Théorème de Burnside :

I Le développement

Le but de ce développement est de montrer le théorème de Burnside qui offre un cas où le fait qu'un groupe d'exposant fini est fini est vrai.

Dans tout ce développement, on fixe un corps $\mathbb{K}$ commutatif de caractéristique nulle et n un entier naturel non nul.

Lemme 1 : [Francinou (1), p.353]
Soit $M \in \mathcal{M}_n(\mathbb{K})$.
La matrice M est nilpotente si, et seulement si, pour tout $k \in [\![1;n]\!]$, $\mathrm{Tr}\left(M^k\right) = 0$.

Preuve :
Soit $M \in \mathcal{M}_n(\mathbb{K})$.
$*$ Si M est nilpotente, alors M est semblable à une matrice strictement triangulaire supérieure T. Donc pour tout $k \in [\![1;n]\!]$, on a M^k semblable à T^k (encore strictement triangulaire supérieure) et puisque la trace est une propriété de classe, on a $\mathrm{Tr}\left(M^k\right) = \mathrm{Tr}\left(T^k\right) = 0$.

$*$ Réciproquement, supposons que pour tout $k \in [\![1;n]\!]$, $\mathrm{Tr}\left(M^k\right) = 0$.
Raisonnons par l'absurde en supposant que M n'est pas nilpotente.
On désigne par $\lambda_1, ..., \lambda_r$ les valeurs propres non nulles de M dans un corps $\mathbb{L}$ de décomposition de χ_M et $m_1, ..., m_r \in \mathbb{N}^*$ leur multiplicité respective.
En trigonalisant la matrice M, notre hypothèse équivaut à :

$$\forall k \in [\![1;n]\!],\ \sum_{i=1}^{r} m_i \lambda_i^k = 0$$

En particulier, on obtient la relation :

$$\underbrace{\begin{pmatrix} \lambda_1 & \dots & \lambda_r \\ \vdots & & \vdots \\ \lambda_1^r & \dots & \lambda_r^r \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix}}_{X} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

On reconnaît un déterminant de Vandermonde :

$$\det(A) = \prod_{i=1}^{r} \lambda_i \prod_{1 \leq i < j \leq n} (\lambda_j - \lambda_i) \neq 0 \text{ (car les } \lambda_i \text{ sont deux à deux distincts)}$$

Ainsi A est inversible et $X \in \mathrm{Ker}(A) = \{0\}$, ce qui est contradictoire avec la définition des m_i (car non nuls). Donc la matrice M est bien nilpotente.

■

Théorème 2 : Théorème de Burnside [Francinou (1), p.353] :
Soit H un sous-groupe de $\mathrm{GL}_n(\mathbb{K})$.
Si H est d'exposant fini, alors il est fini.

Preuve :
Soit H un sous-groupe de $\mathrm{GL}_n(\mathbb{K})$.
$*$ En appliquant le théorème de la base extraite à la famille génératrice H de $\mathrm{Vect}(H)$, on obtient une base $(M_1, ..., M_m) \in H^m$ de $\mathrm{Vect}(H)$.
On définie alors l'application :

$$f : \left| \begin{array}{ccc} H & \longrightarrow & \mathbb{K}^m \\ A & \longmapsto & (\mathrm{Tr}(AM_1), ..., \mathrm{Tr}(AM_m)) \end{array} \right.$$

$*$ Par hypothèse, il existe $N \in \mathbb{N}^*$ tel que pour tout $M \in H$ on ait $M^N = I_n$. En particulier, les éléments de H sont racines du polynôme $X^N - 1$ qui est scindé à racines simples dans $\mathbb{L}$ un corps de décomposition. Donc tous les éléments de H sont diagonalisables et leurs valeurs propres sont des racines N-ième de l'unité.

$*$ Montrons que la fonction f est injective :
Soient $A, B \in H$ tels que $f(A) = f(B)$.
Comme la famille $(M_1, ..., M_m)$ engendre $\mathrm{Vect}(H)$, on a $\mathrm{Tr}(AM) = \mathrm{Tr}(BM)$ pour tout élément $M \in H$. De plus, en notant $D = AB^{-1} \in H$, on a :

$$\forall k \in \mathbb{N},\ \mathrm{Tr}\left(D^{k+1}\right) = \mathrm{Tr}\left(AB^{-1}D^k\right) = \mathrm{Tr}\left(BB^{-1}D^k\right) = \mathrm{Tr}\left(D^k\right)$$

et donc par récurrence immédiate, on a $\mathrm{Tr}\left(D^k\right) = \mathrm{Tr}\left(D^0\right) = \mathrm{Tr}(I_n) = n$.

