Algèbre des polynômes à plusieurs indéterminées. Applications

1/42

Cadre : A anneau commutatif unitaire. K un corps
$n \in \mathbb{N}$ $n \geq 2$. $i \in \mathbb{N}^n$. $i = (i_1, \dots, i_n)$ $|i| = \sum_{j=1}^{n} i_j$

I. POLYNÔMES À n INDÉTERMINÉES. [RDO]

1. Algèbre $A[X_1, \dots, X_n]$

Déf 1 On appelle polynôme à n indéterminées sur A toute famille presque nulle d'éléments de A indexée par $\mathbb{N}^n$. Il est alors de la forme $P = (a_i)_{i \in \mathbb{N}^n}$.
L'ensemble des polynômes à n indéterminées à coefficients dans A est noté $A[X_1, \dots, X_n]$.

Déf 2 Soient $P = (a_i)_{i \in \mathbb{N}^n}$, $Q = (b_i)_{i \in \mathbb{N}^n} \in A[X_1, \dots, X_n]$. $\lambda \in A$.
On définit une addition : $(P+Q) = (a_i + b_i)_i$
une multiplication $(P.Q) = \left(\sum_{k+l=i} a_k b_l\right)_i$;
une multiplication par un scalaire $(\lambda P) = (\lambda a_i)_i$;

Thm 3 Muni de ces opérations, l'ensemble $A[X_1, \dots, X_n]$ est une A algèbre commutative.

Thm 4 Dans $A[X_1, \dots, X_n]$, tout polynôme s'écrit de façon unique comme combinaison linéaire de $(X_1^{i_1} \dots X_n^{i_n})_{(i_1, \dots, i_n) \in \mathbb{N}^n}$ des coefficients de la combinaison linéaire sont ceux du polynôme.

Propr 5 Propriété universelle [GOB]
Soient $\varphi : A \to R$ une A-algèbre et $(x_1, \dots, x_n) \in R^n$.
Alors il existe un unique morphisme de A-algèbres $\Phi : A[X_1, \dots, X_n] \to R$ tel que $\Phi(X_i) = x_i$ $\forall i \in [\![1, n]\!]$.

Thm 6 Isomorphisme canonique. [RDO]
$A[X_1, \dots, X_{n-1}, X_n]$ et $A[X_1, \dots, X_{n-1}][X_n]$ sont isomorphes via $\Phi : P = \sum_{i \in \mathbb{N}^n} a_i X_1^{i_1} \dots X_n^{i_n} \longrightarrow \sum_{k \in \mathbb{N}} \left(\sum_{i_1, \dots, i_{n-1} \in \mathbb{N}^{n-1}} a_{i_1, \dots, i_{n-1}, k} X_1^{i_1} \dots X_{n-1}^{i_{n-1}} \right) X_n^k$

Ex 7 Le déterminant est un polynôme à plusieurs indéterminées des coefficients : les polynômes caractéristiques sont des polynômes à plusieurs indéterminées.

2. Degré et polynômes homogènes. [RDO]

Déf 8 Soient $n, q \in \mathbb{N}$ tels que $1 \leq q \leq n$. On appelle degré partiel des polynôme P de $A[X_1, \dots, X_n]$ relativement à l'indéterminée X_q, le degré de P comme élément de $A[X_1, \dots, X_{q-1}, X_{q+1}, \dots, X_n][X_q]$. Ce degré est noté $\deg_{X_q}(P)$

Déf 9 Soit $P = (a_i)_i \in A[X_1, \dots, X_n]$. Si $P = 0$, $\deg(P) = -\infty$.
Si $P \neq 0$ $\deg P = \max \{ |i| \mid i \in \mathbb{N}^n, a_i \neq 0 \}$
$\deg(P)$ est appelé le degré total de P.

Prop 10 quels que soient les polynômes $P, Q \in A[X_1, \dots, X_n]$.
$\deg(P+Q) \leq \sup(\deg P, \deg Q)$
$\deg(P.Q) \leq \deg(P) + \deg Q$ (égalité si A intègre).

Ex 11 $P = Y - X^2 + XYZ$ est de degré total 3.

Appli 12 A intègre $\Rightarrow A[X_1, \dots, X_n]$ intègre [TALU] p212

Déf 13 $p \in \mathbb{N}$, $P = (a_i)_i \in A[X_1, \dots, X_n]$ est dit p-homogène ssi l'inégalité $|i| \neq p \Rightarrow a_i = 0$

Ex 14 $P = X^2 + XY$ est homogène.

