Concours Agrégation, Mathématiques générales

Leçon 42- Algèbre des polynômes à plusieurs indéterminées. Applications.

Commentaires du jury 2015 :
La leçon ne doit pas se concentrer exclusivement sur les aspects formels ni sur les les polynômes symétriques. Les aspects arithmétiques ne doivent pas être négligés. Il faut savoir montrer l'irréductibilité d'un polynôme à plusieurs indéterminées en travaillant sur un anneau de type $A[X]$, où A est factoriel. Le théorème fondamental sur la structure de l'algèbre des polynômes symétriques est vrai sur $\mathbb{Z}$. L'algorithme peut être présenté sur un exemple. Les applications aux quadriques, aux relations racines cœfficients ne doivent pas être négligées. On peut faire agir le groupe $GL(n,\mathbb{R})$ sur les polynômes à n indéterminées de degré inférieur à 2.
Commentaires du jury 2016 : La leçon ne doit pas se concentrer exclusivement sur les aspects formels ni sur les les polynômes symétriques. Les aspects arithmétiques ne doivent pas être négligés. Il faut savoir montrer l'irréductibilité d'un polynôme à plusieurs indéterminées en travaillant sur un anneau de type $A[X]$, où A est factoriel. Le théorème fondamental sur la structure de l'algèbre des polynômes symétriques est vrai sur $\mathbb{Z}$. L'algorithme peut être présenté sur un exemple. Les applications aux quadriques, aux relations racines cœfficients ne doivent pas être négligées. On peut faire agir le groupe $GL(n,\mathbb{R})$ sur les polynômes à n indéterminées de degré inférieur à 2. S'ils désirent aller plus loin, les candidats peuvent s'aventurer vers la géométrie algébrique et présenter le Nullstellensatz.

Développements conseillés :

(1) L'anneau des polynôme $K[X_1,...,X_n]$ est noethérien, [Fr. F] p. 228 et toute intersection d'hypersurfaces est une intersection finie, [Fr. F] p. 246.
(2) Le théorème de structure de l'algèbre des polynômes symétriques sur un anneau, [F. M. 2] p. 217.
(3) Théorème des zéros et systèmes linéaires, [F. M. 2] p. 271 et exercice ci-dessous.

Exercice 1 Une application du théorème des zéros de Hilbert (dans la question 2 il faut corriger en ... et que T^4+T^3+1 est un PGCD de P et de Q si la caractéristique de K est égale à 2, [Fr. F] p. 246.

Exercice 2 Théorème des zéros et systèmes linéaires, [F. M. 2] p. 271.

(1) *Rappels.*
Soit k un corps algébriquement clos, $A := k[X_1,...,X_n]$ et $I \subset A$ un idéal.
   (a) L'idéal I est de type fini i.e. il existe $P_1,...,P_s \in A$ avec $I = \sum_{1\leq i\leq s} AP_i$ (propriété noethérienne des anneaux de polynômes).
   (b) Soit $\underline{a} := (a_1,a_2,...,a_n) \in k^n$ et $eval_{\underline{a}} : A \to k$ avec $eval_{\underline{a}}(P) = P(\underline{a})$. Alors $\ker eval_{\underline{a}} = \sum_{1\leq i\leq n} A(X_i - a_i)$. Réciproquement les idéaux maximaux de A sont de cette forme (k est algébriquement clos).
   (c) Soit $I = \sum_{1\leq i\leq s} AP_i$ et $V(I) := \{\underline{a} := (a_1,a_2,...,a_n) \in k^n \ |\forall i, eval_{\underline{a}}(P_i) = 0\}$. Le "théorème des zéros de Hilbert" dit que $P \in A,\ P(V(I)) = 0$ si et seulement si il existe $t > 0$ tel que $P^t \in I$.
   (d) Avec les mêmes notations, $V(I) = \emptyset$ si et seulement si $I = A$ autrement dit si il existe $U_i \in A$ avec $\sum_{1\leq i\leq s} U_iP_i = 1$ (cela provient de la caractérisation des idéaux maximaux).
(2) *Le problème*
On donne $A_{s,n} \in M_{s,n}(k)$ et $A_{s,n+1} = (a_{i,j}) \in M_{s,n+1}(k)$ qui est la concaténation de $A_{s,n}$ pour les n premières colonnes et du vecteur colonne ${}^t(a_{1,n+1},...,a_{s,n+1})$.
Pour $1 \leq i \leq s$, on définit $P_i := \sum_{1\leq j\leq n} a_{i,j}X_j - a_{i,n+1}$. Soit $S(k) := \{\underline{x} := (x_1,x_2,...,x_n) \in k^n,\ |\forall i, P_i(\underline{x}) = 0\}$. Il s'agit de montrer que $S(k) = \emptyset$ si et seulement si il existe $\mu_i \in k$ avec $\sum_{1\leq i\leq s} \mu_iP_i = 1$.

(3) *Par l'algèbre linéaire*

(a) Montrer que $S(k) = \emptyset$ si et seulement si $(A_{s,n}) < (A_{s,n+1})$.

Preuve. $S(k) = \emptyset$ *ssi* ${}^t(a_{1,n+1}, ..., a_{s,n+1})$ *n'est pas dans l'image de* $A_{s,n}$ *ce qui compte tenu de l'inclusion* $\operatorname{Im} A_{s,n} \subset \operatorname{Im} A_{s,n+1}$ *équivaut à* $(A_{s,n}) < (A_{s,n+1})$.///

(b) On suppose que $S(k) = \emptyset$, montrer en utilisant le pivot de Gauss sur les lignes qu'il existe $\mu_i \in k$ avec $\sum_{1\leq i\leq s} \mu_i L_i = 0$ et $\sum_{1\leq i\leq s} \mu_i a_{i,n+1} \neq 0$, où L_i est la i-ième ligne de $A_{s,n}$ et conclure.

Preuve. Le pivot de Gauss sur les lignes de la matrice $A_{s,n+1}$ *aboutit à s lignes* $(L'_i, a'_{i,n+1})$ *où* $L'_i := \sum_{1\leq j\leq n} \mu_{j,i} L_j$ *et* $a'_{i,n+1}) := \sum_{1\leq j\leq n} \mu_{j,i} a_{j,n+1}$ *avec les r premières lignes* L'_i *linéairement indépendantes et les suivantes nulles, ainsi* $r = (A_{s,n})$ *et enfin* $a'_{r+1,n+1}) \neq 0$ *puisque* $(A_{s,n}) < (A_{s,n+1})$. *Ainsi* $\sum_{1\leq j\leq s} \mu_{j,r+1} P_j = -\sum_{1\leq j\leq s} \mu_{j,r+1} a_{j,n+1} = -a'_{r+1,n+1} \neq 0$. *On conclut donc en divisant cette égalité par* $a'_{r+1,n+1}$.///

(4) *Par le Nullstellensatz*

Preuve. Remarque. Notons que la partie d) du rappel fournit une CNS pour que $S(k) = \emptyset$ *: Il existe* $U_i \in A = k[X_1, ..., X_n]$ *avec* $\sum_{1\leq i\leq s} U_i P_i = 1$, *mais il ne semble pas possible d'en déduire une relation avec des* $U_i \in k$.///

(a) Soit $f_1, ..., f_t \in A$ des polynômes homogènes de degré 1. Montrer que l'idéal $\sum_{1\leq i\leq t} A f_i$ est un idéal premier de A.

