106

Groupe linéaire d'un ev de dimension finie E. Sous groupes de GL(E). Applications

Dans toute la leçon, on prendra k un corps commutatif et E un k-ev de dimension $n \geq 1$ $(n < +\infty)$

I) Généralités sur le groupe linéaire

1) Premières définitions et propriétés [Per] [Gou]

Def 1: Le groupe linéaire $GL(E)$ est le groupe des k-automorphismes de E. C'est-à-dire les applications k-linéaires de E dans E.

Def 2: Si on se donne une base de E, on a un isomorphisme entre $GL(E)$ et $GL(n,k) = GL_n(k)$, le groupes des matrices $n \times n$, inversibles, à coefficients dans k.

Appli 3: Etudier $GL(E)$ grâce à cet isomorphisme qui permet l'utilisation du calcul matriciel.

Prop 4: $u \in GL(E) \iff u$ envoie une base sur une base.

Def 5: Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E, il existe une unique forme n-linéaire alternée sur E prenant la valeur 1 sur $\mathcal{B}$. On l'appelle le déterminant dans la base $\mathcal{B}$ et on le note $\det_{\mathcal{B}}$.
Si $x_1, \dots, x_n \in E$ $\left(x_i = \sum_{j=1}^{n} x_{ij} e_j\right)$, le déterminant de $(x_1, \dots, x_n)$ dans la base $\mathcal{B}$ est :

$$\det_{\mathcal{B}}(x_1, \dots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma)\, x_{1\sigma(1)} \cdots x_{n\sigma(n)}$$

Prop 6. $\mathfrak{S}_n$, le groupe des permutations, s'injecte dans $GL_n(k)$ par l'application

$$\begin{array}{rcl} \mathfrak{S}_n & \longrightarrow & GL_n(k) \\ \sigma & \longmapsto & M_\sigma = (a_{ij})_{i,j} \end{array} \quad \text{avec } a_{ij} = \delta_{\sigma(i),j}$$

Thm 7. (Cayley)

Tout groupe fini de cardinal n est isomorphe à un sous groupe de $\mathfrak{S}_n$

Corollaire 8: Tout groupe fini de cardinal n s'injecte dans $GL_n(k)$

Thm 9: (Burnside) [X-ENS 2]

Un sous groupe de $GL_n(\mathbb{C})$ d'exposant fini est fini DVLPT

2) Générateurs [Per] [Esc]

Prop-def 10: Soit H un hyperplan de E et $u \in GL(E)$ tels que $u_{|H} = Id_H$. On a équivalence entre les points suivants

1) $\det u = \lambda \neq 1$
2) u admet une valeur propre $\lambda \neq 1$ et u est diagonalisable
3) On a $\mathrm{Im}(u - Id) \not\subset H$
4) dans une base convenable, u a pour matrice

$$\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ & 1 & \\ 0 & & \lambda \end{pmatrix} ; \text{ avec } \lambda \in k^*, \ \lambda \neq 1$$

On dit alors que u est une dilatation d'hyperplan H, de droite D (propre pour λ), de rapport λ.
On a $D = \mathrm{Im}(u - Id)$, $K = \ker(u - Id)$

Rque 11: Si $\lambda = -1$ et $\mathrm{car}(k) \neq 2$, u est appelée une réflexion

Prop-def 12: Soit H un hyperplan de E, d'équation $f \in E^*$ $(H = \ker f$ avec $f \neq 0)$
Soit $u \in GL(E)$, $u \neq Id$, tel que $u_{|H} = Id_H$. Les conditions suivantes sont équivalentes :

1) On a $\det u = 1$
2) u n'est pas diagonalisable
3) On a $D = \mathrm{Im}(U - Id) \subset H$
4) l'homomorphisme induit, $\bar{u} : E/H \to E/H$ est l'identité de E/H

5) Il existe $a \in H$, $a \neq 0$ tel que :

$$\forall x \in E, \ u(x) = x + f(x)a$$

6) Dans une base convenable, u a pour matrice

$$\begin{pmatrix} 1 & & 0 \\ & \ddots & 1 \\ 0 & & 1 \end{pmatrix}$$

On dit alors que u est une transvection d'hyperplan H, et de droite D. On a $D = (a)$ et $D \subset H$

Def 13 : Une matrice carrée d'ordre n de la forme

$T_{ij}(\alpha) = I + \alpha E_{ij}$, avec $j \neq i$ $\left(E_{ij} = \begin{array}{c} \\ i\text{-ème ligne} \end{array} \begin{pmatrix} & 0 & \\ 0 & 1 & 0 \\ & 0 & \end{pmatrix}^{j\text{-ième colonne}} \right)$

est appelée matrice de transvection.

