ANNEAU D'INVARIANTS
D'UN SOUS-GROUPE FINI DE $\mathbf{GL}_n$

JEAN-PAUL CALVI

Le problème étudie certaines propriétés de l'anneau des invariants d'un groupe fini de matrices.

Notations et rappels

a) $\mathbb{C}[x_1,x_2,\dots,x_n]$ désigne l'anneau des polynômes à coefficients complexes à n indéterminées. On rappelle que

(1) Tout polynôme $p \in \mathbb{C}[x_1,x_2,\dots,x_n]$ s'écrit $p = \sum_{\alpha\in\Delta} c_\alpha x^\alpha$ où $c_\alpha \in \mathbb{C}$, Δ est un ensemble fini de multi-indice $\alpha = (\alpha_1,\alpha_2,\dots,\alpha_n) \in \mathbb{N}^n$ et $x^\alpha = x_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}$. On regardera couramment p comme une fonction du vecteur $x = (x_1,\dots,x_n)$. On écrit parfois $p(x)$ au lieu de p.

(2) La *longueur* $|\alpha|$ du multi-indice α est le nombre $|\alpha| = \alpha_1+\alpha_2+\dots+\alpha_n$. Le *degré* du polynôme p est donné par $\deg p = \max\{|\alpha| \,:\, c_\alpha \neq 0\}$. Le degré du polynôme nul est égal à $-\infty$.

(3) Un polynôme h est dit *homogène* de degré k si $h(\lambda x) = \lambda^k h(x)$. On notera que le polynôme nul est homogène de tout degré. Tout polynôme p admet une représentation unique de la forme $p = \sum_{i=0}^{\deg p} h_i$ où h_i est un polynôme homogène de degré i. Les polynômes h_i s'appellent les *composantes homogènes* de p.

b) Notant $s_i(x) = (x_1+x_2+\dots+x_r)^i$, $i = 1,2...$, on pourra librement utiliser le fait que *tout polynôme **symétrique** $p \in \mathbb{C}[x_1,x_2,\dots,x_r]$ s'écrit $p = q(s_1,s_2,\dots,s_r)$ pour un certain polynôme $q \in \mathbb{C}[x_1,x_2,\dots,x_r]$*.

c) Pour $n \in \mathbb{N}^\star$, $\mathbf{GL}_n$ désigne le groupe des matrices $n\times n$ *inversibles* à coefficients complexes. Le sous-groupe des matrices orthogonales (c'est-à-dire vérifiant ${}^tAA = I$) est noté $\mathbf{O}_n$.

d) Pour $n \in \mathbb{N}^\star$, $\mathbf{S}_n$ désigne le groupe des permutations de l'ensemble $\{1,2,\dots,n\}$.

e) L'ordre d'un groupe G est noté $|G|$.

---

1. Sous-groupes finis de $\mathbf{GL}_n$

1.1. Soit G un sous-ensemble non vide, fini de $\mathbf{GL}_n$. Montrer que les assertions suivantes sont équivalentes :

(1) G est un sous-groupe de $\mathbf{GL}_n$,

(2) G est stable pour la multiplication des matrices.

1.2. Déterminer le sous-groupe de $\mathbf{GL}_2$ engendré par $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Ce sous-groupe sera noté C_4.

Date: 16 janvier 2005.

Préparation au concours interne de l'agrégation de mathématiques. Merci de signaler les erreurs et les imprécisions en écrivant à calvi@picard.ups-tlse.fr.

1.3. Déterminer le sous-groupe de $\mathbf{GL}_2$ engendré par les matrices $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Ce sous-groupe sera noté V_4.

1.4. Donner pour tout $n \in \mathbb{N}^\star$ un exemple de sous-groupe non cyclique d'ordre $2n$ de $\mathbf{GL}_2$.

1.5. Pour tout $\sigma \in \mathbf{S}_n$, on définit M_σ la matrice $n \times n$ dont tous les coefficients sont nuls excepté, pour $i = 1,2,\dots,n$, le $\sigma(i)$-ième coefficient de la i-ème colonne qui vaut 1.

(1) Montrer que $M_\sigma \in GL_n$.
(2) L'application qui à $\sigma \in \mathbf{S}_n$ fait correspondre $M_\sigma \in \mathbf{GL}_n$ est-elle un morphisme de groupe ?

Si H est un sous-groupe de S_n. On note $G_H = \{M_\sigma \,:\, \sigma \in H\}$.

(3) Montrer que G_H est un sous-groupe fini de $\mathbf{GL}_n$.

2. Définition de l'anneau des invariants

Soit G un sous-groupe fini de $\mathbf{GL}_n$. On dit qu'un polynôme $p \in \mathbb{C}[x_1,x_2,\dots,x_n]$ est invariant par G si $p(A.x) = p(x)$ pour tout $A \in G$. L'ensemble des polynômes invariants par G est noté $\mathbb{C}[x_1,x_2,\dots,x_n]^G$

2.1. Montrer qu'un polynôme p est *invariant* par G si et seulement si toutes ses composantes homogènes sont invariantes par G.

2.2. Montrer que $\mathbb{C}[x_1,x_2,\dots,x_n]^G$ est un sous-anneau de $\mathbb{C}[x_1,x_2,\dots,x_n]$. Cet anneau est appelé *l'anneau des invariants* de G.

2.3. Quel est l'anneau $\mathbb{C}[x_1,x_2,\dots,x_n]^{G_{\mathbf{S}_n}}$?

2.4. Montrer que si le groupe G est engendré par les matrices $A_1,\dots,A_k$ alors pour que p soit invariant par G il faut et il suffit que $p(A_i.x) = p(x)$ pour $i = 1,\dots,k$.