Preuve. Quitte à réordonner on peut supposer que $f_1, ..., f_r$ *sont k-linéairement indépendants et qu'ils engendrent tous les* f_i *alors l'idéal* $I := \sum_{1\leq i\leq r} f_i = \sum_{1\leq i\leq t} f_i$. *On peut alors compléter la famille libre* $(Y_i := f_i,\ 1 \leq i \leq r)$ *par* $(Y_i,\ r+1 \leq i \leq n)$ *en une base du k-espace vectoriel* $H_{1,n} := \sum_{1\leq i\leq n} X_i$ *des polynômes homogènes de degré* 1. *Alors* $A = k[Y_1, ..., Y_n]$ *et donc* $\frac{A}{I} \simeq k[Y_{r+1}, ..., Y_n]$ *est intègre.*///

(b) Soit $\tilde{P}_i := \sum_{1\leq j\leq n} a_{i,j} Y_j - a_{i,n+1} Y_{n+1} \in k[Y_1, ..., Y_{n+1}]$. Montrer que $S(k) = \emptyset$ si et seulement si $V(\tilde{P}_i) \subset V(Y_{n+1})$.

Preuve. On a $V(\tilde{P}_i) = \{(y_1, ..., y_{n+1})\}$ *avec* $y_{n+1} = 0$ *et* $\sum_{1\leq j\leq n} a_{i,j} y_j = 0$ *union* $y_{n+1} \neq 0$ *et* $(\frac{y_1}{y_{n+1}}, ..., \frac{y_n}{y_{n+1}}) \in S(k)$.///

(c) En déduire que $S(k) = \emptyset$ si et seulement si il existe $m > 0$ avec $Y_{n+1}^m \in \sum_{1\leq i\leq s} \tilde{P}_i k[Y_1, ..., Y_{n+1}]$.

Preuve. Cela suit immédiatement de la question précédente et du Nullstellensatz qui reste vrai si k n'est pas algébriquement clos.

(d) Déduire de a) que l'on peut supposer que $m = 1$

Preuve. Par a) il suit que l'idéal $\sum_{1\leq i\leq s} \tilde{P}_i k[Y_1, ..., Y_{n+1}]$ *est premier , ainsi* $Y_{n+1} \in \sum_{1\leq i\leq s} \tilde{P}_i k[Y_1, ..., Y_{n+}$

(e) Conclure.

Preuve. Ainsi $Y_{n+1} = \sum_{1\leq i\leq s} U_i \tilde{P}_i$ *avec* $U_i \in k[Y_1, ..., Y_{n+1}]$. *Par l'unicité de la décomposition en composantes homogènes il suit que* $Y_{n+1} = \sum_{1\leq i\leq s} \mu_i \tilde{P}_i$ *où* $\mu_i \in k$ *est la composante homogène de degré* 0 *de* U_i. *On conclut en spécialisant à* $Y_{n+1} = 1$.///

Exercice 3 Le complémentaire d'une hypersurface est un ouvert dense, [Fr. F] exercice 2.8.12 p. 127.

Exercice 4 Une courbe plane dans $\mathbb{C}^2$ n'a pas de point isolé, [F. M. 2] lemme p. 209.

Soit $P(X, Y) \in \mathbb{C}[X, Y]$ et n est son degré total. On veut montrer que les zéros de $P(X, Y)$ dans $\mathbb{C} \times \mathbb{C}$ ne sont pas isolés. Quitte à faire une translation on suppose que $P(0, 0) = 0$

1. Montrer qu'il existe $c \in \mathbb{C}$ avec $P(X + cY, Y) = p_0(X) + p_1(X)Y + ... + p_n(X)Y^n$ avec $p_i(X) \in \mathbb{C}[X]$, et $deg_i(p_i(X)) \leq n - i$ et $p_n(X) \in \mathbb{C} - \{0\}$.

Preuve. $P = \sum_{0\leq i\leq n} P_i$ la décomposition de P en composantes homogènes alors $P_n \neq 0$. Puisque le degré total de P est égal à n, seul P_n est susceptible de contribuer au coefficient de Y^n dans $P(X+cY,Y)$. On écrit alors $P_n = \sum_{0\leq k\leq n} a_k X^{n-k}Y^k$, alors le coefficient de Y^n dans $P_n(X+cY,Y)$ vaut $\sum_{0\leq k\leq n} a_k c^{n-k}$. Puisque $(a_0, a_1, ..., a_n) \neq (0, 0, ..., 0)$ il suit qu'il existe $c \in \mathbb{C}$ avec $\sum_{0\leq k\leq n} a_k c^{n-k} \neq 0$.

2. On suppose donc que $P = p_0(X) + p_1(X)Y + ... + p_n(X)Y^n$ avec $p_n(X) \in \mathbb{C} - \{0\}$ et $P(0,0) = 0$. Pour pour tout $k > 0$ on note $Q_k(Y) := P(\frac{1}{k}, Y)$, et on note $y_i(k), 1 \leq i \leq n$ les n racines de $Q_k(Y)$ dans $\mathbb{C}$ avec $|y_1(k)| \leq |y_2(k)|... \leq |y_n(k)|$. Montrer que la suite $(\frac{1}{k}, y_1(k))$ converge vers $(0,0)$ et conclure.

Preuve. En effet $|y_1(k)|^n \leq \prod_{1\leq i\leq n} |y_i(k)| = \frac{|p_0(\frac{1}{k})|}{|p_n|} \to 0$.

Exercice 5 Le polynôme $X^a - Y^b \in k[X,Y]$ avec $\text{pgcd}(a,b) = 1$ est irréductible, [F. M. 2] p. 190. Notez le lien avec le semi-groupe $\mathbb{N}a + \mathbb{N}b$ et le théorème de Sylvester, [F. M. 2] p. 194.

Soit k un corps commutatif et a, b deux entiers > 0. Soit $\mathcal{P}$ l'idéal $(X^a - Y^b) \subset k[X,Y]$.

(1) On suppose que $(a,b) = (2,3)$.

(a) Montrer qu'il existe un unique homomorphisme f de k-algèbres de $k[X,Y]$ dans $k[Z]$ tel que $f(X) = Z^b$ et $f(Y) = Z^a$.

Preuve. C'est la propriété universelle des anneaux de polynômes. ///

(b) Montrer que $\text{Ker}\, f = \mathcal{P}$ (on pourra faire la division de $Q \in \text{Ker}\, f$ par $X^2 - Y^3$ dans l'anneau $(k[Y])[X]$).

