MINISTÈRE DE L'ÉDUCATION NATIONALE

DIRECTION GÉNÉRALE DES RESSOURCES HUMAINES

RAPPORT DE JURY DE CONCOURS

AGRÉGATION DE MATHÉMATIQUES

CONCOURS EXTERNE

Session 2007

SOMMAIRE

LES RAPPORTS DES JURYS DES CONCOURS SONT ÉTABLIS SOUS LA RESPONSABILITÉ DES PRÉSIDENTS DE JURY

Composition du jury

Directoire

Moisan Jacques, président	Inspecteur général de l'éducation nationale
Chevallier Jean-Marie, secrétaire général	Maître de conférences
Foulon Patrick, vice-président	Professeur des universités
Bougé Luc, vice-président	Professeur des universités
Torossian Charles, vice-président	Maître de conférences
van der Oord Eric, vice-président	Inspecteur général de l'éducation nationale
Boisson François	Professeur de chaire supérieure
Fayolle Guy	Directeur de recherches
Le Dret Hervé	Professeur des universités
Mestre Jean-François	Professeur des universités
Petazzoni Bruno	Professeur de chaire supérieure

Jury

Abergel Luc	Professeur de chaire supérieure
Airault Hélène	Professeure des universités
Apparicio Carine	Professeure agrégée
Aymard Catherine	Professeure de chaire supérieure
Barbolosi Dominique	Maître de conférences
Bardet Jean-Marc	Professeur des universités
Barou Geneviève	Maître de conférences
Barral Julien	Maître de conférences
Beaurpère Karine	Professeure agrégée
Bechata Abdellah	Professeur agrégé
Becker Marc	Professeur de chaire supérieure
Belabas Karim	Professeur des universités
Bennequin Daniel	Professeur des universités
Bernis Laurent	Professeur de chaire supérieure
Bonnefont Claire	Professeure de chaire supérieure
Borel Agnès	Professeure de chaire supérieure
Boucher Delphine	Maître de conférences
Boyer Franck	Chargé de recherches
Burban Anne	Professeure de chaire supérieure
Cabane Robert	Professeur de chaire supérieure
Cadre Benoît	Professeur des universités
Chafaï Djalil	Maître de conférences
Caldero Philippe	Maître de conférences
Cerf-Danon Hélène	Professeure de chaire supérieure

Chanet Françoise	Professeure de chaire supérieure
Chardin Marc	Chargé de recherches
Chevallier Marie-Elisabeth	Professeure de chaire supérieure
Clozel Laurent	Professeur des universités
Contejean Evelyne	Chargée de recherches
Cori René	Maître de conférences
d'Angelo Yves	Professeur des universités
de la Bretèche Régis	Maître de conférences
Delebecque François	Directeur de recherches
Devie Hervé	Professeur de chaire supérieure
Domelevo Komla	Maître de conférences
Dumas Laurent	Maître de conférences
Durand-Lose Jérôme	Professeur des universités
Esman Romuald	Professeur agrégé
Favennec Denis	Professeur de chaire supérieure
Feauveau Jean-Christophe	Professeur de chaire supérieure
Fernandez Catherine	Professeure de chaire supérieure
Fleurant Sandrine	Professeure agrégée
Fontaine Philippe	Professeur agrégé
Fouquet Mireille	Maître de conférences
Furter Jean-Philippe	Maître de conférences
Gaudry Pierrick	Chargé de recherches
Gaussier Hervé	Professeur des universités
Geoffre Rosemarie	Professeure de chaire supérieure
Goldsztejn Emmanuel	Professeur de chaire supérieure
Goudon Thierry	Professeur des universités
Guelfi Pascal	Professeur de chaire supérieure
Guibert Gil	Professeur agrégé
Hanrot Guillaume	Chargé de recherches
Harinck Pascale	Chargée de recherches
Hernandez David	Chargé de recherches
Hijazi Oussama	Professeur des universités
Hirsinger Odile	Professeure agrégée
Isaïa Jérôme	Professeur agrégé
Lafitte Pauline	Maître de conférences
Latrémoliére-Quercia Evelyne	Professeure de chaire supérieure
Le Calvez Patrice	Professeur des universités
Le Goff Claire	Professeure agrégée
Le Nagard Eric	Professeur de chaire supérieure
Lefevre Pascal	Maître de conférences
Lévy Thierry	Chargé de recherches
Lévy-Véhel Jacques	Directeur de recherches
Lods Véronique	Professeure agrégée
Loiseau Bernard	Professeur de chaire supérieure
Loubes Jean-Michel	Chargé de recherches
Louboutin Roland	Professeur de chaire supérieure
Maggi Pascale	Professeure agrégée
Mahieux Annick	Professeure de chaire supérieure

Maillot Vincent	Chargé de recherches
Martineau Catherine	Professeure de chaire supérieure
Meier Isabelle	Professeure de chaire supérieure
Méril Alex	Professeur des universités
Méthou Edith	Professeure de chaire supérieure
Mézard Ariane	Maître de conférences
Mneimné Rached	Maître de conférences
Monier Marie	Professeure agrégée
Mons Pascal	Professeur de chaire supérieure
Moroianu Andrei	Chargé de recherches
Nizard Alain	IA-IPR
Paoluzzi Luisa	Maître de conférences
Paradan Paul-Emile	Maître de conférences
Pennequin Denis	Maître de conférences
Prieur Clémentine	Maître de conférences
Quentin Thierry	Maître de conférences
Quercia Michel	Professeur de chaire supérieure
Régnier Mireille	Directrice de recherches
Rigny Agnès	Professeure de chaire supérieure
Saada Ellen	Chargée de recherches
Sauloy Jacques	Maître de conférences
Seuret Stéphane	Maître de conférences
Sidaner Sophie	Professeure de chaire supérieure
Sitz-Carmona Nathalie	Professeure de chaire supérieure
Suffrin Frédéric	Professeur de chaire supérieure
Taieb Franck	Professeur agrégé
Tosel Nicolas	Professeur de chaire supérieure
Vaugelade Elisabeth	Maître de conférences
Vincent Christiane	Professeure de chaire supérieure
Wagschal Claude	Professeur des universités
Weil Jacques-Arthur	Maître de conférences
Yebbou Johan	Professeur de chaire supérieure
Zayana Karim	Professeur agrégé
Zeitoun Marc	Professeur des universités

Déroulement du concours

Les épreuves écrites se sont déroulées selon le calendrier suivant :

- Épreuve de mathématiques générales : jeudi 12 avril 2007 ;
- Épreuve d'analyse et probabilités : vendredi 13 avril 2007 .

La liste d'admissibilité a été publiée le mardi 5 juin 2007.

L'oral s'est déroulé du 25 juin au 14 juillet au lycée Marcelin-Berthelot de Saint-Maur-des-Fossés. La liste d'admission a été publiée le lundi 16 juillet 2006.

Le concours 2006 a vu la nouvelle organisation en quatre options pour l'épreuve de modélisation parmi lesquelles l'option D (informatique) est caractérisée par la singularité des trois épreuves orales. En 2007 comme en 2006, on peut constater que dans les trois premières options, les nombres d'inscrits sont similaires ; ils sont toujours – et c'est bien compréhensible – nettement inférieurs dans l'option D. Dans les quatre options, les pourcentages d'admis sont similaires. Nous continuons, tant que ces options ne sont pas stabilisées, à ne pas donner de statistiques détaillées par option.

L'agrégation externe de mathématiques

Le nom officiel, « concours externe de recrutement de professeurs agrégés stagiaires », montre clairement que, par le concours d'agrégation, le ministère recrute des professeurs agrégés destinés, selon leur statut, à l'enseignement secondaire (lycées d'enseignement général et technologique et, exceptionnellement, collège) ou à l'enseignement supérieur (universités, instituts universitaires de technologie, grandes Écoles, classes préparatoires aux grandes Écoles, sections de techniciens supérieurs). À l'issue du concours, les candidats admis sont normalement placés comme stagiaires. Les différentes possibilités de stage (stage en formation à l'IUFM, stage en situation dans un établissement secondaire, stage en CPGE, stage comme ATER, etc.) sont détaillées dans la note de service n°2005-038 du 2 mars 2005. Des reports de stage peuvent être accordés par la DGRH[1] pour permettre aux lauréats d'effectuer des études doctorales ou des travaux de recherche dans un établissement ou organisme public français[2] ; les élèves des Écoles Normales Supérieures en bénéficient automatiquement pour terminer leur période de scolarité.

Le programme, la nature des épreuves écrites et orales, font l'objet de publications au bulletin officiel du ministère de l'éducation nationale (B.O.), et leur actualisation peut être consultée sous forme électronique sur le site de la DPE, à l'adresse

`http://www.education.gouv.fr/siac/siac2/default.htm`

ou sur le site de l'agrégation externe de mathématiques, à l'adresse

`http://www.agreg.org`,

où se trouvent aussi tous les renseignements pratiques concernant les sessions à venir.

[1] Direction générale des ressources humaines (personnels enseignants de second degré) du ministère de l'éducation nationale.

[2] La DGRH demande une attestation de poursuite de recherches, ou à défaut une autorisation à s'inscrire dans une formation de troisième cycle universitaire. Les candidats doivent se munir d'une telle attestation et la fournir pendant l'oral.

Statistiques et commentaires généraux sur la session 2007

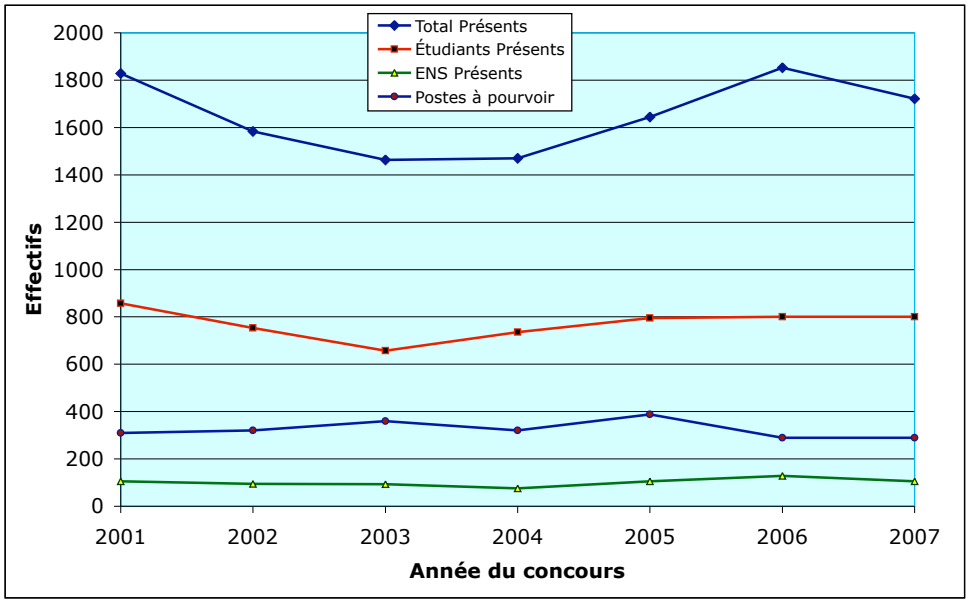
Après la diminution sensible du nombre de postes au concours 2006 (de 388 postes en 2005 à 290 postes en 2006, soit une diminution de plus de 23 %), le nombre de postes proposés au concours 2007 est resté constant.

