150

Exemples d'actions de groupes sur des espaces de matrices

Dans toute la suite, K est un corps quelconque (sauf contre-indication) et E est un K-espace vectoriel de dimension finie n, et F est un K-espace vectoriel de dimension finie m.

I) Action par translation : [H2G2, chap I.A et I.B]

<u>Déf 1 :</u> $GL_n(K)$ agit sur $M_{n,m}(K)$ par translation à gauche via l'application
$$\tau_L : \begin{array}{ccc} GL_n(K) & \to & (M_{n,m}(K) \to M_{n,m}(K)) \\ A & \to & (M \to AM) \end{array}$$

<u>Déf 2 :</u> $GL_m(K)$ agit sur $M_{n,m}(K)$ par translation à droite via l'application
$$\tau_R : \begin{array}{ccc} GL_m(K) & \to & (M_{n,m}(K) \to M_{n,m}(K)) \\ A & \to & (M \to MA^{-1}) \end{array}$$

<u>Prop 3 :</u> Les orbites par l'action par τ_L sont caractérisées par le noyau : pour $A, B \in M_{n,m}(K)$, A et B sont dans la même orbite ssi $\mathrm{Ker}(A) = \mathrm{Ker}(B)$

<u>Prop 4 :</u> Les orbites par l'action par τ_R sont caractérisées par le noyau : pour $A, B \in M_{n,m}(K)$, A et B sont dans la même orbite ssi $\mathrm{Im}(A) = \mathrm{Im}(B)$

<u>Ex 5 :</u> Pour $A = \begin{pmatrix} 2 & 3 & 1 \\ 0 & 2 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} A = B$ et $\mathrm{Ker}(A) = \mathrm{Ker}(B) = \mathrm{Vect}\left(\begin{pmatrix} 1 \\ -2 \\ 4 \end{pmatrix}\right)$

De plus, $A \begin{pmatrix} 1 & -1 & -1/2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = B$, et $\mathrm{Im}(A) = \mathrm{Im}(B) = K^2$

<u>Thm 6 :</u> Par le pivot de Gauss à gauche (resp. à droite), on peut trouver dans chaque orbite une matrice échelonnée en lignes (resp. échelonnée en colonnes).

<u>Appli 7 :</u> * Les transvections engendrent $SL_n(K)$.
* Les transvections et dilatations engendrent $GL_n(K)$

II) Action de Steinitz, par équivalence

1) Définition, caractérisation des orbites [H2G2, chap I.2 et I.3]

<u>Déf 8 :</u> * $GL_n(K) \times GL_m(K)$ agit par équivalence sur $M_{n,m}(K)$ via l'application
$$\alpha : \begin{array}{ccc} GL_n(K) \times GL_m(K) & \to & (M_{n,m}(K) \to M_{n,m}(K)) \\ (A \ , \ B) & \to & (M \to AMB^{-1}) \end{array}$$

* 2 matrices M et N de $M_{n,m}(K)$ sont dites équivalentes si elles sont dans la même orbite

<u>Prop 9 :</u> 2 matrices équivalentes représentent la même application linéaire $u \in \mathcal{L}(F,E)$ dans 2 paires de bases différentes

<u>Ex 10 :</u> On note (e_1, e_2, e_3) la base canonique de $\mathbb{R}^3$ et (e_1', e_2') celle de $\mathbb{R}^2$ et $u \in \mathcal{L}(\mathbb{R}^3, \mathbb{R}^2)$ dont la matrice dans ces bases est $\begin{pmatrix} 1/2 & 1/2 & 1 \\ 1/2 & -1/2 & 1 \end{pmatrix} = M$; sa matrice dans les bases (e_2, e_1, e_3) et $(e_1' + e_2', e_1' - e_2')$ est $\begin{pmatrix} 0 & \frac{1}{2} & 1 \\ \frac{1}{2} & 0 & 0 \end{pmatrix} = N$, et on a :
$$\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & -1/2 \end{pmatrix} M \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = N$$

<u>Thm 11 (théorème du rang) :</u> Pour $M \in M_{n,m}(K)$, si M est de rang r, elle est dans l'orbite de la matrice $J_r = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$.