Preuve. Puisque $f(X^a - Y^b) = (Z^b)^a - (Z^a)^b = 0$, il suit que $\mathcal{P} \subset \text{Ker}\, f$. Soit donc $Q \in \text{Ker}\, f$, on fait la division de Q par $X^2 - Y^3$ dans l'anneau $(k[Y])[X]$. Ainsi $Q = U(X^2 - Y^3) + V$ avec $U \in (k[Y])[X]$ et $V = S(Y) + T(Y)X$ où $S(Y), T(Y) \in k[Y]$. Alors $0 = f(Q) = f(V) = S(Z^2) + T(Z^2)Z^3$. On écrit $S(Y) = s_0 + s_1Y + ... + s_dY^d$, $T(Y) = t_0 + t_1Y + ... + t_dY^d$. Alors $S(Z^2)+T(Z^2)Z^3 = \sum_i s_iZ^{2i} + \sum_i t_iZ^{2i+3} = 0$. Et puisque $2i+3$ est impair il suit que $s_i = t_i = 0$, ainsi $V = 0$ et donc $Q = U(X^2 - Y^3) \in \mathcal{P}$. ///

(c) Montrer que $\mathcal{P}$ est un idéal premier de $k[X,Y]$ qui n'est pas maximal.

Preuve. L'homomorphisme f induit un isomorphisme d'anneau de $\frac{k[X,Y]}{\mathcal{P}}$ avec $\text{Im}\, f \subset k[Z]$, il est donc intègre et donc $\mathcal{P}$ est un idéal premier. Puisque le seul sous corps de $k[Z]$ contenant k est $k \neq \text{Im}\, f$, il suit que $\mathcal{P}$ n'est pas maximal. ///

(d) Montrer que $X^2 - Y^3$ est irréductible dans $k[X,Y]$.

Preuve. Puisque $\mathcal{P} = (X^2 - Y^3)$ est premier le résultat suit. ///

(e) Montrer que $Z^i \in k[Z^2, Z^3]$ si et seulement si $i \neq 1$ et en déduire que $\text{Im}\, f$ est un sous-k-espace vectoriel de $k[Z]$ de codimension 1.

Preuve. Soit $i \geq 3$, puisque $(2,3) = 1$, il existe $u, v \in \mathbb{Z}$ avec $i = 2u + 3v$. La division euclidienne donne $v = 2w + r$ avec $r \in \{0,1\}$. Ainsi $i = 2(u + 3w) + 3r$ et puisque $i - 3r \geq 0$, il suit que $u+3w \geq 0$; ainsi $Z^i = f(X^{u+3w}Y^r) \in \text{Im}\, f$. Soit $Q \in k[X,Y]$, on peut écrire $Q = U(X^2-Y^3)+V$ avec $U \in (k[Y])[X]$ et $V = S(Y)+T(Y)X$; alors $f(Q) = f(V) = S(Z^2)+T(Z^2)Z^3$ et par ce qui précède $Z^2k[Z] \subset \text{Im}\, f$. Ainsi $\text{Im}\, f = k[Z^2] + Z^2k[Z] = k \bigoplus_{I\geq 2} kZ^i$ et $\text{Im}\, f$ est l'hyperplan $\text{Ker}\, \varphi$ où $\varphi(\sum_{i\geq 0} a_iZ^i) = a_2$. ///

Plus généralement, on suppose que a et b sont premiers entre eux. Montrer que $(X^a - Y^b)$ est un idéal premier de de $k[X,Y]$ et que $k[Z^a, Z^b]$ est un sous-k-espace vectoriel de $k[Z]$ de codimension $\leq (a-1)(b-1)$ (Sylvester a montré que cette codimension est : $\frac{(a-1)(b-1)}{2}$, voir correction).

Preuve. On considère l'unique homomorphisme f de k-algèbres de $k[X,Y]$ dans $k[Z]$ tel que $f(X) = Z^b$ et $f(Y) = Z^a$. On a $\mathcal{P} \subset \text{Ker}\, f$. Soit donc $Q \in \text{Ker}\, f$, on fait la division de Q par $X^a - Y^b$ dans l'anneau $(k[Y])[X]$. Ainsi $Q = U(X^a - Y^b) + V$ avec $U \in (k[Y])[X]$ et $V = S_0(Y) + S_1(Y)X + ... + S_{a-1}(Y)X^{a-1}$ où $S_i(Y) \in k[Y]$. Alors $0 = f(Q) = f(V) = S_0(Z^a)+S_1(Z^a)Z^b+...+S_{a-1}(Z^a)Z^{b(a-1)}$.

Il s'agit de voir que les contributions ne se mélangent pas. Les contributions de $S_i(Z^a)Z^{bi}$ sont dans les monômes de degré $ja+bi$ avec $j \in \mathbb{N}$. Or l'égalité $ja+bi = j'a+bi'$ avec $0 \leq i, i' < a$ devient $(j-j')a = (i'-i)b$ et puisque $(a,b)=1$ il suit que $a|(i'-i)$ et donc $i=i'$ et $j=j'$. Ainsi $S_i(Y)=0$ et donc $V=0$. On conclut alors comme dans le cas particulier.

Le point délicat est le calcul de la codimension de $\operatorname{Im} f = k[Z^a, Z^b]$ *dans* $k[Z]$.

(a) *Si $0 \leq n < ab$, il existe au plus un couple $(i,j) \in \mathbb{N} \times \mathbb{N}$ avec $n = ia+jb$.*

Preuve. Supposons que $n = ia+jb < ab$ avec $(i,j) \in \mathbb{N} \times \mathbb{N}$ alors $0 \leq i < b$ et $0 \leq j < a$.

Alors $ia+jb = i'a+j'b$ avec $0 \leq i, i' < b$ devient $(j-j')a = (i'-i)b$ et puisque $(a,b)=1$ il suit que $b|(i'-i)$ et donc $i=i'$ et $j=j'$.

(b) *Si $(a-1)(b-1) = ab-a-b+1 \leq n$, il existe au moins un couple $(i,j) \in \mathbb{N} \times \mathbb{N}$ avec $n = ia+jb$.*

Preuve. Puisque $(a,b)=1$, il existe $u, v \in \mathbb{Z}$ avec $n = au+bv$. La division euclidienne donne $v = wa+r$ avec $r \in \{0, .., a-1\}$. Ainsi $n = (u+wb)a + rb \geq (a-1)(b-1)$ i.e. $(u+wb)a \geq (a-1-r)b - a + 1 \geq -a+1$. Ainsi $u+wb \geq -1 + \frac{1}{a}$ et il suit que $u+wb \geq 0$ et puisque $r \geq 0$, il suit que $n \in a\mathbb{N} + b\mathbb{N}$.

(c) *La codimension est : $\frac{(a-1)(b-1)}{2}$.*

Si $n \geq ab-a-b+1$ on a $n \in a\mathbb{N}+b\mathbb{N}$ et donc $Z^n \in k[Z^a, Z^b]$. Il s'agit donc de calculer le cardinal des $0 \leq n \leq ab-a-b$ avec $n \notin a\mathbb{N}+b\mathbb{N}$.

