

Agrégation
externe

Léon Lévy

Développements abordables et détaillés pour l'agrégation de Mathématiques



Références sciences

Développements abordables et détaillés pour l'agrégation de Mathématiques

Léon Lévy



Collection Références sciences

dirigée par Paul de Laboulaye
paul.delaboulaye@editions-ellipses.fr

*Retrouvez tous les livres de la collection
et des extraits sur www.editions-ellipses.fr*



ISBN 9782340-120846

Dépôt légal : octobre 2026

©Ellipses Édition Marketing S.A.
8/10 rue la Quintinie 75015 Paris



Le Code de la propriété intellectuelle et artistique n'autorisant, aux termes des alinéas 2 et 3 de l'article L. 122-5, d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale, ou partielle, faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause, est illicite » (alinéa 1^{er} de l'article L. 122-4).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

www.editions-ellipses.fr

Avant-propos

L'épreuve orale de l'agrégation externe de mathématiques est découpée en trois phases :

- une première phase de 6 minutes où le candidat présente son plan de la leçon tirée.
- une deuxième phase de 15 minutes où le candidat démontre un résultat caractéristique de son plan : c'est ce qu'on appelle un développement.
- une dernière phase d'environ 35 minutes d'échanges avec le jury.

Ce livre se concentre sur la deuxième phase, celle du développement.

Ce livre ne détaillera pas le déroulement des oraux ni la manière de s'y préparer. De nombreuses ressources et conseils sont disponibles en ligne, et cela est aussi très bien présenté dans [18] et [14].

L'objectif de cet ouvrage est de vous présenter une liste de développements abordables pour l'oral de l'agrégation. La plupart des développements sont classiques : si vous espérez trouver de l'originalité dans ce livre, vous allez être déçu.

Les développements proposés sont généralement d'un niveau accessible : le but est de proposer une démonstration de son niveau et d'en maîtriser toutes les subtilités. Lors de ma préparation, j'ai vu des étudiants présenter des développements qui n'étaient pas du tout à leur portée, ce qui se voyait immédiatement lors de la phase des questions. Il vaut mieux avoir un développement d'un niveau moyen mais le connaître sur le bout des doigts, plutôt que de vouloir impressionner le jury (qui, spoiler, ne sera pas impressionné) en présentant des notions non maîtrisées.

L'idée d'écrire ce livre vient du fait que durant ma préparation, c'est un travail qui m'a pris beaucoup de temps d'aller tout d'abord trouver un développement accessible à mon niveau, puis rechercher la preuve dans des ouvrages de référence. Je remercie pour cela le site agreg-maths.fr qui m'a été salvateur, et tous les agrégés y ayant mis à disposition leurs développements. Ce site est une mine d'or pour avoir des idées de développements et trouver des références.

Après cette étape, je devais encore retravailler la preuve car celle-ci manquait en général de détail. Ce n'est absolument pas une critique envers les auteurs de ces livres, ces manuels ne sont pas à la base destinés à l'agrégation, et si tous les manuels devaient expliciter au maximum les preuves des théorèmes, les sacs des étudiants seraient beaucoup trop lourds.

C'est dans ce souci de compréhension que j'ai essayé que chaque développement soit le plus détaillé possible, afin de ne laisser aucune zone d'ombre.

Cette idée de rassembler tous mes développements afin qu'ils profitent à tous m'est venue après avoir obtenu l'agrégation, en m'inspirant de deux ouvrages sur le même principe ([18] et [14]) qui m'ont accompagné pendant toute mon année.

J'attire votre attention sur l'importance de choisir ses développements. Il faut connaître son niveau mathématique et faire ses choix en conséquence. Certains développements de ce livre vous paraîtront d'une simplicité absolue tandis que d'autres vous paraîtront inaccessibles.

La tentation peut être forte de prendre un développement « compliqué » qui se recasera dans beaucoup de leçons. S'il est maîtrisé, c'est un bon calcul. Sinon, il vaut mieux prendre plusieurs développements qui seront plus simples à comprendre et à retenir.

Vous l'aurez compris, cet ouvrage a deux objectifs : rassembler des développements d'un niveau standard mais suffisant pour obtenir l'agrégation, et détailler leur preuve le plus clairement possible.