<u>Corollaire 12 :</u> M et N sont dans la même orbite ssi $rg(M) = rg(N)$
(On note O_r l'orbite des matrices de rang r)

<u>Prop 13 :</u> Lorsque $m = n$, on a : pour tout $M \in M_{n,m}(K)$, $rg(M) = rg({}^tM)$

DEV1 [FGN1, exo 7.16]

<u>Théorème 13.5 :</u> Soit T_s l'ensemble des matrices triangulaires supérieures inversibles. $T_s \times T_s$ agit par équivalence sur $GL_n(K)$. Alors $\{P_\sigma \mid \sigma \in \mathfrak{S}_n\}$ est un système de représentants des orbites, et on a $GL_n(K) = \coprod_{\sigma \in \mathfrak{S}_n} T_s P_\sigma T_s$

2) Topologie des orbites (cas où $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$) [H2G2, chap I.4]

Prop 14: L'adhérence de l'orbite de rang r est l'ensemble des matrices de rang plus petit :

$$\overline{\mathcal{O}_r} = \bigsqcup_{k\in[\![0;r]\!]} \mathcal{O}_k$$

Cor 15: $GL_n(K) = \mathcal{O}_n$ est dense dans $M_n(K)$

Prop 16: $\mathcal{O}_0 = \{0\}$ est l'unique orbite fermée pour l'action par équivalence

$\mathcal{O}_{\min(n,m)}$ est l'unique orbite ouverte pour l'action par équivalence

Cor 17: $GL_n(K)$ est un ouvert de $M_n(K)$

Cor 18: Le rang n'est pas une application continue sur $M_{n,m}(K)$

III) Actions par conjugaison : matrices semblables

1) Généralités [H2G2, chap III.1 à III.4]

Déf 19: * $GL_n(K)$ agit par conjugaison sur $M_n(K)$ via l'application :

$$\beta : \begin{array}{ccc} GL_n(K) & \to & (M_n(K) \to M_n(K)) \\ P & \to & (M \to PMP^{-1}) \end{array}$$

* 2 matrices sont dites semblables si elles sont dans une même orbite par β

Prop 20: 2 matrices semblables représentent le même endomorphisme $u\in L(E)$ dans 2 bases différentes

Déf 21: Une matrice est dite diagonalisable si elle est dans l'orbite d'une matrice diagonale.
Une matrice est dite trigonalisable si elle est dans l'orbite d'une matrice triangulaire supérieure

Prop 22: Le polynôme minimal, le polynôme caractéristique, le rang, le déterminant et la trace sont des invariants pour cette action.

Cor 23: Une matrice est diagonalisable ssi son polynôme minimal est scindé à racines simples.
Une matrice est trigonalisable ssi son polynôme minimal est scindé ssi son polynôme caractéristique est scindé

Cor 24: Si K est algébriquement clos, toute matrice de $M_n(K)$ est trigonalisable

2) Classification des orbites [H2G2, chap III.1 à III.4]

Thm 25: Les orbites de matrices diagonalisables sont caractérisées par le polynôme caractéristique

Contre-ex 26: Le polynôme minimal n'est pas un invariant total de similitude :
$\begin{pmatrix}1&0&0\\0&2&0\\0&0&2\end{pmatrix}$ et $\begin{pmatrix}1&0&0\\0&1&0\\0&0&2\end{pmatrix}$ ont pour polynôme minimal $(X-1)(X-2)$, mais ne sont pas semblables.

Thm 27: Si $A\in M_n(\mathbb{C})$, A est diagonalisable ssi son orbite est fermée

Déf 28: On appelle bloc de Jordan de taille p associé à λ la matrice $J_p(\lambda) = \begin{pmatrix}\lambda & 1 & \\ & \ddots & 1 \\ 0 & & \lambda\end{pmatrix} \in M_p(K)$

Thm 29: Toute matrice nilpotente est dans l'orbite d'une matrice diagonale par blocs
$\begin{pmatrix}J_{p_1}(0) & & 0 \\ & \ddots & \\ 0 & & J_{p_k}(0)\end{pmatrix}$ (dite réduite de Jordan) avec $p_1 \geq \dots \geq p_k$

Exemple 30: $N = \begin{pmatrix}0&1&0&-3&6\\0&0&1&-2&4\\0&0&0&0&2\\0&0&0&0&1\\0&0&0&0&0\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\0&1&2&3&4\\0&0&1&2&3\\0&0&0&1&2\\0&0&0&0&1\end{pmatrix}\begin{pmatrix}0&1&0&0&0\\0&0&1&0&0\\0&0&0&0&0\\0&0&0&0&1\\0&0&0&0&0\end{pmatrix}\begin{pmatrix}1&-2&1&0&0\\0&1&-2&1&0\\0&0&1&-2&1\\0&0&0&1&-2\\0&0&0&0&1\end{pmatrix}$

Appli 31: Le nombre d'orbites de matrices nilpotentes est égale au nombre de partitions de l'entier n.