Rq Si deux polynômes de $A[X_1, \dots, X_n]$ sont respectivement p-homogène et q-homogène, leur produit est $(p+q)$-homogène

Classification des polynômes homogènes (de degré ≤ 2)
degré 0 : les constantes $\lambda \in A$ ...
degré 1 : les formes linéaires
degré 2 : les formes quadratiques

Appli 15 Théorème de Molien. [LEI] et [PEY] DVPT
$\forall k \in \mathbb{N}$, on note A_k l'espace des polynômes homogènes de degré k de $A[X_1, \dots, X_n]$. Soit G groupe fini de $GL_n(\mathbb{C})$. On définit une action de G sur les A_k. On note $a_k(G) = \dim A_k^G$
Alors $\sum_{k \geq 0} a_k(G) X^k = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I - gX)}$

Déf 16 On appelle polynôme dérivé partiel de $P \in A[X_1, \dots, X_n]$ par rapport à l'indéterminée X_q $(1 \leq q \leq n)$ le polynôme dérivé de P considéré comme un élément de $A[X_1, \dots, X_{q-1}, X_{q+1}, \dots, X_n][X_q]$. On le note $\partial P / \partial X_q$. [RDO]

p185 p171 p188 p189 p190 p195 et p221 p193

sans référence

p196

Thm 17 D'EULER [RDO]

Soit K un corps commutatif de caractéristique nulle, $P \in K[X_1, \dots, X_n]$. Sont équivalents :

1) P est p-homogène. 2) $\sum_{q=1}^{n} X_q \frac{\partial P}{\partial X_q} = pP$.

3. Propriétés arithmétiques

p199

Prop 18 A factoriel $\Rightarrow A[X_1, \dots, X_n]$ factoriel.

Prop 19 On se place ici dans un corps commutatif K.

Sur $n \geq 2$, l'anneau $K[X_1, \dots, X_n]$ n'est pas principal.

Prop 18 : $K[X_1, \dots, X_n]$ factoriel.

↳ existence d'une décomposition unique en produit de polynômes irréductibles non associés

↳ existence du PGCD et du PPCM

↳ le théorème de Gauss subsiste (mais pas le théorème de Bézout).

p198

Prop 20 Dans $K[X_1, \dots, X_n]$, le polynôme A est divisible par le polynôme $X_n - B$ (B polynôme de $K[X_1, \dots, X_{n-1}]$) ssi le polynôme obtenu en substituant, dans A, le polynôme B à l'indéterminée X_n soit le polynôme nul.

Ex 21 Dans $\mathbb{Q}[X, Y, Z]$, $X^3 + Y^3 + Z^3 + mXYZ$ est divisible par $X+Y+Z$ ssi $m = -3$

Coro 22 $A \in K[X_1, \dots, X_n]$ est divisible par $\prod_{1 \leq i < j \leq n} (X_j - X_i)$ ssi A est divisible séparément par chacun des $X_j - X_i$ $(1 \leq i < j \leq n)$.

II. FONCTIONS POLYNÔMES

1. Fonctions polynômes et prolongement des identités

[RDO] p191

Def 23 $P = \sum a_{i_1 \dots i_n} X_1^{i_1} \dots X_n^{i_n} \in A[X_1, \dots, X_n]$. L'application $\tilde{P} : A^n \to A$, $(x_1, \dots, x_n) \mapsto \sum_{i \in \mathbb{N}^n} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}$ est appelée fonction polynôme de n variables (abus d'écriture : $P = \tilde{P}$)

Prop 24 Soient A intègre et $(A_i)_{1 \leq i \leq n}$ une famille de sous-ensembles infinis de A. Alors pour tout polynôme $P \neq 0$ de $A[X_1, \dots, X_n]$, il existe une infinité de points de $\prod_{i=1}^{n} A_i$ en lesquels la fonction polynôme $\tilde{P}$ prend une valeur non nulle.

p192

Thm 25 Si A intègre infini, alors $\Psi : P \in A[X_1, \dots, X_n] \to \tilde{P}$ est un isomorphisme de $A[X_1, \dots, X_n]$ sur l'algèbre des fonctions polynômes de n variables sur A.