J'espère que ces objectifs seront atteints et que ce livre vous aidera dans ce marathon qu'est l'agrégation.

Si cela vous intéresse, mon profil sur agreg-maths.fr est Mr_Syndrome. J'y ai publié tous ces développements ainsi que d'autres, et également tous mes plans de leçons que j'avais préparés.

Bon courage pour cette année !

Remerciements

Préparer l'agrégation de mathématiques n'est pas une chose aisée et nécessite d'être bien entouré. Je profite donc de cet ouvrage pour remercier les personnes qui m'ont accompagné, de près ou de loin, durant mon année de préparation.

Merci à mes parents de m'avoir mis dans les meilleures dispositions possibles pour réussir ce concours, et d'avoir été présents tout au long de l'année.

Merci à Nelson et Salvador pour leur bonne humeur et les discussions mathématiques.

Merci à Baptiste et Charlotte qui, malgré leurs lointains souvenirs mathématiques, ont vécu cette aventure avec moi et ont fait preuve d'une amitié sans faille.

Merci à Léo d'avoir été là durant toutes ces heures à la BU.

Merci à Aimé pour son écoute et son aide mathématique.

Merci à Georges Skandalis pour la relecture de certains développements, une tâche ô combien ingrate mais nécessaire.

Couplage des leçons

Dans cette partie, on donne les leçons qui sont concernées par les développements de ce livre. La liste des leçons est celle de 2026. Ces recasages sont personnels et il est possible que vous ne soyez pas d'accord avec certains. C'est à chaque candidat de savoir si un développement est pertinent dans la leçon présentée.

101 : Groupe opérant sur un ensemble. Exemples et applications.

- Classification des groupes d'ordre p^2
- Formule de Burnside

102 : Groupe des nombres complexes de module 1. Racines de l'unité. Applications.

- Théorème de Kronecker
- Irréductibilité des polynômes cyclotomiques

103 : Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.

- Classification des groupes d'ordre p^2
- Sous-groupes distingués de $\mathcal{S}_n$

104 : Groupes finis. Exemples et applications.

- Classification des groupes d'ordre p^2
- Formule de Burnside
- Sous-groupes distingués de $\mathcal{S}_n$

105 : Groupe des permutations d'un ensemble fini. Applications.

- Formule de Burnside
- Sous-groupes distingués de $\mathcal{S}_n$

106 : Groupe linéaire d'un espace vectoriel de dimension finie E , sous-groupes de $GL(E)$. Applications.

- Décomposition polaire

108 : Exemples de parties génératrices d'un groupe. Applications.

- Sous-groupes distingués de $\mathcal{S}_n$

120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.

- Critère d'Eisenstein

121 : Nombres premiers. Applications.

- Existence et unicité des corps finis
- Critère d'Eisenstein

122 : Anneaux principaux. Exemples et applications.

- Critère d'Eisenstein

123 : Corps finis. Applications.

- Existence et unicité des corps finis
- Irréductibilité des polynômes cyclotomiques

125 : Extensions de corps. Exemples et applications

- Éléments et extensions algébriques
- Existence et unicité des corps finis
- Irréductibilité des polynômes cyclotomiques

127 : Exemples de nombres remarquables. Exemples d'anneaux de nombres remarquables. Applications.

- Éléments et extensions algébriques
- Irréductibilité des polynômes cyclotomiques

141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

- Existence et unicité des corps finis
- Critère d'Eisenstein
- Irréductibilité des polynômes cyclotomiques

142 : PGCD et PPCM, algorithmes de calcul. Applications.

- Critère d'Eisenstein

144 : Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.

- Éléments et extensions algébriques
- Théorème de Kronecker
- Irréductibilité des polynômes cyclotomiques

148 : Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.

- Éléments et extensions algébriques
- Théorème spectral
- Trigonalisation simultanée
- Loi d'inertie de Sylvester

149 : Déterminant. Exemples et applications.

- Critère de nilpotence par la trace
- Différentielle du déterminant

150 : Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.