On en déduit que pour tout $k \in \mathbb{N}$, on a :

$$\begin{aligned} \mathrm{Tr}\left((D - I_n)^k\right) &\underset{comm.}{=} \sum_{i=0}^{k} \binom{k}{i} \mathrm{Tr}\left(D^i\right)(-1)^{k-i} = n \sum_{i=0}^{k} \binom{k}{i} \times 1^i \times (-1)^{k-i} \\ &= n(1-1)^k = 0 \end{aligned}$$

Donc par le lemme précédent, $D - I_n$ est nilpotente. De plus, $D \in H$, donc D et $D - I_n$ sont diagonalisables, d'où $D - I_n = 0$ (car $D - I_n$ est une matrice nilpotente et diagonalisable), soit $A = B$.

$*$ Ainsi, f est injective et d'après le deuxième point, $f(H) \subseteq X^m$, où :

$$X = \left\{\lambda_1 + ... + \lambda_n \in \mathbb{L} \text{ tq } \forall i \in [\![1;n]\!],\ \lambda_i^N = 1\right\}$$

Comme X est fini, X^m l'est aussi et donc H également (car f injective).

Finalement, le sous-groupe H est un sous-groupe fini de $\mathrm{GL}_n(\mathbb{K})$.

■

II Remarques sur le développement

II.1 Résultat(s) utilisé(s)

Ce développement tourne autour de la notion d'exposant dont on rappelle la définition ainsi qu'un premier résultat utile de connaître :

Définition 3 : Groupe d'exposant fini [Berhuy, p.344] :
On dit que G est **d'exposant fini** lorsqu'il existe un entier $n \in \mathbb{N}^*$ tel que pour tout $x \in G$, $x^n = e_G$. Dans ce cas, on appelle **exposant de** G le plus petit entier $n \in \mathbb{N}^*$ vérifiant cette propriété et on le note $\exp(G)$.

Proposition 4 : [Berhuy, p.344]
Si G est un groupe d'exposant fini, alors $\exp(G) = \mathrm{PPCM}(\{o(x),\ x \in G\})$.
De plus, si G est fini, on a $\exp(G)$ qui divise $\mathrm{Card}(G)$.

On remarque que si un groupe est fini, alors il est d'exposant fini (par le théorème de Lagrange). Cependant la réciproque est fausse comme le montre le groupe $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ qui est infini mais d'exposant égal à 2.

Soulignons le fait que le lemme 1 ne se généralise pas en caractéristique non nulle. En effet, si $\mathbb{K}$ est un corps de caractéristique $p \in \mathbb{N}^*$, alors $I_p \in \mathcal{M}_p(\mathbb{K})$ n'est pas nilpotente mais pourtant pour tout $k \in \mathbb{N}$, $\mathrm{Tr}\left(I_p^k\right) = 0$. De même, le théorème de Burnside est faux en caractéristique non nulle. Si l'on considère par exemple $\mathbb{K} = \mathbb{F}_p(T)$ (avec p un nombre premier), alors :

$$G = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{K}),\ a \in \mathbb{K} \right\}$$

est un sous-groupe infini de $\mathrm{GL}_2(\mathbb{K})$ d'exposant p.

Remarque 5 :
$*$ Grâce à la démonstration, on obtient les inégalités $\dim(\mathrm{Vect}(H)) \leq n^2$ et $\mathrm{Card}(X) \leq N^n$, ce qui nous permet d'obtenir $\mathrm{Card}(H) \leq N^{n^3}$.
$*$ Si G est un sous-groupe commutatif de $\mathrm{GL}_n(\mathbb{K})$ d'exposant N, on peut améliorer la majoration de $\mathrm{Card}(H)$. En effet, comme les éléments de G commutent et sont racines de $X^N - 1$ (scindé à racines simples dans un corps de décomposition), ils sont simultanément diagonalisables. Il existe donc $P \in \mathrm{GL}_n(\mathbb{L})$ tel que :

$$PHP^{-1} \subseteq \left\{ \mathrm{Diag}(\lambda_1, ..., \lambda_n) \in \mathcal{M}_n(\mathbb{L}) \text{ tq } \forall i \in [\![1;n]\!],\ \lambda_i^N = 1 \right\}$$

et on obtient donc la majoration $\mathrm{Card}(H) \leq N^n$ qui est optimale.

