

Rapport du jury

Dans un premier temps, la notion de conjugaison dans un groupe introduite brièvement doit être développée et illustrée dans des situations variées. On doit proposer des situations où la conjugaison aide à résoudre certains problèmes (par exemple, en transformant un élément en un autre plus simple à manipuler). On peut aussi illustrer et utiliser le principe du "transport par conjugaison" voulant que ghg^{-1} ait la même "nature géométrique" que g . Ensuite, il est attendu de développer l'intérêt de la notion de sous-groupe distingué en particulier en regard de la structure de groupe obtenue par quotient d'un groupe, le lien entre sous-groupe distingué et noyau de morphisme de groupes, ainsi que la factorisation d'un morphisme de groupe au travers d'un tel quotient. Il est indispensable de proposer quelques résultats bien choisis mettant en évidence l'utilisation de ces notions : citons par exemple le lien entre les sous-groupes de l'un et de l'autre et la caractérisation interne des produits directs. L'examen de la simplicité de certains groupes peut être proposé. Comme indiqué dans le sujet, il est demandé de présenter des exemples pertinents utilisés pour obtenir des résultats significatifs. De tels exemples sont nombreux en théorie des groupes mais il est souhaitable d'en proposer dans d'autres domaines, comme en arithmétique, en géométrie et en algèbre linéaire. Pour aller plus loin, les candidates et candidats peuvent poursuivre en illustrant ces notions en théorie des représentations des groupes finis (classes de conjugaison et nombre de représentations irréductibles, treillis des sous-groupes distingués lu dans la table de caractères, etc.). La notion de produit semi-direct et les théorèmes de Sylow débordent du programme. Il est possible de les évoquer, mais en veillant à les illustrer par des exemples et des applications.

Références

- [Cours d'Algèbre - Daniel Perrin](#)
- [Mathématiques pour l'Agrégation \(Algèbre\) - J.E. Rombaldi](#)

Développements

- [Automorphismes de \$S_n\$](#)

- [Probas sur GL2\(Fq\)](#)

Méta-plan

1. Sous-groupes normaux. Quotients
 1. Sous-groupe normal
 2. Quotient par un sous-groupe
2. Action de conjugaison
3. Conjugaison dans des groupes particuliers
 1. Matrice semblables
 2. p -groupes

Plan détaillé

I - Sous-groupes normaux. Quotients

1 - Sous-groupes normaux

1. Définition : sous-groupe normal.
2. Exemples :
 1. Les groupes 1 et G sont toujours normaux dans G .
 2. Tout sous-groupe d'un groupe abélien est normal mais la réciproque est fausse : dans $\mathfrak{S}_3$, si τ est une transposition, le sous-groupe $\langle \tau \rangle$ est abélien mais pas normal pour autant.
 3. Si $p < q$ sont deux nombres premiers, tout groupe d'ordre pq admet un sous-groupe normal isomorphe à Z/pZ .
3. Proposition : le centre et le groupe dérivés sont toujours des sous-groupes normaux.
4. Exemples :
 1. $\mathfrak{A}_n$ est distingué dans $\mathfrak{S}_n$.
 2. Si K est un corps, $SL_n(K)$ est distingué dans $GL_n(K)$.
 3. Le groupe des translations est distingué dans le groupe affine d'un espace affine.
5. Définition : groupe simple
6. Théorème : $\mathfrak{A}_n$ est simple pour $n \geq 5$.

2 - Structures quotients

1. Définition : quotient par un sous-groupe (quelconque)
2. Théorème : H est normal dans G si, et seulement si, G/H admet une unique structure de groupe qui rend la projection naturelle un morphisme de groupes.
3. Corollaire : H est normal dans G si, et seulement si, il existe un groupe N et un morphisme $\phi : G \rightarrow N$ tel que $H = \ker(\phi)$.
4. Définition : indice d'un sous-groupe (pas forcément normal).
5. Remarque : G , ainsi que n'importe lequel de ses sous-groupe, agit sur G/H via $g \cdot hH := (gh)H$, et ce même si H est non normal.
6. Application : théorème de Lagrange.
7. Théorème : isomorphisme de Noether
8. Application : Soit $O \in \mathcal{E}$ un point d'un $\mathbb{R}$ -espace affine euclidien. Toute isométrie affine de $\mathcal{E}$ est la composée d'une isométrie qui laisse O stable et d'une translation.
9. Proposition : Soit H un sous-groupe distingué de G . On suppose qu'on connaît une partie S_H génératrice de H et une partie $S_{G/H}$ génératrice de G/H . Si le morphisme de projection $G \rightarrow G/H$ admet une section, l'union de ces parties génératrices envoyées dans G est une famille génératrice de G .
10. Exemples :
 1. Les transvections et les dilatations engendrent $SL_n(K)$.
 2. Les réflexions et les translations engendrent $Iso(\mathcal{E})$.

