le polynôme f_i est donc bien le produit des facteurs irréductibles unitaires de f de degré strictement supérieur à i.
3. c) Comme `DegDistDeg`, appliquée à f_1 donne $[[1,1],[3,3],[6,6]]$, alors $f_1 = g_1g_3g_6$. Comme g_1 est de degré 1, il est irréductible. Le polynôme g_3 est produit de polynômes irréductibles de degré

3. Comme il est de degré 3, il est irréductible. De même, g_6 est irréductible. La factorisation est donc complète. $f_2 = g_{10}g_{90}g_{488}$, où g_{10} est de degré 20. Comme les facteurs irréductibles de g_{10} sont de degré 10, ce polynôme est produit de deux facteurs irréductibles de degré 10. La factorisation n'est pas complète.

5. Comme f est sans facteurs carrés, il en va de même de pgcd $\left(\prod_{d\in I}\left(x^{p^d}-x\right), f\right)$. D'autre part, il est clair que $\prod_{Q\in\mathcal{D}(I)} Q$ est lui aussi sans facteurs carrés. Comme ces deux polynômes sont tous deux unitaires, il suffit de montrer qu'ils ont les mêmes facteurs irréductibles. Soit $Q \in \mathcal{D}(I)$. Alors il existe $i \in I$ tel que $Q \in \mathcal{D}(i)$ et Q divise $x^{p^i} - x$, qui divise $\prod_{d\in I}\left(x^{p^d}-x\right)$. Comme Q divise aussi f, il divise bien pgcd $\left(\prod_{d\in I}\left(x^{p^d}-x\right), f\right)$. Soit maintenant un facteur irréductible Q de pgcd $\left(\prod_{d\in I}\left(x^{p^d}-x\right), f\right)$. Alors Q est un diviseur de f. Comme Q est irréductible et qu'il divise le produit $\prod_{d\in I}\left(x^{p^d}-x\right)$, il divise l'un des termes $x^{p^i} - x$ de ce produit (où $i \in I$). On en déduit que $Q \in \mathcal{D}_f(i) \subset \mathcal{D}_f(I)$.

6. Soit Q un facteur irréductible de h_k. Alors $\deg Q \geq a_k > \deg f$. C'est absurde car Q divise f. Donc h_k est le produit vide : il est égal à 1.

7. Montrons que pour tout $i \in \mathbb{N}$, le polynôme H_i est égal à h_i et le polynôme F_i est le produit des facteurs irréductibles unitaires de f de degré supérieur ou égal à a_{i+1}.

Pour $i = 0$, comme $F_{-1} = f$, le polynôme h_0 est $H_0 = \text{pgcd}\left(\prod_{d\in I_0}\left(x^{p^d}-x\right), f\right) = \prod_{Q\in\mathcal{D}_f(I_0} Q$ D'après la question **5**. Montrons que $\mathcal{E}_f(I_0) = \mathcal{D}_f(I_0)$. L'inclusion $\mathcal{E}_f(I_0) \subset \mathcal{D}_f(I_0)$ est claire. Montrons l'autre inclusion. Soit $Q \in \mathcal{D}_t(I_0)$. Soit $d = \deg Q$. L'entier d divise un élément de $I_0 = [[1, a_1]]$, donc $d \in I_0$, ce qui prouve que $Q \in \mathcal{E}_f(I_0)$. On a donc montré que $\mathcal{E}_f(I_0) = \mathcal{D}_f(I_0)$, donc $H_0 \prod_{Q\in\mathcal{D}_f(I_0} Q = \prod_{Q\in\mathcal{E}_f(I_0} Q = h_0$. Supposons la propriété vraie pour $i-1$ et montrons là pour i. D'après la question **5**, pgcd $\left(\prod_{d\in I_i}\left(x^{p^d}-x\right), F_{i-1}\right)$ est le produit des facteurs irréductibles unitaires de F_{i-1} dont le degré divise un élément de $I_i = [[a_i, a_{i+1} - 1]]$. Si d est l'un l'un de ces degrés, on en déduit que $d \leq a_{i+1} - 1$. Comme le degré des facteurs irréductibles de F_{i-1} est supérieur ou égal à a_i, on en déduit que $d \geq a_i$. On obtient que $d \in I_i$ et donc que $Q \in \mathcal{E}_f(I_i)$. Réciproquement, si $Q \in \mathcal{E}_f(I_i)$, il est clair que Q divise $\prod_{d\in I_i}\left(x^{p^d}-x\right)$ et F_i, donc il divise leur pgcd. On en déduit que $H_i = h_i$. Quant à F_i, c'est le même raisonnement que celui utilisé pour f_i dans la question **2**.

9. a) Si h_i est irréductible, alors $h_i \in \mathcal{E}_f(I_i)$, donc $\deg h_i \in I_i$. Réciproquement, si h_i n'est pas irréductible, soient r et s deux polynômes irréductibles qui divisent h_i. Alors les degrés de r et s appartiennent à $I_i = [[2^i, 2^{i+1} - 1]]$. On en déduit que $\deg h_i \geq 2^{i+1}$, donc que $h_i \notin I_i$.

b) Pour $f_3 = x^{12} + x^6 + x - 1$, on trouve la liste $[[0, 1], [1, 2], [2, 9]]$. Ainsi, $\deg h_2 = 9 \notin I_2 = [[4, 7]]$. D'après le **a)**, h_2 est réductible. La factorisation n'est donc pas complète.

