Note sur les polynômes à plusieurs indéterminées

Daniel Ferrand (Novembre 2005)

La correction de copies m'a fait penser qu'un résumé, en forme de guide de lecture, serait peut-être utile aux agrégatifs sur ce sujet. Il est suivi par deux exemples qui mettent en oeuvre la plupart des notions signalées.

Sigles pour les références
A IV = Bourbaki, *Algèbre,* ch IV
AF = Arnaudiès - Fraysse, *Algèbre,*
G = Gourdon, *Algèbre,*
J = Jacobson, *Basic Algebra I*
LFA = Lelong-Ferrand et Arnaudies, *Algèbre*

1. - Définitions

1.1. Il y a deux points de vue pour aborder les polynômes : on peut commencer par définir ce qu'est *un* polynôme, puis introduire les opérations qui font de leur ensemble une algèbre. De ce point de vue, rappelons que tout élément de $A[X_1, \dots, X_n]$ s'écrit de façon unique comme combinaison linéaire, à coefficients dans A, des monômes $X^m = X_1^{m(1)} \cdots X_n^{m(n)}$, où m parcourt l'ensemble des suites de n entiers ≥ 0. Le produit des polynômes est défini en prolongeant par linéarité le produit des monômes, lequel est associé à la somme des n-uples :

$$X^m X^{m'} = X_1^{m(1)} \cdots X_n^{m(n)} X_1^{m'(1)} \cdots X_n^{m'(n)} = X_1^{m(1)+m'(1)} \cdots X_n^{m(n)+m'(n)} = X^{m+m'}.$$

Certains manuels, dans le souci louable d'être immédiatement compréhensibles, introduisent d'abord l'anneau $A[X]$ des polynômes à une indéterminée, et définissent ensuite l'anneau $A[X_1, \dots, X_n]$ de proche en proche par la règle $A[X_1, \dots, X_n] = (A[X_1, \dots, X_{n-1}])[X_n]$.

Le second point de vue consiste à définir d'abord l'algèbre des polynômes par ses relations avec les autres algèbres, et, si nécessaire, préciser ensuite la forme de ses éléments. Cela s'exprime par une propriété universelle, trop souvent négligée.

Soit A un anneau (commutatif et unitaire). Pour une indéterminée, la propriété universelle de $A[X]$ s'énonce ainsi : le couple $(A \to A[X], X)$ est universel parmi les couples $(\varphi : A \to B, b)$ formés d'une A-algèbre commutative et d'un élément $b \in B$; cela signifie que pour tout tel couple il existe un unique morphisme de A-algèbres $\varphi_{X \to b} : A[X] \to B$, tel que $\varphi_{X \to b}(X) = b$.

Pour n indéterminées, la propriété est analogue : pour toute A-algèbre commutative $\varphi : A \to B$, et toute suite $b_\cdot = (b_1, \dots, b_n)$ de n éléments de B, il existe un unique morphisme de A-algèbres

$$\varphi_{X_\cdot \to b_\cdot} : A[X_1, \dots, X_n] \quad \longrightarrow \quad B,$$

qui envoie X_i sur b_i, pour $1 \leq i \leq n$.

Réf : AF p.406 ; J p.120

1.2. Cette propriété universelle facilite certaines vérifications.

Considérons, par exemple, un groupe G agissant sur un espace vectoriel V sur un corps K ; une telle action est la donnée, pour tout $g \in G$, d'un isomorphisme K-linéaire $g_V : V \to V$, de telle sorte que $1_V = \mathrm{Id}_V$, et que pour g et h dans G, on ait $(gh)_V = g_V \circ h_V$.

Si V est de dimension n, le choix d'une base permet d'identifier V avec le sous-espace de $\mathsf{S} = K[X_1, \dots, X_n]$ formé des polynômes homogènes de degré 1, et on considère dorénavent les X_i comme

formant une base de V. On étend l'action de G sur V en une action de G sur la K-algèbre S, de la façon suivante :

Pour $g \in G$, $g_{\mathsf{S}} : \mathsf{S} = K[X_1, ..., X_n] \longrightarrow \mathsf{S}$ est l'unique morphisme de K-algèbres tel que $g_{\mathsf{S}}(X_i) = g_V(X_i)$; la restriction de ce morphisme au sous-espace des polynômes de degré 1 est précisément l'automorphisme donné g_V. Pour g et h dans G, on a $(gh)_{\mathsf{S}} = g_{\mathsf{S}} \circ h_{\mathsf{S}}$ puisque ces deux morphismes ont même restriction à $V = KX_1 \oplus \cdots \oplus KX_n$, et que l'extension à S est unique. Comme chaque élément de G admet un inverse, chacun des morphismes g_{S} admet un morphisme réciproque, et est donc un *automorphisme* de la K-algèbre S ; de plus, l'application $G \to \mathrm{Aut}_{K-\mathrm{alg}}(\mathsf{S}), \quad g \mapsto g_{\mathsf{S}}$ est un morphisme de groupes.