Appli 26 Si $K = \mathbb{R}$ ou $\mathbb{C}$, $P \in K[X_1, \dots, X_n]$. Si $\tilde{P}$ s'annule sur un ouvert non vide, le polynôme P est nul.

Def 27 Une identité entre m polynômes $F_1, \dots, F_m$ de $A[X_1, \dots, X_n]$ est une égalité de la forme $G(F_1(X_1, \dots, X_n), \dots, F_m(X_1, \dots, X_n)) = 0$ où $G(Y_1, \dots, Y_m) \in A[Y_1, \dots, Y_m]$ [GOB]

p172 (A)

Prop 28 PROLONGEMENT DES IDENTITÉS. [GOB] p173.

A intègre de cardinal infini. $P_1, \dots, P_m \in A[X_1, \dots, X_n] \setminus \{0\}$.

Soit $V(P_j) = \{x \in A^n / P_j(x) = 0\}$. Si $F_1, F_2 \in A[X_1, \dots, X_n]$ sont tels que $\forall x \in A^n \setminus (\bigcup_j V(P_j))$, $F_1(x) = F_2(x)$, alors $F_1 = F_2$.

Appli 29 K un corps ; $M, N \in \mathcal{M}_n(K)$. Alors $\chi(MN) = \chi(NM)$

2. Corps finis [SER] p 13-14

Soit q une puissance d'un nombre premier p et soit K un corps à q éléments.

Thm 30 CHEVALLEY-WARNING. DVPT

Soient $P_1, \dots, P_r \in K[X_1, \dots, X_n]$ tels que $\sum_{i=1}^{r} \deg(P_i) < n$. et V l'ensemble de leurs zéros communs dans K^n.

On a card $V \equiv 0 [p]$.

Coro 31 Avec les mêmes conditions et si les P_i sont sans terme constant, alors ils ont un zéro commun non trivial.

Appli 32 Toute forme quadratique d'au moins 3 variables sur K a un zéro non trivial.

3. Corps $\mathbb{R}$ ou $\mathbb{C}$. [GOB] p173

Prop 33 Si F_1, $F_2 \in \mathbb{K}[X_1, \dots, X_n]$ ($\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$) tels que les fonctions polynômes coïncident sur un ouvert non vide de $\mathbb{K}^n$. Alors $F_1 = F_2$.

Appli 34 On obtient le théorème de Cayley-Hamilton.

III APPLICATION : POLYNÔMES SYMÉTRIQUES ET SEMI-SYM.

1. Polynômes symétriques

[RDO] p200 **Def 35** $P \in A[X_1, \dots, X_n]$ est dit symétrique si $\forall \sigma \in \mathfrak{S}_n$ $\sigma(P) = P$ où $\sigma(P)$ est le polynôme obtenu en substituant aux n indéterminées $X_1, \dots, X_n$ les n polynômes $X_{\sigma(1)}, \dots, X_{\sigma(n)}$.

Def 36 Dans $A[X_1, \dots, X_n]$, on définit pour $k \in [\![1, n]\!]$
$$\sigma_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} X_{i_1} \dots X_{i_k}.$$ On pose $\sigma_0 = 1$.

[RDO] p201 ou [GOB] p177 **Prop 37** Soit $P \in A[X_1, \dots, X_n, Y]$, $P = \prod_{i=1}^{n} (Y - X_i)$
alors $P = \sum_{k=1}^{n} (-1)^k \sigma_k(X_1, \dots, X_n) Y^{n-k}$.

Rq On retrouve les relations coefficients-racines connues dans $A[X]$.

[RDO] p201 **Thm 38** Les polynômes σ_k sont symétriques et appelés polynômes symétriques élémentaires. Ils sont k-homogènes.

[FGN Alg 1] **Thm 39** KRONECKER.
Soit P polynôme unitaire de $\mathbb{Z}[X]$ dont les racines complexes sont toutes de module plus petit que 1 et tel que $P(0) \neq 0$.
Alors les racines de P sont des racines de l'unité.

[RDO] p202 **Def 40** • On appelle poids du monôme $X_1^{i_1} \dots X_n^{i_n}$ l'entier $\sum_{k=1}^{n} k i_k$
• Le poids d'un polynôme P est le maximum des poids de ses monômes. Il vaut $-\infty$ si $P = 0$. On le note $\pi(P)$.

(B) **Thm / Def 41** Soit P un polynôme symétrique de $A[X_1, \dots, X_n]$.
P a même degré partiel par rapport à chaque indéterminée.
Ce degré s'appelle ordre de P et est noté $\omega(P)$.