Voici la solution de Sylvester. Notons S les entiers de l'intervalle $[0, ab-a-b]$ dans $a\mathbb{N}+b\mathbb{N}$ et S' le complémentaire. Le point clé est que la symétrie σ par rapport à $\frac{(a-1)(b-1)-1}{2}$ (ce n'est pas un entier puisque $(a-1)(b-1)$ est pair) échange S et S'. Soit $c = ax+by \in S$ avec $x, y \geq 0$ alors $\sigma(c) = ab-a-b-c$. Supposons que $\sigma(c) = az+bt$ avec $z, t \geq 0$ et montrons une contradiction. On a donc $ab = c+\sigma(c)+a+b = a(x+z+1)+b(y+t+1)$ et donc $b|(x+z+1)$ et $a|(y+t+1)$. Mais puisque $x+z+1 \geq 1$ et $y+t+1 \geq 1$ il suit que $a(x+z+1)+b(y+t+1) \geq 2ab$. Contradiction. Ainsi $|S'| = |S| = \frac{(a-1)(b-1)}{2}$.

Une autre preuve consiste à remarquer que les polynômes $P := 1+X^a+X^{2a}+...+X^{ba}$ et $Q := 1+X^b+X^{2b}+...+X^{ab}$ sont des polynômes réciproques et ainsi il en est de même du produit PQ. On développe PQ. On remarque que $ia+jb = i'a+j'b$ avec $0 \leq i, i' \leq b$ et $0 \leq j, j' \leq a$ implique $i=i'$ et $j=j'$ ou $ia+jb = ba+0b = 0a+ab$. Ainsi les coefficients de PQ sont égaux à 0 ou 1 sauf le coefficient de X^{ab} qui vaut 2. On décompte de deux manières la valeur $P(1)Q(1) = (a+1)(b+1)$. C'est aussi 2 plus 2 fois le nombre de monômes X^i de PQ avec $i \in [0, ab-1]$. On scinde l'intervalle en $[0, ab-a-b]$ et $[ab-a-b+1, ab-1]$. Avec les notations précédentes $(a+1)(b+1) = 2+2(|S|+(ab-1)-(ab-a-b+1)+1)$. D'où $|S| = \frac{(a-1)(b-1)}{2}$.

(2) *Preuve. Complément : le dénumérant.*

Une formule pour le dénumérant $p(n) := |\{(i,j) \in \mathbb{N} \times \mathbb{N} \mid ia+jb = n|$ de n.

On note $F := \sum_{0 \leq n} p(n)X^n \in \mathbb{C}[[X]]$, la série génératrice des $p(n)$. On vérifie que $F = \frac{1}{(1-X^a)(1-X^b)}$.

(a) *On montre que $p(n+ab) = p(n)+1$ pour $n \geq 0$.*

On remarque que $(1-X)(1-X^{ab})F \in \mathbb{C}[X]$. En effet $\frac{(1-X^a)(1-X^b)}{1-X} \in \mathbb{C}[X]$, n'a que des racines simples qui sont toutes des racines ab-ièmes de 1 ; ainsi $(1-X^{ab}) = N(X)\frac{(1-X^a)(1-X^b)}{1-X}$ où $N(X) \in \mathbb{C}[X]$ est de degré $\leq ab-a-b+1$, de plus $N(1)=1$. Ainsi donc $(1-X^{ab})F = \frac{X^{ab-a-b+1}}{1-X} + P(X)$ avec $P(X) = \frac{N(X)-X^{ab-a-b+1}}{1-X} \in \mathbb{C}[X]$ de degré $ab-a-b$.

(b) *On montre que P est un polynôme réciproque (on retrouve ainsi la symétrie dans les preuves précédentes).*

On a $P = \frac{(1-X)(1-X^{ab})-X^{ab-a-b+1}(1-X^a)(1-X^b)}{(1-X)(1-X^a)(1-X^b)}$ et $X^{ab-a-b}P(\frac{1}{X}) = P(X)$.

(c) *On détermine les coefficients de $p(n)$, pour $0 \leq n \leq ab$.*

Puisque $F = P + \frac{X^{ab-a-b+1}}{1-X} + X^{ab}F$ et que $\deg P \leq ab-a-b$, il suit que $P = \sum_{0 \leq n \leq ab-a-b} p(n)X^n$ avec $p(n) \in \{0,1\}$ par (2)(a). Puisque P est réciproque on retrouve le retrouve le résultat de Sylvester sur le nombre de "trous".

En fait on peut donner une formule pour $p(n)$. Voyons d'abord quelques notations.

Si $0 \leq n \leq ab-a-b$ alors $p(n) \in \{0,1\}$ et si on note $1 \leq a'(n) \leq b$ l'entier tel que $a'(n)a = -n \mod b$ et $1 \leq b'(n) \leq a$ l'entier tel que $b'(n)b = -n \mod a$ alors $ab|(a'(n)a+b'(n)b+n)$ et puisque $0 < a'(n)a + b'(n)b + n < 3ab$, alors $(a'(n)a + b'(n)b + n) = ab$ ou $2ab$.

(i) *Cas 1. Si $a'(n)a + b'(n)b + n = ab$, alors $p(n) = 0$.*

Supposons que $p(n) > 0$, ainsi il existe $i, j \geq 0$ avec $ia+jb = n$ et donc $a'(n)a+b'(n)b+ia+jb = ab$ c'est à dire $(a'(n)+i)a + (b'(n)+j)b = ab$; ainsi $0 < b'(n) + j \leq a$ et $0 < a'(n) + i \leq b$ et $a = b'(n) + j$ et $b = a'(n) + i$. Il suit que $2ab = ab$ ce qui donne une contradiction.

(ii) *Cas 2. Si $a'(n)a + b'(n)b + n = 2ab$, alors $p(n) = 1$.*

On remarque que $n = a(b - a'(n)) + b(a - b'(n))$. Ainsi $p(n) = 1$.

Au final on obtient pour $n \geq 0$ la formule $p(n) = \frac{n+a'(n)a+b'(n)b}{ab} - 1$. ///

Exercice 6 L'espace vectoriel $H_{d,n}$ des polynômes homogènes de degré d à n indéterminées et puissances d-ièmes des polynômes homogènes de degré 1, [Fr. A] ex. 1.4.14 p. 82.

Soit K un corps commutatif de caractéristique nulle. Soit $H_{d,n}$ le sous-K-espace vectoriel de $K[X_1, X_2, ..., X_n]$ des polynômes homogènes de degré d auxquels on adjoint $\{0\}$. Soit $A_d := \{\alpha := (\alpha_1, ..., \alpha_n) \in \mathbb{N}^n \mid \alpha_1 + ... + \alpha_n = d\}$. Si $P \in H_{d,n}$. on pose $\Delta_\alpha(P) = \frac{\partial^d}{\partial^{\alpha_1} X_1 ... \partial^{\alpha_n} X_n}(P) \in K$.

(1) (a) Montrer que $(\frac{1}{\alpha_1!...\alpha_n!}\Delta_\alpha)_{\alpha \in A_d}$ est la base duale de la base $(X^\alpha)_{\alpha \in A_d}$ de $H_{d,n}$.