- Théorème spectral
- Décomposition de Dunford et exponentielle de matrice
- Surjectivité de l'exponentielle matricielle

151 : Sous-espaces stables par un endomorphisme ou une famille d'endo morphismes d'un espace vectoriel de dimension finie. Applications.

- Trigonalisation simultanée
- Décomposition de Dunford et exponentielle de matrice

152 : Endomorphismes diagonalisables en dimension finie.

- Théorème spectral
- Décomposition de Dunford et exponentielle de matrice
- Décomposition polaire

153 : Valeurs propres, vecteurs propres. Calculs exacts ou approchés d'éléments propres. Applications.

- Théorème spectral
- Critère de nilpotence par la trace

155 : Exponentielle de matrices. Applications.

- Décomposition de Dunford et exponentielle de matrice
- Surjectivité de l'exponentielle matricielle

156 : Endomorphismes trigonalisables. Endomorphismes nilpotents.

- Trigonalisation simultanée
- Critère de nilpotence par la trace
- Décomposition de Dunford et exponentielle de matrice

157 : Matrices symétriques réelles, matrices hermitiennes.

- Théorème spectral
- Décomposition polaire

158 : Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie).

- Théorème spectral
- Décomposition polaire

159 : Formes linéaires et dualité en dimension finie. Exemples et applications.

- Loi d'inertie de Sylvester

162 : Systèmes d'équations linéaires ; opérations élémentaires, aspects algorithmiques et conséquences théoriques.

- Critère de nilpotence par la trace

170 : Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité. Applications.

- Loi d'inertie de Sylvester

171 : Formes quadratiques réelles. Coniques. Exemples et applications.

- Loi d'inertie de Sylvester

190 : Méthodes combinatoires, problèmes de dénombrement.

- Formule de Burnside
- Nombres de Bell

201 : Espaces de fonctions. Exemples et applications.

- Théorème de Weierstrass par les probabilités
- Inégalités de Young-Hölder-Minkowski

203 : Utilisation de la notion de compacité.

- Théorème de Heine
- Equivalence des normes en dimension finie et théorème de Riesz

204 : Connexité. Exemples et applications.

- Principe du prolongement analytique et théorème des zéros isolés

205 : Espaces complets. Exemples et applications.

- Théorème du point fixe de Picard
- Théorème de Cauchy-Lipschitz linéaire

206 : Exemples d'utilisation de la notion de dimension finie en analyse.

- Equivalence des normes en dimension finie et théorème de Riesz

208 : Espaces vectoriels normés, applications linéaires continues. Exemples.

- Equivalence des normes en dimension finie et théorème de Riesz
- Inégalités de Young-Hölder-Minkowski

209 : Approximation d'une fonction par des fonctions régulières. Exemples d'applications.

- Théorème de Weierstrass par les probabilités

215 : Applications différentiables définies sur un ouvert de $\mathbb{R}^n$. Exemples et applications.

- Différentielle du déterminant

218 : Formules de Taylor. Exemples et applications.

- Théorème central limite

220 : Illustrer par des exemples la théorie des équations différentielles ordinaires.

- Equation de Bessel

221 : Equations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications.

- Théorème de Cauchy-Lipschitz linéaire
- Equation de Bessel

223 : Suites réelles et complexes. Convergence, valeurs d'adhérence. Exemples et applications.

- Théorème du point fixe de Picard
- Développement asymptotique de la série harmonique

224 : Exemples de développements asymptotiques de suites et de fonctions.

- Développement asymptotique de la série harmonique
- Formule de Stirling avec le TCL

226 : Suites vectorielles et réelles définies par une relation de récurrence $u_{n+1} = f(u_n)$. Exemples. Applications à la résolution approchée d'équations.

- Théorème du point fixe de Picard

228 : Continuité, dérivabilité des fonctions réelles d'une variable réelle. Exemples et applications.

- Théorème de Heine
- Intégrale de Dirichlet

230 : Séries de nombres réels et complexes. Comportement des restes ou des sommes partielles des séries numériques. Exemples.

- Développement asymptotique de la série harmonique
- Règle de Raabe-Duhamel

234 : Fonctions et espaces de fonctions Lebesgue-intégrables.

