Université Claude Bernard LYON 1
Master MA Mathématiques générales
Algèbre et calcul formel

Partiel du 5 février 2014

durée 2h

Exercice 1.

Soient $f = \sum_{i=0}^{m} a_i X^i \in K[X]$ et $g = \sum_{j=0}^{n} b_j X^j \in K[X]$ des polynômes non constants de degrés respectifs m et n où K est un corps de *caractéristique nulle.*

1. Montrer que si $h_1 \equiv h_2 \mod f$ on a $a_m^{-d_1} R_X(f, h_1) = a_m^{-d_2} R_X(f, h_2)$ avec $h_1, h_2 \in K[X]$ non nuls de degrés respectifs d_1 et d_2.
2. Montrer que $R_X(f\,g, (f\,g)') = (-1)^{mn} R_X(f, f') R_X(g, g') R_X(f, g)^2$
3. En conclure que $\mathrm{discrim}_X(f\,g) = \mathrm{discrim}_X(f)\ \mathrm{discrim}_X(g)\ R_X(f, g)^2$

Exercice 2.

Soit $M \in \mathbf{M}_{m,n}(K)$ de rang r ; on considère la forme échelonnée *réduite en lignes* $L \in \mathbf{M}_{m,n}(K)$ de M ;

1. Montrer que $\mathrm{Ker}(L) = \mathrm{Ker}(M)$.
2. On *suppose* que $M \in \mathbf{M}_{m,n}(K)$ est telle que L soit de la forme $L = \begin{pmatrix} \mathrm{I}_r & L' \\ 0 & 0 \end{pmatrix}$ avec $L' \in \mathbf{M}_{r,n-r}(K)$. Montrer que les colonnes de la matrice $\mathcal{K} = \begin{pmatrix} L' \\ -\mathrm{I}_{n-r} \end{pmatrix} \in \mathbf{M}_{n,n-r}(K)$ forment une base de $\mathrm{Ker}(M)$.
3. Pour $M \in \mathbf{M}_{m,n}(K)$ quelconque, montrer qu'il existe une matrice de permutation $\pi_\sigma \in \mathbf{GL}_n(K)$ telle que $L\,\pi_\sigma$ soit de la forme $\begin{pmatrix} \mathrm{I}_r & L' \\ 0 & 0 \end{pmatrix}$.
4. En déduire une base de $\mathrm{Ker}(M)$.

Exercice 3.

1. Soient $\mathbb{F}_q$ un corps fini avec $q = p^m$, $S = \{x_1, \ldots, x_n\} \subset \mathbb{F}_q$ et $k \leq n$ un entier non nul ; on considère l'application $\mathbb{F}_q$-linéaire :

$$\begin{array}{rcl} c : \mathbb{F}_q[X]_{\leq k-1} & \longrightarrow & (\mathbb{F}_q)^n \\ f & \longrightarrow & c(f) = (f(x_1), \cdots, f(x_n)) \end{array}$$

   (a) Montrer que $C_{k,S} = \mathrm{Im}(c)$ est un code linéaire et déterminer sa dimension.

   (b) Montrer que tout mot du code $C_{k,S}$ de poids $w < n - k + 1$ est nul. En déduire la distance minimale d du code $C_{k,S}$.

   (c) Donner une matrice génératrice pour le code $C_{k,S}$.

2. (a) Déterminer la forme de la décomposition en facteurs irréductibles (ie. nombre de facteurs et degrés de chacun) de $\overline{\Phi}_7$ dans $\mathbb{F}_2[X]$.

(b) Factoriser $\overline{\Phi}_7$ dans $\mathbb{F}_2[X]$.

3. On pose $q = 8$. On considère le corps fini $\mathbb{F}_q = \mathbb{F}_2[\alpha]$ où $p_{\alpha,\mathbb{F}_2}$ est l'un des facteurs irréductibles de $\overline{\Phi}_7$ dans $\mathbb{F}_2[X]$.
   (a) Vérifier que $(\mathbb{F}_q)^\star = \langle \alpha \rangle$.
   (b) On prend $n = q - 1$, $k = 4$ et $S = \{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$;
      i. Quels sont les *paramètres* (*ie.* la longueur, la dimension et la distance minimale) du code $C_{k,S}$.
      ii. Montrer que le code $C_{k,S}$ est cyclique.