Ex 14 : Si $n = 3$ $\quad T_{23}(\alpha) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & \alpha \\ 0 & 0 & 1 \end{pmatrix}$

Prop 15 : Soient $T = \{ T_{ij}(\alpha) \mid \alpha \in \mathbb{R}^* \}$ et D l'ensemble des matrices diagonales inversibles de $GL(\mathbb{R}^n)$, alors $T \cup D$ engendre $GL(\mathbb{R}^n)$

Prop 16 : Les transvections et les dilatations engendrent $GL(E)$

Prop 17 : Les transvections sont conjuguées dans $GL(E)$

II) Exemples de sous groupes

1) Groupe spécial linéaire $SL(E)$ [Per]

Def 18 : Le noyau de l'application déterminant est appelé groupe spécial linéaire et est noté $SL(E)$

Prop 19 : $SL(E)$ est isomorphe au groupe $SL(n, k) = SL_n(k)$ des matrices de déterminant 1.

Prop 20 : Les transvections engendrent $SL(E)$

Prop 21 : Si $n \geq 3$, les transvections sont conjuguées dans $SL(E)$

2) Centre et dérivé [Per] [OA]

Thm 22 :

- Le centre Z de $GL(E)$ est formé des homothéties $x \mapsto \lambda x$, avec λ appartenant à k^*.
  Z est donc isomorphe à k^*
- Le centre de $SL(E)$ est $Z \cap SL(E)$, il est isomorphe à $\mu_n(k) = \{ \lambda \in k \mid \lambda^n = 1 \}$

Def 23 :
- Le quotient de $GL(E)$ par son centre est appelé le groupe projectif linéaire et est noté $PGL(E)$
- De même le quotient de $SL(E)$ par son centre est noté $PSL(E)$

Thm 24 :

- On a $D(GL_n(k)) = SL_n(k)$, sauf pour $n = 2$ et $k = \mathbb{F}_2$
- On a $D(SL_n(k)) = SL_n(k)$ sauf pour $n = 2$ et $k = \mathbb{F}_2$ ou $n = 2$ et $k = \mathbb{F}_3$

Appli 25 : (Théorème de Frobenius-Zolotarev) [OA]

Soient p un nombre premier ≥ 3, $\mathbb{F}_p$ le corps fini à p éléments et V un ev sur $\mathbb{F}_p$ de dimension finie. Alors, pour tout $u \in GL(V)$, on a

$$\varepsilon(u) = \left(\frac{\det(u)}{p} \right) \quad \text{(symbole de Legendre)}$$

DVLPT

3) Groupes unitaires, orthogonal et symplectique [Per] [Gri]

Def 26 : Soit f une forme sesquilinéaire sur E, non dégénérée, on appelle isométries de E (relativement à f) les automorphismes $u \in GL(E)$ tels que :

$$\forall x, y \in E, \quad f(u(x), u(y)) = f(x, y)$$

Thm 27 :

L'ensemble G des isométries forment un sous groupe de $GL(E)$

Def 28 : • Si f est hermitienne, G est appelé groupe unitaire noté $U(f)$

• Si f est symétrique, G est appelé groupe orthogonal noté $O(f)$
• Si f est alternée, G est appelé groupe symplectique noté $Sp(f)$.

Def 29: $O(n,\mathbb{R}) := \{A \in \mathcal{M}_n(\mathbb{R}) \mid {}^tAA = I\} = \{A \in \mathcal{M}_n(\mathbb{R}) \mid A^tA = I\}$ est un sous groupe de $GL_n(\mathbb{R})$ dit groupe orthogonal.

Exemple 30: (Etude de $O(2,\mathbb{R})$) [Gri]

• $O(2,\mathbb{R})$: $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$A \in O(2,\mathbb{R}) \iff \begin{cases} a^2+c^2 = 1 \\ b^2+d^2 = 1 \\ ab+cd = 0 \end{cases}$

ce qui finit par donner :

• Soit $A \in SO(2,\mathbb{R})$ (isométries de déterminant 1) et

$A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ rotation d'angle θ et de centre O

• Soit $A \notin SO(2,\mathbb{R})$ et $A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$

symétrie orthogonale par rapport à la droite d'angle polaire $\theta/2$

Exemple 31: Etude de $O(3,\mathbb{R})$

III) Action de $GL(E)$ [Per] [Ulm] [Gou]

Prop 32: $GL(E)$ agit transitivement par translation à gauche sur E. $\forall g \in GL(E)$, $\forall x \in E$, $g.x = g(x)$.