Thm 42 THÉORÈME DE STRUCTURE [RDO] p204
Soit P un polynôme symétrique de $A[X_1, \dots, X_n]$ de degré p et d'ordre ω. Alors il existe un unique polynôme Φ de $A[Y_1, \dots, Y_n]$ tel que $P(X_1, \dots, X_n) = \Phi(\sigma_1, \dots, \sigma_n)$.
Ce polynôme Φ est de poids p et de degré ω.

(C) (D)

Algorithme pour déterminer Φ [RDO] p205
Soit $P \in A[X_1, \dots, X_n]$ symétrique non nul.
On suppose P homogène $P = \sum_{i_1 + \dots + i_n = p} a_{i_1, \dots, i_n} X_1^{i_1} \dots X_n^{i_n}$.
On ordonne $\mathbb{N}^n$ avec l'ordre lexicographique.
Soit $k = (k_1, \dots, k_n)$ le plus grand n-uplet tel que $a_{i_1, \dots, i_n} \neq 0$.
↳ On peut montrer que $k_1 \geq \dots \geq k_n$.
On calcule alors $\Phi = P - a_k \sigma_1^{k_1 - k_2} \sigma_2^{k_2 - k_3} \dots (\sigma_{n-1})^{k_{n-1} - k_n} (\sigma_n)^{k_n}$
On a Φ • symétrique homogène.
• nul ou de degré inférieur à k strictement pour l'ordre lexicographique.
Si Φ nul, l'algorithme est terminé.
Sinon on recommence l'opération avec Φ.
↳ En un nombre fini d'opération, on aboutira à un polynôme nul. (Car décroissance stricte de la suite des degrés)

2. Polynômes semi-symétriques [GOB] p180

Def 43 Un polynôme $P \in A[X_1, \dots, X_n]$ est dit semi-symétrique si $\forall \tau \in \mathcal{A}_n$ $\tau(P) = P$

Rq on aurait pu définir les polynômes alternés :
Si F est alterné, $\forall \sigma \in \mathfrak{S}_n$, $\sigma(F) = \varepsilon(\sigma) F$.
↳ les polynômes alternés sont des polynômes semi-symétriques particuliers.

Def 44 On définit $V(X_1, \dots, X_n) = \prod_{i<j} (X_i - X_j)$.

Ex 45 V est semi-symétrique (et symétrique en caractéristique 2)

Prop 46 Soit $\mathbb{K}$ un corps avec car $\mathbb{K} \neq 2$. Pour que $F \in \mathbb{K}[X_1, \dots, X_n]$ soit semi-symétrique, il faut il suffit qu'il existe P, Φ symétriques (nécessairement uniques) tels que $F = P + V\Phi$.

Références

- [RDO] Ramis, Deschamps, Odoux, Algèbre 1, 2ème édition
- [GOB] Gobet, Algèbre commutative 2ème édition.
- [SER] Serre, Cours d'arithmétique.
- [TAU] Tauvel, Algèbre
- FGN Algèbre 1 pour dipt Kronecker.

Autres dépts possibles.

- Thm de structure
- Irréductibilité de Dst
- Polynômes semi-symétriques
- Etude des fonctions polynomiales associées.

(A) On aurait pu réfuter le cas important de $A = \mathbb{Z}$.

(B) " " " " le degré du polynôme obtenu en remplaçant les indéterminées par les T_k. [RDO] p202.

(C) " " " . le fait que l'algèbre des polynômes symétriques de $A[X_1, \dots X_n]$ est engendré par les polynômes symétriques élémentaires [TAU] p219

(D) . les relations de Newton [RDO] p207

On peut faire une partie "Résultant"

Théorème de Chevalley-Warning

Camille FRANCINI

Référence : SERRE : Cours d'arithmétique, p. 12-13 ou ZAVIDOVIQUE : Un Max de Math, p. 32

Soit $\mathbb{K}$ un corps fini de cardinal $q = p^k$ avec p premier. Donc $\text{car}(\mathbb{K}) = p$.