- Inégalités de Young-Hölder-Minkowski
- Intégrale de Dirichlet

235 : Problèmes d'interversion de symboles en analyse.

- Intégrale de Dirichlet
- Fonction caractéristique et moments de la loi Gamma

236 : Illustrer par des exemples quelques méthodes de calcul d'intégrales de fonctions d'une ou plusieurs variables.

- Intégrale de Dirichlet
- Fonction caractéristique et moments de la loi Gamma
- Transformée de Fourier de la Gaussienne

239 : Fonctions définies par une intégrale dépendant d'un paramètre. Exemples et applications.

- Intégrale de Dirichlet
- Fonction caractéristique et moments de la loi Gamma
- Transformée de Fourier de la Gaussienne

241 : Suites et séries de fonctions. Exemples et contre-exemples.

- Théorème de Weierstrass par les probabilités
- Nombres de Bell

243 : Séries entières, propriétés de la somme. Exemples et applications.

- Nombres de Bell
- Equation de Bessel

245 : Fonctions holomorphes et méromorphes sur un ouvert de $\mathbb{C}$. Exemples et applications.

- Fonction caractéristique et moments de la loi Gamma
- Principe du prolongement analytique et théorème des zéros isolés
- Transformée de Fourier de la Gaussienne

250 : Transformation de Fourier. Applications.

- Transformée de Fourier de la Gaussienne
- Théorème central limite

261 : Loi d'une variable aléatoire: caractérisations, exemples, applications.

- Fonction caractéristique et moments de la loi Gamma
- Lemme de Scheffé et convergence de loi binomiale vers une loi de Poisson
- Théorème central limite
- Formule de Stirling avec le TCL

262 : Convergences d'une suite de variables aléatoires. Théorèmes limite. Exemples et applications.

- Lemme de Scheffé et convergence de loi binomiale vers une loi de Poisson
- Théorème central limite
- Formule de Stirling avec le TCL

264 : Variables aléatoires discrètes. Exemples et applications.

- Théorème de Weierstrass par les probabilités
- Lemme de Scheffé et convergence de loi binomiale vers une loi de Poisson

266 : Utilisation de la notion d'indépendance en probabilités.

- Théorème central limite
- Formule de Stirling avec le TCL

Notations

Notations générales

$A \setminus B$	Complémentaire de l'ensemble B dans l'ensemble A
A^*	Ensemble A privé de 0
$a \wedge b$	PGCD de a et b
δ_j^i	Symbole de Kronecker (vaut 1 si $i = j$, 0 sinon)
$\llbracket 1; n \rrbracket$	Ensemble des entiers de 1 à n
$n!$	Factorielle de n
$\binom{n}{k}$	Coefficient binomial de k parmi n
$\mathcal{P}(E)$	Ensemble des parties de E
$ X $	Cardinal de l'ensemble X
$\emptyset$	Ensemble vide
$\mathbb{1}_A$	Fonction indicatrice de A

Groupes

$\mathcal{A}(E)$	Groupe alterné de E
$\varepsilon(\sigma)$	Signature de la permutation σ
$\text{Fix}(g)$	Fixateur de g
φ	Fonction indicatrice d'Euler
$\langle g \rangle$	Sous-groupe engendré par g
G/H	Ensemble des classes à gauche modulo H
$\mathcal{O}_x, \text{Orb}(x)$	Orbite de x
$\mathbb{P}_n$	Ensemble des racines primitives n -ièmes de l'unité
$\mathcal{S}_n$	Groupe des permutations de $\llbracket 1; n \rrbracket$
$\text{Stab}(x), \text{St}_x$	Stabilisateur de x

$\mathbb{U}_n$	Groupe des racines complexes n -ièmes de l'unité
$Z(G)$	Centre du groupe G

Anneaux, corps et polynômes

$\text{car}(K)$	Caractéristique du corps K
$c(P)$	Contenu du polynôme P
$\deg(P)$	Degré du polynôme P
$\text{Frac}(A)$	Corps des fractions de l'anneau intègre A
$\mathbb{F}_q$	Corps fini à q éléments
Φ_n	Polynôme cyclotomique d'indice n
$K[X]$	Ensemble des polynômes à coefficients dans K
L/K	L est une extension du corps K
$[L:K]$	Dimension du corps L comme K -espace vectoriel
π_α^K	Polynôme minimal de α sur K