Prop 33:
$|GL_n(\mathbb{F}_q)| = (q^n-1)\dots(q^n-q^{n-1})$
$|SL_n(\mathbb{F}_q)| = (q^n-1)\dots(q^n-q^{n-2})q^{n-1} = |PGL_n(\mathbb{F}_q)|$
$|PSL_n(\mathbb{F}_q)| = \dfrac{|SL_n(\mathbb{F}_q)|}{d}$ où $d = \mathrm{pgcd}(n, q-1)$

Prop 34: $GL(E)$ agit sur $\mathbb{P}(E)$ par translation à gauche

Appli 35: On a les isomorphismes exceptionnels suivants
1) $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) = PGL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$
2) $PGL_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$ et $PGL_2(\mathbb{F}_2) \simeq \mathfrak{A}_4$
3) $PGL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4) \simeq \mathfrak{A}_5$
4) $PGL_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$ et $PSL_2(\mathbb{F}_5) \simeq \mathfrak{A}_5$

DVLPT

Prop 36: $GL_n(k)$ agit par congruence sur $\mathcal{M}_n(k)$

Prop 37: $GL_n(k)$ agit par translation sur les bases de k^n.

Appli 38: Changement de base, matrice de passage.

IV) Topologie pour $k = \mathbb{R}$ ou $\mathbb{C}$ [Mnei]

1) Densité

Thm 39: $GL_n(k)$ est un ouvert dense dans $\mathcal{M}_n(k)$

Appli 40: $A, B \in \mathcal{M}_n(k)$, AB et BA ont même polynôme caractéristiques

Appli 41: il existe une base de $\mathcal{M}_n(k)$ formée de matrices inversibles

2) Connexité

Prop 42: $GL_n(\mathbb{C})$ et $SL_n(\mathbb{C})$ sont connexes par arcs

Appli 43: si $p \leq n-1$, l'ensemble A_p des matrices de rang p est une partie connexe de $\mathcal{M}_n(k)$

Appli 44: L'ensemble des projecteurs de rang p dans $\mathcal{M}_n(\mathbb{R})$ est connexe.

3) Compacité

Prop 45: $O(n)$ et $SO(n)$ sont compacts dans $\mathcal{M}_n(\mathbb{R})$

Appli 46: la décomposition polaire
$$O(n) \times S_n^{++}(\mathbb{R}) \to GL_n(\mathbb{R}) \quad \text{est un homéomorphisme}$$
$$(O, S) \mapsto OS$$

Référence : [Per] Perrin, Cours d'analyse

[Gou] Gourdon, Analyse

[OA] Objectif Agregation

[Gri] Grifone Algèbre linéaire

[Esc] Escofier, toute l'algèbre de la licence

[Mnei] Mneimné Testard Intro à la theorie des groupes de Lie classiques.

Théorème de Frobenius-Zolotarev

Théorème 1. *Soit $p \in \mathcal{P}$ un nombre premier impair et V un $\mathbb{F}_p$-espace vectoriel de dimension finie n. Alors, pour tout $u \in GL(V)$ on a* $\varepsilon(u) = \text{signature}(u) = \left(\frac{\det(u)}{p}\right)$.

Démonstration. Soit $n = \dim_{\mathbb{F}_p}(V)$, on a alors $p^n = \text{card}(V)$ et la signature ε est un morphisme de groupe défini sur $GL(V)$ puisque : $GL(V) \subset \text{Bij}(V) \simeq S_{p^n}$ le groupe des bijections de $[\![1, p^n]\!]$.

Méthode 1.

