HASSINA KETRANE
LAËTITIA ELINEAU

ÉPREUVE ORALE D'EXEMPLES ET D'EXERCICES

AGRÉGATION INTERNE/CAERPA MATHÉMATIQUES

DUNOD

Création graphique de la couverture : Hokus Pokus Créations

11 rue Paul Bert, 92240
Malakoff www.dunod.com

ISBN 978-2-10-080104-6

Avant-propos

À tous ceux qui démarrent cette aventure…

À travers cet ouvrage, nous avons voulu apporter le point de vue de personnes qui ont enduré cette épreuve (dans tous les sens du terme !), partager notre expérience et nos travaux dans l'espoir de contribuer à la réussite de certains. Le point de départ de ce projet est certainement aussi le manque que nous avons nous-mêmes ressenti lorsque nous avons préparé l'agrégation.

Il faut bien comprendre que pour préparer l'agrégation, il faut avant tout réussir à se dégager du temps, et du temps on en a peu quand on doit concilier cela avec un emploi, une vie de famille, etc. Il faut donc travailler durement mais surtout efficacement. Abordez ce challenge avec un état d'esprit conquérant. Avec moins de 10% de réussite, seuls les plus coriaces arrivent au bout. Jamais, jamais, n'abandonnez jamais : la persévérance et la hargne sont, selon nous, les principaux facteurs de réussite.

Ce que nous vous proposons dans ce livre, c'est, pour chaque leçon traitée : un choix d'exercices, des idées de commentaires et un développement (dit « résolution commentée » dans le rapport du jury). N'y voyez surtout pas des modèles « prêts à l'emploi » mais avant tout un point de départ, une base de travail, des compléments d'idées. Il est d'ailleurs essentiel de personnaliser vos leçons dans la mesure où vos choix doivent être défendus devant le jury.

Déroulement de l'épreuve :

Vous trouverez sur le site **http://agrint.agreg.org/archives.html** les sujets et rapports des années précédentes. Voici quelques extraits du rapport de jury de 2015 :

« Le candidat choisit trois à six exercices portant sur le thème retenu et rédige un document comportant la liste des énoncés, ainsi que les motivations et remarques correspondantes. À l'issue de la préparation, des photocopies de ce document sont réalisées par les appariteurs et sont remises aux examinateurs.

L'épreuve orale se déroule en trois temps :

1) Présentation motivée de l'ensemble des exercices sélectionnés par le candidat (durée maximale de 10 minutes).

2) Résolution commentée d'un des exercices au choix du candidat parmi ceux qu'il vient de présenter (durée de 15 minutes).

3) Questions du jury (durée minimale de 20 minutes). »

« L'épreuve n'est pas censée représenter une séance devant une classe de collège ou de lycée ; des objectifs plus ambitieux et un rythme plus soutenus peuvent être adoptés sous réserve d'une bonne maitrise des notions mathématiques sous-jacentes et d'une réelle qualité d'exposition. »

« Il s'agit d'expliquer soigneusement les raisons qui ont conduit au choix des exercices. Motiver le choix d'une liste d'exercices, c'est expliquer la pertinence de ce choix par des raisons d'ordre pédagogique ou mathématique (l'un n'excluant pas l'autre), préciser les prérequis, situer les exercices dans leur contexte, commenter leur apport sur le plan pédagogique, etc ».

Préparation des leçons :

L'épreuve orale d'exercices est assez technique et demande à être préparée minutieusement. L'idéal est d'arriver le jour de l'oral en ayant déjà une idée des exercices que l'on peut proposer. Ainsi, le temps de préparation pourra être mis à profit pour bien maitriser le développement et pour se remettre en tête les idées principales de résolution de chaque exercice.

Quelques conseils de préparation :

- Ne commencez surtout pas la préparation des leçons seulement une fois les écrits passés. Réfléchir à 160 leçons, à un niveau approfondi, et en deux mois, relève des travaux d'Hercule ! Le mieux est donc de s'y mettre dès le début des révisions et de « la jouer stratégique ». Choisissez en priorité celles qui vous permettent de préparer parallèlement les écrits et laissez les thèmes moins classiques pour plus tard. Par exemple, les séries de fonctions vous seront certainement d'un plus grand secours que les équations fonctionnelles.
- Apprenez à gérer votre temps de préparation aux leçons. Au départ, passer beaucoup de temps sur une seule leçon est tout à fait naturel et permet même d'approfondir les notions visées. Vous vous devez d'avoir un certain recul par rapport à ce que vous proposez. Toutefois, à l'approche des oraux, vous devriez avoir acquis un minimum de bagage mathématiques qui vous permettra de limiter ce temps de préparation. La vitesse d'exécution fait partie des qualités requises le jour de l'oral.
- Maitrisez le niveau de la leçon traitée.
- Évitez de ne choisir que des exercices de haut vol. Le jour J, le temps passe vite, et on doit être capable de résoudre chacun des exercices proposés ou au moins d'en donner les grandes lignes de résolution.
- Choisissez-en au moins deux conséquents pour donner de la substance à la leçon. Les autres, plus simples, doivent servir à alimenter vos commentaires.
- N'hésitez pas à vous servir du tableau pour faire des schémas, rappeler des théorèmes importants,...
- Une fois les écrits passés, établissez-vous un planning pour traiter et synthétiser sur fiche toutes les leçons, sans oublier les développements. Laissez-vous une semaine à 10 jours avant votre passage pour lire, relire et apprendre vos fiches.
- Le choix du développement est primordial. Choisir un exercice trop calculatoire ne mettrait pas en valeur vos compétences mathématiques et, lié au stress, serait risque d'erreur. Le jour J, il est impératif d'avoir levé en amont toutes les difficultés de l'exercice choisi. L'idéal est d'être capable de se le remettre en tête en maximum vingt minutes.