Thm 32 (invariant de similitude sur $\mathbb{C}$) toute matrice de $M_n(\mathbb{C})$ (on note $\lambda_1,\dots,\lambda_r$ ses valeurs propres) est dans l'orbite d'une matrice de la forme $\begin{pmatrix}J_{p_1}(\lambda_1) & & 0 \\ & \ddots & \\ 0 & & J_{p_r}(\lambda_r)\end{pmatrix}$

Prop 33 : Soient $A, B \in M_n(\mathbb{R})$ telles que A et B sont dans la même orbite sous l'action de $GL_n(\mathbb{C})$, alors elles sont dans la même orbite sous l'action de $GL_n(\mathbb{R})$.

Cor 34 : L'orbite de $M \in M_n(\mathbb{R})$ sous l'action de $GL_n(\mathbb{R})$ est l'intersection de son orbite sous l'action de $GL_n(\mathbb{C})$ avec $M_n(\mathbb{R})$

Déf 35 : On note, pour $P(X) = X^n - \sum_{i=0}^{n-1} a_i X^i \in K[X]$, la matrice compagnon C_P associée :

$$C_P = \begin{pmatrix} 0 & & -a_0 \\ & & -a_1 \\ I_{deg(P)-1} & & \vdots \\ & & -a_{n-1} \end{pmatrix} \in M_{deg(P)}(K)$$

Thm 36 (décomposition de Frobenius) : Soit $M \in M_n(K)$. Alors il existe une famille de polynômes unitaires non constants $F_1, \dots, F_s \in K[X]$ telle que

1. $F_s | \dots | F_1$
2. M est dans l'orbite de la matrice diagonale par blocs $\begin{pmatrix} C_{F_1} & & 0 \\ & \ddots & \\ 0 & & C_{F_s} \end{pmatrix}$

Th 37 (de Brauer) : [Objectif Agrég]
Soient $\sigma, \tau \in \mathfrak{S}_n$; σ et τ sont conjuguées dans $\mathfrak{S}_n$ ssi P_σ et P_τ sont conjuguées par β dans K (où K est de caractéristique nulle)

3) Action de $O_n(\mathbb{R})$ [Gourdon], chap 5, §3.2]

Déf 38 : $O_n(\mathbb{R})$ agit sur $M_n(\mathbb{R})$ par conjugaison (restriction à $O_n(\mathbb{R})$ de β, notée γ).
Cela correspond à un changement de base orthonormée

Déf 39 : Une matrice $M \in M_n(\mathbb{R})$ est dite normale si ${}^tMM = M{}^tM$

Thm 40 : Toute matrice normale est dans l'orbite d'une matrice de la forme

$$\begin{pmatrix} \lambda_1 & & & & & 0 \\ & \ddots & & & & \\ & & \lambda_r & & & \\ & & & P_1 & & \\ & & & & \ddots & \\ 0 & & & & & P_s \end{pmatrix}$$

où les λ_i sont réels et les P_j sont des blocs de la forme $\begin{pmatrix} a_j & -b_j \\ b_j & a_j \end{pmatrix}$.

Si $M \in S_n(\mathbb{R})$, alors $s = 0$

Rq 41 : On peut aussi faire agir $U_n(\mathbb{C})$ sur $M_n(\mathbb{C})$ et obtenir un résultat similaire (en se rappelant que l'adjoint de M est ${}^t\overline{M}$) au théorème 40, où les blocs $\begin{pmatrix} a_j & -b_j \\ b_j & a_j \end{pmatrix}$ sont remplacés par $\begin{pmatrix} a_j + ib_j & 0 \\ 0 & a_j - ib_j \end{pmatrix}$

IV) Action par congruence [H2G2, chap V]

Dans cette partie, K est un corps de caractéristique $\neq 2$

Déf 42 : * $GL_n(K)$ agit sur $S_n(K)$ par congruence via l'application :

$$\eta : \begin{array}{l} GL_n(K) \to (S_n(K) \to S_n(K)) \\ P \to (M \to PM{}^tP) \end{array}$$

* 2 matrices sont dites congruentes si elles sont dans la même orbite

Rem 43 : 2 matrices congruentes représentent la même forme quadratique dans 2 bases différentes

Exemple 44 : La forme quadratique $q(x) = x_1^2 + 3x_2^2 + 7x_3^2 + 2x_1x_2 + 8x_2x_3$ est représentée par les matrices $\begin{pmatrix} 1 & 1 & 0 \\ 1 & 3 & 4 \\ 0 & 4 & 7 \end{pmatrix} = M$ et $N = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ (on trouve N par la réduction de Gauss), et on a :

$$\begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 2 & -2 & 1 \end{pmatrix} M \begin{pmatrix} 1 & -1 & 2 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} = N$$

