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

Corrigé du partiel

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 $h_1 \equiv h_2 \bmod f$ 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 $\mathrm{discrim}_X(f\,g) = \mathrm{discrim}_X(f)\ \mathrm{discrim}_X(g)\ R_X(f, g)^2$

Corrigé.
On a la formule de Poisson $R_X(f, h_1) = a_m^{d_1} \det(m_{h_1})$ et $R_X(f, h_2) = a_m^{d_2} \det(m_{h_2})$ et l'on a $m_{h_1} = m_{h_2}$. En utilisant la multiplicativité des degrés et la question précédent en remarquant que $m + n - 1 = \deg((f\,g)') = \deg(f'g + f\,g') = \deg(f'g) = \deg(f\,g')$

$$\begin{aligned} R_X(f\,g, (f\,g)') &= R_X(f\,g, f'g + f\,g') \\ &= R_X(f, f'g + f\,g') R_X(g, f'g + f\,g') \\ &= R_X(f, f'g) R_X(g, f\,g') \\ &= R_X(f, f') R_X(f, g) R_X(g, g') R_X(g, f) \\ &= (-1)^{mn} R_X(f, f') R_X(g, g') R_X(f, g)^2 \end{aligned}$$

Or on a :

$$\begin{aligned} \mathrm{discrim}_X(f) &= (-1)^{m(m-1)/2} a_m^{-1} R_X(f, f') \\ \mathrm{discrim}_X(g) &= (-1)^{n(n-1)/2} b_n^{-1} R_X(g, g') \\ \mathrm{discrim}_X(f\,g) &= (-1)^{(m+n)(m+n-1)/2} (a_m b_n)^{-1} R_X(f\,g, (f\,g)') \end{aligned}$$

Il reste donc à vérifier que :

$$(-1)^{(m+n)(m+n-1)/2} = (-1)^{mn} (-1)^{m(m-1)/2} (-1)^{n(n-1)/2}$$

or on a $mn + m(m-1)/2 + n(n-1)/2 = (m+n)(m+n-1)$.

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 $\mathrm{Ker}(M)$.

Corrigé.
Il existe $U \in \mathbf{GL}_m(K)$ tel que $L = U\,M$ de sorte que $\mathrm{Ker}(M) = \mathrm{Ker}(L)$. M s'identifie à une application K-linéaire $K^n \longrightarrow K^m$; comme cette application est de rang r $\dim_K(\mathrm{Ker}(M)) = n - r$.

Or on a $L = \begin{pmatrix} \mathrm{I}_r & L' \\ 0 & 0 \end{pmatrix}$ de sorte que :

$$L\,\mathcal{K} = \begin{pmatrix} \mathrm{I}_r & L' \\ 0 & 0 \end{pmatrix} \begin{pmatrix} L' \\ -\mathrm{I}_{n-r} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

et $\mathcal{K}$ est de rang $n - r$ donc ses colonnes forment une base du noyau.

Dans le cas général, soit $s(i)$ la colonne de pivot de la $i^{\text{ème}}$ ligne $(1 \leq i \leq r)$ et considérons la matrice π_σ associée à la permutation $(1, s(1)) \cdots (r, s(r))$ de sorte que l'on a $L\pi_\sigma = \begin{pmatrix} \mathrm{I}_r & L' \\ 0 & 0 \end{pmatrix}$.
Comme $L = U\,M$ avec $U \in \mathbf{GL}_m(K)$ on a $L\pi_\sigma = U\,M\pi_\sigma$ de sorte que $L\pi_\sigma$ est la forme échelonnée réduite de $M\pi_\sigma$.
Alors 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 $\mathrm{Ker}(M\,\pi_\sigma)$.
Or on a $\mathrm{Ker}(M\,\pi_\sigma) = \pi_\sigma^{-1}.\mathrm{Ker}(M)$.
Il en résulte que les colonnes de la matrice $\pi_\sigma\mathcal{K}$ forment 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 :

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

   (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.