Algèbre linéaire

$\ A\ $	Norme de $A \in M_n(K)$ subordonnée à une norme de K^n
$\text{com}(A), \tilde{A}$	Comatrice de la matrice A
$\det(A)$	Déterminant de la matrice A
$\dim(E)$	Dimension de l'espace vectoriel E
$E_\lambda(u)$	Sous-espace propre de u associé à la valeur propre λ
$F^\perp$	Orthogonal de F
$F \oplus G$	Somme directe de F et G
$\text{GL}_n(K)$	Groupe des matrices inversibles à coefficients dans K
$H_n(\mathbb{C})$	Ensemble des matrices hermitiennes de $M_n(\mathbb{C})$
I_n	Matrice identité d'ordre n
$\text{Im}(u)$	Image de l'endomorphisme u
$\rho(A)$	Rayon spectral de la matrice A
$\text{Ker}(u)$	Noyau de l'endomorphisme u
$\mathcal{L}(E)$	Ensemble des endomorphismes de E , c'est-à-dire des applications linéaires de E dans E

$M_{n,p}(K)$	Ensemble des matrices à n lignes et p colonnes à coefficients dans K
$M_n(K)$	Ensemble des matrices de taille $n \times n$ à coefficients dans K
$\text{Mat}_{\mathcal{B}}(u)$	Matrice de l'endomorphisme u dans la base $\mathcal{B}$
$\mathcal{N}_i(u)$	Sous-espace caractéristique de u associé à la valeur propre λ_i
$O_n(\mathbb{R})$	Ensemble des matrices orthogonales de $M_n(\mathbb{R})$
$P_{\mathcal{B} \rightarrow \mathcal{B}'}$	Matrice de passage de la base $\mathcal{B}$ à la base $\mathcal{B}'$
$\text{rg}(u)$	Rang de l'endomorphisme u
$\text{Sp}(u), \text{Sp}(A)$	Spectre de l'endomorphisme u , de la matrice A
$S_n(\mathbb{R})$	Ensemble des matrices symétriques réelles
$S_n^+(\mathbb{R})$	Ensemble des matrices réelles symétriques positives
$S_n^{++}(\mathbb{R})$	Ensemble des matrices réelles symétriques définies positives
$\text{tr}(A)$	Trace de la matrice A
$A^\top$	Transposée de la matrice A
u^*	Adjoint de l'endomorphisme u
$U_n(\mathbb{C})$	Ensembles des matrices unitaires de $M_n(\mathbb{C})$
$\text{vect}(A)$	Espace vectoriel engendré par A
χ_u, χ_A	Polynôme caractéristique de l'endomorphisme u , de la matrice A
μ_A	Polynôme minimal de la matrice A
0_n	Matrice nulle d'ordre n

Analyse fonctionnelle

$\mathcal{B}(\mathbb{R})$	Tribu borélienne de $\mathbb{R}$
$\mathcal{C}(X, Y)$	Espace vectoriel des fonctions continues de X dans Y
C^k	Ensemble des fonctions k fois dérivables de dérivée k -ième continue pour un entier $k \geq 1$
C^∞	Ensemble des fonctions de classe C^k pour tout $k \geq 1$
$df(a)$	Différentielle de f au point a
$\frac{\partial f}{\partial x}$	Dérivée partielle de la fonction f par rapport à la variable x
$\ f\ _\infty$	Norme infinie de la fonction bornée f
$\ f\ _p$	$(\int_X f ^p d\mu)^{1/p}$ pour $f \in \mathcal{L}^p(X, \mathcal{A}, \mu)$

$\hat{f}, \mathcal{F}(f)$	Transformée de Fourier de f
$\mathcal{L}^p(X, \mathcal{A}, \mu),$ $p \geq 1$	Ensemble des applications mesurables de $(X, \mathcal{A}, \mu)$ dans $(\mathbb{R}, \mathcal{B}(\mathbb{R}))$ qui sont p -intégrables
$L^p(X, \mathcal{A}, \mu),$ $p \geq 1$	Ensemble des classes d'équivalence des fonctions de $\mathcal{L}^p(X, \mathcal{A}, \mu)$ pour la relation d'égalité μ -presque partout
λ	Mesure de Lebesgue

