Théorème de Burnside

Références : [FGN09] p.185-186 ([Gou94] et [Mé06]).

Théorème 0.1 Soit G un sous-groupe de $GL_n(\mathbb{C})$. Alors G est fini si et seulement si G est d'indice fini, ie $\exists N \in \mathbb{N}$, tel que $\forall A \in G$, $A^N = I$.

Démonstration (\Rightarrow) On suppose G fini et on pose n = |G|. Alors d'après le théorème de Lagrange, $\forall g \in G, g^N = e$. D'où G d'indice fini N = n.

 (\Leftarrow) On suppose G d'exposant fini N. On procède en 4 étapes.

Étape 1 : Montrons que si $A \in \mathcal{M}_n(\mathbb{C})$ est telle que $\forall k \in \mathbb{N}^*, \ tr(A^k) = 0$. Alors A est nilpotente. Le polynôme caractéristique de A est scindé sur \mathbb{C} .

Raisonnons par l'absurde et supposons A non nilpotente.

Alors A possède des valeurs propres complexes non nulles, notons-les $\lambda_1, \ldots, \lambda_r$ (avec $r \geq 1$) et notons leurs multiplicités n_1, \ldots, n_r .

Nous savons que A est semblable à une matrice triangulaire T avec sur la diagonale les valeurs propres qui apparaissent autant de fois que leur multiplicité. En élevant à la puissance k cette matrice triangulaire, on obtient une matrice semblable à A telle que $\forall k \geq 1$:

$$tr(A^k) = tr(PT^kP^{-1}) = tr(PP^{-1}T^k) = tr(D^k) = n_1\lambda_1^k + \dots + n_r\lambda_r^k$$

Ainsi (n_1, \ldots, n_r) est solution du système linéaire :

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

Or ce système est de Cramer (car le nombre de lignes est égale au nombre de colonnes dans la matrice) et puisque le déterminant de la matrice est non nul, car il vaut :

$$\lambda_1 \dots \lambda_r \prod_{i < j} (\lambda_j - \lambda_i) \neq 0$$

Nécessairement, on a donc $n_1 = n_2 = \ldots = n_r = 0$, ce qui contredit le fait que A ne soit pas nilpotente. Donc A est nilpotente.

Étape 2 : Soit $(M_i)_{1 \le i \le m} \in G^m$ une base de G > S. Soit l'application :

$$f: G \longrightarrow \mathbb{C}^m$$

 $A \longmapsto (tr(AM_i))_{1 \le i \le m}$

Montrons que si f(A) = f(B), alors $AB^{-1} - Id$ est nilpotente.

Par linéarité de la trace, on a pour tout $M \in G > 0$:

$$tr(AM) = tr(BM)$$

(car f(A) = f(B)) et donc cette égalité est vraie en particulier pour tout $M \in G$. On pose $D = AB^{-1}$. $D \in G$ car G est un groupe, donc $\forall k \in \mathbb{N}^*$:

$$\begin{split} tr(D^k) &= tr((AB^{-1})^k) = tr((AB^{-1})(AB^{-1})^{k-1})\\ &= tr(BB^{-1}D^{k-1})\quad \text{d'après ce qu'on vient de montrer}\,;\\ &= tr(D^{k-1}) \end{split}$$

Donc par récurrence sur k, on montre que $tr(D^k) = tr(Id) = n$. Ainsi pour $k \ge 1$:

$$tr((D - Id)^{k}) = tr\left(\sum_{j=1}^{k} C_{k}^{j} (-1)^{j} D^{k-j}\right)$$
$$= \sum_{j=1}^{k} C_{k}^{j} (-1)^{j} tr(D^{k-j})$$
$$= n \sum_{j=1}^{k} C_{k}^{j} (-1)^{j} = n(-1+1)^{k} = 0$$

Donc d'après l'étape 1, on sait que D-Id est nilpotente.

Étape 3 : Déduisons-en que G est fini, via l'injectivité de f. Comme G est d'exposant fini N, alors $\forall A \in G$, $A^N = Id$, ie A est annulée par $X^n - 1$ qui est scindé à racines simples. Donc toute matrice de G est diagonalisable.

Dans ce cas, si on considère de nouveau $D = AB^{-1}$, alors D est diagonalisable car dans G, d'où D-Id est aussi diagonalisable. Or d'après l'étape 2, D-Id est nilpotente, donc nécessairement D-Id=0, ie D=Id, ie A=B, ie f est injective.

Par conséquent pour montrer que G est fini, il suffit de montrer que l'image X de G par f est fini. Or l'image X de f est incluse dans l'ensemble des traces des éléments de G (par définition de f) et d'après ce qu'on vient de faire, les valeurs propres des éléments de G appartiennent à l'ensemble fini des racines N-ième de l'unité. Donc X est fini, d'où G fini car f injective et donc $|G| \leq |X|$.