Déf 55 : Si 2 matrices M et N vérifient $N = PM{}^tP$, on a $\det(N) = (\det(P))^2 \det(M)$
Ainsi, l'image du déterminant dans $K^*/(K^*)^2$ est invariant par l'action par congruence.
On l'appelle le discriminant (de la matrice ou de la forme quadratique associée)

Déf 56 : On appelle rang d'une forme quadratique le rang d'une matrice qui la représente (bien défini car invariant par l'action par congruence)

Thm 57 : Si $K = \mathbb{C}$, toute matrice d'une forme quadratique de rang r est dans l'orbite de $\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$

Thm 58 (d'inertie de Sylvester) : Si $K = \mathbb{R}$, pour toute matrice M d'une forme quadratique de rang r, il existe $p \in [\![0; r]\!]$ tel que M soit dans l'orbite de $\begin{pmatrix} I_p & 0 & 0 \\ 0 & -I_{r-p} & 0 \\ 0 & 0 & 0 \end{pmatrix}$, où p ne dépend que de la forme quadratique (il est invariant).

DEV 2

Thm 59 : Si $K = \mathbb{F}_q$ (q impair) et si $\alpha \in \mathbb{F}_q^*$ n'est pas un carré dans $\mathbb{F}_q^*$, alors un système de représentant des orbites de l'action par congruence est :

$$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & I_r \end{pmatrix} \middle| r \in [\![0; n]\!] \right\} \cup \left\{ \begin{pmatrix} 0 & 0 & 0 \\ 0 & I_r & 0 \\ 0 & 0 & \alpha \end{pmatrix} \middle| r \in [\![0; n-1]\!] \right\}$$

Rem 60 : 2 matrices inversibles de $M_n(\mathbb{F}_q)$ sont congruentes ssi elles ont même discriminant

[H2G2] : Histoires hédonistes de groupes et géométries, Caldero, Germoni
[FGN1] : Oraux X-ENS, algèbre 1, Francinou, Gianella, Nicolas
[Gourdon] : Les maths en tête, algèbre, Gourdon

Décomposition de Bruhat

Bastien Thomas

Soit T_s l'ensemble des matrices triangulaires supérieures inversibles. On désigne par P_σ la matrice qui applique la permutation σ sur les vecteurs de la base canonique.

Théorème 1. *Le groupe $T_s \times T_s$ agit sur $GL_n(\mathbb{K})$ et un système de représentants des orbites est $\{P_\sigma, \sigma \in \mathfrak{S}_n\}$*

Pour $M = (m_{i,j}) \in \mathrm{GL}_n(\mathbb{K})$, on considère l'algorithme suivant :

for $j \leftarrow 1$ **to** n **do**
  Soit $i_j = \max\{k, m_{k,j} \neq 0\}$;
  $L_{i_j} \leftarrow \frac{1}{m_{i_j,j}} L_{i_j}$;
  for $i \leftarrow 1$ **to** $i_j - 1$ **do**
    $L_i \leftarrow L_i - m_{i,j} L_{i_j}$;
  end
  for $j' \leftarrow j+1$ **to** n **do**
    $C_{j'} \leftarrow C_{j'} - m_{i_j,j'} C_j$;
  end
end

— Comme M est toujours inversible, les indices (i_j) sont tous bien définis, et forment une application de $\{1, \ldots, n\}$ dans lui-même injective, donc une permutation σ.
— L'algorithme renvoie une matrice dont tous les coefficients sont nuls sauf les $m_{i_j,j}$ qui valent 1. C'est donc P_σ.
— Les opérations élémentaires effectuée par l'algorithme reviennent toutes à multiplier M à gauche ou à droite par une matrice triangulaire supérieure inversible.

L'algorithme montre bien qu'il existe T_1 et T_2 dans T_s telles que $M = T_1 P_\sigma T_2$.

Montrons maintenant l'unicité de σ.

Soit $\sigma, \tau \in (\mathfrak{S}_n)^2$, soient $T_1, T_2, T_3, T_4 \in (T_s)^4$ telles que $T_1 P_\sigma T_2 = T_3 P_\tau T_4$.

Posons $T = T_3{}^{-1} T_1$ et $T' = T_4 T_2{}^{-1}$, T et T' sont triangulaires supérieures inversibles et $P_\tau T' = T P_\sigma$.