2.5. Déterminer $\mathbb{C}[x_1,x_2]^G$ lorsque $G = \{\pm Id\}$.

2.6. Trouver un sous-groupe G de $\mathbf{GL}_2$ tel que
$$\mathbb{C}[x_1,x_2]^G = \{p(x_1^2,x_2^2) \,:\, p \in \mathbb{C}[x_1,x_2]\}.$$

2.7. Montrer que si G est un sous-groupe de $\mathbf{O}_n$ alors
$$\{p(x_1^2 + x_2^2 + \dots + x_n^2) \,:\, p \in \mathbb{C}[x_1]\} \subset \mathbb{C}[x_1,x_2,\dots,x_n]^G.$$

3. L'opérateur de Reynolds

Soit G un sous-groupe fini de $\mathbf{GL}_n$. L'opérateur de Reynolds de G est l'application R_G définie par
$$R_G \,:\, \begin{array}{ccc} \mathbb{C}[x_1,x_2,\dots,x_n] & \longrightarrow & \mathbb{C}[x_1,x_2,\dots,x_n] \\ p(x) & \longmapsto & \frac{1}{|G|}\sum_{A\in G} p(A.x) \end{array}$$

Il est immédiat que R_G est une application $\mathbb{C}$-linéaire de $\mathbb{C}[x_1,x_2,\dots,x_n]$.

3.1. Montrer les assertions suivantes

(1) Pour tout $p \in \mathbb{C}[x_1,x_2,\dots,x_n]$, on a $R_G(p) \in \mathbb{C}[x_1,x_2,\dots,x_n]^G$,
(2) Pour tout $p \in \mathbb{C}[x_1,x_2,\dots,x_n]^G$, on a $R_G(p) = p$.

3.2. Calculer $R_{C_4}(p)(x_1,x_2)$.

4. Le théorème de Noether

Soit G un sous-groupe fini de $\mathbf{GL}_n$. On dit qu'une famille $f_1,f_2,\dots,f_l$ d'éléments de $\mathbb{C}[x_1,x_2,\dots,x_n]^G$ *engendre* $\mathbb{C}[x_1,x_2,\dots,x_n]^G$ lorsque pour tout polynôme p invariant par G, il existe $h \in \mathbb{C}[x_1,x_2,\dots,x_l]$ tel que $p = h(f_1,f_2,\dots,f_l)$. On note alors

$$\mathbb{C}[x_1,x_2,\dots,x_n]^G = \mathbb{C}[f_1,f_2,\dots,f_l].$$

4.1. Quelle(s) famille(s) connaissez-vous qui engendre(nt) $\mathbb{C}[x_1,x_2,\dots,x_n]^{G_{S_n}}$? (On ne demande pas de démonstration.)

Le but de cette partie est de démontrer le théorème suivant dû à *Emmy Noether.*

Théorème 4.1.

$$\mathbb{C}[x_1,x_2,\dots,x_n]^G = \mathbb{C}[R_G(x^\alpha) \,:\, |\alpha| \leq |G|].$$

4.2. Montrer que pour tout $k \in \mathbb{N}$, il existe des entiers non nuls a_α tels que

$$(x_1 + x_2 + \cdots + x_n)^k = \sum_{|\alpha|=k} a_\alpha x^\alpha.$$

4.3. Etant donnée une matrice $A = (a_{ij})$, on note $A_i = (a_{i1},\dots,a_{in})$ la i-ième ligne de A et $A_i \cdot x$ le produit du vecteur A_i par le vecteur x c'est-à-dire $A_i \cdot x = a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n$. Pour $u = (u_1,u_2,\dots,u_n) \in \mathbb{C}^n$, on pose

$$S_k(u,x) = \sum_{A\in G} (u_1A_1 \cdot x + u_2A_2 \cdot x + \cdots + u_nA_n \cdot x)^k.$$

(1) Montrer que

$$S_k(u,x) = \sum_{|\alpha|=k} b_\alpha R_G(x^\alpha) u^\alpha$$

où les b_α sont des coefficients non nuls que l'on précisera.

(2) On note $U_A = u_1A_1 \cdot x + u_2A_2 \cdot x + \cdots + u_nA_n \cdot x$. Montrer que $S_k(u,x)$ est une fonction polynomiale symétrique des U_A, $A \in G$. En déduire qu'il existe un polynôme $q \in \mathbb{C}[x_1,x_2,\dots,x_{|G|}]$ tel que

$$S_k(u,x) = q(S_1(u,x),\dots,S_{|G|}(u,x)).$$

(3) En déduire une preuve du théorème de Noether.

4.4. Déterminer trois polynômes f_1,f_2 et f_3 tels que $\mathbb{C}[x_1,x_2]^{C_4} = \mathbb{C}[f_1,f_2,f_3]$. (Le théorème précédent fournit, après calcul, seulement quatre polynômes distincts et on montre qu'un de ces quatre polynômes peut être éliminé.)

4.5. Déduire du théorème de Noether qu'il existe toujours une famille d'au plus $\binom{n+|G|}{n}$ éléments qui engendre l'anneau des invariants d'un groupe d'ordre $|G|$.

Laboratoire de Mathématiques E. Picard, Université Paul Sabatier 31062 Toulouse Cedex 4 FRANCE.

E-mail address: `calvi@picard.ups-tlse.fr`