- *Montrons qu'il existe un unique morphisme de groupe $f : \mathbb{F}_p^* \longrightarrow \{-1, 1\}$ tel que $\varepsilon = f \circ \det$*
- *Montrons que $f = \left(\frac{\div}{p}\right)$ où $\left(\frac{\div}{p}\right)$ désigne le symbole de Legendre modulo p.*

Lemme 1. *Pour tout groupe abélien G et tout morphisme de groupe $\alpha : GL(V) \longrightarrow G$ il existe un unique morphisme $f : \mathbb{F}_p^* \longrightarrow G$ tel que $\alpha = f \circ \det$.*

On appliquera le résultat à $G = \{-1, 1\} \simeq \mathbb{Z}/2\mathbb{Z}$ et $\alpha = \varepsilon$.

Démonstration. :
Existence : Soient G un groupe abélien et $\alpha : GL(V) \longrightarrow G$ un morphisme de groupe.

Objectif 1. *montrons que $SL(V) \subset$* Ker(α), *le but étant clairement de pouvoir* passer au quotient *et obtenir un* diagramme commutatif.

Or, pour $p \geq 3$, $D(GL(V)) = SL(V)$ et $D(GL(V))$ étant engendré par les commutateurs, il suffit de montrer que pour tout $[f, g] = f \circ g \circ f^{-1} \circ g^{-1}$ on a $[f, g] \in \text{Ker}(\alpha)$. Alors, G étant abélien et α un morphisme, on a immédiatement :

$$\alpha(f \circ g \circ f^{-1} \circ g^{-1}) = \alpha(f)\alpha(g)\alpha(f)^{-1}\alpha(g)^{-1} = \alpha(f)\alpha(f)^{-1}\alpha(g)\alpha(g)^{-1} = 1_G.$$

D'où $SL(V) \subset \text{Ker}(\alpha)$ et il existe une unique application $\overline{\alpha}$ telle que

$$\overline{\alpha} : GL(V)/SL(V) \longrightarrow G \text{ et } \alpha = \overline{\alpha} \circ \pi$$

où π désigne la surjection canonique de $GL(V) \longrightarrow GL(V)/SL(V)$. Or, $\det : GL(V) \longrightarrow \mathbb{F}_p^*$ est un morphisme de groupe surjectif de noyau $SL(V)$, par passage au quotient il existe un unique isomophisme de groupe noté $\overline{\det}$ tel que :

$$\overline{\det} : GL(V)/SL(V) \longrightarrow \mathbb{F}_p^* \text{ et } \det = \overline{\det} \circ \pi$$

Ainsi, on a naturellement $\alpha = \overline{\alpha} \circ \pi$ et $\det = \overline{\det} \circ \pi$. Par bijectivité de $\overline{\det}$, on déduit que $\pi = \overline{\det}^{-1} \circ \det$ et :

$$\alpha = (\overline{\alpha} \circ \overline{\det}^{-1}) \circ \det = f \circ \det \text{ où on a posé } f = \overline{\alpha} \circ \overline{\det}^{-1}.$$

Unicité : Supposons qu'il existe f' morphisme de $\mathbb{F}_p^* \longrightarrow G$ tel que $\alpha = f' \circ \det$ et montrons que $f = f'$. Pour $x \in \mathbb{F}_p^*$, par surjectivité de det, il existe $u \in GL(V)$ tel que $x = \det(u)$ et :

$$f'(x) = f'(\det(u)) = (f' \circ \det)(u) = \alpha(u)$$

de même $f(x) = f(\det(u)) = (f \circ \det)(u) = \alpha(u)$ Ce qui donne finalement $f = f'$. □

Méthode 2. *On va appliquer le lemme au cas où $\alpha = \varepsilon$ défini par*

$$\varepsilon : \begin{array}{ccc} GL(V) & \longrightarrow & \{-1, 1\} \\ u & \longmapsto & \text{signature}(u) \end{array}$$

et au groupe à 2 éléments $\{1, -1\} \simeq \mathbb{Z}/2\mathbb{Z}$.

D'après ce qui précède, il existe un unique morphisme $f : \mathbb{F}_p^* \longrightarrow \{1, -1\}$ tel que $\varepsilon = f \circ \det$. Il reste à montrer que f est exactement le **symbole de Legendre** $\left(\frac{\div}{p}\right)$ modulo p. Or, $\mathbb{F}_p^*$ étant cyclique, définir un morphisme de $\mathbb{F}_p^* \longmapsto \{1, -1\}$ revient à *définir l'image d'un générateur.* Ainsi, pour ζ un générateur de $\mathbb{F}_p^*$, soit $f(\zeta) = 1$ et f est trivial, soit $f(\zeta) = -1$ et f est non trivial. Ainsi, il y a exactement deux morphismes de $\mathbb{F}_p^*$ dans $\{-1, 1\}$ dont un seul est non trivial.

