université de BORDEAUX	**ANNEE UNIVERSITAIRE 2014/2015** **Examen première session** **Master 1** **Code UE : MSIN820, MSMA820** **Epreuve : Algèbre et calcul formel** **Date : 22/04/2015** **Heure : 8h00** **Durée : 3h** **Corrigé**	**Collège Sciences et technologies**

Exercice 1

1. $Q(x) = \sum_{i=0}^{m-1} x^k$.

2. Supposons que $2^n - 1$ est premier. Écrivons $n = km$ où $m \geq 2$ et montrons que $k = 1$. Cela montrera le résultat

$$2^n - 1 = (2^k)^m - 1 = (2^k - 1) \sum_{i=0}^{m-1} 2^{ki}$$

Comme $2^n - 1$ est premier, et comme $m \geq 2$, c'est que $2^k - 1 = 1$, donc $k = 1$.

3. a) D'après le relations entre racines et coefficients d'un polynôme, $\alpha + \beta = 4$, $\alpha\beta = 1$. On pouvait retrouver facilement ces relations en écrivant

$$x^2 - 4x + 1 = (x - \alpha)(x - \beta) = x^2 - (\alpha + \beta)x + \alpha\beta.$$

b) Pour $i = 0$: $\alpha^{2^0} + \beta^{2^0} = \alpha + \beta = 4$. C'est bien l'image de L_1 dans $\mathbb{F}_p$.
On suppose que $\alpha^{2^{i-1}} + \beta^{2^{i-1}} = L_i \mod p$. Alors

$$\begin{aligned}(L_{i+1} \mod p) &= (\alpha^{2^{i-1}} + \beta^{2^{i-1}})^2 - 2 \\ &= \alpha^{2^i} + \beta^{2^i} + 2(\alpha\beta)^{2^{i-1}} - 2 \\ &= \alpha^{2^i} + \beta^{2^i}\end{aligned}$$

puisque $\alpha\beta = 1$.

c) Comme $L_{n-1} \equiv 0 \mod p$, la question précédente montre que $\alpha^{2^{n-2}} + \beta^{2^{n-2}} = 0$, donc $\alpha^{2^{n-2}} = -\beta^{2^{n-2}}$. En multipliant les deux membres de cette égalité par $\alpha^{2^{n-2}}$, on obtient $\alpha^{2^{n-1}} = -1$. On en déduit que l'ordre de α est égal à 2^n (puisque $\alpha^{2^n} = 1$ et $\alpha^{2^{n-1}} \neq 1$).

d) Supposons par l'absurde que M_n n'est pas premier. Comme p est le plus petit diviseur premier de M_n, alors $M_n \geq p^2$. D'autre part, α est un élément d'ordre 2^n de $(\mathbb{F}_{p^2})^*$, donc $2^n \leq p^2 - 1$, ce qui prouve que $M_n \leq p^2 - 2$, ce qui est absurde.

4. [Application sur machine] Voir le fichier `Exam.sage`.

Exercice 2

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

b) $P = x^{10} - x + 1 \in \mathbb{F}_{11}$. $\mathrm{pgcd}(P, x^{11} - x) = x + 9 = x - 2$ (le calcul est fait dans $\mathbb{F}_{11}[x]$). Ainsi, P s'écrit $P = (x - 2)Q(x)$ où Q n'a pas de facteurs de degrés 1, donc pas de racines dans $\mathbb{F}_{11}$. 2 est donc la seule racine de P dans $\mathbb{F}_{11}$.

2. Comme p divise p^k, si $P(r) \equiv 0 \mod p^n$, alors $P(r) \equiv 0 \mod p$.

3. On utilise la formule du binome.

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

puisque si $j \geq 2$, l'entier p^{kj} est divisible par p^{2k}. On pose $P(x) = \sum_{i=0}^{d} a_i x^i$. Alors

$$\begin{aligned} P(x+tp^k) = \sum_{i=0}^{d} a_i (x+tp^k)^i &\equiv \sum_{i=0}^{d} a_i x^i + \sum_{i=1}^{d} i a_i t p^k x^{i-1} \mod p^{2k} \\ &\equiv P(x) + tp^k P'(x) \mod p^{2k} \end{aligned}$$

4.

$$\frac{P(r_k)}{p^k} + t_k P'(r_k) \equiv 0 \mod p^k \Leftrightarrow t_k \equiv -\frac{P(r_k)}{p^k} P'(r_k)^{-1} \mod p^k$$