Pour $f_4 = x^{100} + x - 1$, on trouve $[[3, 14], [4, 20], [6, 66]]$. On voit que $14 \in I_3$, $20 \in I_4$ et $66 \in I_6$, donc la factorisation est complète.

Exercice 3 [À propos du théorème de Rabin-Miller] On rappelle l'énoncé de ce théorème.

Théorème (Rabin-Miller). *Soit n un nombre premier impair. Soit $(e, q) \in \mathbb{N}^2$ le couple d'entiers tel que $n - 1 = 2^e q$ et $q \equiv 1 \mod 2$. Soit a un entier premier à n, alors*

(i) soit $a^q \equiv 1 \mod n$,

(ii) soit il existe i vérifiant $0 \leq i < e$ et $a^{2^i q} \equiv -1 \mod n$.

On rappelle aussi qu'un entier n est appelé *nombre de Carmichael* s'il est composé et si pour tout entier a premier à n, $a^n \equiv 1 \mod n$. Nous avons vu qu'un tel nombre est sans facteur carré.

Soit n un entier impair composé. Pour tout entier a, on note $[a]_n$ la classe de a modulo n. Si a est un entier qui ne vérifie aucune des condition (i) ou (ii) du théorème, on dit que a et $[a]_n$ sont

des *témoins de non primalité* pour n. S'il vérifie l'une de ces conditions, on dit que a et $[a]_n$ sont des *faux témoins de primalité* pour n. Nous allons démontrer le résultat suivant (nous avons vu un résultat plus fort en cours mais avec une preuve différente, et plus difficile).

Théorème. *Soit $M(n)$ l'ensemble des faux témoins de primalité pour n de $\mathbb{Z}/n\mathbb{Z}$. Alors*

$$\text{Card}M(n) \leq \frac{\varphi(n)}{2}$$

où $\varphi = \text{Card}(\mathbb{Z}/n\mathbb{Z})^*$ désigne l'indicatrice d'Euler.

1. a) Soit h l'application de $(\mathbb{Z}/n\mathbb{Z})^*$ dans $(\mathbb{Z}/n\mathbb{Z})^*$ telle que $h(x) = x^{n-1}$. Alors $h(xy) = h(x)h(y)$, donc h est un morphisme de groupes et $F(n) = \ker h$ est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$. Soit $x \in M(n)$. Alors soit $x^q = 1$, soit il existe $i \in [[0, e-1]]$ tel que $x^{2^i q} = -1$. Comme q divise $n-1$, il est clair que dans le premier cas $x^{n-1} = 1$. Dans le second cas, $(x^{2^i q})^2 = x^{2^{i+1} q} = 1$, donc $x^{n-1} = 1$. On en déduit que $F(n)$ contient $M(n)$

b) Si n n'est pas un nombre de Carmichael, alors $\text{Card}F(n) \neq (\mathbb{Z}/n\mathbb{Z})^*$. Le cardinal de $F(n)$ est donc inférieur ou égal au plus grand diviseur de $\varphi(n)$ distinct de $\varphi(n)$. On en déduit que $\text{Card}F(n) \leq \varphi(n)/2$, d'où le résultat.

2. a) Comme n est un nombre de Carmichael, $u^{n-1} = u^{2^e q} = 1$ pour tout $u \in (\mathbb{Z}/n\mathbb{Z})^*$, donc $e \in I$. Comme q est impair, $(-1)^q = -1 \neq 1$, donc $0 \notin I$.

b) Si $i \in I$, $u^{2^i q} = 1$ pour tout $u \in (\mathbb{Z}/n\mathbb{Z})^*$. Donc $(u^{2^i q})^2 = u^{2^{i+1} q} = 1$ pour tout u. Comme $i \in [[0, e-1]]$, $i+1 \in [[1, e]]$ donc $i \in I$.

3. a) Soit h' l'application de $(\mathbb{Z}/n\mathbb{Z})^*$ dans $(\mathbb{Z}/n\mathbb{Z})^*$ telle que $h'(x) = x^{2^l q}$. Alors $h(xy) = h(x)h(y)$, donc h est un morphisme de groupes et $G = h'^{-1}(\{-1, 1\}$. Comme $\{-1, 1\}$ est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$, son image réciproque G est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$. Soit $x \in M(n)$. Alors si $x^q = 1$, il est clair que $x^{2^l q} = 1$. Sinon, il existe $i \in [[0, e-1]]$ tel que $x^{2^i q} = -1$, donc $i \notin I$, donc $i \leq l$, donc $x^{2^l q} = -1$ si $i = l$ et $x^{2^l q} = 1$ si $i > l$. Par conséquent, $x \in G$. On a montré que $M(n) \subset G$.

b) Si pour tout nombre premier p divisant n et tout entier b premier à p on avait $b^{2^l q} \equiv 1 \mod p$, alors comme n est sans facteurs carrés, on pourrait en déduire que pour tout b premier à n, $b^{2^l q} \equiv 1 \mod n$ et donc que $l \in I$. C'est absurde.

c) Comme n est sans facteurs carrés, p est premier à n/p. Le théorème des restes chinois montre alors l'existence d'un entier c tel que $c \equiv b \mod p$ et $c \equiv 1 \mod n/p$.

d) Comme $c^{2^l q} \equiv -1 \mod p$ et $c^{2^l q} \equiv -1 \mod n/p$, on voit que $[c]_n \notin G$. Par le même raisonnement qu'au **1. a)**, on obtient les inégalités

$$\text{Card}M(n) \leq \text{Card}G \leq \frac{\varphi(n)}{2}$$