Le jour J :

- Prévoyez des mini post-it pour marquer les pages des livres.
- Prévoyez une montre chronomètre pour gérer votre temps au tableau.
- La fatigue psychologique et physique est lourde. Pourquoi ne pas réserver une chambre d'hôtel près du lieu d'examen pour s'économiser au maximum ?
- Pensez-y, vous pouvez déposer vos valises de livres la veille de votre premier passage.

Présentation du livre :

Chacune des leçons est présentée de la manière suivante :

- **Énoncés des exercices :** Dans cette partie figurent des exemples de choix d'exercices, ainsi que les références des ouvrages dont ils sont issus ou inspirés. On pourra faire usage d'un même énoncé pour plusieurs leçons. Cela fait évidemment partie de la stratégie de préparation.
- **Idées de commentaires :** Dans cette partie, nous donnons des idées pour la présentation orale en précisant dans chaque exercice les notions abordées et le lien avec le thème de la leçon.

Fil directeur

Le fil directeur indique la motivation générale du choix du ou des exercices suivants.

Attention !

Ces passages indiquent des notions importantes à maitriser.

Tableau

Ces passages permettent d'identifier les notions qu'il convient d'écrire au tableau.

Exercice 0 [RÉFÉRENCE] Développement 00

Choix du développement. La grande majorité d'entre eux vous sont proposés en fin d'ouvrage. Vous y trouverez aussi la liste de toutes les leçons dans lesquelles l'exercice peut figurer, en souligné s'il peut faire office de développement.

Exercice 0

Autre développement possible. Certains de ces « autres développements possibles » vous sont proposés en fin d'ouvrage.

Si malgré tout le soin apporté à l'élaboration de cet ouvrage, des erreurs apparaissaient, vous pouvez nous contacter à l'adresse mail suivante : agreg.ek@gmail.com

« La chute n'est pas un échec. L'échec, c'est de rester là où on est tombé. »

Socrate

« Impossible n'est pas une donnée, c'est une opinion. Impossible n'est pas une fatalité, c'est un défi. Impossible est une chance. Impossible est provisoire. Impossible n'est rien. »

Mohamed Ali

Remerciements

C'est Laëtitia qui a eu l'idée de cet ouvrage et c'est à elle que revient tout le mérite de la mise en page. Merci à toi de m'avoir associée à ce projet.

Je dois beaucoup à Matthieu Fradelizi, vers qui je me suis très souvent tournée lors de mes questionnements mathématiques. C'est aussi lui qui s'est soumis de bonne grâce à la relecture de ce manuscrit. Je lui exprime sincèrement toute ma gratitude pour son aide précieuse.

Jean-Marie Monier nous a fait bénéficier d'une relecture finale très méticuleuse, accompagnée de judicieux commentaires. Qu'il en soit chaleureusement remercié.

Je pense aussi à tous ceux qui m'ont transmis leur savoir, qui m'ont donné de leur temps et qui ont répondu à toutes mes interrogations avec une infinie patience : Pierre-André Zitt, Pierre Puchol, Romain Dujardin, et bien d'autres encore...
Qu'ils trouvent ici mes remerciements.

Un mot pour les éditions Dunod, qui nous ont pleinement accordé leur confiance. Un grand merci à eux, mais aussi à tous les autres éditeurs apparaissant dans la bibliographie, qui nous ont donné leur accord pour les droits de reproduction.
Sans eux, ce livre n'aurait jamais vu le jour.

Merci à Nadia, qui a toujours cru en moi. Merci à Sophie, Meggie, Ilhem, Laëtitia, Fahed, Jessica, Cécile, Alexandre, Sébastien... qui m'ont rendu la préparation tellement plus agréable.

Je remercie enfin et surtout ma famille qui m'a supportée dans tous mes projets et qui a contribué à chacune de mes réussites : Abdenour, mon meilleur soutien ; mon frère Ahmed et ma sœur Souade ; mes parents, à qui je dois tout.

Je dédis, pour ma part, ce livre à mes filles Ilham et Yasmine. Je souhaite leur dire qu'avec du travail et de la volonté, on peut faire bien des choses. On ne m'en voudra pas de le dédier également à toutes les mamans et tous les papas qui se lancent dans cette aventure qu'est l'agrégation. Il faut un peu plus de courage mais on peut y arriver !

Hassina

Merci à...

- Hassina, sans qui le livre n'existerait pas, de m'avoir toujours encouragée et motivée dans les moments de doute, tant durant l'écriture que la préparation du concours.

- Matthieu Fradelizi, pour sa relecture attentive et minutieuse de cet ouvrage et l'écriture de la préface.

- tous les enseignants de la préparation à l'agrégation interne de mathématiques de l'université Paris-Est Marne-la-Vallée, pour leurs enseignements et leurs conseils qui m'ont permis d'obtenir brillamment le concours.

- la maison d'édition Dunod, qui a accepté de publier notre ouvrage ainsi que les éditions Bréal, Cassini, Cépaduès, EDP Sciences, Publibook, Vuibert... qui nous ont donné leur accord pour citer des parties de leurs ouvrages, sans quoi notre projet n'aurait pu voir le jour.

- Jean-Marie Monier, pour sa relecture finale d'une extrême précision.

- mon mari, Mody, pour son soutien sans faille tout au long de ma préparation au concours et de la rédaction du livre.

- ma famille, en particulier mes parents Alain et Marie-Hélène, ma sœur Audrey et mon grand-père Guy, pour tous leurs encouragements qui m'ont donné confiance et motivée pour aller jusqu'au bout de ces deux aventures.

- Hassina, Mélanie, Sophie, Cécile, Ilhème, Sandrine, Meggie, Stéphane, Sébastien, Alexandre... avec qui la préparation à l'agrégation s'est avérée très plaisante et efficace.

- Frédéric Bro, pour son aide et ses conseils sur l'utilisation de LyX et de Latex.

Laëtitia

Préface

Cet ouvrage présente un panorama de leçons d'exemples et exercices pour la seconde épreuve d'oral du concours de l'agrégation interne de mathématiques. Il a été rédigé par Hassina Ketrane et Laëtitia Elineau, deux lauréates du concours de l'année 2015, qui l'avaient préparé à l'Université Paris-Est Marne-la-Vallée.