II - Action de conjugaison

1. Définition (action de conjugaison) : G agit naturellement sur lui-même via

$$\begin{aligned}\rho : G &\rightarrow \text{Aut}(G) \\ g &\mapsto (x \mapsto g^{-1}xg)\end{aligned}$$

Les éléments de l'image de ρ sont appelés automorphismes intérieurs.

2. Exemple : si $\sigma \in \mathfrak{S}_n$, pour tout cycle $c = (i_1 \dots i_k)$, on a $\rho(\sigma)(c) = (\sigma(i_1) \dots \sigma(i_k))$.
3. Lemme : le noyau de ρ est le centre de G . En particulier, tous les automorphismes ne sont pas intérieurs en général.
4. Définition : centralisateur d'un élément, d'une partie.

5. Proposition : soit ϕ un isomorphisme de $G_1 \rightarrow G_2$, et soit $g \in G_1$. Alors ϕ induit un isomorphisme de $C(g)$ dans $C(g_1)$.
6. Lemme : soit ϕ un automorphisme de $\mathfrak{S}_n$. Si ϕ envoie toute transposition sur une transposition, alors ϕ est intérieur (DVT 1)
7. Théorème : les automorphismes de $\mathfrak{S}_n$ sont intérieurs, sauf éventuellement si $n = 6$. (DVT 1)

III - Conjugaison dans des groupes particuliers

1 - Conjugaison dans les groupes de matrices

1. Définition : matrices semblables
2. Lemme : deux matrices sont semblables si, et seulement si, il existe $\phi \in \mathcal{L}(K^n)$ et deux bases de K^n telles que ces matrices soient les matrices de ϕ dans ces bases.
3. Corollaire : deux matrices semblables partagent un grand nombre de propriétés : le rang, les polynômes caractéristique et minimal, le déterminant.
4. Exemples : la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$ est diagonalisable de spectre $\{1, 2\}$, c'est-à-dire qu'elle est conjuguée à la matrice $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$.
5. Contre-exemple : aucun des invariants évoqués, ni-même aucune combinaison de ces invariants, ne permet de décrire complètement les orbites de conjugaison. Par exemple, les matrices :

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

ont même rang, même déterminant, mêmes polynômes caractéristique et minimal, mais ne sont pas semblables.

6. Lemme : une matrice M est diagonalisable (resp. trigonalisable) ssi toutes les matrices de son orbite de similitude le sont.
7. Application : la probabilité que deux matrices commutent dans $GL_2(\mathbb{F}_q)$ est $\frac{1}{q^2 - q}$. (DVT 2)
8. Définition : matrice compagnon

9. Théorème (Frobenius) : soit $M \in M_n(K)$. Il existe une unique suite de polynômes $P_r | \dots | P_1$ unitaires telle que M soit équivalente à la forme par blocs de Frobenius. Ces polynômes sont appelés "invariants de similitude"
10. Corollaire : Deux matrices sont semblables si, et seulement si, elles ont les mêmes invariants de similitude.
11. Application : soit L/K une extension de corps, A et B dans $M_n(K)$. Alors A et B sont K -semblables ssi elles sont L -semblables.

2 - Utilisation pour l'étude des p -groupes

Dans toute la suite, on considère p un nombre premier.

1. Définition : p -groupe
2. Proposition : équation aux classes
3. Corollaire : le centre d'un p -groupe est non-trivial. De plus, un groupe d'ordre p^2 est toujours abélien.
4. Remarque : en particulier, un p -groupe d'ordre $p^\alpha, \alpha \geq 2$ n'est jamais simple.
5. Définition : p -Sylow
6. Théorèmes (Sylow)
7. Application : un groupe d'ordre 63 n'est jamais simple.