Réf : LFA p.156

2. Degrés

2.1. Il est souvent très utile de décomposer $\mathsf{S} = K[X_1, ..., X_n]$ en une somme directe de sous-modules (libres) de type fini. Pour cela, on introduit divers *degrés* : une suite d'entiers ≥ 0, $d_1, \ldots, d_n$ étant choisie, on attribue à X_i le degré (ou poids) d_i. Attribuer le degré 0 à une indéterminée revient à la considérer comme un scalaire, c'est-à-dire à l'adjoindre à l'anneau de base.

Le degré d'un monôme est alors défini par la formule

$$\deg(X^m) \quad = \quad d_1 m(1) + d_2 m(2) + \cdots + d_n m(n).$$

Une combinaison linéaire de monômes de même degré d sera nommée un polynôme homogène de degré d. Tout polynôme F s'écrit alors de façon unique comme une somme finie

$$F = F_0 + F_1 + \cdots + F_s,$$

où F_d est homogène de degré d : c'est la somme des monômes de degré d qui figurent dans F. Autrement dit, l'attribution de degré aux indéterminées conduit à une décomposition de S en la somme directe

$$\mathsf{S} \ = \ \mathsf{S}_0 \oplus \mathsf{S}_1 \oplus \cdots \oplus \mathsf{S}_d \oplus \cdots$$

où S_d désigne le module des polynômes homogènes de degré d. La règle de multiplication des monômes montre que le produit dans S induit des applications $\mathsf{S}_d \times \mathsf{S}_e \longrightarrow \mathsf{S}_{d+e}$; en particulier, S_0 est un sous-anneau de S.

Il faut bien comprendre qu'attribuer des degrés aux X_i ne change pas l'anneau des polynômes ; c'est seulement organiser un façon de le voir (de même que choisir une base d'une espace vectoriel ne le modifie pas). Rappelons un exemple familier : les polynômes $s_1 = X+Y$ et $s_2 = XY$ sont, dans l'anneau $K[X, Y]$, de degré 1 et 2 respectivement ; on sait (voir 6.1) qu'ils sont algébriquement indépendants et que, par suite, le sous-anneau $K[s_1, s_2] \subset K[X, Y]$ est isomorphe à l'anneau des polynômes en 2 indéterminées ; de ce point de vue on attribue, souvent le degré 1 à s_1 et à s_2.

2.2. Critère : *Pour qu'un polynôme F soit homogène de degré d, il faut et il suffit que, dans l'anneau $\mathsf{S}[Z]$, l'on ait $F(Z^{d_1}X_1, \ldots, Z^{d_n}X_n) = Z^d F(X_1, \ldots, X_n)$*

Lorsque on munit les indéterminées du degré 1, on retrouve ce qui sert de définition de l'homogénéité en analyse.

Application à l'irréductibilité :

2.3. *Soit K un anneau factoriel, par exemple un corps, et $F_d, F_{d+1} \in K[X_1, ..., X_n]$ deux polynômes homogènes de degré respectivement d et $d+1$. Si ces polynômes sont premiers entre eux, alors $F_d + F_{d+1}$ est irréductible (donc premier).*

Considérons en effet une factorisation

$$F_d + F_{d+1} = G.H = (G_r + \cdots + G_s)(H_t + \cdots + H_u)$$

où les G_i sont de degré i et les H_j de degré j ; on suppose aussi que les composantes extrêmes G_r, G_s, H_t et H_u sont non nulles. On a donc $F_d = G_r H_t$, d'où $d = r+t$, ainsi que $F_{d+1} = G_s H_u$, d'où $d+1 = s+u$;

on tire de ces égalités la relation

$$(s-r)+(u-t)=1.$$

Comme les deux entiers écrits entre parenthèses sont ≥ 0, on a $s=r$ ou $u=t$, disons $s=r$; alors $G=G_r$, et ce polynôme divise F_d et F_{d+1}, donc G est une constante inversible.□

Cet énoncé admet des variantes :