Leur histoire, que l'on pourrait appeler une « success story », représente de façon emblématique le parcours idéal, mais aussi assez typique, des lauréats du concours et illustre parfaitement le fameux adage à propos du talent : un peu d'inspiration, mais surtout beaucoup de transpiration. Après un échec lors de la session 2014, pour laquelle elles n'avaient pas été admissibles, elles ne se sont pas découragées et ont poursuivi leur travail pour réussir brillamment en 2015 ; Hassina a même été reçue première au concours. Cette réussite remarquable peut servir de modèle à tous les enseignants qui s'engagent dans la préparation de ce concours et qui peuvent se trouver confrontés à un échec. Elle vient récompenser la persévérance et la détermination qui sont nécessaires pour progresser en mathématiques. Dans leur cas, cette détermination se manifestait à travers les nombreuses questions qu'elles venaient nous poser régulièrement. Le résultat obtenu est admirable.

Comme le concours requiert une expérience de cinq années de service public, les candidats doivent tous attendre au moins cinq ans après leur CAPES, avant de pouvoir passer l'agrégation interne. Bien sûr, occupés par leurs enseignements, ils n'ont plus eu le temps de faire des mathématiques à un niveau postbac, il leur faut donc s'y remettre sérieusement afin de préparer le concours. Les écrits ayant lieu en janvier, ils n'ont que quatre mois de préparation la première année ce qui est tout à fait insuffisant. Cela explique qu'il faut, dès le départ, envisager la préparation du concours sur plusieurs années et se préparer à un échec la première année. À la préparation au concours de l'agrégation interne de Mathématiques de l'Université Paris-Est Marne-le-Vallée, à laquelle je participe depuis dix ans, nous proposons donc une formation en deux ans. Une première année, dite de propédeutique, permet une remise à niveau générale et, lors de la deuxième année, nous insistons sur la préparation à l'oral. Pour l'écrit, nous organisons une dizaine d'épreuves blanches et un stage de révision à la Toussaint tandis que pour l'oral, les candidats passent des oraux blancs corrigés et commentés deux après-midi par semaine. Grâce à l'engagement de tous, nous obtenons de très bons résultats (une quinzaine de candidats admissibles et une dizaine d'admis en moyenne chaque année, parmi les meilleurs classés, comme le montre la réussite des auteurs de ce livre). Cependant, les heures qui nous sont allouées diminuent progressivement ce qui nous conduit à ne pouvoir traiter de moins en moins de leçons chaque année. C'est ainsi que les candidats

doivent de plus en plus s'appuyer sur leur travail personnel. Heureusement, celui-ci sera grandement facilité par la parution de ce livre qui deviendra bien vite, j'en suis sûr, un classique parmi les candidats de notre formation et de toutes les formations de France.

L'ouvrage rédigé par Hassina et Laëtitia est à la fois original, vivant, et utile. Il est le premier entièrement consacré à cette difficile épreuve d'oral d'exemples et exercices. Celle-ci, d'une durée de quarante-cinq minutes, se décompose en trois temps : une présentation motivée d'exercices en dix minutes au maximum, la résolution commentée d'un des exercices en quinze minutes et enfin de questions du jury, en vingt minutes au minimum. Hassina et Laëtitia apportent dans cet ouvrage tous les éléments nécessaires à ces trois étapes. En particulier, elles montrent, par l'exemple, comment le candidat peut se saisir de la première partie de l'épreuve, la présentation de son choix d'exercices, pour montrer au jury sa maitrise et sa connaissance du sujet. Il fera ainsi une bonne première impression, ce qui est déterminant. De plus, elles donnent également de nombreux choix d'exercices classiques issus de livres de références pour les candidats, mais dont elles détaillent les solutions afin que chacun puisse appréhender et se saisir de ces résolutions plus rapidement. Enfin, tous ces exercices sont commentés, analysés et décortiqués pour tenter d'anticiper les questions du jury.

Je suis très heureux de préfacer, en quelques lignes, cet ouvrage vivant sur la préparation à la leçon d'exemples et exercices du concours de l'agrégation interne. Il constitue une introduction, facile d'accès et d'utilisation, qui se révèlera bientôt indispensable à tout lecteur souhaitant préparer ce concours.

Matthieu Fradelizi, maitre de conférence à l'Université Paris-Est Marne-la-Vallée et enseignant en préparation à l'agrégation interne

Table des matières

Première partie

Leçons d'algèbre

Leçon 301 par H.K.

Exercices sur les groupes

Choix d'exercices

Exercice 1 **[XAN1] 1.13**

Soit G un sous-groupe de $(\mathbb{R},+)$ non réduit à $\{0\}$.
Montrer que G est soit de la forme $a\mathbb{Z}$, $a \in \mathbb{R}_+^*$, soit dense dans $\mathbb{R}$.

Exercice 2 **[XALG1] 4.13**

Soit p un nombre premier.

1) Soit q un nombre premier qui divise $p-1$. Établir l'existence d'un élément de $\left((\mathbb{Z}/p\mathbb{Z})^*,\times\right)$ d'ordre multiplicatif q.

2) Soit q un nombre premier et $\alpha \in \mathbb{N}^*$ tels que q^α divise $p-1$. Montrer l'existence d'un élément de $\left((\mathbb{Z}/p\mathbb{Z})^*,\times\right)$ d'ordre q^α.

3) En déduire que $\left((\mathbb{Z}/p\mathbb{Z})^*,\times\right)$ est cyclique.

Exercice 3 **[COM] p 44** **Développement 1**

On dispose d'un fil circulaire, de 4 perles bleues, de 3 perles blanches et de 2 perles oranges. Combien de colliers différents peut-on faire avec ce matériel ?

Exercice 4 **[SOR, Alg] 1.8 + [MER]**

Soit $n \in \mathbb{N}^*$.