Analyse complexe

$\mathcal{A}(\Omega)$	Ensemble des fonctions analytiques sur un ouvert Ω de $\mathbb{C}$
$\mathcal{H}(\Omega)$	Ensemble des fonctions holomorphes sur un ouvert Ω de $\mathbb{C}$
$\text{Im}(z)$	Partie imaginaire du nombre complexe z
$\text{Re}(z)$	Partie réelle du nombre complexe z

Probabilités

$\mathbb{E}[X]$	Espérance de la variable aléatoire X
ϕ_X	Fonction caractéristique de la variable aléatoire X
F_X	Fonction de répartition de la variable aléatoire X
$\mathbb{P}(E)$	Probabilité de l'événement E
$\text{Var}(X)$	Variance de la variable aléatoire X
$\mathcal{U}(\{x_1, \dots, x_n\})$	Loi uniforme discrète sur $\{x_1, \dots, x_n\}$
$\text{Ber}(p)$	Loi de Bernoulli de paramètre p
$\text{Bin}(n, p)$	Loi binomiale de paramètres n et p
$\mathcal{P}(\lambda)$	Loi de Poisson de paramètre λ
$\mathcal{U}([a; b])$	Loi uniforme continue sur $[a; b]$
$\mathcal{E}(\lambda)$	Loi exponentielle de paramètre λ
$\mathcal{N}(\mu, \sigma^2)$	Loi normale d'espérance μ et de variance σ^2
$\Gamma(r, \lambda)$	Loi Gamma de paramètres r et λ

DÉVELOPPEMENTS

1 Classification des groupes d'ordre p^2

Présentation

Dans ce développement, on cherche à classer les groupes d'ordre p^2 où p est premier. Les groupes d'ordre premier sont déjà connus : ils sont cycliques. La question naturelle suivante est donc : que se passe-t-il pour p^2 ?

Nous allons montrer qu'il n'existe que deux groupes d'ordre p^2 où p est premier, à isomorphisme près.

Ce développement n'est pas compliqué, et utilise de nombreux résultats sur les actions de groupe, ce qui permet de revoir cette notion.

Les étapes du développement sont des résultats classiques et doivent être connues de tout candidat à l'agrégation.

Prérequis

Définition 1.1. Soit G un groupe. Le **centre** de G , noté $Z(G)$, est l'ensemble des éléments de G qui commutent avec tous les autres. C'est un sous-groupe distingué de G .

Définition 1.2. Soit G un groupe agissant sur un ensemble X . Soit $x \in X$.

- L'ensemble $\text{Stab}(x) = \text{St}_x = \{g \in G; g \cdot x = x\}$ est appelé le **stabilisateur** de x . C'est un sous-groupe de G .
- L'ensemble $\text{Orb}(x) = \mathcal{O}_x = \{g \cdot x; g \in G\} \subset X$ est appelé **orbite** de x sous l'action de G .

Définition 1.3. Soit G un groupe et H un sous-groupe de G . On définit une relation d'équivalence sur G par :

$$x \mathcal{R} y \Leftrightarrow x^{-1}y \in H.$$

Les classes d'équivalence de cette relation sont appelées **classes à gauche modulo H** . Leur ensemble est noté G/H .

On note donc $G/\text{Stab}(x)$ l'ensemble des classes à gauche modulo $\text{Stab}(x)$.

Attention, il n'y a aucune raison pour que $G/\text{Stab}(x)$ ait une structure de groupe, étant donné que $\text{Stab}(x)$ n'est pas forcément un sous-groupe distingué.

Proposition 1.4. Formule des classes

Soit $x \in X$. L'application

$$\begin{aligned} f_x: G/\text{Stab}(x) &\rightarrow \mathcal{O}_x \\ \bar{g} &\mapsto g \cdot x \end{aligned}$$

est une bijection. Ainsi si G est fini, on a la relation :

$$|G| = |\mathcal{O}_x| \times |\text{Stab}(x)|.$$

Démonstration.

