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

Corrigé de la fiche de TD 1

Exercice 1.
Soient $f, g \in K[X]$ de degrés respectifs m et n ; on considère l'application K-linéaire :

$$\begin{array}{rccl} \partial_{f,g}^{m,n} & : & K[X]_{\leq n-1} \oplus K[X]_{\leq m-1} & \longrightarrow & K[X]_{\leq m+n-1} \\ & & (u, v) & \longrightarrow & u\,f + v\,g \end{array}$$

Déterminer l'image et le noyau de $\partial_{f,g}^{m,n}$.

Corrigé.
Soit $\Delta = \mathrm{pgcd}(f, g)$; on a :

$$\begin{cases} f = \Delta \widetilde{f} \\ g = \Delta \widetilde{G} \end{cases}$$

avec $\widetilde{f}$ et $\widetilde{g}$ premiers entre eux. On a donc que :

$$\mathrm{Im}(\partial_{f,g}^{m,n}) \subset K[X]_{\leq m+n-d-1}\Delta$$

Soient $(u, v) \in \mathrm{Ker}(\partial_{f,g}^{m,n})$; on a $u\widetilde{f} + v\widetilde{g}$ de sorte que $v = \widetilde{f}q$ et par suite $u = -q\widetilde{g}$. On a donc que :

$$\mathrm{Ker}(\partial_{f,g}^{m,n}) \subset K[X]_{\leq d-1}(-\widetilde{f}, \widetilde{g})$$

On conclut par un argument de dimension.

Exercice 2.

1. Soit $f = \sum_{i=1}^{m} a_i X^i \in K[X]$ de degré m ; on considère l'application K-linéaire :

$$\begin{array}{rccl} \epsilon_f^{m,n} & : & K[X]_{\leq m+n-1} & \longrightarrow & K[X]_{\leq n-1} \oplus K[X]_{\leq m-1} \\ & & h & \longrightarrow & (q, r) \end{array}$$

   où, pour tout $h \in K[X]$ q et r sont le quotient et le reste de la division euclidienne de h par f.
   Montrer que $\epsilon_f^{m,n}$ est bijective et calculer $\det(\epsilon_f^{m,n})$.
2. Pour tout $g \in K[X]$ de degré n, on considère l'application K-linéaire :

$$\begin{array}{rccl} m_g : K[X]/\langle f\rangle & \longrightarrow & K[X]/\langle f\rangle \\ \overline{h} & \longrightarrow & \overline{gh} \end{array}$$

   Montrer que

$$\det(m_g) = \det(\mu_g)$$

   où $\mu_g : K[X]_{\leq m-1} \longrightarrow K[X]_{\leq m-1}$ est l'application K-linéaire définie par la condition que, $\mu_g(h)$ est le reste de la division euclidienne de gh par f pour tout $h \in K[X]_{\leq m-1}$.

3. En déduire que :

$$R_X(f,g) = a_m^n \det(m_{\overline{g}})$$

Corrigé.

1. l'application induite par la *division euclidienne* par f :

$$\begin{array}{rccc} \epsilon_f^{m,n} : & K[X]_{\leq m+n-1} & \longrightarrow & K[X]_{\leq n-1} \oplus K[X]_{\leq m-1} \\ & h & \longrightarrow & (q_f(h), r_f(h)) \end{array}$$

où $h = fq_f(h) + r_f(h)$ avec $r_f(h) \in K[X]_{\leq m-1}$ de sorte que $q_f(h) \in K[X]_{\leq n-1}$.
La matrice de $\epsilon_f^{m,n}$ dans les bases canoniques est de la forme :

$$\begin{pmatrix} T & 0 \\ \star & \mathrm{I} \end{pmatrix}$$

où T est une matrice triangulaire inférieure de la forme :

$$T = \begin{pmatrix} a_m^{-1} & 0 & \cdots & 0 \\ \star & a_m^{-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \star & \star & \cdots & a_m - 1 \end{pmatrix}$$

de sorte que :

$$\det(\epsilon_f^{m,n}) = a_m^{-n}$$

2. Soit $f = \sum_{i=1}^{m} a_i X^i \in K[X]$ un polynôme de degré m ; on lui associe la K-algèbre

$$A = K[X]/K[X]f$$

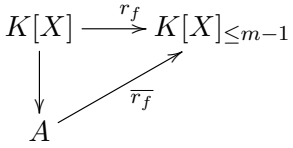
de rang m ; l'application K-linéaire :

$$\begin{array}{rcl} K[X]_{\leq m-1} & \longrightarrow & A \\ r & \longrightarrow & \overline{r} \end{array}$$

est bijective, l'application réciproque :

$$\overline{r_f} : A \longrightarrow K[X]_{\leq m-1}$$

étant induite par l'application r_f associant $h \in K[X]$ le *reste* $r_f(h)$ de la *division euclidienne* de h par r.