1) Montrer que le groupe S_n est engendré par les transpositions de $\{1,\dots,n\}$.

2) En déduire :

a) tous les morphismes du groupe S_n dans le groupe multiplicatif $\mathbb{R}^*$.

b) le nombre d'isométries qui conservent un tétraèdre régulier $T = \{A,B,C,D\}$.

Exercice 5 [MER]

1) Soient (d) et (d') deux droites sécantes en I et soient A, B, C (resp. A', B', C') trois points de (d) (resp. (d')) distincts de I. On suppose que les droites (AB') et (BA') sont parallèles, ainsi que (AC') et (CA'). Montrer que (BC') et (CB') sont parallèles.

2) Soit ABC un triangle et soient P, Q, R des points distincts de A, B, C situés respectivement sur (BC), (CA) et (AB). On suppose ces points distincts des sommets du triangle. Montrer que les points P, Q, R sont alignés si et seulement si on a l'égalité : $\dfrac{\overline{PB}}{\overline{PC}} \times \dfrac{\overline{QC}}{\overline{QA}} \times \dfrac{\overline{RA}}{\overline{RB}} = 1$.

Exercice 6 [XALG2] 3.8

1) Soit $A \in \mathscr{M}_n(\mathbb{C})$ telle que $\mathrm{Tr}\left(A^k\right) = 0$ pour tout $k \in \mathbb{N}^*$. Montrer que A est nilpotente.

2) Soit G un sous-groupe de $\mathscr{G}\ell_n(\mathbb{C})$, $(M_i)_{1\leq i\leq m} \in G^m$ une base de $\mathrm{Vect}(G)$ et $f : G \longrightarrow \mathbb{C}^m$ l'application qui à $A \in G$ associe $(\mathrm{Tr}(AM_i))_{1\leq i\leq m}$. Montrer que si $f(A) = f(B)$ alors $AB^{-1} - I$ est nilpotente.

3) On suppose que toutes les matrices de G sont diagonalisables. Montrer que f est injective.

4) En déduire qu'un sous-groupe de $\mathscr{G}\ell_n(\mathbb{C})$ 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.

Idées de commentaires

Fil directeur

Les groupes : le sujet parait bien vaste et il est difficile de se restreindre uniquement à six exercices sur ce thème. J'ai souhaité, pour ma part, mettre en avant les différents domaines d'utilisation : algèbre, géométrie, dénombrement, mais aussi mettre à l'honneur les groupes incontournables tels que : $\mathbb{R}$, $\mathbb{Z}/n\mathbb{Z}$, S_n, $O(2)$, $O(3)$,... à travers l'étude de leurs générateurs, sous-groupes ou encore de leurs applications.

Exercice 1 Sous-groupes additifs de $\mathbb{R}$

Niveau L1, classique/difficile

- Ce premier exemple, très classique mais de bon niveau tout de même, permet d'aborder la structure des sous-groupes additifs de $\mathbb{R}$. Il nécessite une bonne compréhension au préalable de certaines propriétés topologiques (borne inf d'une partie minorée, densité) et de la notion de groupe.
- Donné à des étudiants, il apparait nécessaire de guider sa résolution en introduisant en premier lieu $G_+ = G \cap \mathbb{R}_+^*$ et $a = \inf G_+$ puis en analysant les deux cas suivants :
  - $a > 0$ et on montre alors que nécessairement $a \in G$ puis $G = a\mathbb{Z}$.
  - $a = 0$ et on montre que G rencontre tout intervalle ouvert de $\mathbb{R}$.
- À la suite de cet exercice, on aurait pu aussi en proposer une application en analyse :

Montrer que $\{\sin n\,;\, n \in \mathbb{N}\}$ est dense dans $[-1,1]$. **[XAN1] 1.13**

Attention !

Si vous proposez oralement cette application, il parait plus sage de connaitre le fil directeur de la démonstration : en s'appuyant sur la structure des sous-groupes de $\mathbb{R}$, on montre que pour $\alpha \notin \mathbb{Q}$, $\mathbb{N}\alpha + \mathbb{Z}$ est dense dans $\mathbb{R}$. On en déduit alors la densité de l'ensemble $X = \{\sin n\,;\, n \in \mathbb{N}\}$ dans $[-1,1]$ en considérant l'application $f : x \mapsto \Im\left(e^{2i\pi x}\right)$ qui envoie l'ensemble $\mathbb{Z} + \dfrac{1}{2\pi}\mathbb{N}$ sur X. Le résultat est alors immédiat puisque f étant continue et $\mathbb{Z} + \dfrac{1}{2\pi}\mathbb{N}$ étant dense dans $\mathbb{R}$, on a $f\left(\mathbb{Z} + \dfrac{1}{2\pi}\mathbb{N}\right) = X$ dense dans $f(\mathbb{R}) = [-1,1]$.

Exercice 2 **Cyclicité de $\left((\mathbb{Z}/p\mathbb{Z})^*,\times\right)$, p premier**

Niveau L2/L3, incontournable

- Lorsque l'on étudie la théorie des groupes, on s'intéresse assez rapidement aux groupes monogènes puis cycliques. Toutefois, avant de proposer cet exemple, il faut avoir défini au préalable la théorie des corps afin de justifier que pour p premier, $\left((\mathbb{Z}/p\mathbb{Z})^*,\times\right)$ est bien un groupe. En effet, si p un nombre premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps, c'est-à-dire que tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible. On rappellera à ce propos que l'inverse se calcule facilement par l'algorithme d'Euclide étendu.
- C'est l'occasion de mettre en application la caractérisation des groupes cycliques suivante :
  Soit G un groupe d'ordre n (de cardinal n). G est cyclique si et seulement si G possède au moins un élément d'ordre n. »
  On fera donc, dans cet exercice, essentiellement un travail sur les ordres des éléments et on y fera également usage de résultats arithmétiques tel que le théorème de Fermat.
- En amont de cet exemple, on pourra faire démontrer par récurrence le résultat suivant sur les groupes commutatifs :
  Si $x_1,\dots,x_r$ sont d'ordres respectifs $p_1,\dots,p_r$, les p_i étant deux à deux premiers entre eux, l'ordre de leur produit $x_1\cdots x_r$ est $p_1\cdots p_r$.