Preuve. Soit $\alpha := (\alpha_1, ..., \alpha_n) \in \mathbb{N}^n$ et $\beta := (\beta_1, ..., \beta_n) \in \mathbb{N}^n$ avec $\alpha_1 + ... + \alpha_n = \beta_1 + ... + \beta_n = d$. Si $\alpha = \beta$ on a $\Delta_\alpha(X_1^{\alpha_1} X_2^{\alpha_2} ... X_n^{\alpha_n}) = \alpha_n! \frac{\partial^{d-\alpha_n}}{\partial^{\alpha_1} X_1 ... \partial^{\alpha_{n-1}} X_{n-1}}(X_1^{\alpha_1} X_2^{\alpha_2} ... X_{n-1}^{\alpha_{n-1}}) = ... = \alpha_n!\alpha_{n-1}!...\alpha_1!$. Si $\alpha \neq \beta$, puisque $\alpha_1 + ... + \alpha_n = \beta_1 + ... + \beta_n = d$, il existe i_0 avec $\alpha_{i_0} > \beta_{i_0}$, alors $\frac{\partial^{\alpha_{i_0}}}{\partial^{\alpha_{i_0}} X_{i_0}}(X_1^{\beta_1} X_2^{\beta_2} ... X_n^{\beta_n}) = 0$ et donc $\Delta_\alpha(X_1^{\beta_1} X_2^{\beta_2} ... X_n^{\beta_n}) = 0$. ///

(b) Soit $Q := a_1X_1 + a_2X_2 + ... + a_nX_n$, montrer que $\Delta_\alpha(Q^d) = d!a_1^{\alpha_1}...a_n^{\alpha_n}$.

Preuve. Puisque $\frac{\partial}{\partial X_1}(Q^d) = da_1Q^{d-1}$, il suit que $\frac{\partial^{\alpha_1}}{\partial X_1^{\alpha_1}}(Q^d) = d(d-1)...(d-\alpha_1+1)a_1^{\alpha_1}Q^{d-\alpha_1}$ d'où le résultat en dérivant par rapport aux autres variables.

Remarque. On retrouve ainsi la formule du multinôme $(\sum_{1 \leq i \leq n} X_i)^d = \sum_{\alpha \in A_d} \frac{d!}{\alpha_1!...\alpha_n!} X_1^{\alpha_1} X_2^{\alpha_2} ... X_n^{\alpha_n} \in \mathbb{Z}[X_1, ..., X_n]$. ///

(c) Soit $f := \sum_{\alpha \in} \lambda_\alpha \Delta_\alpha \in H_{d,n}^\star$ avec $\lambda_\alpha \in K$. Calculer $f((a_1X_1 + a_2X_2 + ... + a_nX_n)^d)$.

Preuve. Par la question précédente on a $f(Q^d) = \sum_{\alpha \in A_d} \lambda_\alpha \Delta_\alpha(Q^d) = d! \sum_{\alpha \in A_d} \lambda_\alpha a_1^{\alpha_1}...a_n^{\alpha_n} = d!P(a_1, ..., a_n)$ où $P = \sum_{\alpha \in A_d} \lambda_\alpha X_1^{\alpha_1}...X_n^{\alpha_n} \in H_{d,n}$. ///

(d) Soit K est un corps infini, montrer par récurrence sur n que l'application K-linéaire *eval* : $K[X_1, X_2, ..., X_n] \to K^{K^n}$ définie par $eval(P)(a_1, ..., a_n) = P(a_1, ..., a_n)$ est injective.

Preuve. La preuve se fait par récurrence sur le nombre d'indéterminées. Si $n = 1$, un polynôme non nul n'a qu'un nombre fini de zéros. Supposons le résultat acquis pour $K[X_1, ..., X_{n-1}]$. Soit $P \in K[X_1, ..., X_n] = K[X_1, ..., X_{n-1}][X_n]$, ainsi $P = p_0(X_1, ..., X_{n-1}) + p_0(X_1, ..., X_{n-1})X_n + ... + p_k(X_1, ..., X_{n-1})X_n^k + ... + p_d(X_1, ..., X_{n-1})X_n^d$. Soit $(x_1, .., x_{n-1}) \in k^{n-1}$, alors $P(x_1, .., x_{n-1}, X_n) = p_0(x_1, ..., x_{n-1}) + p_0(x_1, ..., x_{n-1})X_n + ... + p_k(x_1, ..., x_{n-1})X_n^k + ... + p_d(x_1, ..., x_{n-1})X_n^d \in K[X_n]$ a en particulier une infinité de zéros (K est infini) et donc $p_k(x_1, ..., x_{n-1}) = 0$ pour $0 \leq k \leq n$ et $(x_1, ..., x_{n-1}) \in K^{n-1}$. Ensuite l'hypothèse de récurrence montre que $p_k = 0$ et donc au final $P = 0$. ///

(e) Déduire de la question précédente que si $f \in H^\star_{d,n}$ est nulle sur le sous-espace vectoriel V de $H_{d,n}$ engendré par les puissances d-ièmes des polynômes homogènes de degré 1 alors $f = 0$.
Preuve. Immédiat par ce qui précède.

(f) En déduire que $V = H_{d,n}$.
Preuve. En effet par ce qui précède, il suit que l'orthogonal V^0 de V pour la dualité est $\{0\}$. ///

(2) Montrer que $X_1X_2^{p-1}$ n'est pas combinaison linéaire de puissances p-ièmes de polynômes homogènes de degré 1 si la caractéristique de K est égale à $p > 0$.
Preuve. En effet $\frac{\partial}{\partial X_1}(X_1X_2^{p-1}) = X_2^{p-1}$. Or si $L \in H_{1,n}$ alors $\frac{\partial}{\partial X_1}(L^p) = 0$ (la caractéristique de K vaut p). ///

Questions annexes :
i. Faites le lien avec les formes quadratiques dans le cas des polynômes homogènes de degré 2
ii. Calcul de la dimension de $H_{d,n}$. Voir [F. M. 1] $n^\circ 1$ pour deux calculs (la preuve avec les séries formelles permet de retrouver facilement la formule). Il y a enfin une preuve combinatoire qui est élémentaire : se donner un n-uplet $(i_1, i_2, ..., i_n)$ avec $i_1 + i_2 + ... + i_n = d$ revient à se donner dans l'intervalle $[1, n + d - 1]$, $n - 1$ entiers (des séparations) placés en $i_1 + 1$, $i_1 + i_2 + 2$,...,$i_1 + i_2 + ... + i_{n-1} + n - 1$. Le nombre de telles séparations est donc le nombre de façons de choisir $n - 1$ boules parmi $n + d - 1$. C'est donc $\binom{n+d-1}{n-1}$, [A. F.] p. 99 et 100.

Exercice 7 On note $A := \mathbb{Z}[X_1, X_2, X_3]$. Soit $D := (X_1 - X_2)^2(X_1 - X_3)^2(X_2 - X_3)^2 \in A$. On note Σ_1, Σ_2, Σ_3 les polynômes symétriques élémentaires $\in A$. Soit $S_1 := X_1 + X_2$ et $S_2 := X_1X_2$.

