UNIVERSITÉ MONTPELLIER 2
SCIENCES ET TECHNIQUES

FLMA607 Calcul Formel – 2010–2011

Contrôle continu numéro 3 (27 avril 2011)

Durée : 2h00. Justifiez toutes vos réponses. Documents, calculatrices et téléphones portables sont interdits.
Le barême est donné à titre indicatif et est susceptible d'être modifié.

Quelques rappels

1) Le discriminant d'un polynôme $P \in K[X]$ de coefficient dominant a et de degré n est donné par la formule

$$\Delta(P) = (-1)^{\frac{n(n-1)}{2}} a^{-1} \mathrm{Res}\,(P, P')$$

où P' est le polynôme dérivé de P.

2) Avec cette définition, si $\alpha_1, \ldots, \alpha_n$ désignent les n racines de P (éventuellement dans un surcorps de K) on rappelle la formule suivante (démontrée au cours du second contrôle continu) :

$$\Delta(P) = a^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2 .$$

Question de cours (1 point) Donner la définition du résultant de deux polynômes.

Exercice 1 (8 points)

Soit $f = x^4 + 2x^3 + 2x + 2 \in \mathbb{F}_3[x]$.

1) Montrer que f est séparable.
2) Combien l'algèbre $A = \mathbb{F}_3[x]/(f)$ a-t-elle d'éléments ?
3) Calculer la sous-algèbre de Berlekamp $\mathcal{B}$ de A (donner une base). Combien comporte-t-elle d'éléments ?
4) Un élément de A correspond à un polynôme $a_0 + a_1 x + a_2 x^2 + a_3 x^3$. On représentera A par un tableau à deux entrées avec $a_0 + a_1 x$ en abscisse et $a_2 x^2 + a_3 x^3$ en ordonnée. Colorier dans ce tableau les cases correspondant aux éléments de $\mathcal{B}$.
5) Combien f a-t-il de facteurs irréductibles ?
6) Factoriser f par la méthode de Berlekamp (on prendra $G = x^3 + x$).
7) En déduire un isomorphisme $A \simeq A_1 \times A_2$ par le théorème chinois.
8) Faire la liste des éléments de A_1 et A_2 puis représenter de nouveau A par un tableau à deux entrées, en mettant cette fois-ci les éléments de A_1 en abscisse et ceux de A_2 en ordonnée. Dessiner $\mathcal{B}$ dans ce nouveau tableau.
9) Dans $\mathcal{B}$, combien y a-t-il d'éléments G tels que la factorisation de Berlekamp soit non triviale ? Dans les tableaux des questions 4 et 8, marquer d'une croix les cases qui correspondent à ces éléments.

Exercice 2 (5 points)

Soit d un entier supérieur ou égal à 2. Soit $P \in \mathbb{R}[X]$ un polynôme *unitaire* de degré d. On note n le nombre de racines réelles de P.

1) Montrer que $\Delta(P) > 0$ entraîne $n \equiv d \pmod 4$ et que $\Delta(P) < 0$ entraîne $n \equiv d - 2 \pmod 4$.
2) Calculer le discriminant du polynôme $F(X) = X^3 + pX + q$.
3) Discuter suivant les valeurs de p et q le nombre de racines réelles de F.

Exercice 3 (6 points)

Soit K un corps et soient $f, g \in K[x]$ deux polynômes non nuls. La *suite euclidienne* de (f, g) est la suite $(\deg r_0, \deg r_1, \ldots, \deg r_l) \in \mathbb{N}^{l+1}$ où $r_0 = f$, $r_1 = g$, r_2, …, r_l sont les restes dans l'algorithme d'Euclide appliqué à f et g. Dans cet exercice, on notera $K_{\leq n}[x]$ (resp. $K_{=n}[x]$) le sous-ensemble de $K[x]$ formé des polynômes de degré inférieur ou égal à n (resp. égal à n) et $SE(n_0, \ldots, n_l)$ l'ensemble des couples (f, g) de polynômes dont la suite euclidienne est $(n_0, \ldots, n_l)$.

1) Si $K = \mathbb{F}_q$, combien de couples (f, g) ont pour suite euclidienne $(4, 3, 1, 0)$? (*Indication :* On pourra considérer l'application φ définie par $\varphi(f, g) = (q_1, q_2, q_3, r_3)$ où les q_i sont les quotients dans l'algorithme d'Euclide, et montrer qu'elle réalise une bijection de $SE(4, 3, 1, 0)$ sur $K_{=1}[x] \times K_{=2}[x] \times K_{=1}[x] \times K_{=0}[x]$.)

2) Généralisez votre réponse pour une suite d'entiers quelconque $(n_0, \ldots, n_l) \in \mathbb{N}^{l+1}$ avec $n_0 \geq n_1 > n_2 > \cdots > n_l \geq 0$ et $l \geq 1$.
3) Pour chacune des quatre suites euclidiennes possibles avec $n_0 = 3$ et $n_1 = 2$, faire la liste des couples (f, g) correspondant dans $(\mathbb{F}_2[x] \setminus \{0\})^2$.
4) On fixe deux entiers $n \geq m > 0$. On choisit deux polynômes au hasard $(f, g) \in K_{=n}[x] \times K_{=m}[x]$ (en prenant $K = \mathbb{F}_q$). Montrer que la probabilité pour que f et g soient premiers entre eux est $1 - \frac{1}{q}$.