2.4. *Soit K un corps, soit $F,G\in K[X_3,\dots,X_n]$ deux polynômes premiers entre eux (pas nécessairement homogènes), et r et s deux entiers premiers entre eux. Alors $X_1^rF+X_2^sG$ est irréductible dans $K[X_1,...,X_n]$. En particulier, X_1F+G, et $X_1^r+X_2^s$ sont irréductibles.*

L'anneau $A=K[X_3,\dots,X_n]$ est factoriel et $K[X_1,...,X_n]=A[X_1,X_2]$. Soient t et u deux entiers ≥ 0 tels que $su-rt=1$; affectons le degré t à X_1, et le degré u à X_2, de sorte que X_1^rF est de degré rt, et X_2^sG est de degré $su=rt+1$. Le résultat précedent permet alors de conclure.□

3. - Écritures

Un élément de $A[X_1,...,X_n]$ peut être écrit de plusieurs façons, et il faut toujours choisir la plus simple, i.e. la moins explicite :

- une seule lettre, u ou F ; il est le plus souvent inutile de s'encombrer de précisions qui ne serviront qu'à perdre le temps de les écrire, et à distraire l'esprit ;
- $u_0+...+u_s$ lorsqu'on fait intervenir la décomposition de u en somme de polynômes homogènes u_d ;
- $u(X_1,...,X_n)$ lorsqu'on pense devoir utiliser la propriété universelle, en particulier lorsqu'on considère la fonction polynôme associée ;
- $\sum a_mX^m$, lorsqu'on doit considérer explicitement les coefficients, par exemple pour certaines questions de divisibilité ;
- $\sum a_{m_1,\dots,m_n}X_1^{m_1}X_2^{m_2}...X_n^{m_n}$; cette pénible écriture est presque toujours évitable.

4.- Binômes

Dans la suite, le passage $A[T]\subset A[[T]]$ de l'anneau des polynômes à celui des séries formelles permet de considérer l'inverse d'un polynôme $F(T)$ tel que $F(0)=1$, comme une série formelle, sur le modèle de la relation de base

$$(1-T)^{-1} \quad = \quad 1+T+T^2+\cdots$$

Plus généralement, pour tout entier n (même négatif !), on a

4.1
$$(1+T)^n \quad = \quad \sum_{d\geq 0}\binom{n}{d}T^d,$$

où $\binom{n}{d}$ désigne la valeur en n du « polynôme binomial »

$$\binom{X}{d} \quad = \quad \frac{X(X-1)\cdots(X-d+1)}{d!}$$

Ainsi, pour un entier $n\geq 0$, on a $\binom{-n}{d}=(-1)^d\binom{n+d-1}{d}$.

Vérifions la formule (4.1) pour les entiers négatifs, par récurrence descendante sur n, à partir du cas $n=-1$ supposé connu (ou admis !). En dérivant les deux membres de la formule 4.1, on trouve

$$n(1+T)^{n-1} \quad = \quad \sum_{d\geq 1}\binom{n}{d}dT^{d-1}.$$

Or, $\binom{n}{d}.\frac{d}{n}=\binom{n-1}{d-1}$.□

Réf : AF p.353 ; LFA p.229

5. - Dimensions

Proposition 5.1 *Soient K un corps et $\mathsf{S} = K[X_1, ..., X_n]$ l'anneau des polynômes à n indéterminées. Attribuons le degré d_i à X_i, et soit S_d le sous-espace des polynômes homogènes de degré d. Alors, dans $\mathbf{Q}[[T]]$, on a la relation*

$$\sum_{d\geq 0} \dim(\mathsf{S}_d)T^d \quad = \quad \frac{1}{(1-T^{d_1})\cdots(1-T^{d_n})}.$$

En particulier, si chaque X_i est doté du degré 1, on a

$$\dim(\mathsf{S}_d) = \binom{n+d-1}{d}$$

Posons $\mathsf{S}' = K[X_1, \ldots, X_{n-1}]$; le noyau du morphisme surjectif $\mathsf{S} \to \mathsf{S}'$, défini par $X_n \mapsto 0$, est engendré par les monômes multiples de X_n ; en degré d, ce noyau est donc $X_n\mathsf{S} \cap \mathsf{S}_d = X_n\mathsf{S}_{d-d_n}$. Cela implique la relation

$$\dim(\mathsf{S}_d) \quad = \quad \dim(\mathsf{S}_{d-d_n}) + \dim(\mathsf{S'}_d).$$

Passant à la série formelle, on obtient

$$\sum_{d\geq 0} \dim(\mathsf{S}_d)T^d \quad = \quad T^{d_n}.\sum_{d\geq 0} \dim(\mathsf{S}_d)T^d \; + \; \sum_{d\geq 0} \dim(\mathsf{S'}_d)T^d,$$

soit

$$(1-T^{d_n})(\sum_{d\geq 0} \dim(\mathsf{S}_d)T^d) = \sum_{d\geq 0} \dim(\mathsf{S'}_d)T^d.$$

On termine la démonstration par récurrence sur le nombre d'indéterminées.