L'augmentation régulière du nombre d'inscrits (et surtout le nombre de présents aux deux épreuves d'écrit) constatée depuis le concours 2004 s'est arrêtée : c'est certainement la conséquence – avec un retard d'un an, dû à la publication tardive – de la diminution du nombre de postes mis au concours.

Une analyse plus fine montre que cette diminution est due à une diminution du nombre de candidats dans les catégories « normaliens » et « enseignants », les étudiants hors ENS[3] gardant un effectif stable de présents aux deux épreuves.

Année	Total Inscrits	Total Présents	Étudiants Présents	ENS Présents	Postes à pourvoir	Présents par poste
2001	**2663**	**1828**	857	105	310	**5,9**
2002	**2343**	**1584**	753	95	320	**5,0**
2003	**2217**	**1463**	657	93	360	**4,1**
2004	**2333**	**1470**	735	76	321	**4,6**
2005	**2560**	**1644**	795	105	388	**4,2**
2006	**2849**	**1853**	800	129	290	**6,4**
2007	**2801**	**1722**	800	106	290	**5,9**

Évolution du nombre de présents aux deux épreuves d'écrit



[3] dans cette population, sont regroupées les catégories « étudiant » et « élève de 1re année d'IUFM ».

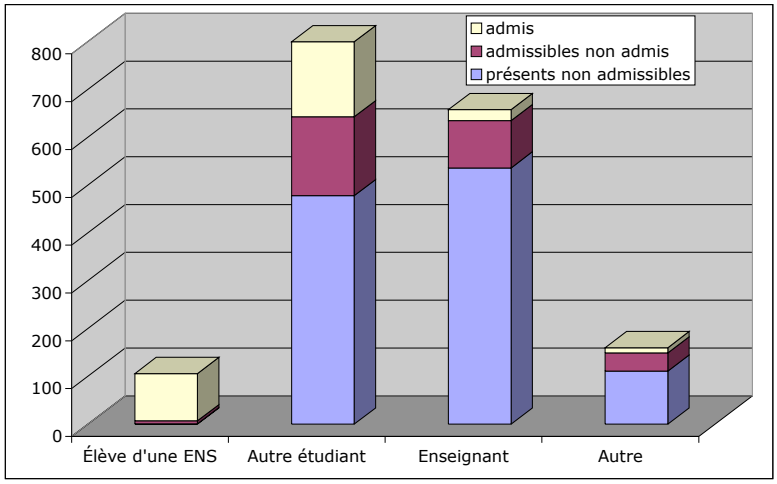
À l'issue de la délibération d'écrit, 598 candidats ont été déclarés admissibles ; le premier admissible avait une moyenne de 20/20 et le dernier une moyenne de 8,25/20. Finalement, à l'issue des épreuves orales, les 290 postes offerts au concours ont été pourvus ; le premier admis a une moyenne de 19,75/20, le dernier admis une moyenne de 9,5/20. Par ailleurs, un candidat étranger a été admis avec un classement bis[4] On trouvera dans les pages qui suivent différents tableaux et graphiques constituant le bilan statistique du concours selon différents critères (géographie, genre, catégorie professionnelle, âge). Dans ces tableaux, **tous les pourcentages sont calculés par rapport aux présents**.

Catégories	Inscrits	Présents	Admissibles	Admis	% admissibles	% admis
ÉLÈVE IUFM 1re ANNÉE	180	140	26	3	18,6	2,1
ÉLÈVE D'UNE ENS	110	106	105	99	99,1	93,4
ÉTUDIANT	768	660	296	154	44,8	23,3
SALARIÉ SECTEUR PRIVÉ	61	26	6	2	23,1	7,7
SANS EMPLOI	168	78	31	7	39,7	9,0
ENSEIGNANT DU SUPÉRIEUR	43	19	7	4	36,8	21,1
CERTIFIÉ	885	411	82	12	20,0	2,9
AUTRE ENSEIGNANT	430	228	33	7	14,5	3,1
AUTRE FONCTIONNAIRE	50	24	5	2	20,8	8,3
SURVEILLANT	30	17	2	0	11,8	0,0
AUTRE	76	15	5	0	33,3	0,0
TOTAL	**2801**	**1724**	**598**	**290**	**34,7**	**16,8**

Résultat du concours par catégories professionnelles[5]

Catégories	Inscrits	Présents	Admissibles	Admis	% admissibles	% admis
Élève d'une ENS	110	106	105	99	99,1	93,4
Autre étudiant	948	800	322	157	40,3	19,6
Enseignant	1358	658	122	23	18,5	3,5
Autre	385	160	49	11	30,6	6,9
TOTAL	**2801**	**1724**	**598**	**290**	**34,7**	**16,8**

Résultat du concours par grandes catégories



[4]Ce candidat est compté parmi les admissibles (en raison des règles d'anonymat) mais n'est pas compté parmi les admis.

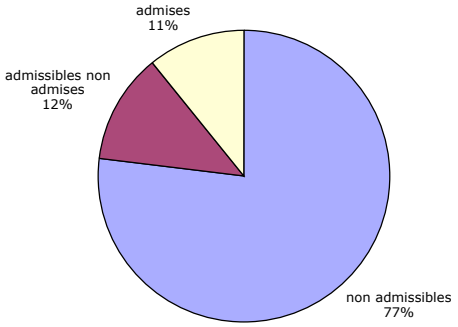
[5] Les catégories professionnelles listées ci-dessus correspondent aux déclarations des candidats lors de l'inscription : elles ne font l'objet d'aucune vérification et doivent être considérées avec prudence.

Ces résultats par grandes catégories confirment que le concours de l'agrégation externe de mathématiques est, comme c'est sa fonction, un concours de recrutement de nouveaux enseignants. La catégorie cumulée des étudiants (ENS et hors ENS) constitue en effet 88 % de l'effectif des admis (comme en 2006).

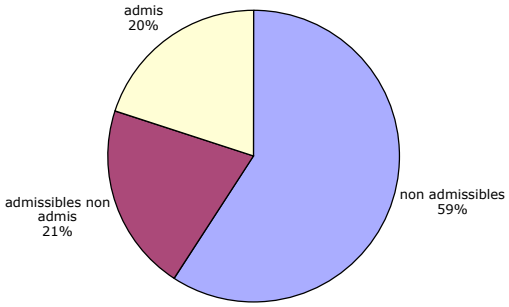
Répartition selon le genre

GENRE	Inscrits	Présents	Admissibles	Admis	% admissibles	% admis
FEMME	955	595	138	65	23,2	10,9
HOMME	1846	1128	460	225	40,8	19,9
TOTAL	2801	1723	598	290	34,7	16,8

Résultat du concours par genres



FEMMES



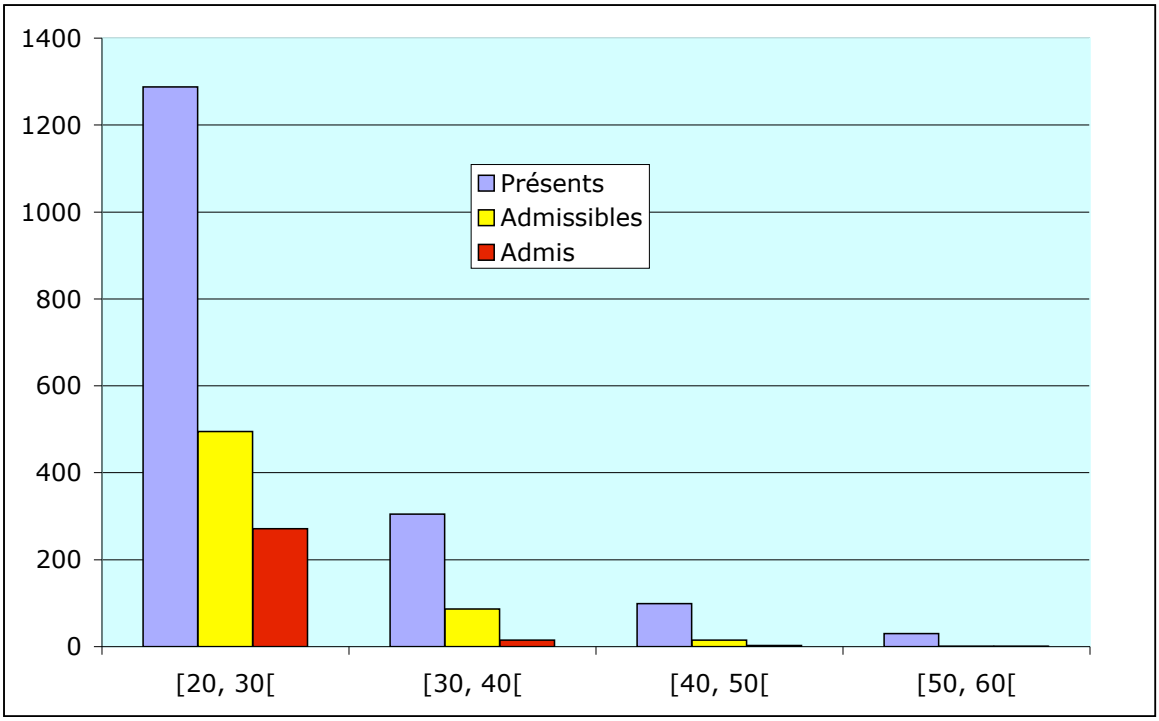
HOMMES

Le net recul de la parité pour le succès au concours, constaté en 2006 (18 % d'admis pour 11 % d'admises) s'accentue en 2007, alors que les taux de succès chez les femmes (23 %) et chez les hommes (24 %) étaient pratiquement identiques en 2005. La diminution du nombre de places au concours entraîne une diminution mécanique du pourcentage de reçues parmi les femmes, puisqu'elles ne représentent qu'un faible pourcentage parmi les candidats issus d'une ENS (10 % cette année, à comparer aux 15 % de 2006). Dans cette catégorie, on trouve en effet, en 2007, 34 % des reçus au concours (contre 26 % en 2005). Si l'on regarde, en revanche, dans la catégorie des étudiants hors ENS, la parité est respectée dans les succès, puisqu'il y a 19, 8 % d'admis chez les hommes et 19, 3 % chez les femmes !

Répartition selon l'âge

Tranche d'âge	Inscrits	Présents	Admissibles	Admis
[20, 30[	1798	1288	495	271
[30, 40[	718	305	87	15
[40, 50[	217	99	15	3
[50, 60[	68	30	1	1
TOTAL	2801	1722	598	290

Répartition par tranches d'âge



Cette répartition par tranches d'âge confirme que l'agrégation externe permet de recruter des jeunes enseignants. Les jeunes constituent en effet l'essentiel des présents mais surtout des admis au concours, puisque 92 % des reçus ont moins de 30 ans.