Pour tout $g \in K[X]$ on considère :

$$\begin{array}{rcl} m_g : A & \longrightarrow & A \\ \overline{h} & \longrightarrow & \overline{gh} \end{array}$$

l'endomorphisme du K-espace vectoriel A induit par la multiplication par g. On a le diagramme commutatif :

$$\begin{array}{ccc} A & \xrightarrow{\overline{r_f}} & K[X]_{\leq m-1} \\ {\scriptstyle m_g}\downarrow & & \downarrow{\scriptstyle \mu_g} \\ A & \xrightarrow[\overline{r_f}]{} & K[X]_{\leq m-1} \end{array}$$

avec $\mu_g(r) = r_f(gr)$ pour tout $r \in K[X]_{\leq m-1}$. On a en particulier :

$$\det(\mu_g) = \det(m_g)$$

3. Soit n le degré de g ; on considère l'application de *Bezout-Sylvester* :

$$\begin{array}{rccc} \partial_{f,g}^{m,n} & : K[X]_{\leq n-1} \oplus K[X]_{\leq m-1} & \longrightarrow & K[X]_{\leq m+n-1} \\ & (u,v) & \longrightarrow & u\,f + v\,g \end{array}$$

Par composition on a : :

$$\begin{array}{rccc} \epsilon_f^{m,n} \circ \partial_{f,g}^{m,n} & : K[X]_{\leq n-1} \oplus K[X]_{\leq m-1} & \longrightarrow & K[X]_{\leq n-1} \oplus K[X]_{\leq m-1} \\ & (u,v) & \longrightarrow & (u + q_f(vg), \mu_g(v)) \end{array}$$

ie. est décomposée en blocs de la forme :

$$\begin{pmatrix} \mathrm{Id} & \star \\ 0 & \mu_g \end{pmatrix}$$

On a donc :

$$\begin{array}{rcl} \det(\epsilon_f^{m,n} \circ \partial_{f,g}^{m,n}) & = & \det(\mu_g) \\ & = & \det(m_g) \\ & = & \det(\epsilon_f^{m,n}) \det(\partial_{f,g}^{m,n})) \\ & = & \det(\epsilon_f^{m,n}) R_X(f,g) \\ & = & a_m^{-n} R_X(f,g) \end{array}$$

Exercice 3.

1. Considérons un corps K et $f \in K[X]$;
   (a) Si K est de caractéristique nulle on a $f' = 0$ si et seulement si f est constant.
   (b) Si K est de caractéristique p on a $f' = 0$ si et seulement s'il existe $g \in K[X]$ avec $f = g(X^p)$.
   (c) Si K est parfait de caractéristique p on a $f' = 0$ si et seulement s'il existe $g \in K[X]$ avec $f = g^p$.
2. On suppose K de caractéristique nulle ou parfait de caractéristique p ; oient $f, g \in K[X]$ avec g irréductible ; on suppose que $g^k | f$ mais que $g^{k+1} \not| f$; montrer que :
   (a) si $p \not| k$ on a $g^{k-1} | f'$ mais que $g^k \not| f'$.
   (b) si $p | k$ on a $g^k | f'$.
3. Montrer que
   (a) Si f et f' sont premiers entre eux montrer que f est sans facteurs multiples.

(b) Supposons K de caractéristique nulle ou parfait de caractéristique p ; si f est sans facteurs multiples montrer que f et f' sont premiers entre eux,

4. Soit $f \in K[X]$, exprimer $\text{pgcd}(f, f')$ en fonction de la décomposition de f en facteurs irréductibles dans les cas où K est de caractéristique nulle ou parfait de caractéristique p. Exprimer la partie sans facteur multiple de f lorsque K est de caractéristique nulle.
5. Montrer que l'on a les conditions équivalentes suivantes :
   (a) f et f' sont premiers entre eux.
   (b) f est sans facteurs multiples dans $L[X]$ pour toute K-extension L.
   (c) f est séparable
6. (a) Si K est de caractéristique nulle ou parfait de caractéristique p montrer que les conditions précédentes équivalents à ce que f n'a pas de facteur multiple.
   (b) Soit $K = \mathbb{F}_p(T)$; vérifier que le polynôme $f = X^p - T \in K[X]$ est sans facteur multiple mais n'est pas séparable.

Corrigé.

1.
Soit $f = \sum_{i=0}^{n} a_i X^i$ on a $f' = \sum_{i=1}^{n} a_i X^{i-1}$.
(a) Si K est de caractéristique nulle on a $a_i = 0$ pour $i \geq 1$ d'où $f = a_0$.
(b) Si K est de caractéristique p, on a $a_i = 0$ pour tout $i \geq 1$ non divisible par p de sorte que $f = \sum_{i=0}^{[n/p]} a_{ip} X^{ip} = g(X^p)$.
(c) Soit $\mathcal{F} : x \to x^p$ le morphisme de Frobenius de K ; ce morphime est injectif (comme tout morphisme de corps) ; *par définition* si parfait de caractéristique p c'est un isomorphisme. Prenant $g = \sum_{i=0}^{r} c_i X^i$, on a $c_i = \widetilde{c_i}^p$ pour $0 \leq i \leq r$ de sorte que $f = \widetilde{g}^p$ avec $\widetilde{g} = \sum_{i=0}^{r} \widetilde{c_i} X^i$.