II.2 Pour aller plus loin...

II.2.1 Les sous-groupes finis de $\mathrm{GL}_n(\mathbb{Q})$

Dans $\mathrm{GL}_n(\mathbb{C})$, on peut trouver des éléments de tous les ordres finis possibles. Nous allons voir que la situation est un peu différente dans $\mathrm{GL}_n(\mathbb{Q})$.

Théorème 6 :
Il existe $r \in \mathbb{N}^*$ tel que pour tout $A \in \mathrm{GL}_n(\mathbb{Q})$ d'ordre fini on ait $A^r = I_n$.
De plus, le plus petit entier naturel non nul r qui possède cette propriété est $r = \mathrm{PPCM}(\{k \in \mathbb{N}^* \text{ tq } \varphi(k) \leq n\})$.

Preuve :
$*$ Si $A \in \mathrm{GL}_n(\mathbb{Q})$ est d'ordre fini, alors il existe $N \in \mathbb{N}^*$ tel que $X^N - 1$ annule la matrice A, donc les valeurs propres de A sont des racines de l'unité.

$*$ Comme $\mathbb{Q}[X]$ est factoriel et par irréductibilité des polynômes cyclotomiques dans $\mathbb{Q}[X]$, le polynôme minimal π_A de A est un produit de polynômes cyclotomiques. On en déduit donc que π_A est un élément de :

$$E = \left\{ \Phi_{n_1} ... \Phi_{n_r} \in \mathbb{Q}[X] \text{ tq } r \in [\![1;n]\!],\ (n_1, ..., n_r) \in (\mathbb{N}^*)^r \text{ et } \sum_{k=1}^{r} \varphi(n_k) = n \right\}$$

Comme la suite $(\varphi(n))_{n \in \mathbb{N}}$ diverge vers $+\infty$, on en déduit que l'ensemble E est fini et on conclut que $r_n = \mathrm{PPCM}(\{k \in \mathbb{N}^* \text{ tq } \varphi(k) \leq n\})$ convient.

■

Remarque 7 :
$*$ Pour les premières valeurs de n, on a par exemple :

$$r_1 = \mathrm{PPCM}(1, 2) = 2 \text{ et } r_2 = \mathrm{PPCM}(1, 2, 3, 4, 6) = 12$$

$*$ Il n'existe pas d'éléments d'ordre r_n pour $n \geq 2$.
$*$ En reprenant la démonstration ci-dessus, on remarque que les ordres finis des éléments de $\mathrm{GL}_n(\mathbb{Z})$ sont exactement les $\mathrm{PPCM}(n_1, ..., n_r) \in \mathbb{N}^*$ (en reprenant les notations de E). Ainsi dans $\mathrm{GL}_2(\mathbb{Z})$, les ordres finis des éléments sont 1,2,3,4 et 6.

Corollaire 8 :
Le groupe $\mathrm{GL}_n(\mathbb{Q})$ ne contient qu'un nombre fini de sous-groupes finis à isomorphisme près.

Preuve :
On note $r_n \in \mathbb{N}^*$ l'entier du théorème précédent.
Si G est un sous-groupe fini de $\mathrm{GL}_n(\mathbb{Q})$, alors son exposant est majoré par r_n. En utilisant alors la majoration obtenue à partir du théorème de Burnside, on en déduit que le cardinal de G se majore par $r_n^{n^3}$.

Ainsi, le groupe $\mathrm{GL}_n(\mathbb{Q})$ ne contient qu'un nombre fini de sous-groupes finis à isomorphisme près.