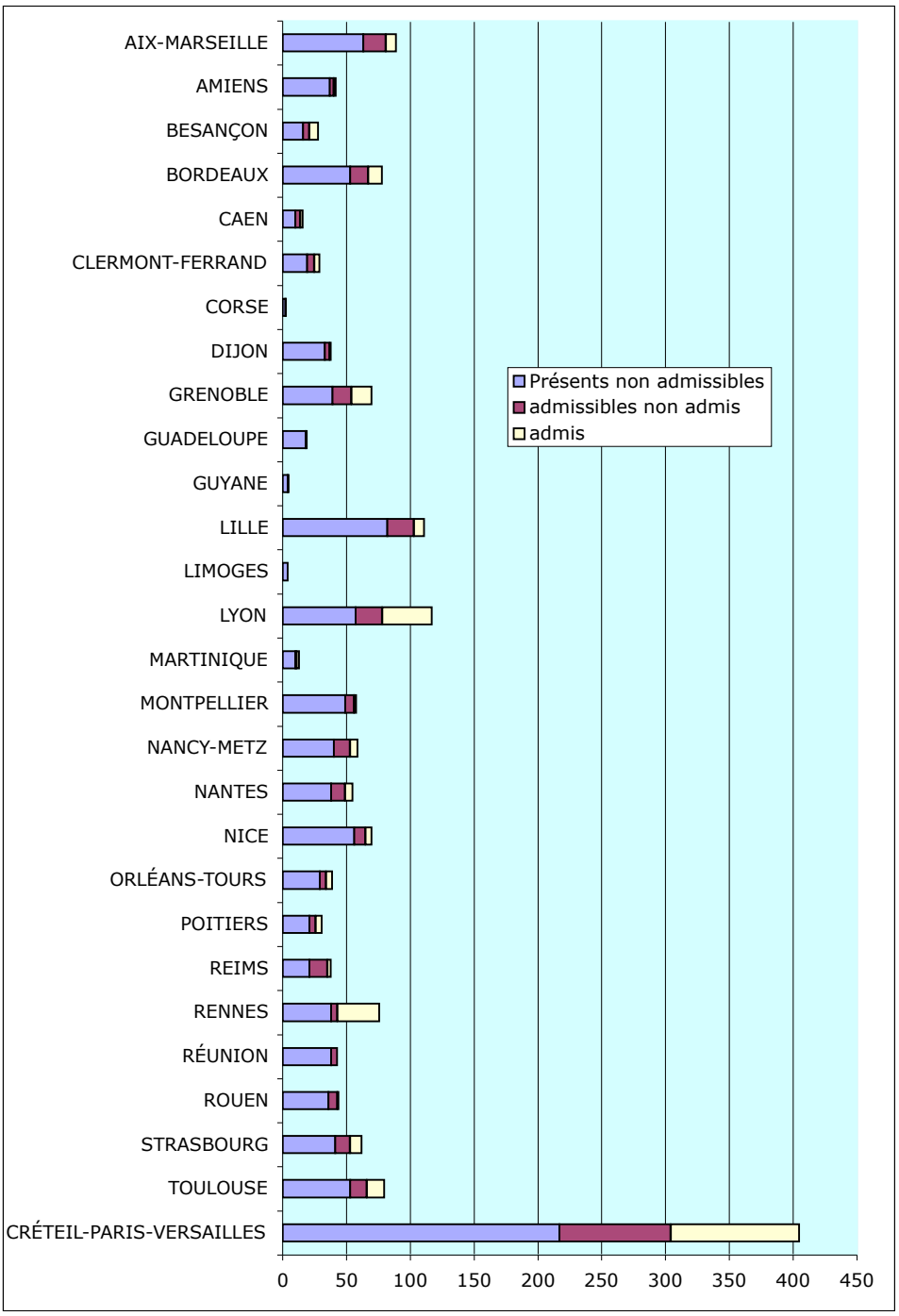
Académie	Candidats	Présents	Admissibles	Admis
AIX-MARSEILLE	151	89	26	8
AMIENS	66	42	5	2
BESANÇON	44	28	12	7
BORDEAUX	108	78	25	11
CAEN	29	16	6	2
CLERMONT-FERRAND	38	29	10	4
CORSE	7	3	1	0
DIJON	54	38	5	1
GRENOBLE	112	70	31	16
GUADELOUPE	41	19	1	0
GUYANE	11	5	1	0
LILLE	178	111	29	8
LIMOGES	13	4	0	0
LYON	173	117	60	39
MARTINIQUE	29	13	3	2
MONTPELLIER	105	58	9	2
NANCY-METZ	96	59	19	6
NANTES	86	55	17	6
NICE	116	70	14	5
ORLÉANS-TOURS	60	39	10	5
POITIERS	44	31	10	5
REIMS	52	38	17	3
RENNES	103	76	38	33
RÉUNION	78	43	5	0
ROUEN	63	44	8	1
STRASBOURG	90	62	21	9
TOULOUSE	118	80	27	14
CRÉTEIL-PARIS-VERSAILLES	736	405	188	101
TOTAL	**2801**	**1722**	**598**	**290**

Résultat du concours par académies

Hors ENS	Candidats	Présents	Admissibles	Admis
CRÉTEIL-PARIS-VERSAILLES	675	348	130	48
RENNES	80	54	16	11
LYON	149	93	37	18

ENS seulement	Candidats	Présents	Admissibles	Admis
CRÉTEIL-PARIS-VERSAILLES	61	58	58	54
RENNES	23	22	22	22
LYON	24	24	23	21

Représentation des résultats par académies (y compris ENS)



Épreuve écrite de mathématiques générales

Les quatre premières parties du problème sont largement indépendantes.

Partie I

Dans cette partie I, on étudie une méthode de calcul de l'inverse d'un élément a d'un groupe multiplicatif G de cardinal fini $N \in \mathbb{N}^*$. L'élément neutre de G est noté 1.

« Écrire un algorithme » signifie le rédiger en français, sous une forme rappelant un programme d'un langage tel que Pascal, Maple, Matlab, etc.

Le coût d'un algorithme est le nombre de multiplications dans le groupe G que nécessite son exécution. On ne tiendra pas compte des autres opérations (en particulier celles dans $\mathbb{N}$).

1. Justifier le fait que a^{N-1} est inverse de a dans G.
2. On écrit la décomposition en base 2 de $N-1$ sous la forme :
$$N-1 = \sum_{i=0}^{k} x_i 2^i \text{ avec } k \in \mathbb{N},\ x_i \in \{0,1\} \text{ pour } i \in [\![0,k]\!] \text{ et } x_k \neq 0.$$
On considère les suites finies $(a_i)_{0\leqslant i\leqslant k+1}$ et $(b_i)_{0\leqslant i\leqslant k+1}$ définies par :
$$a_0 = 1,\ b_0 = a \text{ et pour } i \in [\![0,k]\!],\ a_{i+1} = a_i b_i^{x_i},\ b_{i+1} = b_i^2.$$
   a) Démontrer que a_{k+1} est l'inverse de a dans G.
   b) En déduire un algorithme de calcul de a^{-1} et préciser, en fonction de k, son coût dans le pire des cas (c'est-à-dire le nombre maximum de multiplications dans G que nécessite le calcul de a^{-1} ; on ne tiendra pas compte du coût éventuel du calcul des x_i, $0 \leqslant i \leqslant k$). L'algorithme doit prendre comme arguments a et N.
3. **Exemple.** Dans cette question, G est le groupe des éléments inversibles de $\mathbb{Z}/148\mathbb{Z}$.
On note encore a la classe dans $\mathbb{Z}/148\mathbb{Z}$ d'un élément a de $\mathbb{Z}$.
   a) Déterminer le cardinal N de G.
   b) Démontrer que 5 est un élément de G et déterminer son inverse par la méthode de la question I.2.
   c) Donner une autre méthode pour déterminer cet inverse.

Partie II

1. a) Soit π un élément d'un groupe multiplicatif G, e un entier relatif et $\alpha = \pi^e$.
On considère l'application f_α de $\mathbb{Z} \times G$ dans G^2 définie par $f_\alpha(k,\tau) = (\pi^k, \tau\,\alpha^k)$.
Exhiber une fonction φ_e de G^2 dans G, ne dépendant que de e et vérifiant
$$\tau = \varphi_e \circ f_\alpha(k,\tau) \text{ pour tout } (k,\tau) \in \mathbb{Z} \times G.$$

b) On suppose le groupe G et l'élément π connus de tous les membres d'une association. L'un d'eux, **A**, garde secret l'entier e et rend public l'élément $\alpha = \pi^e$, ainsi donc que la fonction f_α. On recherche une procédure permettant à chacun d'envoyer à **A** un message crypté sous la forme d'un (ou de plusieurs) élément(s) τ de G, telle que la seule connaissance de e suffise à retrouver le message initial.

Justifier le fait que, si l'auteur décompose son message en parties telles que chacune puisse être représentée par un élément τ_i du groupe, choisit pour chacune d'elles un entier k_i et envoie les couples $f_\alpha(k_i, \tau_i) = (\lambda_i, \mu_i)$ à **A**, alors ce dernier peut les décrypter grâce à φ_e.

2. Dans cette question, G est le groupe $\mathbb{F}_{29}^*$ des inversibles du corps à 29 éléments et les nombres $\pi = 2$ et $\alpha = 18$ sont supposés publics.

Chaque associé sait que les entiers (1, 2, ..., 26, 27, 28) modulo 29, dans cet ordre, représentent les éléments du 28-uplet (`A`, `B`, ..., `Z`, ‘ ’, ·), où ‘ ’ figure l'espace séparant deux mots et · est le point de fin de phrase.

a) Sachant que l'algorithme de décryptage employé par **A** repose sur la seule table ci-dessous des résidus modulo 29 des puissances dix-septièmes des entiers entre 2 et 28 :

λ	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
λ^{17}	21	2	6	9	13	24	10	4	15	3	12	22	11	18	7	17	26	14	25	19	5	16	20	23	27	8	28

conjecturer la valeur de e et la contrôler grâce à α.

b) Décrypter le message suivant (on donne la suite des couples (λ_i, μ_i)) :

(16, 17), (18, 24), (28, 22), (17, 21), (23, 23), (24, 8).

Partie III

Dans cette partie III, le corps de base est le corps fini $\mathbb{F}_{16}$ à 16 éléments, unique à isomorphisme près.

1. a) Comment peut-on construire $\mathbb{F}_{16}$?

b) Démontrer que le groupe multiplicatif $\mathbb{F}_{16}^*$ est formé des puissances successives d'un élément ω vérifiant l'égalité $\omega^4 + \omega^3 + 1 = 0$.

c) Démontrer que ω, ω^2, ω^4 et ω^8 sont les racines du polynôme $X^4 + X^3 + 1$ dans $\mathbb{F}_{16}$.

d) Démontrer que la famille $(\omega, \omega^2, \omega^4, \omega^8)$ est une base de $\mathbb{F}_{16}$ sur $\mathbb{F}_2$.

2. a) Soit $a \in \mathbb{F}_{16}$. Résoudre dans $\mathbb{F}_{16}$ l'équation $x^5 = a$, en discutant éventuellement selon la valeur de a.

b) Démontrer qu'il existe quatre éléments $\gamma \in \mathbb{F}_{16}$ tels que, pour chacun d'eux, la famille $(\gamma, \gamma^2, \gamma^4, \gamma^8)$ est une base de $\mathbb{F}_{16}$ sur $\mathbb{F}_2$ telle que le produit de deux de ses éléments appartient à la base ou est égal à 1.

Expliquer rapidement pourquoi les calculs dans $\mathbb{F}_{16}$ sont plus faciles dans une telle base.