Lemmes utilisés

Lemme 0.1 (Théorème de Lagrange) Soit G un groupe fini de cardinal N. Alors $g^N=e$ pour tout $g \in G$ et le plus petit des entiers non nul n tel que $g^n = e$ divise le cardinal de G.

Démonstration Soit $H = \{g^n, n \in \mathbb{N}\}$. H est un ensemble fini puisque G l'est. Donc $\exists a, b \in \mathbb{N}$ et a > b tels que $g^a = g^b$, ie en multipliant par $(g^{-1})^b$, que $g^{a-b} = e$. Soit t le plus petit entier tel que $g^t = e$.

Montrons maintenant que H est un sous-groupe de G.

- $\begin{array}{l} -H\subset G,\, \operatorname{car}\, \forall g\in G,\, \forall n\in \mathbb{N},\, g^n\in G \,\operatorname{car}\, G \,\operatorname{groupe}.\\ -\operatorname{soient}\, g^a,g^b\in H,\, \operatorname{alors}\, g^ag^b=g^{a+b}\in H. \end{array}$
- soit $g^a \in H$. Comme t est le plus petit entier tel que $g^t = e$. Alors g^{t-1} est l'inverse de g. D'où $g^{a(t-1)}$ est l'inverse de g^a et cet inverse est dans H.

Montrons que le cardinal de H est t. Soit n un entier, on effectue la division euclidienne de n par t, alors il existe $(q,r) \in \mathbb{N}^2$, tels que n = tq + r et $0 \le r < t$. Alors $g^n = g^{tq+r} = (g^t)^q g^r = g^r$. Ainsi $H = \{1, g, g^2, \dots, g^{t-1}\}$; mais $g^r = g^s$ avec $1 \le r < s \le t$, ainsi l'argument donné au début de cette preuve nous donne que $g^{s-r} = e$, ce qui contredit la minimalité de t. Ainsi H a t éléments et on conclut par le fait que le cardinal de H divise le cardinal de G.

Lemme 0.2 (Déterminant de Van der Monde) Soient $a_1, \ldots, a_n \in \mathbb{C}$. On pose :

$$V(a_1, \dots, a_n) = \begin{vmatrix} 1 & a_1 & \dots & a_1^{n-1} \\ 1 & a_2 & \dots & a_2^{n-1} \\ \vdots & & & \vdots \\ 1 & a_n & \dots & a_n^{n-1} \end{vmatrix}$$

Alors $V(a_1, \ldots, a_n) = \prod_{i < j} (a_j - a_i)$.

Démonstration On procède par récurrence sur n.

- \rightsquigarrow Pour n=1 le résultat est évident.
- \rightarrow Supposons le résultat vrai au rang n-1 et montrons-le au rang n.

$$V(a_1, \dots, a_n) = \begin{vmatrix} 1 & a_1 & \dots & a_1^{n-1} \\ 1 & a_2 & \dots & a_2^{n-1} \\ \vdots & & & \vdots \\ 1 & a_n & \dots & a_n^{n-1} \end{vmatrix}$$

On retranche à chaque colonne a_1 fois la précédente :

$$V(a_1, \dots, a_n) = \begin{vmatrix} 1 & 0 & \dots & 0 \\ 1 & a_2 - a_1 & \dots & a_2^{n-1} - a_1 a_2^{n-2} \\ \vdots & & & \vdots \\ 1 & a_n - a_1 & \dots & a_n^{n-1} - a_1 a_n^{n-2} \end{vmatrix} = \begin{vmatrix} a_2 - a_1 & \dots & a_2^{n-1} - a_1 a_2^{n-2} \\ \vdots & & & \vdots \\ a_n - a_1 & \dots & a_n^{n-1} - a_1 a_n^{n-2} \end{vmatrix}$$

(après développement par rapport à la première ligne). On factorise ensuite chaque ligne par $(a_i - a_1)$, ce qui donne :

$$V(a_1, \dots, a_n) = (a_2 - a_1) \dots (a_n - a_1) \begin{vmatrix} 1 & a_2 & \dots & a_2^{n-2} \\ \vdots & \vdots & & \vdots \\ 1 & a_n & & a_n^{n-2} \end{vmatrix} = \prod_{i=2}^n (a_i - a_1) V(a_2, \dots, a_n)$$

Or par hypothèse de récurrence :

$$V(a_2, \dots, a_n) = \prod_{2 \le i < j \le n} (a_j - a_i)$$

D'où le résultat.

Références

[FGN09] Serge Francinou, Hervé Gianella, and Serge Nicolas. Oraux x-ens algèbre 2. Cassini, 2009.

[Gou94] Xavier Gourdon. Algèbre. Ellipses, 1994.

[Mé06] Jean-Yves Mérindol. Nombres et algèbre. EDP Sciences, 2006.