■

Remarque 9 :
$*$ On peut par exemple montrer que les sous-groupes finis de $\mathrm{GL}_2(\mathbb{Q})$ sont à l'isomorphisme près exactement les suivants :

$$\{I_n\},\ \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/6\mathbb{Z},\ D_2,\ D_3,\ D_4 \text{ et } D_6$$

$*$ Le groupe $\mathrm{GL}_n(\mathbb{Q})$ contient tout les groupes de cardinal au plus n. En effet, si G est un groupe de cardinal $k \leq n$, on a avec le théorème de Cayley un morphisme de groupes injectif $\lambda : G \longrightarrow \mathfrak{S}_k$.
D'autre part, si on désigne par $(E_1, ..., E_n)$ la base canonique de $\mathbb{C}^n$, on obtient en utilisant les matrices de permutations un morphisme de groupes injectif :

$$\varphi : \left| \begin{array}{ccc} \mathfrak{S}_n & \longrightarrow & \mathrm{GL}_n(\mathbb{Z}) \\ \sigma & \longmapsto & \left(E_{\sigma(1)}, ..., E_{\sigma(n)}\right) \end{array} \right.$$

Comme $\mathfrak{S}_k$ s'injecte naturellement dans $\mathfrak{S}_n$, on obtient par composition un morphisme de groupes injectif de G dans $\mathrm{GL}_n(\mathbb{Z}) \subseteq \mathrm{GL}_n(\mathbb{Q})$.

II.2.2 Les sous-groupes finis de $\mathrm{GL}_n(\mathbb{Z})$

Les résultats précédents s'appliquent encore ici, mais on peut obtenir un meilleur majoration pour le cardinal du groupe dans ce cas.

Théorème 10 : [Francinou (2), p.377]
Soit p un nombre premier impair.
Si G est un sous-groupe fini de $\mathrm{GL}_n(\mathbb{Z})$, alors la restriction à G de la réduction modulo p de $\mathrm{GL}_n(\mathbb{Z})$ dans $\mathrm{GL}_n(\mathbb{F}_p)$ est injective.

Preuve :
Soient p un nombre premier impair et G est un sous-groupe fini de $\mathrm{GL}_n(\mathbb{Z})$.
on note $\pi = G \longrightarrow \mathrm{GL}_n(\mathbb{F}_p)$ la réduction modulo p.
Si $M \in \mathrm{Ker}(\pi)$, alors il existe une matrice $A \in \mathcal{M}_n(\mathbb{Z})$ telle que $M = I_n + pA$. Or, comme G est fini, il existe $N \in \mathbb{N}^*$ tel que $M^N = I_n$.
On en déduit qu'il existe une matrice $P \in \mathrm{GL}_n(\mathbb{C})$ et des racines N-ième de l'unité $\omega_1, ..., \omega_n \in \mathbb{C}^*$ telles que $A = PDP^{-1}$, avec :

$$D = \mathrm{Diag}\left(\frac{\omega_1 - 1}{p}, ..., \frac{\omega_n - 1}{p}\right)$$

Comme $p > 2$, on en déduit que $\left(D^k\right)_{k\in\mathbb{N}}$ converge vers la matrice nulle et donc que $\left(A^k\right)_{k\in\mathbb{N}}$ converge aussi vers la matrice nulle (par continuité du produit matriciel).
Or, puisque $A \in \mathcal{M}_n(\mathbb{Z})$, il existe $k_0 \in \mathbb{N}$ tel que $A^{k_0} = 0$ et donc A est nilpotente, soit $A = 0$ (car A également diagonalisable).

Ceci donne donc $\mathrm{Ker}(M) = \{I_n\}$ et donc π est injective.

■

Remarque 11 : [Francinou (2), p.377]
Si G est un sous-groupe fini de $\mathrm{GL}_n(\mathbb{Z})$, alors on a la majoration suivante :

$$\mathrm{Card}(G) \leq \mathrm{Card}(\mathrm{GL}_n(\mathbb{F}_3)) = \prod_{k=0}^{n-1}\left(3^n - 3^k\right) \leq 3^{n^2}$$

II.3 Recasages

Recasages : 104 - 106 - 149 - 156.

III Bibliographie

— Serge Francinou, *Exercices de mathématiques, Oraux X-ENS, Algèbre 2*.

— Grégory Berhuy, *Algèbre : le grand combat*.

— Serge Francinou, *Oraux X-ENS, Algèbre 3*.