Partie IV

Une *cubique* sur un corps $\mathbb{K}$ est l'ensemble Γ des points $M = (x, y) \in \mathbb{K}^2$ annulant un polynôme du troisième degré $P(X, Y) = a\,X^3 + b\,X^2Y + c\,XY^2 + d\,Y^3 + e\,X^2 + f\,XY + g\,Y^2 + h\,X + i\,Y + j$ à coefficients dans $\mathbb{K}$.

Dans toute la suite, P est supposé non nul.

Remarque : il existe plusieurs polynômes donnant le même sous-ensemble de $\mathbb{K}^2$, comme le montre l'exemple des polynômes XY^2 et X^2Y. Il est systématiquement sous-entendu que l'on a fait un choix particulier de P (ou de l'un de ses produits par les éléments de $\mathbb{K}^*$).

Cette partie étudie quelques cubiques particulières sur le corps $\mathbb{R}$.

1. Dans cette question, on prend la cubique Γ définie par le polynôme $P = X^3 - Y \in \mathbb{R}[X, Y]$.

   a) La tracer à main levée.

   b) Démontrer que toute droite coupe Γ en exactement un ou trois points en comptant leur multiplicité éventuelle et que, lorsqu'il existe trois points d'intersection notés $A = (x_A, y_A)$, $B = (x_B, y_B)$, $C = (x_C, y_C)$:

   $$x_A + x_B + x_C = 0.$$

   On note Ω le point de coordonnées $(0, 0)$ de Γ. Pour tout couple (A, B) de points de Γ, on considère le troisième point C d'intersection avec Γ de la droite AB (ou de la tangente en A à Γ si $B = A$), puis le troisième point d'intersection $A * B$ de la droite ΩC avec Γ. Ceci définit sur Γ une loi multiplicative $*$ (on peut compléter le dessin du IV.1.a).

   c) Démontrer que $(\Gamma, *)$ est un groupe isomorphe à $(\mathbb{R}, +)$.

2. Reprendre la question 1. pour $P = X^3 - 3\,XY - 1 \in \mathbb{R}[X, Y]$ et $\Omega = (1, 0)$, en précisant à quel groupe usuel est isomorphe $(\Gamma, *)$ dans cet exemple.

3. On étudie dans la suite des cubiques du plan projectif.
   On considère un polynôme non nul homogène à trois variables :

   $$\overline{P}(X, Y, Z) = a\,X^3 + b\,X^2Y + c\,XY^2 + d\,Y^3 + e\,X^2Z + f\,XYZ + g\,Y^2Z + h\,XZ^2 + i\,YZ^2 + jZ^3.$$

   La cubique associée est l'ensemble Γ des points du plan projectif dont les coordonnées homogènes (X, Y, Z) vérifient $\overline{P}(X, Y, Z) = 0$.
   Démontrer que l'intersection de Γ avec toute droite du plan projectif est constituée d'exactement un ou trois points, en comptant toujours les multiplicités éventuelles.

4. Dans cette question 4, on considère $P = Y^3 - X^2 - Y^2$ et le polynôme homogène associé $\overline{P}(X, Y, Z) = Y^3 - X^2Z - Y^2Z$.

   a) Dans cette question 4.a, on se place dans le plan affine euclidien $\mathbb{R}^2$ et on considère la courbe γ d'équation $y^3 = x^2 + y^2$ privée du point $(0, 0)$.
   En choisissant un paramétrage de γ (par exemple en coordonnées polaires), étudier cette courbe et la tracer, en précisant l'allure des branches infinies s'il en existe.
   On ne demande pas d'étudier les éventuels points d'inflexion.

Dans la suite de la question 4., on considère dans le plan projectif la cubique Γ *d'équation* $Y^3 - X^2Z - Y^2Z = 0$, *privée du point de coordonnées* $(0,0,1)$.
On choisit pour Ω *le point à l'infini* $(1,0,0)$ *et on définit le composé* $A * B$ *de deux points quelconques de* Γ *comme en IV.1.*

b) Montrer que Γ admet comme paramétrage :

$$\begin{cases} X = \cos\theta \\ Y = \sin\theta \\ Z = \sin^3\theta \end{cases} \qquad \theta \text{ décrivant } \mathbb{R}.$$

Si A et B sont deux points de Γ, caractériser le point C tel que $C = A * B$.

c) Démontrer que $(\Gamma, *)$ est isomorphe à un groupe usuel que l'on précisera.
Quels sont les points d'ordre 6 ?

Partie V

Dans cette partie V, on étudie la courbe Γ' *définie dans le plan* $\mathbb{F}_{16}^2$ *par l'équation :*

$$y^2 + y = x^3 + x.$$

1. Montrer que la courbe Γ' contient au plus 32 points de $\mathbb{F}_{16}^2$.
2. On introduit le polynôme homogène

$$\overline{P}(X,Y,Z) = X^3 + XZ^2 - Y^2Z - YZ^2$$

Définir, par analogie avec la partie IV, un point à l'infini Ω et une multiplication interne à l'ensemble Γ réunion de Γ' et de Ω.

3. a) Montrer que cette multiplication, notée $*$, est commutative et admet un élément neutre, vis-à-vis duquel tout point admet un inverse.
   b) Calculer l'inverse d'un élément $A = (\alpha, \beta)$ de Γ'.

On admettra que cette loi est associative et munit donc Γ *d'une structure de groupe commutatif.*

4. On se propose de calculer le carré $A^2 = A * A$ d'un élément $A = (\alpha, \beta)$ de Γ'.
On est amené à considérer la droite D passant par A telle que son intersection avec Γ' admet A comme point double.
   a) Montrer que cette droite – appelée tangente en A à la courbe Γ' – a pour équation

$$P'_X(\alpha,\beta)(x-\alpha) + P'_Y(\alpha,\beta)(y-\beta) = 0$$

où P'_X et P'_Y désignent les polynômes dérivés du polynôme P, respectivement par rapport à X et Y.
   b) Déterminer les coordonnées de $A * A$.
   c) En déduire que, pour tout point A de Γ' : $A^4 = A^{-1}$.
   d) En déduire le cardinal de Γ et sa décomposition en produit direct de groupes cycliques.

5. Indiquer brièvement comment implanter un système de cryptographie du type de celui de la partie II à l'aide de Γ.

Corrigé de l'épreuve de mathématiques générales

Partie I

1. G étant un groupe de cardinal fini N, le théorème de Lagrange assure que $a^N = 1$ donc $\boxed{a^{N-1} \text{ est l'inverse de } a \text{ dans } G}$.

2. a) Par une récurrence immédiate : $b_i = a^{2^i}$ pour $i \in [\![0, k+1]\!]$ et $a_{i+1} = a^{\left[\sum_{j=0}^{i} x_j 2^j\right]}$ pour $i \in [\![0, k]\!]$.

   En particulier : $\boxed{a_{k+1} = a^{N-1} = a^{-1}}$.

   b) On sait que les x_i sont les restes des divisions euclidiennes successives de $N-1$ par 2. On peut donc utiliser l'algorithme suivant :
   - Initialiser trois variables $A = 1$, $B = a$ et $M = N - 1$;
   - tant que $M \neq 0$:
     - calculer le reste x de la division euclidienne de M par 2 ;
     - remplacer A par $A * B^x$ (c'est-à-dire par A ou $A * B$ selon si x vaut 0 ou 1) et B par $B * B$;
     - remplacer M par le quotient de la division euclidienne de M par 2 ;
   - fin du « tant que » ;
   - renvoyer A.

   La boucle est parcourue autant de fois qu'il y a de chiffres dans la décomposition de $N-1$ en base 2, c'est-à-dire $k+1$ fois et coûte à chaque fois deux multiplications au pire.

   $\boxed{\text{Le coût de l'algorithme est } 2(k+1)}$.

3. a) Les éléments inversibles de G sont les classes des entiers $a \in [\![0, 147]\!]$ premiers avec 148.

   En notant φ l'indicatrice d'Euler, le cardinal de G est
   $\varphi(148) = \varphi(2^2 \times 37) = \varphi(2^2)\varphi(37) = 2 \times 36$ donc $\boxed{N = 72}$.

   b) 5 est premier avec 148 donc inversible dans $\mathbb{Z}/148\mathbb{Z}$: $\boxed{5 \in G}$.

   71 s'écrit en base 2 sous la forme $72 = 2^0 + 2^1 + 2^2 + 2^6$.

   Ici : $b_0 = 5$, $b_1 = 25$, $b_2 = 33$, $b_3 = 53$, $b_4 = -3$, $b_5 = 9$, $b_6 = 81$ et

   $a_0 = 1$, $a_1 = 5$, $a_2 = 125 = -23$, $a_3 = -23 \times 33 = -19 = a_4 = a_5 = a_6$ donc $\boxed{a_7 = -19 \times 81 = -59 = a^{-1}}$.

   c) Comme 5 et 148 sont premiers entre eux, le théorème de Bézout assure l'existence d'un couple d'entiers (u, v) tel que $5u + 148v = 1$, ce qui signifie que u est inverse de 5 dans $\mathbb{Z}/148\mathbb{Z}$.

   On peut déterminer u et v par l'algorithme d'Euclide :

   $148 = 5 \times 29 + 3$ puis $5 = 3 + 2$ et $3 = 2 + 1$ donc

   $1 = 3 - 2 = 2 \times 3 - 5 = 2 \times 148 - 59 \times 5$.

   On retrouve bien que $\boxed{\text{l'inverse de 5 dans } \mathbb{Z}/148\mathbb{Z} \text{ est } -59}$.

Partie II

1. a) Considérons l'application $\boxed{\varphi_e : G^2 \to G, (x,y) \mapsto yx^{-e}}$.
   Alors, pour tout $(k,\tau) \in \mathbb{Z} \times \ G : \varphi_e \circ f_\alpha(k,\tau) = \varphi_e\left(\pi^k, \tau\alpha^k\right) = \tau\pi^{ek}\pi^{-ek} = \tau$.
   b) Il suffit que **A** fasse $\varphi_e(\lambda_i, \mu_i)$ pour retrouver τ_i.
2. a) Dans $\mathbb{F}_{29}^*$, on a $\lambda^{28} = 1$ pour tout λ donc $\lambda^{17} = \lambda^{-11}$ ce qui laisse penser que $\boxed{e = 11}$.
   On vérifie bien que $e^5 = 3$ donc $e^{11} = 2\left(2^5\right)^2 = 18$ et ça convient.
   b) En calculant pour chaque couple $\lambda_i^{17}\mu_i$ modulo 29, on trouve la suite 3, 15, 7, 9, 20, 15 donc le message est $\boxed{\text{COGITO}}$.