Lemme 2. *Le symbole de Legendre $\left(\frac{\div}{p}\right)$ est l'unique morphisme non trivial de $\mathbb{F}_p^*$ dans $\{-1, 1\}$.*

Démonstration. Le symbole de Legendre est multiplicatif, vaut 1 sur les carrés de $\mathbb{F}_p^*$ et -1 sinon. Il s'agit alors bien d'un morphisme de groupe de $\mathbb{F}_p^*$ sur $\{1,-1\}$ qui est non trivial puisqu'il y a exactement $\frac{p-1}{2}$ éléments dans $\mathbb{F}_p^*$ qui ne sont pas des carrés. C'est le seul morphisme non trivial via l'étude effectuée sur l'image d'un générateur de $\mathbb{F}_p^*$ par un morphisme de groupe de $\mathbb{F}_p^* \longrightarrow \{-1,1\}$. □

Méthode 3. *montrons que* $f = \left(\frac{\cdot}{p}\right)$ *en prouvant qu'il est non trivial.*

Pour ce faire montrons qu'il existe $u \in GL(V)$ tel que pour $\det(u) \in \mathbb{F}_p^*$ on ait :

$$f(\det(u)) = \varepsilon(u) = -1 \text{ } i.e \text{ cherchons } u \in GL(V) \text{ de signature } -1$$

Comme V est un $\mathbb{F}_p$-espace vectoriel de dimension n, naturellement $V \simeq (\mathbb{F}_p)^n \simeq \mathbb{F}_{p^n}$ où l'on note $\mathbb{F}_{p^n}$ l'unique corps (à isomorphisme près) de cardinal p^n. On a également $GL(V) \simeq GL(\mathbb{F}_{p^n})$ en tant que groupes. Via ce dernier isomorphisme qui nous permet *d'identifier* ces deux structures, il nous suffit de montrer l'existence de $u \in GL(\mathbb{F}_{p^n})$ de signature -1. Définissons l'application ϕ_g pour g un générateur du groupe cyclique $\mathbb{F}_{p^n}^*$ par :

$$\phi_g : \begin{array}{ccc} \mathbb{F}_{p^n} & \longrightarrow & \mathbb{F}_{p^n} \\ x & \longmapsto & g.x \end{array}$$

qui est bien une permutation de $\mathbb{F}_{p^n}$, $i.e$ une bijection de $\mathbb{F}_{p^n}$. Plus précisément, g étant d'ordre $p^n - 1$, il s'agit d'un (p^n-1)-cycle qui peut s'écrire sous la forme d'une permutation par :

$$\phi_g = (g, g^2, \dots, g^{p^n-2}, 1) \text{ où } 0 \text{ est point fixe.}$$

La signature de ce (p^n-1)-cycle est alors naturellement :

$$\varepsilon(\phi_g) = (-1)^{p^n} = -1 \text{ car } p \text{ est un nombre impair.}$$

Enfin, comme ϕ_g est clairement $\mathbb{F}_p$-linéaire, $\phi_g \in GL(\mathbb{F}_{p^n})$ de signature -1 ce qui prouve que f tel que $\varepsilon = f \circ \det$ est non trivial et donne le résultat. □

Rappel 1. *Si V est un $\mathbb{F}_p$-espace vectoriel de dimension finie n, V est un ensemble de cardinal p^n et $u \in GL(V)$ est en particulier une bijection de V sur V et peut-être vu comme une permutation de S_{p^n}. Mais $GL(V) \neq S_{p^n}$.*

Démonstration. $GL(V) \simeq GL_n(\mathbb{F}_p) \subset \mathcal{M}_n(\mathbb{F}_p)$ où $\mathrm{card}(\mathcal{M}_n(\mathbb{F}_p)) = p^{n^2}$. Ainsi si on suppose $GL(V) \simeq S_{p^n}$, alors $(p^n)! \leq p^{n^2}$, absurde. □

Rappel 2. *Si $\mathbb{K}$ est un corps fini, $\mathbb{K}^*$ est cyclique.*

Rappel 3. $D(GL_n(\mathbb{F}_p)) = SL_n(\mathbb{F}_p)$ *si* $(n, \mathbb{F}_p) \neq (2, \mathbb{F}_2)$.