La dernière assertion provient de 4.1, qui s'écrit ici

$$\frac{1}{(1-T)^n} \; = \; \sum_{d\geq 0} \binom{n+d-1}{d} T^d.$$

□

Réf : G, p.82

6. -Polynômes symétriques élémentaires

Étant données $n+1$ indéterminées $T, X_1, \ldots, X_n$, on définit le *polynôme symétrique élémentaire de degré i*, noté (ce sont les notations de Bourbaki) $s_i(X_1, \ldots, X_n)$, par la relation

$$\prod_{i=1}^{n}(1+TX_i) \quad = \quad 1 + s_1T + s_2T^2 + \cdots + s_nT^n.$$

On a donc

$$s_i(X_1, \ldots, X_n) \quad = \quad \sum_H \prod_{j\in H} X_j,$$

où H parcourt l'ensemble des parties à i éléments de $\{1, 2, \ldots, n\}$. Le théorème suivant est fondamental.

Théorème 6.1. *Soit K un anneau (commutatif et unitaire). Posons $\mathsf{S} = K[X_1, ..., X_n]$, et désignons par $\mathsf{S}^{\mathfrak{S}_n}$ le sous-anneau des polynômes symétriques.*

a) La K-algèbre des polynômes symétriques est engendrée par $s_1, \ldots, s_n$: $\mathsf{S}^{\mathfrak{S}_n} = K[s_1, \ldots, s_n]$.

b) Les éléments $s_1, \ldots, s_n$ sont algébriquement indépendants sur K.

c) La famille des monômes $X^m = X_1^{m(1)} \dots X_n^{m(n)}$ *tels que* $0 \leq m(i) < i$ *pour* $1 \leq i \leq n$, *est une base de* S *comme module sur le sous-anneau* $\mathsf{S}^{\mathfrak{S}_n}$. *En particulier,* S *est un* $\mathsf{S}^{\mathfrak{S}_n}$*-module libre de rang* $n!$.

Réf :
A IV p.58 particulièrement clair.
AF p.424, mais avec l'hypothèse stupide que $K = \mathbf{C}$.
G p.78 sans démonstration, mais avec un procédé de calcul compréhensible.
J p.133 court, efficace ; l'anneau de base est quelconque.
LFA p.160, très détaillé, mais K est supposé être un corps algébriquement clos de caractéristique zéro

7. - Comment vérifier que des éléments sont algébriquement indépendants ?

Il n'y a pas de procédé général, aussi un exemple simple suffira pour indiquer des méthodes possibles.

Deux éléments a et b d'une $\mathbf{C}$-algèbre A sont algébriquement indépendants (sur $\mathbf{C}$) s'il n'y a pas de polynôme non nul $F \in \mathbf{C}[X,Y]$ tel que $F(a,b) = 0$, autrement dit si le morphisme de $\mathbf{C}$-algèbres $\mathbf{C}[S,T] \longrightarrow A$, défini par $S \mapsto a$ et $T \mapsto b$ est injectif. Dans ce paragraphe, je note : $\left\{\begin{smallmatrix} a \\ b \end{smallmatrix}\right\}$ le morphisme

$$\mathbf{C}[S,T] \longrightarrow A, \quad S \mapsto a,\ T \mapsto b.$$

La démarche proposée consiste à factoriser ce morphisme en un composé de morphismes suffisamment simples pour être visiblement injectifs.

Voici un exemple explicite qui sera utilisé plus bas (§11).

7.1. *Les polynômes* $X^4 + Y^4$ *et* X^2Y^2 *de* $\mathbf{C}[X,Y]$ *sont algébriquement indépendants.*

Commençons par une remarque.