Partie III

1. a) On sait que $\mathbb{F}_{16}$ est un $\mathbb{F}_2$-espace vectoriel de dimension 4, construit comme $\dfrac{\mathbb{F}_2[X]}{(Q)}$ où (Q) est l'idéal engendré par un quelconque polynôme Q de degré 4 irréductible sur $\mathbb{F}_2$. En notant ω une racine de Q dans $\mathbb{F}_{16}$, $\mathbb{F}_{16}$ admet alors pour base sur $\mathbb{F}_2$ la famille $(1, \omega, \omega^2, \omega^3)$.
   Remarque : cette réponse est celle qu'il faut donner si on a lu la suite du problème mais toute autre solution juste est bien sûr acceptable ...
   b) $Q = X^4 + X^3 + 1$ est un polynôme de degré 4 sur $\mathbb{F}_2$. 0 et 1 n'en sont pas racine, donc il ne peut être réductible que s'il se décompose comme produit de deux trinômes.
   Dans ce cas, il existerait a et b dans $\mathbb{F}_2$ tels que :
   $$Q = \left(X^2 + aX + 1\right)\left(X^2 + bX + 1\right) = X^4 + (a+b)X^3 + abX^2 + (a+b)X + 1$$
   et on aurait $1 = a + b = 0$: absurde. Ainsi Q est irréductible sur $\mathbb{F}_2[X]$.

   On note ω une racine de Q : $(1, \omega, \omega^2, \omega^3)$ est une base de $\mathbb{F}_{16}$ sur $\mathbb{F}_2$.
   $\mathbb{F}_{16}^*$ est un groupe fini de cardinal 15, donc ω est d'ordre 1, 3, 5 ou 15 dans $\mathbb{F}_{16}^*$.
   La liberté de $(1, \omega, \omega^2, \omega^3)$ assure que ω et ω^3 sont différents de 1 : ω n'est d'ordre ni 1 ni 3.
   Par ailleurs, $\omega^5 = \omega\omega^4 = \omega(-1 - \omega^3) = \omega + \omega^4 = 1 + \omega + \omega^3$ est également différent de 1 car $(1, \omega, \omega^2, \omega^3)$ est libre : ω n'est pas d'ordre 5.
   Finalement ω est d'ordre 15 donc : $\boxed{\mathbb{F}_{16}^* = \left\{\omega^k, k \in [\![0, 15]\!]\right\}}$.
   c) Comme on est en caractéristique 2 : $\forall (x,y) \in \mathbb{F}_{16}, (x+y)^2 = x^2 + y^2$.
   Ainsi $\omega^4 + \omega^3 + 1 = 0$ donne en passant au carré :
   $$\omega^8 + \omega^6 + 1 = 0 \text{ puis } \omega^{16} + \omega^{12} + 1 = 0 \text{ et } \omega^{32} + \omega^{24} + 1 = 0$$
   ce qui montre que $\boxed{\omega,\ \omega^2,\ \omega^4 \text{ et } \omega^8 \text{ sont racines de } X^4 + X^3 + 1}$ et ce sont les seules puisque le polynôme est de degré 4 et qu'elles sont distinctes deux à deux.
   d) ω, ω^2, ω^4 et ω^8 sont les racines de $X^4 + X^3 + 1$ donc leur somme est $-1 = 1$.
   Vu le polynôme : $\omega^3 = 1 + \omega^4 = \omega + \omega^2 + \omega^8$, donc la famille $\left(\omega, \omega^2, \omega^4, \omega^8\right)$ engendre $(1, \omega, \omega^2, \omega^3)$ qui est une base de $\mathbb{F}_{16}$. Comme cette famille a quatre éléments, $\boxed{\left(\omega, \omega^2, \omega^4, \omega^8\right) \text{ est une base de } \mathbb{F}_{16}}$.

2. a) Le cas $a = 0$ est trivial. Prenons $a \neq 0$ dans la suite.
S'il existe x tel que $x^5 = a$, alors $a^3 = x^{15} = 1$ donc
$\boxed{\text{si } a^3 \neq 1, \text{ il n'y a pas de solution}}$.
Si $a^3 = 1$, il existe $k \in \mathbb{N}$ tel que $a = \omega^{5k}$.
Alors $\boxed{x^5 = a \text{ a pour solutions } \omega^k,\ \omega^{k+3},\ \omega^{k+6},\ \omega^{k+9} \text{ et } \omega^{k+12}}$.

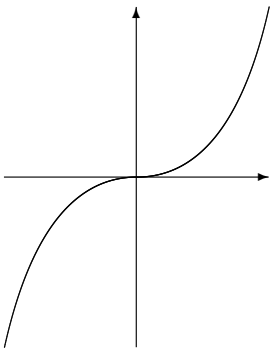
b) Si γ convient, γ^3 doit être égal à 1, γ, γ^2, γ^4 ou γ^8.
* $\gamma^3 = 1$ est impossible sinon $\gamma = \gamma^4$.
* $\gamma^3 = \gamma$ est impossible sinon on aurait $\gamma^2 = 1 = \gamma^4$.
* $\gamma^3 = \gamma^2$ ou $\gamma^3 = \gamma^4$ est impossible sinon γ serait égal à 1.
Finalement, il faut : $\gamma^5 = 1$ donc $\gamma \in \left\{\omega^3, \omega^6, \omega^9, \omega^{12}\right\}$.
Pour l'une quelconque des quatre valeurs précédentes, $\left\{\gamma, \gamma^2, \gamma^4, \gamma^8\right\}$ est la famille $\left\{\omega^3, \omega^6, \omega^9, \omega^{12}\right\}$.
ω^3 est racine de $X^5 + 1 = (X + 1)(X^4 + X^3 + X^2 + X + 1)$ et différent de 1, donc ω^3 est racine de $Q = X^4 + X^3 + X^2 + X + 1$.
0 et 1 ne sont pas racines de Q. Si celui-ci est réductible dans $\mathbb{F}_2[X]$, il doit se décomposer sous la forme :
$Q = (aX^2 + bX + c)(dX^2 + eX + f)$ avec a, b, c, d, e, f dans $\mathbb{F}_2$.
Alors : $a = d = 1$, $c = f = 1$ et les coefficients de X^3 et X imposent $b = 1 + e$.
Le coefficient de X^2 serait alors $af+cd+be = 0$ d'où contradiction : Q est irréductible dans $\mathbb{F}_2[X]$.
La famille $\left\{\omega^3, \omega^6, \omega^9, \omega^{12}\right\}$ est de la forme x, x^2, x^3, x^4 avec x racine d'un polynôme irréductible de degré 4 de $\mathbb{F}_2[X]$, donc est bien une base de $\mathbb{F}_{16}$ et elle vérifie les conditions demandées.
Il y a donc quatre éléments qui conviennent : $\boxed{\omega^3,\ \omega^6,\ \omega^9,\ \omega^{12}}$.

Les sommes se font évidemment bien et les produits aussi puisque les produits des termes de la base restent dans la base.

Partie IV

On comptera toutes les racines avec leur ordre de multiplicité. « Deux racines » peut donc en fait signifier « une racine double ».

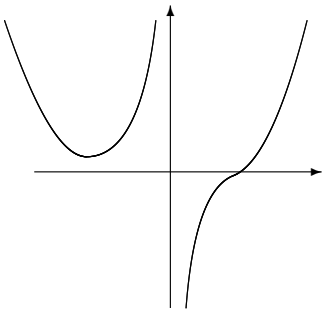
1. a) Considérons une droite D, d'équation $\alpha x + \beta y + \gamma = 0$ où α, β, γ sont des réels.
$M = (x, y)$ est point d'intersection de Γ et D si et seulement si $\begin{cases} y = x^3 \\ \alpha x + \beta y + \gamma = 0 \end{cases}$ ce qui est équivalent à résoudre $\alpha x + \beta x^3 + \gamma = 0$.
$\boxed{\text{Il y a donc une ou trois racines réelles}}$ (en comptant les multiplicités) et dans le cas où il y en a trois les relations entre coefficients et racines donnent $\boxed{x_A + x_B + x_C = 0}$.



b) En notant (x_{A*B}, y_{A*B}) les coordonnées de $A * B$, on sait que $A * B$ est déterminé par $x_{A*B} = -x_\Omega - x_C = x_A + x_B$ donc a pour coordonnées $\left(x_A + x_B, (x_A + x_B)^3\right)$.
$*$ est une loi interne à Γ par définition, associative par associativité de $+$ dans $\mathbb{R}$, a pour élément neutre $\Omega = (0, 0)$ et tout élément $A = (x_A, y_A = x_A^3)$ de Γ admet pour symétrique $(-x_A, -y_A)$: $\boxed{(\Gamma, *) \text{ est un groupe (abélien en plus)}}$.

$\varphi : \mathbb{R} \to \Gamma, x \mapsto M = (x, x^3)$ est visiblement un isomorphisme :
$\boxed{(\Gamma, *) \text{ est isomorphe à } (\mathbb{R}, +)}$.

2. a) On remarque que Γ ne contient aucun point d'abscisse nulle.
Toutes les abscisses considérées dans la suite de cette question sont non nulles.
La cubique a pour équation : $y = \dfrac{x^3-1}{3x}$.
La fonction $x \mapsto \dfrac{x^3-1}{3x}$ est définie sur $\mathbb{R}^*$, croissante sur $\mathbb{R}_+^*$ et $\left[-2^{-1/3}, 0\right[$, décroissante sur $\left]-\infty, -2^{-1/3}\right]$.
Elle admet pour limite $+\infty$ en $-\infty$, en 0 à gauche et en $+\infty$. Sa limite en 0 à droite est $-\infty$, ce qui donne l'allure sommaire ci-contre.



b) Soit D une droite quelconque, d'équation $\alpha x + \beta y + \gamma = 0$ (différente de $x = 0$).
Un point (x, y) est intersection de Γ et D si et seulement si $y = \dfrac{x^3-1}{3x}$ et $\alpha x + \beta\dfrac{x^3-1}{3x} + \gamma = 0$, ce qui revient à résoudre $\beta x^3 + 3\alpha x^2 + 3\gamma x - \beta = 0$.
Si on sait déjà qu'il existe deux solutions x_A et x_B, D n'est pas une droite « verticale » ($\beta \neq 0$) donc il existe exactement une troisième solution x_C et on trouve encore que
$\boxed{C \text{ existe et est unique}}$.
De plus, les relations entre coefficients et racines assurent que le produit des racines est 1 donc C est caractérisé par $\boxed{x_A x_B x_C = 1}$.

c) Alors $x_{A*B} = \dfrac{1}{x_\Omega x_C} = x_A x_B$: $(\Gamma, *)$ est un groupe ; l'élément neutre est Ω et le symétrique de $A = (x_A, y_A)$ est le point d'abscisse $\dfrac{1}{x_A}$.
Par l'application $\varphi : \mathbb{R} \to \Gamma, x \mapsto M = \left(x, \dfrac{x^3-1}{3x}\right)$,
$\boxed{(\Gamma, *) \text{ est un groupe commutatif isomorphe à } (\mathbb{R}^*, \times)}$.

3. Une droite D du plan projectif a une équation de la forme $\alpha X + \beta Y + \gamma Z = 0$, α, β, γ étant des réels non tous nuls. On suppose qu'on n'est pas dans le cas où la cubique contient D.
Chercher les intersections de Γ et D revient à résoudre le système $\begin{cases} \overline{P}(X, Y, Z) = 0 \\ \alpha X + \beta Y + \gamma Z = 0 \end{cases}$
Comme α, β et γ sont non tous nuls, l'une des variables peut s'exprimer en fonction des deux autres, par exemple X en fonction Y et Z. En remplaçant dans $\overline{P}$, on se ramène à une équation $Q(Y, Z) = 0$ où Q est un polynôme homogène de degré 3, de la forme :
$$Q(Y, Z) = aY^3 + bY^2Z + cYZ^2 + dZ^3.$$
On cherche des solutions (X, Y, Z) différentes de $(0, 0, 0)$ ce qui exclut que (Y, Z) soit le couple $(0, 0)$.
Premier cas : $d \neq 0$.
Alors les solutions (Y, Z) vérifient $Y \neq 0$. En posant $t = \dfrac{Z}{Y}$, résoudre le problème est, vu l'homogénéité des coordonnées, équivalent à trouver t tel que $dt^3 + ct^2 + bt + a = 0$: on a exactement une ou trois solutions réelles.
Deuxième cas : $d = 0$.