Premièrement, on montre que f_x est bien définie.

Tout d'abord, f_x envoie bien $\bar{g}$ dans l'orbite de x .

Soit $\bar{g}_1 = \bar{g}_2$. Ainsi $g_1 \text{Stab}(x) = g_2 \text{Stab}(x)$. Alors comme $e \in \text{Stab}(x)$, on a que $g_1 \in g_2 \text{Stab}(x)$, donc il existe $h \in \text{Stab}(x)$ tel que $g_1 = g_2 h$.

Alors :

$$g_1 \cdot x = (g_2 h) \cdot x = g_2 \cdot (h \cdot x) = g_2 \cdot x,$$

car $h \in \text{Stab}(x)$.

Donc f_x est bien définie.

Par définition de l'orbite de x , f_x est surjective.

On montre que f_x est injective.

Soit $\bar{g}_1, \bar{g}_2 \in G/\text{Stab}(x)$ tel que $g_1 \cdot x = g_2 \cdot x$. Alors :

$$x = g_1^{-1} \cdot (g_1 \cdot x) = g_1^{-1} \cdot (g_2 \cdot x) = (g_1^{-1} g_2) \cdot x.$$

Donc $g_1^{-1} g_2 \in \text{Stab}(x)$ et alors il existe $h \in \text{Stab}(x)$ tel que $g_1^{-1} g_2 = h$, ce qui équivaut à $g_2 = g_1 h$. Finalement :

$$g_2 \text{Stab}(x) = g_1 h \text{Stab}(x) = g_1 \text{Stab}(x).$$

On a bien prouvé l'injectivité.

Donc : $G/\text{Stab}(x) \simeq \mathcal{O}_x$.

En utilisant le théorème de Lagrange, on obtient l'égalité des cardinaux dans le cas où G est fini. □

Dans la démonstration, on a en fait construit la bijection canonique $G/\text{Stab}(x) \rightarrow \mathcal{O}_x$.

Théorème 1.5. Equation des classes

Soit G un groupe fini agissant sur un ensemble fini X .

Soit T un système de représentants des orbites distinctes. Alors :

$$|X| = \sum_{x \in T} |\mathcal{O}_x| = \sum_{x \in T} \frac{|G|}{|\text{Stab}(x)|}.$$

Définition 1.6. Soit p un nombre premier. Un **p -groupe** est un groupe d'ordre p^α où $\alpha \in \mathbb{N}^*$.

Développement

Lemme 1.7. Soit G un groupe. Si $G/Z(G)$ est monogène, alors G est abélien.

Démonstration.

Comme $G/Z(G)$ est monogène, il existe $a \in G$ tel que $G/Z(G) = \langle \bar{a} \rangle$.

Ainsi tout élément de G s'écrit sous la forme $a^k z$ avec $z \in Z(G)$ et $k \in \mathbb{Z}$, et donc commute avec a . Cela prouve que $a \in Z(G)$ et alors $\bar{a} = \bar{1}$.

D'où $G/Z(G) = \langle \bar{a} \rangle = \langle \bar{1} \rangle$. Donc $G = Z(G)$ et finalement G est un groupe abélien. $\square$

Lemme 1.8. Le centre d'un p -groupe est non trivial.

Démonstration.

Soit G un p -groupe tel que $|G| = p^\alpha$ avec $\alpha \in \mathbb{N}^*$.

On considère l'action par conjugaison de G sur lui-même et on va utiliser l'équation des classes.

On observe que l'orbite d'un élément x est réduite à $\{x\}$ si et seulement si $x \in Z(G)$.

Ainsi si $x \notin Z(G)$, $|\mathcal{O}_x| > 1$ et d'après la formule des classes, $|\mathcal{O}_x|$ divise $|G| = p^\alpha$.

Donc $|\mathcal{O}_x| \equiv 0 [p]$.

Soit T un système de représentants des orbites distinctes.