7.2. *Si* p *et* q *sont des entiers* ≥ 1, *le morphisme* $\mathbf{C}[X,Y] \to \mathbf{C}[X,Y]$ *défini par* $X \mapsto X^p$, $Y \mapsto Y^q$, *c'est-à-dire* $\left\{\begin{smallmatrix} X^p \\ Y^q \end{smallmatrix}\right\}$, *est injectif.*

Car l'image de la base $(X^iY^j)_{(i,j)}$ est la partie libre $(X^{pi}Y^{qj})_{(i,j)}$.□

Pour vérifier 7.1, il suffit donc de vérifier que $X^2 + Y^2$ et XY sont algébriquement indépendants, puisque le morphisme $\left\{\begin{smallmatrix} X^4+Y^4 \\ X^2Y^2 \end{smallmatrix}\right\}$ se factorise en

$$\mathbf{C}[S,T] \overset{\left\{\begin{smallmatrix} X^2+Y^2 \\ XY \end{smallmatrix}\right\}}{\longrightarrow} \mathbf{C}[X,Y] \overset{\left\{\begin{smallmatrix} X^2 \\ Y^2 \end{smallmatrix}\right\}}{\longrightarrow} \mathbf{C}[X,Y].$$

Or, le morphisme $\left\{\begin{smallmatrix} X^2+Y^2 \\ XY \end{smallmatrix}\right\}$ se décompose en

$$\mathbf{C}[S,T] \overset{\left\{\begin{smallmatrix} U-2V \\ V \end{smallmatrix}\right\}}{\longrightarrow} \mathbf{C}[U,V] \overset{\left\{\begin{smallmatrix} U^2 \\ V \end{smallmatrix}\right\}}{\longrightarrow} \mathbf{C}[U,V] \overset{\left\{\begin{smallmatrix} X+Y \\ XY \end{smallmatrix}\right\}}{\longrightarrow} \mathbf{C}[X,Y]$$

Le premier morphisme $\left\{\begin{smallmatrix} U-2V \\ V \end{smallmatrix}\right\}$ est un isomorphisme, le second est injectif d'après 7.2, et $\left\{\begin{smallmatrix} X+Y \\ XY \end{smallmatrix}\right\}$ est injectif puisque ses composantes sont les polynômes symétriques élémentaires en X et Y (voir 6.1).□

8. - Relations de Newton et de Waring

Les sommes de puissances, parce que ce sont des polynômes symétriques, s'expriment en fonction des s_i ; on a pour elles des formules explicites dues à Newton et Waring. Plaçons nous dans l'anneau $\mathbf{Z}[T, X_1, \dots, X_n]$. Posons (notations de Bourbaki)

$$p_d \quad = \quad X_1^d + \dots + X_n^d.$$

Considérons le polynôme $F(T) = \prod_{i=1}^n (1 - TX_i) = 1 - s_1T + s_2T^2 - \dots + (-1)^n s_nT^n$. On a

$$\frac{-TF'(T)}{F(T)} = \frac{TX_1}{1-TX_1} + \dots + \frac{TX_n}{1-TX_n}.$$

En utilisant de nouveau le developpement en série formelle $(1-Z)^{-1} = \sum_{m\geq 0} Z^m$, avec $Z = TX_i$, on trouve

$$\frac{-TF'(T)}{F(T)} \quad = \quad \sum_{m\geq 1} T^m p_m,$$

soit, après simplification par T, la *relation de Newton* (c'est une égalité dans l'anneau $\mathbf{Z}[X_1,\dots,X_n][[T]]$)

8.1 $$\boxed{F(T).(\sum_{m\geq 1} T^{m-1}p_m) + F'(T) = 0.}$$

En considérant le coefficient de T^k, on trouve la forme usuelle (A IV, p.65 ; AF, p.428 ; G, p.81 ; LFA p.166)

On peut aller plus loin, suivant Waring, en « intégrant » cette relation, mais cela oblige à introduire des dénominateurs entiers, et donc à se placer dans l'anneau $\mathbf{Q}[X_1,\dots,X_n][[T]]$. Posons

$$P(T) \quad = \quad \sum_{m\geq 1} \frac{p_m}{m} T^m.$$

La relation de Newton s'écrit

$$\frac{F'(T)}{F(T)} \quad = \quad -P'(T).$$

On en déduit par « intégration »

8.2 $$\boxed{F(T) = \exp(-P(T)) = 1 - P(T) + \frac{1}{2}P(T)^2 - \frac{1}{3!}P(T)^3 \dots}$$

Il faut remarquer que le second membre a bien un sens puisque $P(T)$ commence par T, donc $P(T)^k$ par T^k ; ainsi, le coeficient de T^k du second membre ne fait intervenir que les $P(T)^j$ pour $j \leq k$.