Attention !

À savoir : il existe un résultat plus général :
Tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique.
(cf. **Leçon 302**, **Exercice 6**)

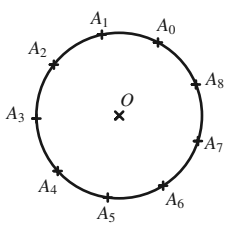
Exercice 3 **Collier de perles**

Niveau L2, approfondissement

- Cet exercice pourra être proposé après l'étude du groupe des isométries $\mathscr{D}_n$ conservant le polygone régulier à n côtés, qui elle-même viendrait après celle du groupe $O(2)$ (groupe orthogonal en dimension 2).

Tableau

Le lien avec le polygone régulier se fait en modélisant le problème.
Sur un cercle, on réserve 9 emplacements $A_0,\dots,A_8$ régulièrement espacés :
On définit le polygone régulier par $P=\{A_0,\dots,A_8\}$ et l'ensemble X des partitions $(4,3,2)$ de P que l'on écrit :
$X = P_{(4,3,2)}$
$\quad = \{(I,J,K)\in\mathscr{P}(P),\, I\cup J\cup K = P, \#I=4, \#J=3, \#K=2\}$



- On réserve l'une de ces partitions pour faire un collier, sachant que deux colliers sont identiques si l'on passe d'une partition à l'autre par l'une des isométries qui conservent P. Et c'est donc très naturellement que l'on est amené à considérer l'action de groupe de $\mathscr{D}_9$ sur l'ensemble X. Le nombre de colliers différents correspond alors au nombre d'orbites N sous cette action. Voilà donc une belle occasion d'appliquer la formule de Burnside :
$$N = \frac{1}{\#\mathscr{D}_9} \times \sum_{g \in \mathscr{D}_9} \#(fix(g)).$$
- Cette formule montre bien la nécessité d'une bonne connaissance du groupe $\mathscr{D}_9$; de son cardinal et des éléments qui le composent.

Exercice 4 **Autour de S_n**

Niveau L2, incontournable

- Cet exercice est destiné à l'étude du groupe S_n. La première question, qui traite des générateurs, est en réalité une question de cours et n'est là que pour rappeler une méthode classique utilisée pour montrer un résultat sur S_n : on l'établit au préalable sur les transpositions de $\{1,\dots,n\}$ puis on l'étend à S_n grâce à la décomposition d'une permutation en produit de transpositions.
- Pour le **a)**, on commencera donc par déterminer à quoi ressemble le morphisme appliqué à une transposition. L'exercice donnera aussi l'occasion de parler « signature » et s'appuiera notamment sur le résultat de cours :
Pour toute transposition τ et τ', $\exists \sigma \in S_n$ telle que $\sigma^{-1} \circ \tau' \circ \sigma = \tau$ i.e. les transpositions sont conjuguées dans S_n.
- Le **b)** nécessite certainement une indication qui donnerait à considérer le morphisme de groupes $\varphi : \mathrm{Is}(T) \to S_{\{A,B,C,D\}}$ et à montrer qu'il est bijectif afin de déterminer $\#(\mathrm{Is}(T))$. L'injectivité ne demande que peu de travail puisque φ est entièrement déterminé par les images de A, B, C et D qui forment un repère affine de l'espace. C'est pour montrer la surjectivité que l'on fera appel à la méthode exposée, en mettant en évidence un antécédent pour chaque transposition. Mieux vaut par conséquent avoir une bonne connaissance de la géométrie du tétraèdre.

Attention !

Une preuve de la surjectivité :
On considère une transposition de $S_{\{A,B,C,D\}}$, par exemple $\tau_{A,B}$. La réflexion $s_{[AB]}$ par rapport au plan médiateur de $[AB]$ échange A et B tandis qu'elle laisse fixe C et D, c'est donc un antécédent par φ de $\tau_{A,B}$. Même argument pour toutes les transpositions. On considère par la suite $\sigma \in S_{\{A,B,C,D\}}$ et une de ses décompositions en produit de transpositions $\sigma = \tau_1 \circ \cdots \circ \tau_k$.
D'après ce qui vient d'être dit :

$$\exists s_1, \ldots, s_k \in \mathrm{Is}(T) \text{ tels que } \varphi(s_1) = \tau_1, ..., \varphi(s_k) = \tau_k.$$

On a alors : $\sigma = \tau_1 \circ \cdots \circ \tau_k = \varphi(s_1) \circ \cdots \circ \varphi(s_k) = \varphi(s_1 \circ \cdots \circ s_k)$
et $s_1 \circ \cdots \circ s_k \in \mathrm{Is}(T)$, ce qui conclut le raisonnement.

Attention !

Une question qui pourrait se poser à la suite de cette application du tétraèdre : « Peut-on envisager un raisonnement identique pour le cube $\mathscr{C} = \{A,B,C,D,E,F,G,H\}$? ». La réponse est non. Le morphisme qui va de $\mathrm{Is}(\mathscr{C})$ dans $S_{\{A,B,C,D,E,F,G,H\}}$ est clairement injectif mais en aucun cas surjectif puisqu'il n'existe pas d'antécédent à $\tau_{A,B}$ par exemple. En effet, il n'existe pas d'isométrie conservant $\mathscr{C}$, fixant six sommets et échangeant deux autres sommets.