Ici, $P'(r_k)$ est bien inversible modulo p^k car $P'(r_k) \equiv P'(r) \mod p$, donc $P'(r_k)$ est premier à p, donc il est premier à p^k.
5. Comme $k \geq 1$, il est clair que $r_{2k} = r_k + t_k p^k \equiv r \mod p$.

$$P(r_{2k}) = P(r_k + t_k p^k) \equiv P(r_k) + t_k p^k P'(r_k) \mod p^{2k}$$

d'après la question 3. Donc

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

puisque d'après la question 4,

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

6. Soit $P = x^3 + x + 1$. On calcule $P(0) = 1$, $P(1) = 3 \equiv 0 \mod 3$ et $P(-1) = -1$. Donc l'unique racine de P vu comme polynôme sur $\mathbb{Z}/3\mathbb{Z}$ est 1. Relevons cette racine en une racine modulo 81. On pose $r = r_1 = 1$. $P' = 3x^2 + 1$, donc $P'(r_1) \equiv 1 \mod 3$. On calcule $t_1 = -\frac{P(r_1)}{3} P'(r_1)^{-1} \mod 3 = -1$. Ainsi, $r_2 = r_1 + 3t_1 = -2 \mod 9$. On vérifie que $P(-2) = -9 \equiv 0 \mod 9$. Maintenant, $P'(-2) \equiv 4 \mod 9$. Son inverse modulo 9 est -2. Ainsi, $t_2 = -\frac{P(r_2)}{9} P'(r_2)^{-1} \mod 9 = -2$. On conclut : $r_4 = -2 - 2.9 = -20 \equiv 61 \mod 81$. L'unique racine de P modulo 81 est donc 61.
7. Voir le fichier `Exam.sage`
8. On trouve.

Exercice 3

1. Soit $P \in I \cap J$. Alors clairement, $P \in K[X_1, \ldots, X_n]$. De plus, $P = TP + (1-T)P \in \mathcal{R}(I, J)$.

Réciproquement, soit $P \in \mathcal{R}(I, J) \cap K[X_1, \ldots, X_n]$. Alors il existe $g_1, \ldots, g_r$ dans I, $h_1, \ldots, h_s$ dans J et $\alpha_1, \ldots, \alpha_r$, $\beta_1, \ldots, \beta_s$ dans $K[X_1, \ldots, X_n, T]$ tels que

$$P = T \sum_{i=1}^{r} g_i \alpha_i + (1-T) \sum_{i=1}^{s} h_i \beta_i.$$

Comme P ne dépend pas de T, on obtient $P(X_1, \ldots, X_n, T) = P(X_1, \ldots, X_n, 0) = P(X_1, \ldots, X_n, 1)$, ce qui donne immédiatement

$$P = \sum_{i=1}^{r} g_i \alpha_i (X_1, \ldots, X_n, 0) = \sum_{i=1}^{s} h_i \beta_i (X_1, \ldots, X_n, 1) \in I \cap J$$

.

2. Comme les g_i et les h_j sont respectivement des éléments de I et J, il est clair que

$$\{Tg_1, \ldots, Tg_r\} \cup \{(1-T)h_1, \ldots, (1-T)h_s\} \subset \mathcal{R}(I, J)$$

et donc l'idéal engendré par cet ensemble est inclus dans $\mathcal{R}(I, J)$. Réciproquement, tout élément Tg où $g \in I$ s'écrit $Tg = \sum_{i=1}^{r} a_i T g_i$, où les a_i appartiennent à $K(X_1, \ldots, X_n, T)$. De même, tout élément $(1-T)h$ où $h \in J$ s'écrit $(1-T)h = \sum_{i=1}^{r} b_i (1-T) h_i$, où les b_i appartiennent à $K(X_1, \ldots, X_n, T)$. Ainsi, tout élément de $TI \cup (1-T)J$ appartient à l'idéal $< \{Tg_1, \ldots, Tg_r\} \cup \{(1-T)h_1, \ldots, (1-T)h_s\} >$, donc $\mathcal{R}(I, J) \subset < \{Tg_1, \ldots, Tg_r\} \cup \{(1-T)h_1, \ldots, (1-T)h_s\} >$.
3. Pour calculer une base de Gröbner de $I \cap J$, on calcule une base de Gröbner G de $\mathcal{R}(I, J)$ pour l'ordre lexicographique $\prec$ tel que $T \succ X_1 \succ \cdots \succ X_n$. Alors, comme $I \cap J = \mathcal{R}(I, J) \cap K[X_1, \ldots, X_n]$, on sait que $G \cap K[X_1, \ldots, X_n]$ est une base de Gröbner de $I \cap J$.