Comme $F(T) = 1 - s_1T + s_2T^2 - \dots + (-1)^n s_nT^n$, en considérant le coefficient de T^k du second membre, on voit que, pour $1 \leq k \leq n$, il existe un polynôme $G_k \in \mathbf{Q}[X_1,\dots,X_n]$, tel que l'on ait

$$s_k(X_1,\dots,X_n) \quad = \quad G_k(p_1,\dots,p_n).$$

Si on y tient, et si on a une bonne machine, la formule 8.2 permet de calculer effectivement ces polynômes.

Si on cherche, à l'inverse, à exprimer les sommes de puissances en fonction des s_i, on utilise le logarithme et 8.2 devient

8.3 $$P(T) \;=\; -\log(F(T)).$$

Un petit commentaire s'impose : on peut écrire $F(T) = 1 - TG(T)$, avec $G(T) = s_1 - s_2T + s_3T^2 \cdots$; le logarithme de F est donc bien défini ; on trouve la série formelle

8.4 $$\boxed{P(T) \;=\; TG + \frac{T^2G^2}{2} + \frac{T^3G^3}{3} + \cdots}$$

Cette formule est explicitée par exemple dans AF p.431.

9. Le théorème de Molien[1]

La compréhension du résultat qui suit n'est pas indispensable pour un agrégatif. Cependant, outre son intérêt culturel évident, il a été, et restera, une source d'inspiration pour les concepteurs des épreuves écrites du concours car il met en oeuvre des notions et des procédés qui sont, eux, explicitement dans le programme.

[1]Theodor Molien, ou Molin, (1861-1941), mathématicien russe qui a commencé ses travaux dans l'entourage de Klein et de Frobenius et qui, n'ayant pu trouver de position académique en Allemagne s'est établi vers 1900 à Tomsk (Sibérie), dans un isolement mathématique peu propice à la recherche. Le résultat cité date de 1897.

On considère ici l'anneau $\mathsf{S} = \mathbf{C}[X_1, \ldots, X_n]$ muni de sa graduation usuelle. On suppose qu'un groupe fini G opère sur l'espace $V = \mathsf{S}_1$ des polynômes homogènes de degré 1, et on étend cette action à S, comme il est expliqué dans 1.2. En utilisant 2.2 on voit que chaque $g \in G$ induit un automorphisme de S_d ; on note S_d^G le sous-espace invariant.

Théorème de Molien *Sous les hypothèses précédentes, on a*

$$\sum_{d\geq 0} \dim(\mathsf{S}_d^G)T^d \quad = \quad \frac{1}{|G|}\sum_{g\in G}\frac{1}{\det(1-Tg_V)}.$$

Notation et définition : Soit $A \subset \mathsf{S} = \mathbf{C}[X_1, \ldots, X_n]$ une sous-$\mathbf{C}$-algèbre qui se décompose en la somme directe $\oplus_{d\geq 0} A_d$, où $A_d = A \cap \mathsf{S}_d$ est l'espace des polynômes homogènes de degré d qui sont dans A. On appelle *série de Poincaré* de A la série formelle

$$P_A(T) = \sum_{d\geq 0} \dim_{\mathbf{C}}(A_d)T^d.$$

Le théorème de Molien porte donc sur la série de Poincaré de l'anneau des invariants $A = \mathsf{S}^G$.

Pour simplifier, notons $g^{(d)}$ l'automorphisme g_{S_d} induit par g_V sur S_d ; d'après la formule de la trace[2], on a

$$\dim(\mathsf{S}_d^G) \quad = \quad \frac{1}{|G|}\sum_{g\in G}\mathrm{Tr}(g^{(d)}).$$

Calculons $\mathrm{Tr}(g^{(d)})$. Comme g_V est d'ordre fini, il est diagonalisable ; choisissons donc une base de V, que l'on persiste à noter $\{X_1, \ldots, X_n\}$, telle que $gX_i = \zeta_i X_i$, où les ζ_i sont les valeurs propres de g_V ; en particulier, on a

$$\det(1 - Tg_V) = \prod_i (1 - \zeta_i T).$$

L'espace S_d admet pour base les monômes X^m, où, comme déjà vu plus haut, m parcourt l'ensemble des suites $m = (m(1), \ldots, m(n))$ d'entiers ≥ 0 de poids $|m| = \sum_i m(i) = d$. On a donc