Exercice 5 Ménélaüs/Pappus

Niveau L1, application

- Voilà deux exemples issus de la géométrie, idéaux pour étudier le groupe des homothéties-translations. L'exercice ne présente pas de difficulté mathématique mais nécessite une bonne connaissance des propriétés de ce groupe. Je citerais parmi elles :
  - *Deux homothéties qui ont même centre commutent.*
  - *Une translation envoie une droite sur une droite parallèle.*
  - *Si le produit de deux homothéties est une homothétie alors les 3 centres sont alignés.*

Exercice 6 Théorème de Burnside

Niveau L3, approfondissement

- Si un groupe G est fini alors, d'après le théorème de Lagrange, il est d'exposant fini. La question que posa Burnside fût la suivante : « Un groupe de type fini (*i.e.* engendré par une partie finie) et d'exposant fini est-il nécessairement fini ? ». Un contre-exemple a été apporté plusieurs années plus tard et la réponse est donc négative. L'exercice propose de montrer que la propriété est toutefois vraie si G est un sous-groupe de $\mathscr{G}\ell_n(\mathbb{C})$.

Attention !

Une question qui pourrait se poser à l'issue de ce problème : « Donner un exemple de groupe infini d'exposant fini ». On peut penser à $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ qui est d'exposant 2.

Leçon 302 par L.E.

Exercices faisant intervenir les notions de congruences et de divisibilité dans $\mathbb{Z}$

Choix d'exercices

Exercice 1 **[SOR, Alg] 2.5.b**

Résoudre l'équation $x^2 - y^2 = 18$ d'inconnue $(x, y) \in \mathbb{Z}^2$.

Exercice 2 **[FRE, MP*] 1.12**

On se donne p et q deux nombres premiers distincts.

1) Justifier que pour $a \in \mathbb{Z}$ non divisible par p et q, $a^{(p-1)(q-1)} \equiv 1\ [pq]$.

2) Soit $d \in \{1, \ldots, (p-1)(q-1)\}$, premier avec $(p-1)(q-1)$. Justifier l'existence de $e \in \{1, \ldots, (p-1)(q-1)\}$ tel que $ed \equiv 1\ [(p-1)(q-1)]$.

3) Montrer que pour tout $a \in \mathbb{Z}$, $a^{de} \equiv a\ [pq]$.

Exercice 3 **[SOR, Alg] 3.8.a et 3.10.b**

Soient $A = X^4 + X^3 + 2X^2 + X + 1$ et $B = 2X^5 - 7X^4 + 9X^3 - 9X^2 + 7X - 2$.
Déterminer la décomposition de A et B en facteurs irréductibles de $\mathbb{Q}[X]$.

Exercice 4 [XALG1] 5.16 Développement 2

1) a) On dit qu'un polynôme non nul de $\mathbb{Z}[X]$ est primitif si le PGCD de ses coefficients est égal à 1.

Montrer que le produit de deux polynômes primitifs de $\mathbb{Z}[X]$ est primitif.

b) Pour $A \in \mathbb{Z}[X]$ non nul, on appelle contenu de A, et on note $c(A)$ le PGCD des coefficients de A. Soit A et B deux polynômes non nuls de $\mathbb{Z}[X]$. Montrer que $c(AB) = c(A)\,c(B)$.

2) Soit $P = p_n X^n + \cdots + p_1 X + p_0 \in \mathbb{Z}[X]$ et p un nombre premier. On suppose que :

(i) p ne divise par a_n ;

(ii) p divise a_0,..., a_{n-1} ;

(iii) p^2 ne divise pas a_0.

Montrer que A est irréductible dans $\mathbb{Q}[X]$.

Exercice 5 [XALG1] 2.11

Soit G un groupe fini de cardinal p^m avec p premier et $m \geq 1$.

1) Montrer que le centre de G, $\mathscr{Z}(G) = \{a \in G ; \forall g \in G, ag = ga\}$, est d'ordre p^k avec $0 < k \leq m$.

2) On suppose que $m = 2$. Montrer que G est abélien.

Exercice 6 [XALG1] 2.8

Soit G un groupe abélien fini. Pour tout $x \in G$, on note $o(x)$ l'ordre de x.

1) Soit $(x,y) \in G^2$, $m = o(x)$, $n = o(y)$. On suppose que m et n sont premiers entre eux. Montrer que $o(xy) = mn$.

2) Soit $(m,n) \in (\mathbb{N}^*)^2$. Montrer l'existence de $(m',n') \in (\mathbb{N}^*)^2$ tel que $m' \mid m$, $n' \mid n$, $\mathrm{PGCD}(m',n') = 1$ et $\mathrm{PPCM}(m,n) = m'n'$.

3) Montrer qu'il existe $z \in G$ tel que $o(z)$ soit le PPCM des ordres des éléments de G (ce PPCM est appelé l'exposant du groupe G).

4) Soit K un corps commutatif, G un sous-groupe fini du groupe multiplicatif K^*. Montrer que G est cyclique.

Idées de commentaires

Fil directeur

Le premier domaine qui vient à l'esprit lorsque l'on parle de congruences et de divisibilité est l'arithmétique. C'est de ce dernier domaine que ces notions sont issues et la congruence s'avère être un outil très performant dans la résolution des problèmes. Lorsque les fondements de l'arithmétique dans $\mathbb{Z}$ sont maitrisés, on peut alors commencer à appréhender ceux dans des anneaux moins « concrets », comme par exemple $\mathbb{Z}[X]$, anneau des polynômes à coefficients dans $\mathbb{Z}$. Nous y trouvons donc aussi de nombreuses applications de ces deux notions. Un dernier domaine que j'ai choisi d'aborder est celui de la théorie des groupes, où il sera surtout question de divisibilité lorsque l'on travaillera sur l'ordre des éléments.

Exercice 1 Équation diophantienne

Niveau L1, application directe

- Ce premier exercice illustre l'efficacité de la congruence pour résoudre une équation diophantienne.

  On appelle équation diophantienne, toute équation $P(x_1,\dots,x_N) = 0$ d'inconnue $(x_1,\dots,x_N) \in \mathbb{Z}^N$, où $N \in \mathbb{N}^*$ et où P est une fonction polynomiale à N variables et à coefficients dans $\mathbb{Z}$.