(1) (a) Montrer que $D(X_1, X_2, 0) = S_1^2S_2^2 - 4S_2^3$.
Preuve. On a $(X_1 - X_2)^2 = S_1^2 - 4S_2$.///

(b) En déduire que $D(X_1, X_2, X_3) = \Sigma_1^2\Sigma_2^2 - 4\Sigma_2^3 + \Sigma_3 h$ où $h \in A$ est homogène et symétrique.
Preuve. Soit $P(X_1, X_2, X_3) := D(X_1, X_2, X_3) - \Sigma_1^2\Sigma_2^2 + 4\Sigma_2^3$. On remarque que P est symétrique et que $P(X_1, X_2, 0) = 0$. Ainsi $P(X_1, X_2, X_3) = X_3Q(X_1, X_2, X_3)$ où $Q \in \mathbb{Z}[X_1, X_2, X_3]$. Soit $\sigma \in S_3$ alors $\sigma \star P(X_1, X_2, X_3) = P(X_{\sigma(1)}, X_{\sigma(2)}, X_{\sigma(3)}) = X_{\sigma(3)}Q(X_{\sigma(1)}, X_{\sigma(2)}, X_{\sigma(3)})$. Ainsi X_i divise $P(X_1, X_2, X_3)$ pour $i = 1, 2, 3$ ainsi les monômes qui contribuent dans l'écriture de P sont des $X_1^{i_1}X_2^{i_2}X_1^{i_2}$ avec $i_j > 0$ pour tout j et donc Σ_3 divise P. Or P est un polynôme homogène et l'unicité de la décomposition en composantes homogènes montre qu'il en est donc de même pour h. Enfin P est symétrique et puisque Σ_3 n'est pas diviseur de 0 dans $\in \mathbb{Z}[X_1, X_2, X_3]$ il suit que h est symétrique.///

(c) Montrer qu'il existe $a, b, c \in \mathbb{Z}$ tels que $h = a\Sigma_1^3 + b\Sigma_1\Sigma_2 + c\Sigma_3$.
Preuve. En effet h est symétrique. Ainsi $h \in \mathbb{Z}[X_1, X_2, X_3]^{S_3} = \mathbb{Z}[\Sigma_1, \Sigma_2, \Sigma_3]$. Enfin h est homogène de degré 3 dans les indéterminées X_i. Puique $\Sigma_1^{i_1}\Sigma_2^{i_2}\Sigma_3^{i_3}$ est homogène de degré $i_1 + 2i_2 + 3i_3$, le résultat suit de l'unicité de la décomposition en composantes homogènes.///

(d) Déterminer a, b, c.
Preuve. En spécialisant en $(X_1, X_2, X_3) = (1, 1, -2)$ on obtient $c = -27$. Puis en $(X_1, X_2, X_3) = (2, 2, -1)$ on obtient $a = -4$. Enfin avec $(X_1, X_2, X_3) = (1, 1, 1)$ on obtient $b = 18$. Ainsi $D(X_1, X_2, X_3) = \Sigma_1^2\Sigma_2^2 - 4\Sigma_2^3 + 18\Sigma_1\Sigma_2 - 27\Sigma_3^2 =: \Delta(\Sigma_1, \Sigma_2, \Sigma_3)$.///

(2) On note $P_3 := \mathbb{C}[X]_3$ le $\mathbb{C}$-espace affine des polynômes unitaires de degré 3. Montrer que le sous-ensemble de P_3 des polynômes séparables est un ouvert de P_3.
Preuve. Si $P(X) = X^3 - \sigma_1X^2 + \sigma_2X - \sigma_3 \in P_3$ et si $x_1, x_2, x_3 \in \mathbb{C}$ sont ses racines alors $\Sigma_i(x_1, x_2, x_3) = \sigma_i$ ainsi P est séparable si et seulement si $\Delta(\sigma_1, \sigma_2, \sigma_3) = D(x_1, x_2, x_3) \neq 0$.///

Exercice 8 Résolution par radicaux de l'équation $\{x \in \mathbb{C},\ P(x) = 0\}$ avec $P(X) := X^3 + pX + q \in \mathbb{C}[X]$ et polynômes symétriques.

Notations. On note $\mathcal{S}_3$, le groupe symétrique sur $\{1,2,3\}$, il est engendré par les cycles $r := (1,2,3)$ et $s := (2,3)$. Le groupe $\mathcal{S}_3$ agit sur $\mathbb{C}[X_1,X_2,X_3]$ par $\sigma \star P(X_1,X_2,X_3) = P(X_{\sigma(1)},X_{\sigma(2)},X_{\sigma(3)})$ et $\mathbb{C}[X_1,X_2,X_3]^{\mathcal{S}_3}$ est le sous-anneau des polynômes symétriques.

Enfin $j := e^{2i\pi/3} \in \mathbb{C}$, $U := X_1 + jX_2 + j^2X_3$ et $V := s \star U$.

(1) (a) Montrer que $r \star U^3 = U^3$.
Preuve. On a $r \star U = X_2 + jX_3 + j^2X_1 = j^2U$. ///

(b) En déduire que $S := U^3 + V^3 \in \mathbb{C}[X_1,X_2,X_3]^{\mathcal{S}_3}$.
Preuve. Puisque $s \star U = V$ *et que* $s^2 = Id$ *il suit que* $s \star S = S$. *Enfin* $r \star V = rs \star U = sr^{-1} \star U = s \star U = V$. *Ainsi* $\mathcal{S}_3$ *agit trivialement sur* S. ///

(c) Montrer que $S(X_1,X_2,0) = 2(X_1+X_2)^3 - 9X_1X_2(X_1+X_2)$.
Preuve. On calcule $S(X_1,X_2,0) = (X_1+jX_2)^3 + (X_1+j^2X_2)^3 = X_1^3 + 3j^2X_1^2X_2 + 3jX_1X_2^2 + X_2^3 + X_1^3 + 3jX_1^2X_2 + 3j^2X_1X_2^2 + X_2^3 = 2(X_1+X_2)^3 - 9X_1X_2(X_1+X_2)$. ///

(d) En déduire que $S - 2(X_1+X_2+X_3)^3 + 9(X_1X_2+X_2X_3+X_3X_1)(X_1+X_2+X_3) = \lambda X_1X_2X_3$.
Preuve. On applique l'algorithme vu dans la leçon. On remarque que $T := S - 2(X_1+X_2+X_3)^3 + 9(X_1X_2+X_2X_3+X_3X_1)(X_1+X_2+X_3) \in \mathbb{C}[X_1,X_2,X_3]^{\mathcal{S}_3}$ *et que* $T(X_1,X_2,0) = 0$, *ainsi* $T \in X_3\mathbb{C}[X_1,X_2,X_3]$. *Ainsi* $T = r \star T \in X_1\mathbb{C}[X_1,X_2,X_3]$ *et* $T = r^2 \star T \in X_2\mathbb{C}[X_1,X_2,X_3]$. *Ainsi dans la décomposition de* T *sur la base* $X_1^{i_1}X_2^{i_2}X_3^{i_3}$ *les coefficients des monômes avec* $i_1i_2i_3 = 0$ *sont nuls ainsi* $T \in X_1X_2X_3\mathbb{C}[X_1,X_2,X_3]$. *Pour conclure on remarque que* T *est homogène de degré* 3. ///

(e) Calculer λ.
Preuve. On évalue l'égalité précédente en $(1,1,1)$. *Ainsi* $0 - 2.3^3 + 9.3.3 = 27 = \lambda$. ///

(2) Soit $P := X^3 + pX + q = (X-x_1)(X-x_2)(X-x_3) \in \mathbb{C}[X]$. On note $u := U(x_1,x_2,x_3), v := V(x_1,x_2,x_3)$.