$$g^{(d)}(X^m) = (gX_1)^{m(1)} \cdots (gX_n)^{m(n)} = \zeta^m X^m.$$

(Bien entendu, ζ^m désigne le produit $\zeta_1^{m(1)} \cdots \zeta_n^{m(n)}$). On en déduit

$$\mathrm{Tr}(g^{(d)}) \quad = \quad \sum_{|m|=d} \zeta^m.$$

Par suite, en réorganisant les sommes, on trouve

$$\sum_{d\geq 0} \mathrm{Tr}(g^{(d)})T^d = \sum_d \sum_{|m|=d} \zeta^m T^d = \sum_m \zeta_1^{m(1)} T^{m(1)} \cdots \zeta_n^{m(n)} T^{m(n)}$$

$$= (\sum_d \zeta_1^d T^d)(\sum_d \zeta_2^d T^d) \cdots (\sum_d \zeta_n^d T^d) = (1-\zeta_1 T)^{-1} \cdots (1-\zeta_n T)^{-1} = \frac{1}{\det(1-Tg_V)}.\square$$

[2]Soit G un groupe fini opérant sur un $\mathbf{C}$-vectoriel V. L'endomorphisme $p = \frac{1}{|G|}\sum_{g\in G} g$ vérifie la relation $hp = p$ pour tout $h \in G$. Cela montre d'abord que c'est un proecteur : $p^2 = p$. Cela montre aussi que $\mathrm{Im}(p)$ est formé d'éléments invariants sous G ; réciproquement si x est invariant, il est clair que $p(x) = x$. Bref, $V^G = \mathrm{Im}(p)$. Par ailleurs, p étant un projecteur, l'espace V est décomposé en somme directe $V = \mathrm{Im}(p) \oplus \mathrm{Ker}(p)$. Comme p est l'identité sur le premier facteur et est nul sur le second, on a $\dim(\mathrm{Im}(p)) = \mathrm{Tr}(p)$. Cela entraîne la *formule de la trace*

$$\dim(V^G) = \frac{1}{|G|}\sum_{g\in G}\mathrm{Tr}(g).$$

10. - Application à certaines fractions rationnelles

On va montrer l'égalité suivante :

10.1 $$\sum_{\omega^n=1} \frac{1}{(1-\omega T)(1-\omega^{-1}T)} \;=\; n.\frac{1+T^n}{(1-T^2)(1-T^n)}.$$

Cela n'apporte rien d'écrire les dénominateurs des termes de gauche sous la forme $T^2-2\cos(\frac{2k\pi}{n})T+1$. Je ne le ferai donc pas. L'idée du calcul est d'interpréter ces polynômes comme des déterminants pour pouvoir utiliser le théorème de Molien.

Considérons le groupe (isomorphe au groupe μ_n des racines n-èmes de l'unité dans $\mathbf{C}$)

$$G \;\subset\; \mathbf{SL}(2,\mathbf{C})$$

formé des matrices $\left(\begin{smallmatrix}\omega & 0\\ 0 & \omega^{-1}\end{smallmatrix}\right)$, où ω est une racine n-ème de l'unité. En notant g_ω l'automorphisme de $\mathbf{C}[X,Y]$ défini par $g_\omega(X)=\omega X$, et $g_\omega(Y)=\omega^{-1}Y$,on a

$$\det(1-g_\omega T) \;=\; (1-\omega T)(1-\omega^{-1}T).$$

Il faut donc déterminer l'anneau des invariants $A=\mathbf{C}[X,Y]^G$.

Comme les g_ω sont diagonaux au sens où ils envoient un monôme sur un monôme du même bidegré, il suffit de caractériser les monômes invariants. Par ailleurs, le groupe G est cyclique engendré par g_ω si ω est une racine primitive. Fixons donc une telle racine primitive n-ème de l'unité. Comme

$$g_\omega(X^iY^j) \;=\; \omega^{i-j}X^iY^j,$$

on voit que ce monôme est invariant si et seulement si $i \equiv j \mod n$. La condition se précise en : il existe trois entiers ≥ 0, a, b et c tels que

$$0 \leq c \leq n-1, \quad i=c+an, \quad j=c+bn.$$

Par suite les monômes invariants X^iY^j sont exactement ceux de la forme

$$(XY)^c(X^n)^a(Y^n)^b.$$

Posons $B=\mathbf{C}[X^n,Y^n]$; on a donc les inclusions $B\subset A\subset \mathbf{C}[X,Y]$. La remarque qui précède signifie qu'on a une décomposition en une somme directe

$$A \;=\; B\oplus XYB\oplus (XY)^2B\oplus\cdots\oplus(XY)^{n-1}B.$$

En degré d, on trouve :