Théorème 1 (*Chevalley-Warning*)

Soient $P_1, P_2, ..., P_r \in \mathbb{K}[X_1, .., X_n]$ et $V = \{x \in \mathbb{K}^n \ / \ \forall i,\ P_i(x) = 0\}$

Si $\sum_{i=1}^{r} \deg P_i < n$ alors $\text{Card}(V) \equiv 0\,[p]$

Lemme 1

Soit m un entier positif ou nul. Alors la somme $S(X^m) = \sum_{x \in \mathbb{K}} x^m$ est égale à $\begin{cases} -1 & \text{si } m \geq 1 \text{ et divisible par } q-1 \\ 0 & \text{sinon.} \end{cases}$

Convention : $x^m = 1$ si $m = 0$ pour tout x même $x = 0$.

Preuve du lemme :

Si $m = 0$

Alors tous les termes de la somme sont égaux à 1. Donc $S(X^m) = q * 1 = 0$ car on est en caractéristique p.

Si $m \geq 1$ et $q - 1 \mid m$

Alors $0^m = 0$ et $x^m = 1$ si $x \neq 0$. Donc $S(X^m) = (q-1) * 1 = -1$.

Si $m \geq 1$ mais $q - 1 \nmid m$

Comme $\text{Card}(\mathbb{K}) = q = p^k$; $\mathbb{K}^*$ est cyclique d'ordre $q - 1$.
Donc il existe un élément $y \in \mathbb{K}^*$ d'ordre $q - 1$ donc tel que $y^m \neq 1$.
Alors $S(X^m) = \sum_{x \in \mathbb{K}^*} x^m = \sum_{x \in \mathbb{K}^*} y^m x^m = y^m S(X^m)$.
Soit $(1 - y^m)S(X^m) = 0$ donc $S(X^m) = 0$. ■

Preuve du théorème :

• Soit

$$P = \prod_{i=1}^{r} (1 - P_i^{q-1})$$

Soit $x \in \mathbb{K}$, avec $x \in V$, alors $\forall i\ P_i(x) = 0$ donc $P(x) = 1$.
Si $x \notin V$, alors $\exists i \ / \ P_i(x) \neq 0$
Donc par le théorème de Lagrange : $P_i(x)^{q-1} = 1$ ie $P(x) = 0$.
Ainsi P est l'indicatrice de V.

• De plus pour $Q \in \mathbb{K}[X_1, .., X_n]$, on pose :

$$\underline{\tilde{S} = \sum_{(x_1,..,x_n)\in\mathbb{K}^n} Q(x_1, .., x_n)}$$

Alors $\underline{\text{Card}(V) \equiv \tilde{S}(P)\,[p]}$ ($\tilde{S}(P) = \sum_{x\in V} 1 + \sum_{x\notin V} 0$ et on utilise la caractéristique p).

Il ne reste donc plus qu'à montrer que $\tilde{S}(P) = 0$.

• Or comme $\sum_{i=1}^{r} \deg P_i < n$ alors $\deg P < n(q-1)$.

Ainsi P est combinaison linéaire de monôme $X^\alpha = X_1^{\alpha_1}...X_n^{\alpha_n}$ avec

$\sum_{i=1}^{n} \alpha_i < n(q-1)$. Il suffit alors de prouver que pour un tel monôme $\tilde{S}(X^\alpha) = 0$.

Or $\tilde{S}(X^\alpha) = \prod_{i=1}^{n} S(X_i^{\alpha_i})$. Et comme $\sum_{i=1}^{n} \alpha_i < n(q-1)$ on a au moins un des $\alpha_i < q-1$. Donc d'après le lemme $S(X_i^{\alpha_i}) = 0$ donc $\tilde{S}(X^\alpha) = 0$.

D'où le résultat : $\tilde{S}(P) = 0$ et donc $\text{Card}(V) \equiv 0\,[p]$ ■

Démonstration détails : $\tilde{S}(X_1^{\alpha_1}..X_n^{\alpha_n}) = S(X^{\alpha_1})...S(X^{\alpha_n})$

$$\begin{aligned}\tilde{S}(X_1^{\alpha_1}..X_n^{\alpha_n}) \sum_{(x_1,..,x_n)\in\mathbb{K}^n} x_1^{\alpha_1}..x_n^{\alpha_n} &= \sum_{x_1\in\mathbb{K}} x_1^{\alpha_1} \sum_{(x_2,..,x_n)\in\mathbb{K}^{n-1}} x_2^{\alpha_2}..x_n^{\alpha_n} \\ &= .. \\ &= S(X^{\alpha_1})...S(X^{\alpha_n})\end{aligned}$$

■

Théorème de Molien

Camille FRANCINI

Référence : LEICHTNAM : Exercices corrigés de mathématiques posés à l'oral des concours Polytechnique et des ENS Tome Algèbre et Géométrie p. 95 (ou PEYRÉ: L'algèbre discrète de la transformée de Fourier : Niveau M1)

Définition 1

On note A_k l'espace des polynômes homogènes à n variables de degré k.