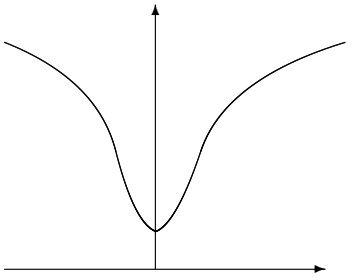
Si $a \neq 0$, on se ramène au cas précédent en échangeant les rôles de Y et Z.
Sinon, il reste à résoudre $bY^2Z + cYZ^2 = 0$ soit $YZ(bY + cZ) = 0$.
À l'homogénéité près, il y a exactement trois solutions : $(1,0)$, $(0,1)$ et $(c,-b)$.

Finalement, $\boxed{\Gamma \text{ coupe bien toute droite en exactement un ou trois points}}$.

4. a) On passe en coordonnées (« presque ») polaires : $\begin{cases} x = r\cos\theta \\ y = r\sin\theta \end{cases}$ (on autorise $r \leqslant 0$).

Un point différent de $(0,0)$ appartient à γ si et seulement si $r^3\sin^3\theta = r^2$ soit $\boxed{r = \dfrac{1}{\sin^3\theta}}$.

$\rho : \theta \mapsto \dfrac{1}{\sin^3\theta}$ est défini sur $\mathbb{R} \setminus \pi\mathbb{Z}$, 2π-périodique, impaire, ce qui permet de faire l'étude sur $]0,\pi[$ et on complètera le tracé par symétrie par rapport à l'axe Oy.
De plus : $\rho(\pi - \theta) = \rho(\theta)$ donc on limite l'étude à $\left]0, \dfrac{\pi}{2}\right]$ et on complète le tracé par symétrie par rapport à l'axe Oy.
ρ est positif sur $\left]0, \dfrac{\pi}{2}\right]$ et tend vers $+\infty$ en 0 : on a une branche infinie de direction Ox.



L'ordonnée du point de paramètre θ est $\dfrac{\sin\theta}{\sin^3\theta} = \dfrac{1}{\sin^2\theta} \xrightarrow{\theta\to 0} +\infty$ donc il n'y a pas de droite asymptote.

b) Soit (X,Y,Z) un point du plan projectif différent de $(0,0,1)$. Alors (X,Y) est différent de $(0,0)$ donc il existe des réels $\lambda \in \mathbb{R}^*$ et $\theta \in \mathbb{R}$ tels que $\begin{cases} X = \lambda\cos\theta \\ Y = \lambda\sin\theta \end{cases}$.
(X,Y,Z) appartient à Γ si et seulement si $\lambda^3\sin^3\theta - \lambda^2 Z = 0$ soit $Z = \lambda\sin^3\theta$.
Compte-tenu de l'homogénéité, on peut donc paramétrer Γ par $\begin{cases} X = \cos\theta \\ Y = \sin\theta \\ Z = \sin^3\theta \end{cases}$, θ décrivant $\mathbb{R}$.

Soit D une droite du plan, d'équation $\alpha X + \beta Y + \gamma Z = 0$.
Un point de Γ de paramètre θ appartient à Γ si et seulement si : $\alpha\cos\theta + \beta\sin\theta + \gamma\sin^3\theta = 0$.
Ceci est équivalent à :

$$\alpha(e^{i\theta} + e^{-i\theta}) - i\beta(e^{i\theta} - e^{-i\theta}) + i\frac{\gamma}{4}\left[e^{3i\theta} - 3e^{i\theta} + 3e^{-i\theta} - e^{3i\theta}\right] = 0.$$

En posant $T = e^{2i\theta}$, c'est équivalent à résoudre :

$$\gamma T^3 + (4\alpha + 3i\gamma - 4i\beta)T^2 + (4\alpha - 3i\gamma + 4i\beta)T - \gamma = 0.$$

Pour $\gamma \neq 0$, il y a exactement trois solutions T_1, T_2, T_3 dans $\mathbb{C}$ dont le produit vaut 1.
Le cas $\gamma = 0$ est exclu dans la suite par le fait qu'il n'y aurait qu'une solution T non nulle.

Soit A et B deux points de Γ, de paramètres θ_A et θ_B. Le résultat précédent montre que la droite AB coupe Γ en un troisième point C de paramètre θ_C caractérisé par :

$$e^{2i(\theta_A+\theta_B+\theta_C)} = 1.$$

En remarquant que Ω est le point de paramètre 0, on en déduit que $A * B$ est le point de paramètre θ caractérisé par $e^{2i\theta_C+2i\theta} = 1$ soit $e^{2i\theta} = e^{2i(\theta_A+\theta_B)}$.

Deux paramètres égaux modulo π donnent le même point (cela multiplie toutes les coordonnées par -1), donc $A * B$ est le point de paramètre $\boxed{\theta = \theta_A + \theta_B}$.

c) L'application qui au point M de Γ de paramètre θ associe $e^{2i\theta}$ est un isomorphisme de $(\Gamma, *)$ sur $(\mathscr{U}, \times)$, où $\mathscr{U}$ est l'ensemble des nombres complexes de module 1.

Les points d'ordre 6 sont ceux qui sont associés par l'isomorphisme précédent aux points d'ordre 6 dans $\mathscr{U}$, *i.e.* qui correspondent à $\theta = \dfrac{\pi}{6}$ ou $\theta = \dfrac{5\pi}{6}$ ce qui donne $\boxed{\text{les deux points } (\pm 4\sqrt{3}, 4, 1)}$.

Partie V

1. Pour chaque $x \in \mathbb{F}_{16}$, l'équation $y^2 + y = x^3 + x$ d'inconnue y a au plus deux solutions. Ainsi, lorsque x parcourt $\mathbb{F}_{16}$,

$$\boxed{\text{il existe au plus 32 couples } (x, y) \text{ vérifiant } x^3 + x = y^2 + y}.$$

2. Considérons Γ dans le plan projectif ; elle contient, en plus des points de Γ', le point à l'infini $\Omega = (0, 1, 0)$.

Comme en IV, intersecter Γ avec une droite projective d'équation $\alpha X + \beta Y + \gamma Z = 0$ revient à résoudre une équation homogène de degré 3 par exemple en Y et Z.

S'il y a déjà deux points d'intersection A et B, il y en a donc également un troisième C. De même, le point $A * B$, troisième intersection de ΩC avec Γ, est toujours bien défini.

3. a) La définition ci-dessus ne fait pas intervenir l'ordre du couple (A, B) :

$$\boxed{\text{l'opération * est commutative}}.$$

Vu la définition également, $\boxed{\Omega \text{ est élément neutre pour } *}$ et tout élément A admet un inverse A^{-1} qui est la troisième intersection de ΩA avec Γ.

b) Avec le Ω ci-dessus, si $A = (\alpha, \beta)$ est un point de Γ', chercher B tel que (AB) ait la direction de Ω revient à faire en sorte que AB soit une droite « verticale », *i.e.* on cherche B de coordonnées (α, y) telles que $y^2 + y = \alpha^3 + \alpha$.

On sait que β est l'une des solutions de cette équation et $-1 = 1$ est la somme des racines donc la deuxième solution est $1 + \beta$.

Ainsi $\boxed{A^{-1} \text{ est le point de coordonnées } (\alpha, 1 + \beta)}$.

4. a) Une droite d'équation $ax + by + c = 0$ intersecte Γ' aux points de coordonnées (x, y) tels que :

$$\begin{cases} ax + by + c = 0 \\ y^2 + y = x^3 + x \end{cases}$$

La droite passe par A si et seulement si $c = a\alpha + b\beta$ ce qui ramène au système équivalent, lorsque $a \neq 0$ par exemple :

$$\begin{cases} a(x - \alpha) + b(y - \beta) = 0 \\ P\left(\dfrac{-by - c}{a}, y\right) = 0 \end{cases}$$

et la droite est tangente en A à Γ' si et seulement s'il y a racine double, i.e. :

$$\frac{d}{dy} P\left(\frac{-b(y - \beta) - a\alpha}{a}, y\right)_{|y=\beta} = 0 \text{ soit } -\frac{b}{a} P'_X(\alpha, \beta) + P'_Y(\alpha, \beta) = 0.$$

On remarque que, pour le polynôme $P(X,Y) = Y^2 + Y - X^3 - X$, il n'existe aucun point singulier dans Γ (tel que $P'_X(\alpha,\beta) = P'_Y(\alpha,\beta) = 0$) et on déduit la condition nécessaire et suffisante de tangence :

$$bP'_X(\alpha,\beta) - aP'_Y(\alpha,\beta) = 0$$

qui donne une tangente d'équation $\boxed{P'_X(\alpha,\beta)(x-\alpha) + P'_Y(\alpha,\beta)(y-\beta) = 0}$.

b) La tangente à Γ' en A a pour équation :
$(2\beta+1)(y-\beta) = (3\alpha^2+1)(x-\alpha)$ soit $y - \beta = (1+\alpha^2)(x-\alpha)$.
En éliminant y dans $x^3 + x = y^2 + y$, on trouve :

$$x^3 + x = (1+\alpha^2)(x-\alpha) + \beta + (1+\alpha^2)^2(x-\alpha)^2 + \beta^2$$

La somme des abscisses des points A, $B = A$ et C est donnée par le coefficient de x^2 : c'est $(1+\alpha^4)$.

C est donc le point de coordonnées
$\left(1+\alpha^4, \beta + (\alpha^2+1)\left(1+\alpha^4-\alpha\right)\right) = \left(1+\alpha^4, \beta+1+\alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^6\right)$
et $A * A$ est le point de coordonnées
$\left(1+\alpha^4, 1+\beta+(\alpha^2+1)\left(1+\alpha^4-\alpha\right)\right) = \left(1+\alpha^4, \beta+\alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^6\right)$.
Comme $\alpha^3 + \alpha = \beta + \beta^2$ et $\alpha^2 + \alpha^6 = (\alpha+\alpha^3)^2 = \beta^2 + \beta^4$, les coordonnées de $A * A$ sont

$$\boxed{\left(1+\alpha^4, \alpha^4+\beta^4\right)}.$$

c) Alors A^4 a pour abscisse $1 + \left(1+\alpha^4\right)^4 = \alpha^{16} = \alpha$ et pour ordonnée $\left(1+\alpha^4\right)^4 + \alpha^{16} + \beta^{16} = 1+\beta$ donc

$$\boxed{A^4 = A^{-1}}.$$

d) Pour tout $A \in \Gamma'$ et même pour $A = \Omega$: $A^5 = \Omega$ donc A peut être d'ordre 1 (dans le cas de Ω) ou 5.

Les éléments de Γ sont tous d'ordre 5, sauf Ω, donc le cardinal de Γ doit être une puissance de 5.