Corrigé.
C est un sous-espace vectoriel de $(\mathbb{F}_q)^n$ ie. un code linéaire. c est injective car si $c(f)=0$, le polynôme f avec $\deg(f)\leq k-1$ possède $n\geq k$ racines donc $f=0$. Il en résulte que le code C est de dimension k.
Tout mot du code C est de la forme $c(f)=(f(x_1),\cdots,f(x_n))$ avec $\deg(f)\leq k-1$. Soit w le poids de f et supposons que $w<n-k+1$. Le nombre de racines de f est $n-w$ et l'on $n-w>k-1$ donc $f=0$. Ainsi tout mot *non nul* de C est de poids $w\geq n-k+1$ d'où $d\geq n-k+1$ et comme on a que $d\leq n-k+1$ on a finalement $d=n-k+1$.
Une matrice génératrice de C est de la forme :

$$\begin{pmatrix} 1 & 1 & \cdots & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_j & \cdots & x_n \\ \vdots & \vdots & \cdots & \vdots & \cdots & \vdots \\ x_1^{k-1} & x_2^{k-1} & \cdots & x_j^{k-1} & \cdots & x_n^{k-1} \end{pmatrix}$$

Soit m l'ordre de $\overline{2}$ dans $(\mathbb{Z}/\mathbb{Z}7)^\times$; on a $\overline{2}^2=\overline{4}$ et $\overline{2}^3=\overline{1}$ de sorte que $m=3$.
Le nombre de facteurs irréductibles de Φ_7 dans $\mathbb{F}_2$ et donc

$$\frac{\varphi(7)}{m}=\frac{6}{3}=2$$

On a donc 2 facteurs irréductibles, chacun de degré 3.
Or $\Phi_7=X^6+X^5+X^4+X^3+X^2+X+1$ Les polynômes unitaires de degré 3 sont :

$$X^3+aX^2+bX+c \text{ avec } a,b,c\in\mathbb{F}_2$$

Il faut déterminer ceux qui sont irréductibles : on doit avoir $a=\overline{1}$ et et il faut que polynôme X^3+aX^2+bX+1 n'ait pas de racine. Il faut donc qu'il n'ait que 3 coefficients non nul on obtient donc deux polynômes X^3+X^2+1 et X^3+X+1.
On a bien :

$$\overline{X^6+X^5+X^4+X^3+X^2+X+1}=(X^3+X^2+\overline{1})(X^3+X+\overline{1})$$

On $q=2^m=8$. On considère le corps fini $\mathbb{F}_q=\mathbb{F}_2[\alpha]$. Comme $p_{\alpha,\mathbb{F}_2}$ est l'un des facteurs irréductibles de $\overline{\Phi}_7$ dans $\mathbb{F}_2[X]$ α est d'ordre 7 dans $(\mathbb{F}_q)^\star$ donc est un générateur.

On prend $n=q-1=7$, $k=4$ et $S=\{1,\alpha,\alpha^2,\cdots,\alpha^6\}$; d'après la première partie le code $C_{k,S}$ est de longueur $n=7$, de dimension $k=4$ et de distance minimale $d=n-k+1=4$.

Le code $C_{k,S}$ est l'image de l'application $\mathbb{F}_8$-linéaire :

$$\begin{array}{rcl} c:\mathbb{F}_8[X]_{\leq 3} & \longrightarrow & (\mathbb{F}_8)^7 \\ f & \longrightarrow & c(f)=(f(1),f(\alpha)\cdots,f(\alpha^5),f(\alpha^6)) \end{array}$$

Il faut montrer pour tout mot $c(f)$ du code, $(f(\alpha^6),f(1),f(\alpha)\cdots,f(\alpha^5))$ est encore un mot du code. Si $f=\sum_{i=0}^{k-1}c_iX^i$, on pose $f_+=\sum_{i=0}^{k-1}\alpha^{6i}c_iX^i$. on a alors $f_+(1)=\sum_{i=0}^{k-1}\alpha^{6i}c_i=f(\alpha^6)$ et pour $1\leq j\leq 6$ $f_+(\alpha^j)=\sum_{i=0}^{k-1}\alpha^{6i}c_i\alpha^{ji}=\sum_{i=0}^{k-1}c_i\alpha^{(j-1)i}=f(\alpha^{j-1})$. On a ainsi :

$$(f(\alpha^6),f(1),f(\alpha)\cdots,f(\alpha^5))=c(f_+)$$

Ainsi le code $C_{k,S}$ est cyclique.