Théorème 1 (*Molien*)

Soit G un groupe fini de $\mathcal{GL}_n(\mathbb{C})$. On définit une action de G sur les A_k, $a_k = \dim A_k$ et $a_k(G) = \dim A_k^G$.
Alors on a :

$$\sum_{k\geq 0} a_k(G)X^k = \frac{1}{|G|}\sum_{g\in G}\frac{1}{\det(I-gX)}$$

Lemme 1

Pour $|z|<1$, $\frac{1}{(1-z)^n} = \sum_{k=0}^{+\infty} a_k z^k$

Preuve du Lemme 1

A_k admet pour base $\{X_1^{i_1}...X_n^{i_n}/i_1,..i_n \in \mathbb{N} \text{ et } i_1+...+i_n = k\}$. Ainsi

$$a_k = \dim A_k = \text{card}\{(i_1,...,i_n)\in\mathbb{N}^n / i_1+...+i_n = k\}$$

D'une part, pour $|z|<1$ on a : $\left(\sum_{p=0}^{+\infty} z^p\right)^n = (\frac{1}{1-z})^n$.

D'autre part, le produit de Cauchy de ces n séries entières donne :

$$\left(\sum_{p=0}^{+\infty} z^p\right)^n = \sum_{k=0}^{+\infty}\left(\sum_{i_1+...+i_n=k} 1\right) z^k$$

Donc a_k est le coefficient de z^k dans le développement de $(\frac{1}{1-z})^n$. Donc :

$$\sum_{k\geq 0} a_k z^k = (\frac{1}{1-z})^n$$

■

Lemme 2

Soit V un $\mathbb{C}$-espace vectoriel de dimension finie n. Soit $\varphi : G \to \mathcal{GL}(V)$ un morphisme de groupe. On note $V^G = \{v\in V/\varphi(g)(v) = v, \forall g\in G\}$.
Alors:

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

Preuve du Lemme 2

On pose pour cela : $p_G = \frac{1}{|G|}\sum_{g\in G}\varphi(g)$

Alors, on remarque que $\forall v\in V, \forall h\in G$ on a :

$$\varphi(h)(p_G(v)) = \frac{1}{|G|}\sum_{g\in G}\varphi(h)\varphi(g)(v)$$

Mais $g \mapsto hg$ est une permutation de G et $\varphi(h)\varphi(g) = \varphi(hg)$
Nous avons donc que $\varphi(h)(p_G(v)) = p_G(v)$ donc $p_G(V) \subset V^G$.
De plus, pour tout $v \in V^G$, on a : $p_G(v) = v$, donc $p_G(V) = V^G$.
Comme $\varphi(h)p_G = p_G$ pour tout $h \in G$ on a $p_G \circ p_G = p_G$.
Ainsi p_G est un projecteur d'image V^G et donc:

$$\underline{\mathrm{rg}(p_G) = \dim V^G = \mathrm{Tr}(p_G) = \frac{1}{|G|}\sum_{g\in G}\mathrm{Tr}(\varphi(g))} \quad \blacksquare$$

Preuve du théorème

Etapes :
1) Création d'un morphisme σ entre G et Aut$A$ tel que $\forall g \in G$ σ_g induit un automorphisme sur A_k
2) A partir du lemme 1, on montre que pour $|z| < 1$, $\dfrac{1}{\det(I - zg)} = \sum_{k=0}^{+\infty} \mathrm{Tr}(g_k)z^k$
3) On conclut alors sur l'égalité.