2.
Soit $f \in K[X]$ avec K de caractéristique nulle ou parfait de caractéristique p, g est un facteur irréductible de f et $k \geq 1$ le plus grand entier tel que $g^k | f$.
(a) on suppose que p ne divise pas k : on a $f = g^k h$ avec g ne divise pas h ; or $f' = kg'g^{k-1}h + g^k h'$. On a $kg'g^{k-1}h \neq 0$ puisque d'une part p ne divise pas k et d'autre part $g' \neq 0$ sinon on aurait $g = \widetilde{g}^p$ et g ne serait pas irréductible. Ainsi $g^{k-1} | f'$. De plus si g^k divisait f' on aurait g qui diviserait $g'h$ et comme g ne divise pas h on aurait g qui diviserait g' d'après le lemme d'Euclide d'où $g' = 0$ ce qui contredit l'irréductibilité de g.
(b) on suppose que $p | k$: on a $f' = g^k h'$ et $g^k | f'$.

3.
$(a) \Rightarrow (b)$ Supposons que f possède un facteur multiple ; il existe donc un polynôme irréductible g tel que $f = g^k h$ avec g ne divise pas h et $k \geq 2$. On a $f' = kg'g^{k-1}h + g^k h'$ de sorte que g divise f' par suite f et f' *ne sont pas* premiers entre eux.
$(b) \Rightarrow (a)$ K de caractéristique nulle ou parfait de caractéristique p ; considérons f sans facteur multiple. Soit g un facteur premier de f ; on a $k = 1$ de sorte que d'après 2(b) g ne divise pas f'. Ainsi f et f' sont premiers entre eux.

4.
Supposons K de caractéristique nulle : on a

$$f = f_1^{a_1} \cdots f_r^{a_r}$$

et

$$f' = \sum_{i=1}^{r} a_i f_i' f_i^{a_i - 1} \prod_{\substack{1 \leq j \leq r \\ j \neq i}} f_j^{a_j}$$

de sorte que :

$$\mathrm{pgcd}(f, f') = f_1^{a_1 - 1} \cdots f_r^{a_r - 1}$$

On a ainsi :

$$\frac{f}{\mathrm{pgcd}(f, f')} = f_1 \cdots f_r$$

Supposons K de caractéristique p : on a

$$f = f_1^{a_1} \cdots f_r^{a_r} f_{r+1}^{p\, b_1} \cdots f_{r+s}^{p\, b_s}$$

avec $f_1, \cdots, f_{r+s}$ irréductibles et deux à eux distincts, $r \geq 1$ et $a_1, \cdots, a_r$ non multiples de p et

$$f' = \sum_{i=1}^{r} a_i f_i' f_i^{a_i - 1} \prod_{\substack{1 \leq j \leq r \\ j \neq i}} f_j^{a_j} \prod_{1 \leq k \leq s} f_{r+k}^{p\, b_k}$$

et l'on a :

$$\mathrm{pgcd}(f, f') = f_1^{a_1 - 1} \cdots f_r^{a_r - 1} f_{r+1}^{p\, b_1} \cdots f_{r+s}^{p\, b_s}$$

5.

$(a) \Rightarrow (b)$ si f et f' sont premiers entre eux dans $K[X]$, la formule de Bezout montre que f et f' restent premiers entre eux dans $L[X]$ pour toute K-extension L. D'après 2.(a), f est sans facteur multiple dans $L[X]$.
$(b) \Rightarrow (c)$ En particulier f est sans facteur multiple dans la clôture algébrique $\overline{K}$ de K ; mais les facteurs irréductibles de f sont alors les $X - a$ où $a \in \overline{K}$ est une racine de f de sorte que les racines sont simples.
$(c) \Rightarrow (a)$ Puisque f a toutes ses racines simples dans $\overline{K}$, f et f' sont premiers entre eux dans $\overline{K}$ et comme la formule de Bezout est rationnelle il sont premiers entre eux dans $K[X]$.

6.

Dans le corps $\mathbb{F}_p(T)$ le morphisme de Frobenius n'est pas surjectif.
Le polynôme $f = X^p - T \in \mathbb{F}_p(T)[X]$ vérifie $f' = 0$ mais n'est pas une puissance $p^{\text{ème}}$. Il est irréductible (donc sans facteurs multiples) mais n'est pas séparable : il possède une unique racine $T^{\frac{1}{p}} \in \overline{\mathbb{F}_p(T)}$ qui est d'ordre p.