Le cardinal de Γ est celui de Γ' auquel on ajoute 1 à cause de Ω : il doit être inférieur à 33 et ne peut donc être que 5 ou 25.

Or Ω, $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$ sont dans Γ. D'après les calculs faits dans la partie III :

$$\omega + \omega^3 = 1 + \omega + \omega^4 = \omega^2 + \omega^8 = (\omega^2+\omega^4) + (\omega^2+\omega^4)^2$$

donc $(\omega, \omega^2+\omega^4)$ est un sixième point de Γ.

Finalement : $\boxed{\operatorname{Card}\Gamma = 25}$ et $\boxed{\Gamma \sim (\mathbb{Z}/5\mathbb{Z})^2}$.

5. On choisit un point A de Γ et un entier e ; on calcule $B = A^e$. On travaille dans le groupe $H = \left\{A^k ; k \in \mathbb{N}\right\}$.

On rend publics H, les points A et B. On demande à l'expéditeur de coder son message par un point $M \in H$, de choisir un entier k (qu'il garde secret) et d'envoyer $(A^k, MB^k) = (Y, Z)$. Les espions ne peuvent alors déterminer ni e ni k, mais le destinataire sait calculer $ZY^{-e} = M$.

Rapport des correcteurs

Les candidats ont principalement abordé les parties I, II et IV ; la partie III s'est révélée extrêmement discriminante.

Dans la partie I, il est utile de rappeler aux candidats que l'on attend d'eux une démonstration précise, même lorsqu'il suffit de faire une récurrence « évidente » : il est tout aussi rapide et beaucoup plus rigoureux de poser précisément la récurrence que de faire un vague discours sur la récurrence que l'on pourrait faire.

L'algorithme demandé est souvent très mal décrit. On attendait la description précise des initialisations de variables et des structures de contrôles utilisées ; il est par contre mal venu de s'encombrer de déclarations d'entrées-sorties, d'appels de bibliothèques ... surtout lorsqu'ils sont liés à un langage particulier.

La partie II a posé peu de problèmes, à part une erreur très courante dans la définition de $\varphi_e : (x, y) \mapsto \dfrac{y}{x^e}$.

La partie III a été la moins bien traitée en général et n'a souvent pas été abordée. $\mathbb{F}_{16}$ a été défini de façon fantaisiste : $\mathbb{Z}/16\mathbb{Z}$ ou $(\mathbb{Z}/17\mathbb{Z})^*$ entre autres.

En partie IV, dans 50% des copies, le tracé de $y = x^3$ est incorrect : la tangente à l'origine n'est pas horizontale. Il faut que dans un tracé, même sommaire, les candidats mettent en évidence les éléments remarquables de la courbe.

L'étude de l'intersection courbe-droite en IV.1.b) a souvent été faite de façon extrêmement compliquée, avec des études multiples de cas particuliers ($y = b$, $y = ax$, $y = ax + b$ ...) et d'énormes difficultés pour discuter le nombre de racines d'un polynôme de degré 3.

Les relations entre coefficients et racines sont très mal connues ce qui rend difficile la détermination des relations entre x_A, x_B, x_C demandées en IV.1 et IV.2.

La question IV.3 était posée de façon incorrecte et a été notée généreusement.

Le tracé de la courbe en coordonnées polaires du IV.4 a souvent été un obstacle insurmontable et la fin du problème n'est pratiquement jamais abordée.

Épreuve écrite d'analyse et probabilités

Notations et définitions

• Soient $\mathscr{B}$ la $\mathbf{C}$-algèbre des fonctions continues et bornées de $\mathbf{R}$ dans $\mathbf{C}$ et $\mathscr{B}^{\mathbf{R}}$ la sous-algèbre réelle des fonctions de $\mathscr{B}$ à valeurs réelles.

Pour f dans $\mathscr{B}^{\mathbf{R}}$ (resp. f dans $\mathscr{B}$), on note $\quad \sup f = \sup\{f(x),\ x \in \mathbf{R}\}$ (resp. $\|f\|_\infty = \sup|f|$).

On rappelle que $(\mathscr{B},\ \|\ \|_\infty)$ est un espace normé.

Pour λ dans $\mathbf{R}$, soit e_λ l'élément de $\mathscr{B}$ défini par : $\quad \forall t \in \mathbf{R}, \quad e_\lambda(t) = \mathrm{e}^{\mathrm{i}\lambda t}$.

On note $\mathscr{P}$ le sous-espace de $\mathscr{B}$ engendrée par $(e_\lambda)_{\lambda\in\mathbf{R}}$ (espace des *polynômes trigonométriques à fréquences réelles*). On démontrera en **I**.A que $(e_\lambda)_{\lambda\in\mathbf{R}}$ est une famille libre de $\mathscr{B}$, donc une base de $\mathscr{P}$. Ceci permet de définir une norme sur $\mathscr{P}$ en posant, pour toute famille presque nulle $(c_\lambda)_{\lambda\in\mathbf{R}}$ de complexes :

$$N\left(\sum_{\lambda\in\mathbf{R}} c_\lambda e_\lambda\right) = \sum_{\lambda\in\mathbf{R}} |c_\lambda|.$$

On a : $\quad \forall p \in \mathscr{P}, \quad \|p\|_\infty \leqslant N(p)$.

• Soit Λ une partie non vide de $\mathbf{R}$.

On note $\mathscr{P}_\Lambda$ le sous-espace de $\mathscr{P}$ engendré par $(e_\lambda)_{\lambda\in\Lambda}$.

On dit que Λ est un *ensemble de Sidon* si et seulement si N et $\|\ \|_\infty$ induisent des normes équivalentes sur $\mathscr{P}_\Lambda$, i.e, compte-tenu de l'inégalité précédente, si et seulement si l'ensemble :

$$\left\{\frac{N(p)}{\|p\|_\infty},\ p \in \mathscr{P}_\Lambda \setminus \{0\}\right\}$$

est majoré. Si tel est le cas, on pose :

$$K(\Lambda) = \sup\left\{\frac{N(p)}{\|p\|_\infty},\ p \in \mathscr{P}_\Lambda \setminus \{0\}\right\}$$

On note $\mathscr{P}_\Lambda^{\mathbf{R}}$ le sous-espace réel $\mathscr{P}_\Lambda \cap \mathscr{B}^{\mathbf{R}}$ de $\mathscr{P}_\Lambda$.

On dit que Λ est symétrique si et seulement si : $\forall x \in \Lambda,\ -x \in \Lambda$.

On dit que Λ est un *ensemble de Sidon réel* si et seulement si Λ est symétrique et s'il existe $C > 0$ tel que :

$$\forall p \in \mathscr{P}_\Lambda^{\mathbf{R}}, \qquad N(p) \leqslant C\sup(p).$$

Si tel est le cas, on a en particulier :

$$\forall p \in \mathscr{P}_\Lambda^{\mathbf{R}} \setminus \{0\}, \qquad \sup(p) > 0,$$

et on pose :

$$K'(\Lambda) = \sup\left\{\frac{N(p)}{\sup(p)}\ ,\ p \in \mathscr{P}_\Lambda^{\mathbf{R}} \setminus \{0\}\right\}.$$

• Soient I un ensemble non vide et $(a_i)_{i\in I}$ une famille de nombres réels. On dit que $(a_i)_{i\in I}$ est **Q**-*libre* si et seulement si, pour toute famille presque nulle $(\lambda_i)_{i\in I}$ de rationnels, on a :

$$\sum_{i\in I} \lambda_i\, a_i = 0 \quad \Rightarrow \quad \forall i \in I,\ \lambda_i = 0.$$

Si $(a_i)_{i\in I}$ n'est pas **Q**-libre, on dit que $(a_i)_{i\in I}$ est **Q**-*liée*.

Si A est une partie de **R**, on dit que A est **Q**-libre si et seulement si la famille $(a)_{a\in A}$ est **Q**-libre.

• Enfin, si E est une partie de **R** et γ un réel, on note γE l'ensemble : $\{\gamma x,\ x \in E\}$.

Objectifs du problème, dépendance des parties

Le but essentiel du problème est de construire des solutions remarquables de l'équation des ondes sur la sphère euclidienne de $\mathbf{R}^3$, découvertes par Yves Meyer. La partie **I** établit quelques résultats préalables concernant les éléments de $\mathscr{P}$ et les polynômes de Legendre. La partie **II** est consacrée aux ensembles de Sidon. La partie **III** étudie un ensemble particulier d'irrationnels quadratiques. La partie **IV** utilise des techniques probabilistes pour obtenir des polynômes trigonométriques ayant des normes quadratique et uniforme assez proches. La partie **V** construit les fonctions désirées.

La partie **II** dépend uniquement de **I.**A. La partie **III** utilise les résultats de la partie **II**. La partie **IV** est indépendante des parties précédentes. La partie **V** utilise les résultats de la partie **I.B,** ainsi que ceux des questions **III.B.**3 et **IV.C.**2.

I. Préliminaires

A. Éléments de $\mathscr{P}$

1. a) Soient $(c_\lambda)_{\lambda\in\mathbf{R}}$ une famille presque nulle de complexes, λ_0 un réel et $p = \sum_{\lambda\in\mathbf{R}} c_\lambda\ e_\lambda$.

   Démontrer que $\dfrac{1}{T}\displaystyle\int_0^T p(t)e_{-\lambda_0}(t)\,\mathrm{d}t$ converge vers une limite à préciser lorsque $T \to +\infty$.

   b) Démontrer que $(e_\lambda)_{\lambda\in\mathbf{R}}$ est une famille libre du **C**-espace vectoriel $\mathscr{B}$.

2. On suppose Λ symétrique.

   a) Soit p dans $\mathscr{P}_\Lambda$. Vérifier que Re p et Im p sont dans $\mathscr{P}_\Lambda^{\mathbf{R}}$.

   b) On suppose que Λ est un ensemble de Sidon réel. Démontrer que Λ est un ensemble de Sidon.

B. Polynômes de Legendre

Si $n \in \mathbf{N}$, U_n désigne le polynôme $(X^2-1)^n$, P_n le polynôme $(U_n)^{(n)}$ (dérivée n-ième de U_n) et L_n le polynôme $\dfrac{P_n}{2^n n!}$.

1. Soient n dans $\mathbf{N}$ et x dans $[-1,1]$.

   a) Soient r dans $\mathbf{R}^{+*}$ et γ le lacet défini par :

   $$\forall \theta \in [-\pi,\pi], \qquad \gamma(\theta) = x + r\ \mathrm{e}^{\mathrm{i}\theta}.$$

   Vérifier la relation :

   $$P_n(x) = \frac{n!}{2\mathrm{i}\pi} \int_\gamma \frac{(z^2-1)^n}{(z-x)^{n+1}}\ \mathrm{d}z.$$

   b) Déduire de a) :

   $$L_n(x) = \frac{1}{2\pi} \int_{-\pi}^{\pi} \Big(x + \mathrm{i}\sqrt{1-x^2}\ \sin\theta\Big)^n\ \mathrm{d}\,\theta.$$

   Indication. Pour x dans $]-1,1[$, on pourra appliquer a) avec $r = \sqrt{1-x^2}$.