(a) En remarquant que $UV = (X_1+X_2+X_3)^2 - 3(X_1X_2+X_2X_3+X_3X_1)$, exprimer x_1,x_2,x_3 à l'aide de radicaux en p,q.
Preuve. On a $(X-x_1)(X-x_2)(X-x_3) = X^3 - (x_1+x_2+x_3)X^2 + (x_1x_2+x_2x_3+x_3x_1)X - x_1x_2x_3$. *Ainsi* $x_1+x_2+x_3 = 0$, $x_1x_2+x_2x_3+x_3x_1 = p$ *et* $x_1x_2x_3 = -q$. *Ainsi* $u^3+v^3 = S(x_1,x_2,x_3) = -27q$ *et* $uv = -3p$. *Il suit que* u^3, v^3 *sont les deux racines du polynôme* $X^2+27q-27p^3$. *Son discriminant est* $\Delta = 27(4p^3+27q^2) = \varpi^2$ *avec* $\varpi \in \mathbb{C}$. *Alors* $u^3 = \frac{-27q+\varpi}{2}, v^3 = \frac{-27q-\varpi}{2}$. *Quitte à permuter les* x_i *on a le système :* $x_1+x_2+x_3 = 0$, $x_1+jx_2+j^2x_3 = u$, $x_1+j^2x_2+jx_3 = v$ *d'où* $x_1 = \frac{u+v}{3}$, $x_2 = \frac{j^2u+jv}{3}$, $x_3 = \frac{ju+j^2v}{3}$ *avec* $u^3 = \frac{-27q+\varpi}{2}, v^3 = \frac{-27q-\varpi}{2}$ *et* $uv = -3p$. ///

(b) Soit $P := (X-1)(X^2+X+2)$. Déduire de la question précédente que

$$\sqrt{3} = \sqrt[3]{2\sqrt{7}+3\sqrt{3}} - \sqrt[3]{2\sqrt{7}-3\sqrt{3}}$$

.
Preuve. Puisque le discriminant de X^2+X+2 *est* -7, 1 *est la seule racine réelle de* P. *Avec les formules précédentes on obtient que* $x_1 == \frac{u+v}{3} = \frac{1}{3}\sqrt{3}(\sqrt[3]{2\sqrt{7}+3\sqrt{3}} - \sqrt[3]{2\sqrt{7}-3\sqrt{3}}) \in \mathbb{R}$ *est racine de* P. ///

Exercice 9 Fractions rationnelles symétriques.

Soit $F \in K(X_1,....,X_n)$ avec $F(X_{\sigma(1)},...X_{\sigma(n)}) = F(X_1,...,X_n)$ pour tout $\sigma \in S_n$. Montrer que $F \in K(S_1,....,S_n)$ où S_i est le i-ième polynôme symétrique élémentaire.

Preuve. Remarquer que $F = \frac{N}{D} = \frac{NQ}{DQ}$ *avec* $N,D,Q \in K[X_1,....,X_n]$ *et* $DQ = \prod_{\sigma \in S_n} D(X_{\sigma(1)},...X_{\sigma(n)})$. *Ainsi si* $F(X_{\sigma(1)},...X_{\sigma(n)}) = F(X_1,...,X_n)$ *pour tout* $\sigma \in S_n$ *puisque* DQ *jouit de cette même propriété, il suit que* $FDQ = NQ$ *a la même propriété et donc* $NQ, DQ \in K[S_1,....,S_n]$. ///

Exercice 10 Un théorème de Kronecker et une application aux matrices $\in \mathrm{GL}_n(\mathbb{Z})$: les polynômes unitaires de $\mathbb{Z}[X]$ dont les racines complexes vérifient $0 < |z| \leq 1$ sont les produits de polynômes cyclotomiques,
[Fr. F] p. 201.

Soit $P(X) \in \mathbb{Z}[X]$ un polynôme unitaire à coefficients entiers, de degré $n \geq 1$. On suppose que les racines complexes de $P(X)$ sont de module ≤ 1.

(1) Notons $s_1, ..., s_n \in \mathbb{Z}[X_1, ..., X_n]$ les polynémes symétriques élémentaires. Soit $r \geq 1$, on note $\rho : \mathbb{Z}[X_1, ..., X_n] \to \mathbb{Z}[X_1, ..., X_n]$ l'unique homomorphisme tel que $\rho(a) = a$ pour $a \in \mathbb{Z}$ et $\rho(X_i) = X_i^r$ pour tout $1 \leq i \leq n$ (c'est la propriété universelle des anneaux de polynômes). Montrer en utilisant ρ que $\forall \sigma \in S_n$ on a $s_k(X_{\sigma(1)}^r, ..., X_{\sigma(n)}^r) = s_k(X_1^r, ..., X_n^r)$, en déduire que pour tout $k \leq n$, il existe $P_{r,k}(S_1, ..., S_n) \in \mathbb{Z}[S_1, ..., S_n]$ tel que $s_k(X_1^r, ..., X_n^r) = P_{r,k}(s_1, ..., s_n)$.

(2) Calculer $s_k(1, ..., 1)$.

(3) Notons $\theta_1, ..., \theta_n$ les racines complexes (éventuellement répétées) de $F(X)$. Montrer que pour tout $r \geq 1$ et tout $k \leq n$, on a

$$s_k(\theta_1^r, ..., \theta_n^r) \in \mathbb{Z}, \quad |s_k(\theta_1^r, ..., \theta_n^r)| \leq \binom{n}{k}.$$

(4) Montrer que l'ensemble $\{\theta_i^r \mid 1 \leq i \leq n, r \geq 1\}$ est fini.

(5) En déduire que pour toute racine θ de $P(X)$, il existe $r \geq 2$ tel que $\theta^r = \theta$. Conclure.

(6) En déduire la décomposition en irréductible de P dans $\mathbb{Z}[X]$.

(7) Une application du théorème de Kronecker.

Soit $M \in \mathrm{GL}_n(\mathbb{Z})$, on suppose que la suite $M^k, k \in \mathbb{N}$ est bornée. Montrer que M est d'ordre fini.