Ceci nous donne : $t_{\sigma(i),j} = t'_{i,\tau^{-1}(j)}$, ce qui se réécrit $t_{\sigma(i),\tau(j)} = t'_{i,j}$.

Alors, si $\sigma \neq \tau$, il existerait i tel que $\tau(i) < \sigma(i)$ D'où $0 = t_{\sigma(i),\tau(i)} = t'_{i,i} \neq 0$ ce qui est absurde.

Donc $\sigma = \tau$, et on a bien l'unicité du terme P_σ dans la décomposition de Bruhat.

Classification des formes quadratiques sur $\mathbb{F}_q$

Bastien Thomas

Théorème 1. *Soit $\mathbb{F}_q$ un corps fini de caractéristique différente de 2. Soit E un $\mathbb{F}_q$-espace vectoriel de dimension n. Soit $\alpha \in \mathbb{F}_q$ qui n'est pas un carré dans $\mathbb{F}_q$. Un système de représentants des orbites de l'action par congruence de $GL_n(\mathbb{F}_q)$ sur $M_n(\mathbb{F}_q)$ est constitué des matrices de la forme :*

$$diag(0,\dots,0,1,\dots,1) \text{ et } diag(0,\dots,0,1,\dots,1,\alpha)$$

Lemme 1. *On a : $\mathbb{F}_q^* = (\mathbb{F}_q^*)^2 \sqcup \alpha(\mathbb{F}_q^*)^2$ et :*
— $\#(\mathbb{F}_q^2) = \frac{q+1}{2}$
— $\#(\alpha(\mathbb{F}_q^*)^2) = \frac{q-1}{2}$

Démonstration. L'application φ définie ci-dessous est un morphisme de groupes.

$$\begin{aligned} \varphi \colon \mathbb{F}_q^* &\to \mathbb{F}_q^* \\ x &\mapsto x^2 \end{aligned}$$

Son noyau est $\{-1,1\}$ de cardinal 2 car on a supposé que $\mathbb{F}_q$ était de caractéristique différente de 2.

Donc $\#(\mathbb{F}_q^*)^2 = \#(\varphi(\mathbb{F}_q^*)) = \frac{q-1}{2}$.

On a alors aussi $\#(\alpha(\mathbb{F}_q^*)^2) = \frac{q-1}{2}$.

Ces deux ensembles étant disjoints, on obtient le résultat. □

Lemme 2. *Pour $a, b \in (\mathbb{F}_q^*)^2$, il existe des solutions à l'équation $ax^2 + by^2 = 1$.*

Démonstration. D'après le Lemme 1 et par un argument de bijectivité, on obtient :

$$\# \{x^2, x \in \mathbb{F}_q\} = \# \left\{ \frac{1-by^2}{a}, y \in \mathbb{F}_q \right\} = \frac{q+1}{2}$$

Ces deux ensembles ne peuvent alors pas être disjoints et possèdent donc un élément en commun. Ceci donne l'existence d'une solution à l'équation $x^2 = \frac{1-by^2}{a}$. □

Démontrons alors le Théorème 1.

Montrons d'abord que toute forme quadratique non dégénérée est congrue à $\operatorname{diag}(1,\dots,1)$ où à $\operatorname{diag}(1,\dots,1,\alpha)$.

Démonstration. Raisonnons par récurrence sur la dimension n de E.

- Si $n = 1$, soit q une forme quadratique non dégénérée sur E, soit x un vecteur non nul de E. D'après le Lemme 1, il existe $b \in \mathbb{F}_q^*$ tel que ou bien $q(x) = b^2$, ou bien $q(x) = \alpha b^2$. On obtient le résultat en considérant la base $(b^{-1}x)$.
- Soit $n \geq 2$, soit q une forme quadratique non dégénérée. On considère un plan engendré par deux vecteurs orthogonaux non isotropes u et v. Notons $q(u) = a$ et $q(v) = b$. Par le Lemme 2, il existe $x, y \in \mathbb{F}_q^2$ tel que $q(xu + yv) = ax^2 + by^2 = 1$. On applique alors l'hypothèse de récurrence à l'orthogonal de $xu + yv$ pour obtenir le résultat.

□

Comme $\mathrm{diag}(1, \ldots, 1)$ et $\mathrm{diag}(1, \ldots, 1, \alpha)$ n'ont pas le même discriminant, elles sont bien dans deux orbites distinctes pour l'action par congruence.

Pour obtenir le résultat demandé, il suffit de raisonner sur un supplémentaire du noyau de la forme quadratique, puis de compléter avec une base du noyau.

Source : H2G2, Perrin