- Pour résoudre une équation diophantienne en utilisant les congruences, l'idée consiste à choisir judicieusement $n \in \mathbb{N}^*$, à « mettre » l'équation étudiée modulo n et à étudier l'équation ainsi obtenue.
- Ici, le bon choix est $\mathbb{Z}/4\mathbb{Z}$ (à indiquer aux étudiants). Dans cet anneau, les seuls carrés sont 0 et 1, on peut donc facilement calculer les valeurs prises par $x^2 - y^2$ afin de résoudre l'équation.

Fil directeur

Un grand domaine d'application des congruences est la cryptographie. Je présente ici le système de chiffrement RSA.

Exercice 2 Codage RSA

Niveau L1, classique

- On considère un entier naturel $n = pq$ avec p et q premiers. Une personne souhaitant communiquer de manière codée publie un couple (n,d) appelé clé publique, mais est la seule à connaitre la clé de décodage e, appelée clé secrète et vérifiant $ed \equiv 1\ [(p-1)(q-1)]$. Notons $g : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\overline{a} \mapsto \overline{a}^d$ la fonction de chiffrement et $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\overline{a} \mapsto \overline{a}^e$ la fonction de déchiffrement. Le but de l'exercice est de prouver que $f \circ g(\overline{a}) = \overline{a}$. Ainsi, on peut chiffrer un message (représenté par un élément $\overline{a}$ de $\mathbb{Z}/n\mathbb{Z}$) avec g, puis on le déchiffre avec f. La sécurité de ce système repose sur le fait que connaissant la clé publique, il est

très difficile de déterminer e : un moyen consiste par exemple à factoriser n pour trouver p et q, ce qui est impossible à réaliser lorsque p et q sont grands.

- On veut tout d'abord montrer que si a n'est multiple ni de p ni de q alors $a^{(p-1)(q-1)} \equiv 1\ [pq]$. Les entiers p et q étant premiers, nous reconnaissons alors $a^{\varphi(pq)}$ et il suffit donc d'appliquer le théorème d'Euler.

  Soit un entier $n > 1$. Si k est un entier premier avec n, on a $k^{\varphi(n)} \equiv 1\ [n]$.

- La question **2)** traite de l'existence d'une clé de décodage lorsqu'une clé de codage est choisie et utilise la propriété des inversibles de $\mathbb{Z}/n\mathbb{Z}$.

  Soit un entier $n \geq 2$ et k un entier. L'élément $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k \wedge n = 1$.

- Le but de la dernière question est de prouver que la clé e est bien une clé de décodage. Cette question distingue trois cas, qui feront intervenir la question **1)**, la définition de la congruence, le lien entre congruence et divisibilité ($k \mid n \iff n \equiv 0\ [k]$), la propriété de transitivité de la congruence et le petit théorème de Fermat.

  Soit $p \geq 2$ un nombre premier. Alors :

$$\forall a \in \mathbb{Z}, \qquad a^p \equiv a\ [p] \qquad \text{et} \qquad \forall a \in \mathbb{Z},\ p \nmid a \qquad a^{p-1} \equiv 1\ [p]$$

Fil directeur

Les propriétés de l'arithmétique dans $\mathbb{Z}$ s'étendent directement à l'étude des polynômes de $\mathbb{Z}[X]$ dès lors que l'on travaille sur les coefficients. C'est l'objet des deux exercices suivants.

Exercice 3 Une méthode de factorisation

Niveau L1, approfondissement

- Cet exercice porte sur la factorisation de polynômes de $\mathbb{Z}[X]$ dans $\mathbb{Q}[X]$. Il s'agit donc d'étudier les racines rationnelles d'un polynôme $P \in \mathbb{Z}[X]$ non nul.

  On note n le degré de P et on pose $P = \sum_{i=0}^{n} a_i X^i$. Si P admet une racine rationnelle $a = p/q$ avec $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ et $p \wedge q = 1$ alors l'égalité $P(p/q) = 0$ donne :

$$a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} + a_0 q^n = 0$$

  donc $\begin{cases} a_n p^n = -q\left(a_{n-1} p^{n-1} + \cdots + a_0 q^{n-1}\right) & ① \\ a_0 q^n = -p\left(a_n p^{n-1} + \cdots + a_1 q^{n-1}\right) & ② \end{cases}$.

  On distingue alors deux cas :

  * soit on aboutit à une absurdité avec un argument de divisibilité dans $\mathbb{Z}$ combiné souvent avec la relation $p \wedge q = 1$. Dans ce cas, P n'a pas de racine dans $\mathbb{Q}$ (polynôme A).
  * soit, au contraire, on peut tirer des renseignements sur p et q (polynôme B).

- Dans les deux cas, on utilise le théorème de Gauss :

  Soient a, b et c trois entiers. Si a divise le produit bc et si a et b sont premiers entre eux, alors a divise c.

- Pour le polynôme A, on obtient une contradiction donc il ne possède pas de racine rationnelle. Mais on réussit à l'écrire sous forme d'un produit de deux polynômes de $\mathbb{Z}[X]$ de degré 2, par identification de coefficients.
- En appliquant le théorème de Gauss dans ① et ②, on obtient que $q \mid a_n$ et $p \mid a_0$. Cela permet de trouver une condition nécessaire pour que $a \in \mathbb{Q}$ soit racine de B. Il ne reste alors plus qu'à tester les valeurs trouvées, qui, dans ce cas, sont au nombre de 6. Par ailleurs, on peut remarquer que 1 est racine évidente de B.

Exercice 4 Critère d'Eisenstein

Niveau L2, incontournable

Tableau

Rappeler la définition d'un polynôme irréductible dans $\mathbb{Z}[X]$:
On dit qu'un polynôme non nul P de $\mathbb{Z}[X]$ est irréductible si l'écriture $P = QR$ avec $(Q,R) \in \mathbb{Z}[X]^2$ impose $Q = \pm 1$ ou $R = \pm 1$.