Etape 1 :

Soit $(e_1, ..., e_n)$ une base de V.
Pour $g \in G$, on définit σ_g tel que si $g(e_h) = \sum_{1\le j\le n} u_{j,h}e_j$, $P \in A$, on pose

$$\sigma_g(P)(X_1, .., X_n) = P(\sum_{1\le j\le n} u_{j,1}X_j, ..., \sum_{1\le j\le n} u_{j,n}X_j)$$

Soit σ : $\begin{array}{ccc} G & \to & \mathrm{Aut}\ A \\ g & \mapsto & \sigma_g \end{array}$ (ie $\sigma_g = \sigma(g)$). Vérifions déjà que l'application σ est bien définie. Déjà:

$$\begin{aligned} \sigma_g \circ \sigma_{g'}(P) &= \sigma_g(\sigma_{g'}(P)) \\ &= \sigma_{g'}(P)\left(\sum_{1\le j\le n} u_{j,1}X_j, ..., \sum_{1\le j\le n} u_{j,n}X_j\right) \\ &= \sigma_{g\circ g'}(P) \end{aligned}$$

De plus on a $\sigma_I = I$ donc $\forall g \in G$, $(\sigma_g)^{-1} = \sigma_{g^{-1}}$ et on a donc que σ_g est bien dans Aut(A)
De plus $\forall k \in \mathbb{N}$, $\forall g \in G$, on a $\sigma_g(A_k) \subset A_k$. Or A_k est de dimension finie et σ_g est injective.
Donc σ_g induit un isomorphisme de A_k que l'on appelle g_k $(= \sigma_{|A_k})$.

Etape 2 :

On sait que $0 \le a_k(G) \le a_k$, donc (d'après le lemme 1) la série $\sum_0^{+\infty} a_k(G)z^k$ converge pour $|z| < 1$.

De plus, d'après le théorème de Lagrange $\forall g \in G$, $g^{|G|} = I$. Or le polynôme $X^{|G|} - 1$ est scindé à racines simples sur $\mathbb{C}$. Ansi, g est diagonalisable, il existe donc $u \in \mathcal{GL}(V)$ tel que : ugu^{-1} admette une matrice diagonale dans la base $(e_1, .., e_n)$. Alors, comme : $\sigma_{|A_k}(ugu^{-1}) = \sigma_{|A_k}(u)\sigma_{|A_k}(g)\sigma_{|A_k}(u^{-1})$, on a :

$$\mathrm{Tr}(g_k) = \mathrm{Tr}(\sigma_{|A_k}(ugu^{-1}))$$

On peut ainsi se ramener au cas où $g \in G$ est une matrice diagonale dans la base $(e_1, .., e_n)$: $\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$

Les λ_i sont de module 1 (car $g^{|G|} = I$).
Ainsi pour $|z| < 1$ on a :

$$\frac{1}{\det(I - zg)} = \prod_{i=1}^{n}\frac{1}{1 - \lambda_i z} = \prod_{i=1}^{n}\left(\sum_{p=0}^{+\infty}\lambda_i^p z^p\right) = \sum_{p=0}^{+\infty} v_p z^p$$

Avec $v_p = \sum_{\substack{k_1,\dots k_n \in \mathbb{N}, \\ k_1+..+k_n=p}} \lambda_1^{k_1}...\lambda_n^{k_n}$ (produit de Cauchy des séries)

Or $g_p(X_1^{k_1}...X_n^{k_n}) = \lambda_1^{k_1}...\lambda_n^{k_n} X_1^{k_1}..X_n^{k_n}$.

Ainsi $v_p = \mathrm{Tr}(g_p)$ et donc $\underline{\dfrac{1}{\det(I - zg)} = \sum_{k=0}^{+\infty} \mathrm{Tr}(g_k) z^k}$

Etape 3 :

Pour tout $k \in \mathbb{N}$: $\varphi : \begin{array}{ccc} G & \to & \mathcal{GL}(A_k) \\ g & \mapsto & g_k \end{array}$ est un morphisme de groupe.
Ainsi, on peut appliquer le lemme 2, et on a:

$$a_k(G) = \dim(A_k^G) = \frac{1}{|G|} \sum_{g \in G} \mathrm{Tr}(g_k)$$

Donc pour $|z| < 1$:

$$\underline{\frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I - zg)} = \sum_{k=0}^{+\infty} a_k(G) z^k}$$

■

Bonus :

$$a_p = \binom{p}{p+n-1}$$

En effet on a $\sum_{p \geq 0} a_p z^p = (\frac{1}{1-z})^n$ et $(\frac{1}{1-z})^{(n-1)} = \frac{(n-1)!}{(1-z)^n} = \sum_{p=0}^{+\infty} (p+n-1)..(p+1) z^p$.
Ainsi en associant les deux on obtient :

$$a_p = \frac{(p+n-1)...(p+1)}{(n-1)!} = \binom{p}{p+n-1}$$