<u>Référence :</u>
- Objectif Agregation.

<u>Leçons concernés :</u>
- Corps finis. Applications.
- Déterminant.
- Exemples de parties génératrices d'un groupe. Applications.

Développement: Théorème de Burnside

Adrien Fontaine

27 novembre 2012

Référence : Oraux X-ENS, Algèbre 2, exercice 3.6p171

Théorème 1 (***Théorème de Burnside***)

Un sous-groupe de $GL_n(\mathbb{C})$ d'exposant fini (c'est à dire qu'il existe un entier N tel que $A^N = I$ pour toute matrice A du groupe) est fini.

Pour démontrer ce théorème, on va avoir besoin de la caractérisation classique des matrices nilpotente suivante :

Lemme 1

Soit $A \in M_n(\mathbb{C})$. On a :

$$A \text{ est nilpotente} \iff \forall k \geq 1, Tr(A^k) = 0$$

Démonstration : Le sens direct est évident en trigonalisant notre matrice A.

Réciproquement, supposons que pour tout $k \geq 1$, $Tr(A^k) = 0$. Par l'absurde, si A n'est pas nilpotente alors soient $\lambda_1, ..., \lambda_r$ les valeurs propres distinctes non nulles de A, de multiplicités respectives $n_1, ..., n_r$. Alors, en trigonalisant A, l'hypothèse sur les traces nous donne;

$$\forall k \geq 1, n_1\lambda_1^k + ... + n_r\lambda_r^k = 0$$

Le vecteur ${}^t(n_1, ..., n_r)$ est donc une solution non nulle du système linéaire :

$$\begin{bmatrix} \lambda_1 & \lambda_2 & \dots & \lambda_r \\ \lambda_1^2 & \lambda_2^2 & \dots & \lambda_r^2 \\ \vdots & & & \vdots \\ \lambda_1^r & \lambda_2^r & \dots & \lambda_r^r \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_r \end{bmatrix} = 0$$

Or, le déterminant de la matrice du système est non nul (c'est un Vandermonde et les λ_i sont tous distincts). D'où, une contradiction. ■

On est désormais en mesure de démontrer le théorème de Burnside.

Démonstration du théorème de Burnside : Soit N l'exposant de G.

Soit $(M_i)_{1\leq i\leq m}$ une base de $Vect(G)$ formée d'éléments de G.

Soit

$$f : \begin{array}{rcl} G & \to & \mathbb{C}^m \\ A & \mapsto & (Tr(AM_i))_{1\leq i\leq m} \end{array}$$

Montrons que f est injective.

Soient $A, B \in G$ telles que $Tr(AM_i) = Tr(BM_i)$ pour tout $1 \leq i \leq m$. Alors, par linéarité, on a :

$$\forall M \in G, Tr(AM) = Tr(BM)$$

Soit $D = AB^{-1} \in G$. Alors on a :

$$\forall k \in \mathbb{N}, Tr(D^{k+1}) = Tr(A\underbrace{B^{-1}D^k}_{\in G}) = Tr(BB^{-1}D^k) = Tr(D^k)$$

D'où par récurrence immédiate :

$$\forall k \in \mathbb{N}, Tr(D^k) = Tr(I_n) = n$$

D et I_n commutent donc on peut appliquer le binôme de Newton, et pour tout $k \geq 1$, on a :

$$\begin{aligned} Tr((D - I_n)^k) &= \sum_{j=0}^{k} \binom{j}{k} (-1)^j Tr(D^{k-j}) \\ &= \sum_{j=0}^{k} \binom{j}{k} (-1)^j n \\ &= n(1-1)^k \\ &= 0 \end{aligned}$$

Donc, d'après le lemme démontré précédemment, $D - I_n$ est nilpotente. Par ailleurs, G étant d'exposant fini N, toutes les matrices de G sont annulées par $X^N - 1$ qui est scindé à racines simples, donc toutes les matrices de G sont diagonalisables. En particulier, D est diagonalisable et donc, $D - I_n$ est diagonalisable.
Par conséquent, $D - I_n = 0$, i.e $D = I_n$. D'où l'injectivité.
Il reste à montrer que l'image de f est finie.
Or, $Im(f) \subset X^m$ où $X = \{Tr(A), a \in G\}$.
Et on a vu que les éléments de G sont annulés par $X^N - 1$, donc les valeurs propres des éléments de G sont dans l'ensemble des racines N-ièmes de l'unité qui sont en nombre fini. Donc X est fini.
D'où G fini. ■

Remarque 1

La démonstration nous donne par ailleurs une majoration sur l'ordre de G. En effet, on a :
- $|G| \leq |X|^m$
- $m \leq n^2$
- $|X| \leq N^n$

Do'ù, $|G| \leq N^{n^3}$.