- Cet exercice établit un critère fort utile pour montrer qu'un polynôme à coefficients entiers est irréductible. Il consiste à trouver un nombre premier p qui divise tous les coefficients sauf le coefficient dominant et tel que p^2 ne divise pas le terme constant. Par exemple, avec $p = 2$, on obtient que le polynôme $X^n - 2$ est irréductible dans $\mathbb{Q}[X]$ pour tout entier $n \geq 1$, ce qui prouve qu'il y a dans $\mathbb{Q}[X]$ des irréductibles de tous degrés.

Attention !

Il peut être intéressant de garder à l'esprit une autre application du critère d'Eisenstein. En effet, il permet aussi de prouver que pour tout p premier, le p-ième polynôme cyclotomique est irréductible dans $\mathbb{Q}[X]$ (cf. **[XALG1] 5.17**).

- Comme nous l'avons vu précédemment, lorsque l'on parle de divisibilité, il est souvent plus aisé de travailler sur les congruences ou sur les classes dans $\mathbb{Z}/p\mathbb{Z}$.
- La preuve de l'exercice repose sur la notion de contenu d'un polynôme. On prouvera notamment, en projetant $P \in \mathbb{Z}[X]$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$ et en raisonnant par l'absurde, que le produit de deux polynômes primitifs est primitif. C'est l'occasion d'utiliser la propriété d'intégrité de $(\mathbb{Z}/p\mathbb{Z})[X]$ car $\mathbb{Z}/p\mathbb{Z}$ est un corps.
- Pour montrer que P est irréductible, on fait de nouveau un raisonnement par l'absurde en supposant qu'il est composé, c'est-à-dire qu'il peut s'écrire sous la forme $P = AB$ où A et B sont dans $\mathbb{Z}[X]$ et de degrés strictement inférieurs à celui de P. On projette à nouveau dans $(\mathbb{Z}/p\mathbb{Z})[X]$ pour utiliser la propriété sur le contenu d'un produit : $c(AB) = c(A)\,c(B)$ et l'unicité de la décomposition en irréductibles dans $(\mathbb{Z}/p\mathbb{Z})[X]$.

Fil directeur

Les deux derniers exercices sont consacrés aux groupes et plus précisément à l'étude de l'ordre de leurs éléments.

Exercice 5 Centre d'un p-groupe

Niveau L3, approfondissement

- Cet exercice permet d'utiliser bon nombre de propriétés sur les groupes :
  - ***Théorème de Lagrange :*** *Soit G un groupe fini. L'ordre de tout sous-groupe H de G divise l'ordre de G.*
  - ***Équation aux classes :*** *Si X et G sont finis, en désignant par Θ une partie de X contenant exactement un représentant de chacune des classes d'intransitivité et $G_x = \{s \cdot x ; s \in G\}$, on a $\#X = \sum_{x \in \Theta} \#G_x$.*
  - *Si $\varphi : G \to G'$ est un morphisme de groupes surjectif et H' un sous-groupe de G' alors :*
    (i) $\varphi^{-1}(H')$ est un sous-groupe de G ;
    (ii) le groupe G' est isomorphe à $G/\mathrm{Ker}\varphi$.
  - *Si H est un sous-groupe distingué de G et si G est fini alors*
    $$\#G = \#(G/H) \times \#H$$
  - *Si G est un groupe d'ordre p premier alors il est cyclique, engendré par tout élément différent de l'élément neutre.*
- Le but de la première question est de montrer que $\mathscr{Z}(G)$ n'est pas réduit à l'élément neutre, et pour cela, on va montrer que son cardinal est divisible par p en utilisant l'équation aux classes et le théorème de Lagrange. C'est l'occasion de faire quelques raisonnements simples de divisibilité : si p est premier et $q \mid p^m$ alors il existe $0 \leq k \leq m$ tel que $q = p^k$, si $p \mid a$ et $p \mid b$ alors $p \mid a+b$.
- Pour montrer que G est abélien, sachant que $\mathscr{Z}(G)$ est abélien, nous allons montrer que $G = \mathscr{Z}(G)$. C'est l'occasion d'utiliser la théorie sur les morphismes de groupes et les groupes quotients. La question précédente permet de dire que le cardinal de $\mathscr{Z}(G)$ est soit p soit p^2 et en utilisant le lemme de Gauss nous prouverons donc que $\#\mathscr{Z}(G) = p^2$.
- **Remarque :** Cet exercice fait l'objet d'un prolongement (cas particulier du théorème de Sylow) dans le **[GDX] p 28**.

Exercice 6 Exposant d'un groupe abélien fini

Niveau L3, incontournable

- L'objectif de l'exercice est de prouver que si K est un corps alors tout sous-groupe fini du groupe multiplicatif K^* est cyclique.
- Pour cela, on montre tout d'abord que si G est un groupe abélien fini et m est le PPCM des ordres des éléments de G (appelé exposant du groupe G) alors il existe $z \in G$ d'ordre m.

- Les deux premières questions de l'exercice illustrent un certain nombre de propriétés d'arithmétique et notamment de divisibilité :
  - *Le lemme de Gauss (déjà rencontré)*
  - *Si m divise k et n divise k avec $m \wedge n = 1$ alors mn divise k.* (On peut alors montrer que si $o(x)$ et $o(y)$ sont premiers entre eux alors $o(xy) = o(x)\,o(y)$, objet de la question **1)**).
  - ***Théorème fondamental de l'arithmétique :*** *Tout entier naturel $n \geq 2$ s'écrit de manière unique à l'ordre près sous la forme $n = \prod_{p \in \mathscr{P}} p^{\nu_p(n)}$, où $\mathscr{P}$ désigne l'ensemble des nombres premiers et les $\nu_p(n)$ des entiers naturels.*
- À partir de ce théorème, on peut traduire facilement toutes les notions liées à la divisibilité par des relations entre les $\nu_p(n)$, $\nu_p(m)$, $\nu_p(n')$ et $\nu_p(m')$ afin de construire deux nombres m' et n' premiers entre eux divisant respectivement m et n et qui conservent leur PPCM comme cela est demandé dans la question **2)**.