Alors d'après l'équation des classes :

$$\begin{aligned} |G| &= \sum_{\substack{x \in T \\ |\mathcal{O}_x|=1}} |\mathcal{O}_x| + \sum_{\substack{x \in T \\ |\mathcal{O}_x|>1}} |\mathcal{O}_x| \\ &\equiv |Z(G)| [p]. \end{aligned}$$

Comme p divise $|G|$, alors p divise $|Z(G)|$. Or $|Z(G)| \geq 1$ car $e \in Z(G)$, donc $|Z(G)| \geq p$. On en déduit que $Z(G)$ n'est pas réduit à l'identité. $\square$

Lemme 1.9. *Soit G un groupe d'ordre p^2 . Alors G est abélien.*

Démonstration.

D'après le théorème de Lagrange, comme le cardinal d'un sous-groupe divise l'ordre du groupe, on obtient que $Z(G)$ est d'ordre 1, p ou p^2 .

- Si $Z(G)$ est d'ordre 1, alors le centre est trivial, ce qui n'est pas possible d'après le lemme 1.8.
- Si $Z(G)$ est d'ordre p , alors $G/Z(G)$ est d'ordre p donc est monogène (et même cyclique). D'après le lemme 1.7, G est abélien et donc $Z(G) = G$. Contradiction avec le fait que $|Z(G)| = p < p^2 = |G|$.
- Si $Z(G)$ est d'ordre p^2 , alors $Z(G) = G$ et donc G est abélien. $\square$

Théorème 1.10. *Soit G un groupe d'ordre p^2 . Alors :*

$$G \simeq \mathbb{Z}/p^2\mathbb{Z} \text{ ou } G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

Démonstration.

D'après le lemme 1.9, on sait que G est abélien. Il y a deux cas :

- Si G possède un élément d'ordre p^2 , alors G est cyclique d'ordre p^2 donc est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$.
- Sinon, tous les éléments de G sont d'ordre 1 ou p .
Comme G est abélien, on peut le munir d'une structure de $\mathbb{Z}/p\mathbb{Z}$ -espace vectoriel (on a besoin d'avoir un groupe commutatif et $\mathbb{Z}/p\mathbb{Z}$ est bien un corps) en définissant la loi externe $\bar{k} \cdot x = x^k$ pour $\bar{k} \in \mathbb{Z}/p\mathbb{Z}$ et $x \in G$.

Il faut montrer que cette loi est bien définie, c'est-à-dire que si $\bar{k} = \bar{k}'$, alors $x^k = x^{k'}$.

En effet, si $\bar{k} = \bar{k}'$, alors $\overline{k - k'} = 0$ et donc $k - k' = p \times n$ avec $n \in \mathbb{Z}$.

D'où : $x^{k-k'} = x^{pn}$. Or x est d'ordre 1 ou p donc forcément $x^{pn} = 1$.

Ainsi $x^k = x^{k'}$.

Et cette multiplication vérifie bien les 4 axiomes d'une loi externe.

Or $|G| < +\infty$ donc c'est un $\mathbb{Z}/p\mathbb{Z}$ -espace vectoriel de dimension finie, qui est alors isomorphe à une puissance de $\mathbb{Z}/p\mathbb{Z}$. Comme $|G| = p^2$, on en déduit que $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

□

Remarques

- Pour $p = 2$, tout groupe d'ordre 4 est donc isomorphe à l'un des deux groupes suivants :

$$\mathbb{Z}/4\mathbb{Z} \text{ ou } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Une manière de voir que ce sont bien deux groupes distincts est que le premier est cyclique et possède un élément d'ordre 4, tandis que dans le second tous les éléments non neutres sont d'ordre 2.

- Pour démontrer le théorème 1.10, on aurait pu utiliser le théorème général suivant :

Théorème 1.11. *Théorème de structure des groupes abéliens finis*

Soit G un groupe abélien fini. Alors il existe des entiers $d_1, \dots, d_s \geq 2$ vérifiant $d_1 | d_2 | \dots | d_s$ tel que :

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z}.$$

De plus, la suite d'entiers $(d_1, \dots, d_s)$ est unique.

- Ce développement est issu de la deuxième édition du livre [18] page 106, où des approfondissements sont proposés.

Recasages

- 101 : Groupe opérant sur un ensemble. Exemples et applications.
- 103 : Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.
- 104 : Groupes finis. Exemples et applications.