Isomorphismes exceptionnels

18 mai 2015

Proposition 1. *Le groupe $GL_n(V)$ agit naturellement sur l'espace projectif $\mathbb{P}(V)$.*
Le groupe $PGL_n(V)$, quotient du groupe linéaire par son centre (formé des homothéties), agit donc fidèlement sur l'espace projectif $\mathbb{P}(V)$.

Application :
On en déduit les isomorphismes exceptionnels suivants en dimension 2 :
1. $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) = PSL(\mathbb{F}_2) \simeq S_3$.
2. $PGL_2(\mathbb{F}_3) \simeq S_4$ et $PSL_2(\mathbb{F}_3) \simeq A_4$.
3. $PGL_2(\mathbb{F}_4) \simeq PSL_2(\mathbb{F}_4) \simeq A_5$.
4. $PGL_2(\mathbb{F}_5) \simeq S_5$ et $PSL_2(\mathbb{F}_5) \simeq A_5$.

Démonstration. On considère l'action de $PGL_2(\mathbb{F}_q)$ sur la droite projective $\mathbb{P}({\mathbb{F}_q}^2)$ de manière fidèle. On note également $\mathbb{P}_1(\mathbb{F}_q)$ cette droite projective, qui contient $q+1$ points, les q points de la droite affine, plus le point à l'infini : $\mathbb{P}_1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}$. A cette action fidèle correspond donc un morphisme de groupe injectif : $\varphi : \; PGL_2(\mathbb{F}_q) \hookrightarrow S_{q+1}$. On aura également besoin de calculer le cardinal du groupe linéaire et de certains de ses sous-groupes :

- $|GL_n(\mathbb{F}_q)| = (q^n-1) \times (q^n-q) \times \ldots \times (q^n - q^{n-1})$
- $|PGL_n(\mathbb{F}_q)| = |SL_n(\mathbb{F}_q)| = \frac{(q^n-1)\times(q^n-q)\times\ldots\times(q^n-q^{n-1})}{q-1}$
- $|PSL_n(\mathbb{F}_q)| = \frac{(q^n-1)\times(q^n-q)\times\ldots\times(q^n-q^{n-1})}{(q-1)\times pgcd(n,q-1)}$

1. Si $q=2$, $|\mathbb{F}_2^*| = 1$ et donc $GL_2(\mathbb{F}_2) = PGL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) = PSL_2(\mathbb{F}_2)$ et sont de cardinal 6. Comme $PGL_2(\mathbb{F}_2)$ s'injecte dans S_3 de cardinal 6 également, ils sont isomorphes.

2. Si $q=3$, $|PGL_2(\mathbb{F}_3)| = 24 = |S_4|$. Par le même raisonnement, on obtient $PGL_2(\mathbb{F}_3) \simeq S_4$. Puis $PSL_2(\mathbb{F}_3)$ étant d'indice 2 dans $PGL_2(\mathbb{F}_3)$, tout comme A_4 dans S_4, on a alors $PSL_2(\mathbb{F}_3) \simeq A_4$.

3. Si $q=4$, on a $SL_2(\mathbb{F}_4) = PGL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4)$, tous de cardinal 60, qui s'injectent dans S_5 de cardinal 120. L'image de $PGL_2(\mathbb{F}_4)$ est un sous-groupe d'indice 2 donc distingué dans S_5, c'est donc A_5.

4. Si $q=5$, on a l'injection $\; PGL_2(\mathbb{F}_5) \hookrightarrow S_6$. De plus $|PGL_2(\mathbb{F}_5)| = 120$ et $|S_6| = 720$ donc l'image de $PGL_2(\mathbb{F}_5)$ est un sous-groupe d'indice 6 de S_6, c'est-à-dire S_5, ainsi $PGL_2(\mathbb{F}_5) \simeq S_5$. Puis, en considérant leur sous-groupe d'indice 2 respectif, on a également $PSL_2(\mathbb{F}_5) \simeq A_5$.

□

Référence : Perrin, cours d'algèbre