Preuve. Si $\lambda \in \mathbb{C}$ est racine de χ_M alors la suite λ^k est bornée ainsi $|\lambda| \leq 1$. Le théorème de Kronecker, [Fr. F] exercice 4.4.2 p. 201, appliqué au polynôme χ_M implique que les racines de χ_M sont des racines de l'unité ; ainsi il existe $m > 0$ avec $\chi_{M^m} = (X-1)^n$ alors $M^m = Id + N$ où N est nilpotente. Montrons que $N = 0$. Pour cela nous allons montrer que si $m_N(X) = X^d$ avec $d \geq 2$ alors la suite M^{mk} est non bornée pour $k \to \infty$. La somme $\mathbb{C}N^0 + \mathbb{C}N + ... + \mathbb{C}N^{d-1} \subset M_n(\mathbb{C})$ est directe ainsi par l'équivalence des normes en dimension finie il existe $c > 0$ avec $\| \sum_{0 \leq i \leq d-1} a_i N^i \| \geq c \max_{0 \leq i \leq d-1} |a_i|$. Puisque $M^{mk} = (Id+N)^k = Id + \binom{k}{1} N + ... + \binom{k}{d-1} N^{d-1}$ et que $d \geq 2$, le résultat suit. ///

A propos des ordres des éléments de $\mathrm{GL}_n(\mathbb{Z})$ voir [F. M. 1] $n°26$ p. 46.

Exercice 11 Discriminant, [F. M. 1] $n°112$ p. 321.

Exercice 12 Les entiers algébriques,[Fr. F] exercice 4.4.4 p. 202. Cette preuve utilise les polynômes symétriques. On peut aussi utiliser le résultant ou bien le théorème de Cayley-Hamilton, [F. M. 2] p. 169.

Exercice 13 Le théorème de Molien, [F. M. 2] p. 180.

Soit $A := \mathbb{C}[X_1, X_2, ..., X_n]$, l'anneau des polynômes à n indéterminées et pour $d \in \mathbb{N}$, $H_{d,n}$ le sous-espace vectoriel réunion de $\{0\}$ et des polynômes homogènes de degré d. Soit G est un sous-groupe fini de $\mathrm{GL}_n(\mathbb{C})$. Si $g \in G$ et $g = (\gamma_{i,j})_{1 \leq i,j \leq n}$, il existe un unique $\mathbb{C}$-endomorphisme $\varphi(g)$ de la $\mathbb{C}$-algèbre A avec $\forall i,\ \varphi(g)(X_i) = \sum_{1 \leq j \leq n} \gamma_{j,i} X_j$. On note A^G la sous-algèbre de A des $P \in A$ avec $\forall g \in G,\ \varphi(g)(P) = P$, $H_{d,n}^G := A^G \cap H_{d,n}$ et h_d sa dimension. On a l'égalité $\frac{1}{|G|} \sum_{g \in G} (\det(Id_n - Tg))^{-1} = \sum_{d \geq 0} h_d T^d$.

Exercice 14 Le théorème d'Emmy Noether sur la $\mathbb{C}$-algèbre de $\mathbb{C}[X_1, ..., X_n]$ des invariants par un sous-groupe de $GL_n(\mathbb{C})$.

On note $\underline{X}^{\underline{i}} := X_1^{i_1} X_2^{i_2} ... X_n^{i_n}$ et $|\underline{i}| := i_1 + i_2 + ... + i_n$. On note $c_{\underline{\alpha}}(d) := \frac{d!}{\alpha_1! \alpha_2! ... \alpha_n!}$ où $\underline{\alpha} = (\alpha_1, \alpha_2, ..., \alpha_n)$ avec $\sum_{1 \leq i \leq n} \alpha_i = d$. On rappelle la formule du multinôme $(X_1 + X_2 + ... + X_n)^d = \sum_{\underline{\alpha}} c_{\underline{\alpha}}(d) \underline{X}^{\underline{\alpha}}$.

(1) Montrer que la $\mathbb{C}$-algèbre A^G est engendrée par les $R_G(\underline{X}^{\underline{i}})$ avec $|\underline{i}| \in \mathbb{N}$.

Preuve. Soit $P = \sum_{\underline{i}} a_{\underline{i}} \underline{X}^{\underline{i}} \in A^G$ alors $P = R_G(P) = \sum_{\underline{i}} a_{\underline{i}} R_G(\underline{X}^{\underline{i}})$.///

(2) Soit $\underline{X}$ (resp. $\underline{Y}$) le vecteur colonne ${}^t(X_1, ..., X_n)$ (resp. le vecteur ligne $(Y_1, ..., Y_n)$). Si $g \in G$. Montrer que $\sum_{g \in G} ({}^t \underline{Y} g \underline{X})^d = |G| \sum_{|\underline{\alpha}| = d} c_{\underline{\alpha}}(d) \underline{Y}^{\underline{\alpha}} R_G(\underline{X}^{\underline{\alpha}})$.

Preuve. On développe avec la formule du multinôme.///

(3) Soit $B := \mathbb{C}[Z_1, Z_2, ..., Z_{|G|}]$ et $p_k = \sum_{1 \leq i \leq |G|} Z_i^k,\ k \in \mathbb{N}^\star$, les polynômes symétriques de Newton en les $|G|$ indéterminées Z_i. Soit $d > |G|$, montrer qu'il existe $F \in B$ avec $p_d = F(p_1, ..., p_{|G|})$.

Preuve. Puisque $\mathbb{Q} \subset \mathbb{C}$ les formules de Waring permettent d'exprimer les polynômes symétriques élémentaires dans $\mathbb{C}[p_1, ..., p_{|G|}]$.///

(4) En déduire que

$|G| \sum_{|\underline{\alpha}| = d} c_{\underline{\alpha}}(d) R_G(\underline{X}^{\underline{\alpha}}) \underline{Y}^{\underline{\alpha}} = F(|G| \sum_{|\underline{\beta}| = 1} c_{\underline{\beta}}(1) R_G(\underline{X}^{\underline{\beta}}) \underline{Y}^{\underline{\beta}}, .., |G| \sum_{|\underline{\beta}| = |G|} c_{\underline{\beta}}(|G|) R_G(\underline{X}^{\underline{\beta}}) \underline{Y}^{\underline{\beta}})$.

Preuve. On applique l'identité $p_d = F(p_1, ..., p_{|G|})$ à $Z_i = {}^t \underline{Y} g_i \underline{X}$ où $g_i,\ 1 \leq i \leq n$ parcourt les éléments de G et on utilise b).

(5) Conclure.

Preuve. Puisque les $\underline{Y}^{\underline{\alpha}}$ sont linéairement indépendant sur $\mathbb{C}[X_1, .., X_n]$, on peut identifier les coefficients de $\underline{Y}^{\underline{\alpha}}$ dans les deux membres de l'égalité précédente.

Remarque. Par la propriété universelle de l'anneau des polynômes on construit un homomorphisme surjectif de $\mathbb{C}$-alèbres $\mathbb{C}[Z_{\underline{i}},\ |\underline{i}| \leq |G|] \to A^G$ en assignant à $Z_{\underline{i}}$ l'élément $R_G(\underline{X}^{\underline{i}})$; le noyau de cet homomorphisme est un idéal d'un anneau de polynômes et donc de type fini puisque $\mathbb{C}[Z_{\underline{i}},\ |\underline{i}| \leq |G|]$ est noethérien (théorème de transfert de Hilbert).///