10.2 $$A_d \;=\; B_d\oplus XYB_{d-2}\oplus\cdots\oplus(XY)^{n-1}B_{d-2n-2}.$$

D'après 7.2, X^n et Y^n sont algébriquement indépendants, et le théorème 5.1 montre que

$$P_B(T) \;=\; \sum_{d\geq 0}\dim_{\mathbf{C}}(B_d)T^d \;=\; \frac{1}{(1-T^n)^2}.$$

Par suite, tenant compte de 10.2, on a

$$P_A(T) \;=\; P_B(T)+T^2P_B(T)+\cdots T^{2n-2}P_B(T) \;=\; \frac{1+T^2+\cdots+T^{2n-2}}{(1-T^n)^2}.$$

En multipliant numérateur et dénominateur par $1-T^2$, et en divisant par $1-T^n$, on trouve

$$P_A(T) \;=\; \frac{1+T^n}{(1-T^2)(1-T^n)}.$$

Le théorème de Molien conduit alors à la formule 10.1 .

11. - Invariants sous le groupe quaternionien

Dans ce paragraphe le théorème de Molien sert à déterminer la structure algébrique (générateurs et relations) de l'anneau des invariants sous le groupe quaternionien $A = \mathbf{C}[X,Y]^{Q_8}$. Pour parvenir vite à ce qui est en cause ici, on définit le groupe quaternionien de la façon suivante.

$$Q_8 = \mathbf{SU}(2, \mathbf{Z}[i]) \subset \mathbf{GL}(2, \mathbf{C}).$$

C'est donc le groupe des matrices M de format $(2,2)$, à coefficients dans l'anneau des entiers de Gauss, de déterminant 1, et qui sont unitaires : $M^t\bar{M} = 1$. En explicitant ces conditions, on trouve les 8 éléments suivants :

11.1
$$\pm\begin{pmatrix}1&0\\0&1\end{pmatrix}, \quad \pm\begin{pmatrix}i&0\\0&-i\end{pmatrix}, \quad \pm\begin{pmatrix}0&-1\\1&0\end{pmatrix}, \quad \pm\begin{pmatrix}0&i\\i&0\end{pmatrix}.$$

Le déterminant de ces éléments est égal à 1, et leur trace est nulle sauf pour les deux premiers où elle vaut 2 et -2. La relation de Molien s'écrit donc

$$P_A(T) \;=\; \frac{1}{8}\Big(\frac{1}{(1+T)^2} + \frac{1}{(1-T)^2} + \frac{6}{1+T^2}\Big) = \frac{1+T^6}{(1-T^4)^2}.$$

Par ailleurs, on peut vérifier (mais évidemment aucun lecteur ne le fera !) que les polynômes

$$u = X^4 + Y^4, \quad v = X^2Y^2, \quad w = XY(X^4 - Y^4)$$

sont invariants. On va montrer que $\mathbf{C}[u,v,w] = A$, et que la seule relation entre ces générateur est la relation évidente

$$w^2 - u^2v + 4v^3 \;=\; 0.$$

D'après 7.1, les polynômes u et v sont algébriquement indépendants. Montrons que la somme (de sous-espaces vectoriels) $B + wB \subset A$ est directe : sinon, en effet, il existe p et q dans B tels que $p = wq$, d'où $p^2 = q^2w^2$; mais la relation ci-dessus montre que w^2 est un polynôme de degré 3 en u et v, ce qui rend impossible la relation $p^2 = q^2w^2$ dans l'anneau de polynômes $B = \mathbf{C}[u,v]$. On peut maintenant montrer que $B \oplus wB$ est égal à A en vérifiant que pour tout d les espaces des polynômes de degré d (en X et Y) $(B \oplus wB)_d$ et A_d ont la même dimension.

Comme u et v sont algébriquement indépendants, et de degré 4 en X, Y, la série de Poincaré de $B = \mathbf{C}[u,v]$ est donnée par 5.1.

$$P_B(T) \;=\; \frac{1}{(1-T^4)^2}.$$

Comme w est de degré 6 la série de Poincaré de $B \oplus wB$ est

$$\frac{1+T^6}{(1-T^4)^2}.$$

C'est la série de Poincaré de A, comme on l'a vu plus haut. D'où le résultat.
On en déduit immédiatement que S^{Q_8} est isomorphe à $\mathbf{C}[U,V,W]/(W^2 - U^2V + 4V^3)$.