2. Si $n \in \mathbf{N}$, calculer $L_n(1)$, $L_n(-1)$ et $\sup\Big\{|L_n(x)|,\ x \in [-1,1]\Big\}$.

3. Soient η dans $]0,1[$ et $I_\eta = [-(1-\eta),\ 1-\eta]$.

   a) Vérifier :

   $$\forall n \in \mathbf{N}, \quad \forall x \in I_\eta, \qquad |L_n(x)| \leqslant \frac{1}{2\pi} \int_{-\pi}^{\pi} \big(1 - \eta\cos^2\theta\big)^{n/2}\ \mathrm{d}\theta.$$

   b) Démontrer que $(L_n)_{n\geqslant 0}$ converge uniformément vers 0 sur I_η.

C. Opérateurs différentiels

Soit V l'espace vectoriel complexe des applications de classe C^2 de $[-1,1]$ dans $\mathbf{C}$. Pour f dans V, soit $D(f)$ l'application de $[-1,1]$ dans $\mathbf{C}$ définie par :

$$\forall x \in [-1,1], \qquad D(f)(x) = (1-x^2)f''(x) - 2xf'(x).$$

Si λ est dans $\mathbf{C}$, soit V_λ le sous-espace de V défini par : $V_\lambda = \{f \in V,\ D(f) = \lambda f\}$.

Enfin, soit : $\Sigma = \Big\{\lambda \in \mathbf{C},\ V_\lambda \neq \{0\}\Big\}$.

1. Soit n dans $\mathbf{N}$.

   a) Vérifier la relation : $(X^2-1){U_n}' = 2nX\ U_n$.

   b) En déduire l'égalité : $D(L_n) = -n(n+1)\ L_n$.

2. Soient f et g dans V. Démontrer l'égalité :

   $$\int_{-1}^{1} D(f)(t)\ g(t)\,\mathrm{d}t = \int_{-1}^{1} f(t)\ D(g)(t)\,\mathrm{d}t.$$

3. Démontrer que : $\Sigma = \{-n(n+1),\ n \in \mathbf{N}\}$.

4. Soit n dans $\mathbf{N}$. Démontrer que $V_{-n(n+1)} = \mathbf{C}\ L_n$.
   Indication. On pourra calculer le wronskien de deux solutions de l'équation différentielle :

$$(E) \qquad (1-x^2)\ y''(x) - 2x\ y'(x) + n(n+1)\ y(x) = 0\ .$$

5. Lorsqu'on cherche les solutions de l'équation des ondes sur la sphère euclidienne tridimensionnelle S^2 de $\mathbf{R}^3$ qui ne dépendent que d'une coordonnée, on est conduit à déterminer l'espace $\mathscr{E}$ des applications u de classe C^2 de $\mathbf{R} \times [-1,1]$ dans $\mathbf{C}$ telles que :

$$\forall (t,x) \in \mathbf{R} \times [-1,1], \qquad \frac{\partial^2 u}{\partial t^2}(t,x) = (1-x^2)\ \frac{\partial^2 u}{\partial x^2}(t,x) - 2x\ \frac{\partial u}{\partial x}(t,x).$$

   Démontrer que les éléments de $\mathscr{E}$ de la forme : $(t,x) \mapsto a(t)\ b(x)$ où a (resp. b) est une application de classe C^2 de $\mathbf{R}$ (resp. $[-1,1]$) dans $\mathbf{C}$, sont les :

$$(t,x) \quad \mapsto \quad L_n(x)\ \left(\alpha\ \mathrm{e}^{\,\mathrm{i}\sqrt{n(n+1)}\,t} + \beta\ \mathrm{e}^{-\mathrm{i}\sqrt{n(n+1)}\,t}\right)$$

   avec $n \in \mathbf{N}^*$ et $(\alpha,\beta) \in \mathbf{C}^2$, et les : $(t,x) \quad \mapsto \quad \lambda t + \mu$ avec $(\lambda,\mu) \in \mathbf{C}^2$.

II. Construction d'ensembles de Sidon

On note $\mathscr{C}$ la sous-algèbre de $\mathscr{B}$ constituée des fonctions continues et 2π-périodiques de $\mathbf{R}$ dans $\mathbf{C}$.

A. Théorème d'approximation de Kronecker et application

Soient n dans $\mathbf{N}^*$, $(\omega_j)_{1\leqslant j\leqslant n}$ une famille de réels, ω l'élément $(\omega_1,\ldots,\omega_n)$ de $\mathbf{R}^n$, G_ω le sous-groupe de $\mathbf{R}^n$ engendré par $\mathbf{R}\omega$ et $2\pi\mathbf{Z}^n$ c'est-à-dire :

$$G_\omega = \mathbf{R}\omega + 2\pi\mathbf{Z}^n = \{s\omega + 2\pi v,\ (s,v) \in \mathbf{R}\times\mathbf{Z}^n\}\,.$$

1. On suppose $(\omega_j)_{1\leqslant j\leqslant n}$ $\mathbf{Q}$-liée.
   a) Démontrer qu'il existe une forme linéaire non identiquement nulle ℓ sur $\mathbf{R}^n$ telle que $\ell(G_\omega)\ \subset \mathbf{Z}$.
   b) Le sous-groupe G_ω est-il dense dans $\mathbf{R}^n$?
2. On suppose $(\omega_j)_{1\leqslant j\leqslant n}$ $\mathbf{Q}$-libre. Si $f_1,\ldots,f_n$ sont dans $\mathscr{C}$ et $T>0$, on pose :

$$J_T(f_1,\ldots,f_n) = \frac{1}{T}\int_0^T \left(\prod_{j=1}^n f_j\,(\omega_j t)\right)\ \mathrm{d}t.$$

   a) Si $f_1,\ldots,f_n$ sont dans $\mathscr{P}_{\mathbf{Z}}$, démontrer :

$$J_T(f_1,\ldots,f_n) \quad \underset{T\to+\infty}{\longrightarrow} \quad \prod_{j=1}^n \left(\frac{1}{2\pi}\int_0^{2\pi} f_j(t)\,\mathrm{d}t\right).$$

   b) Si $f_1,\ldots,f_n$ sont dans $\mathscr{C}$, démontrer :

$$J_T(f_1,\ldots,f_n) \quad \underset{T\to+\infty}{\longrightarrow} \quad \prod_{j=1}^n \left(\frac{1}{2\pi}\int_0^{2\pi} f_j(t)\,\mathrm{d}t\right).$$

c) Démontrer que G_ω est dense dans $\mathbf{R}^n$.

3. On suppose $(\omega_j)_{1\leqslant j\leqslant n}$ $\mathbf{Q}$-libre. Soient $(g_j)_{1\leqslant j\leqslant n}$ une famille d'éléments de $\mathscr{C}$ à valeurs réelles et g la fonction de $\mathbf{R}$ dans $\mathbf{R}$ définie par :
$$\forall t \in \mathbf{R}, \qquad g(t) = \sum_{j=1}^{n} g_j(\omega_j\, t).$$
Établir la relation : $\sup(g) = \displaystyle\sum_{j=1}^{n} \sup(g_j)$.

4. Soient Γ une partie non vide $\mathbf{Q}$-libre de $\mathbf{R}$ et c dans $\mathbf{R}^{+*}$. Pour tout γ de Γ, soit Λ_γ un ensemble de Sidon réel contenu dans $\mathbf{Z}^*$ et tel que $K'(\Lambda_\gamma) \leqslant c$. On définit $\Lambda = \displaystyle\bigcup_{\gamma\in\Gamma} \gamma\, \Lambda_\gamma$.
Démontrer que Λ est un ensemble de Sidon réel et que $K'(\Lambda) \leqslant c$.

B. Parties dissociées de Z

Soit Λ une partie infinie et symétrique de $\mathbf{Z}^*$. On peut donc écrire :
$$\Lambda = \{\lambda_j,\ j \geqslant 1\} \cup \{-\lambda_j,\ j \geqslant 1\},$$
où $(\lambda_j)_{j\geqslant 1}$ est une suite strictement croissante d'éléments de $\mathbf{N}^*$. On dit que Λ est dissociée si et seulement si, pour tout n de $\mathbf{Z}$, il existe au plus une suite presque nulle $(\varepsilon_j)_{j\geqslant 1}$ d'éléments de $\{0,-1,1\}$ telle que :
$$n = \sum_{j\geqslant 1} \varepsilon_j\ \lambda_j.$$
Si f est dans $\mathscr{C}$ et n dans $\mathbf{Z}$, on note :
$$\hat{f}(n) = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(t)\ \mathrm{e}^{-\mathrm{i}nt}\ \mathrm{d}t.$$

1. Dans cette question, on suppose Λ dissociée. Soient $\varphi = (\varphi_j)_{j\geqslant 1}$ une suite réelle et, pour k dans $\mathbf{N}^*$, R_k^φ l'élément de $\mathscr{P}_\mathbf{Z}$ défini par :
$$\forall t \in \mathbf{R}, \qquad R_k^\varphi(t) = \prod_{j=1}^{k} \left(1 + \cos\left(\lambda_j t + \varphi_j\right)\right).$$
a) Soient k et m dans $\mathbf{N}^*$ avec $m \leqslant k$. Calculer : $\widehat{R_k^\varphi}(0)$, $\widehat{R_k^\varphi}(\lambda_m)$ et $\widehat{R_k^\varphi}(-\lambda_m)$.
b) Soit p dans $\mathscr{P}_\Lambda^\mathbf{R}$. Démontrer que l'on peut déterminer k et φ de façon à avoir :
$$\frac{1}{2\pi}\int_{-\pi}^{\pi} p(t)\ R_k^\varphi(t)\,\mathrm{d}t = \sum_{m\geqslant 1} \left|\widehat{p}(\lambda_m)\right|.$$
c) Démontrer que Λ est un ensemble de Sidon réel et que $K'(\Lambda) \leqslant 2$.

2. On suppose que pour tout entier j strictement positif, on a : $\lambda_{j+1} \geqslant 3\lambda_j$.
Démontrer que Λ est dissociée.

III. Un ensemble de Sidon d'irrationnels quadratiques

On note Q l'ensemble des éléments de $\mathbf{N}^*$ qui ne sont divisibles par aucun carré de nombre premier. En d'autres termes, les élément de Q sont 1 et les produits $p_1 \times \cdots \times p_r$ où $r \in \mathbf{N}^*$ et $p_1, \ldots, p_r$ sont r nombres premiers distincts.

A. Équation de Pell-Fermat

1. a) Soit G un sous-groupe de $(\mathbf{R},+)$. On suppose que 0 est un point isolé de $G\cap\mathbf{R}^+$. Démontrer qu'il existe $c\in\mathbf{R}^+$ tel que $G=c\mathbf{Z}$.

   b) Décrire les sous-groupes de $(\mathbf{R}^{+*},\times)$ tels que 1 soit un point isolé de $G\cap[1,+\infty[$.

2. Soit m dans $\mathbf{N}^*$.

   a) Soit (x,y) dans $\mathbf{Z}^2$ tel que $x+y\sqrt{m}>1$ et $x^2-my^2=1$.

   Ranger par ordre croissant les réels $x+y\sqrt{m}$, $x-y\sqrt{m}$, $-x+y\sqrt{m}$; en déduire : $x+y\sqrt{m}\geqslant 1+\sqrt{m}$.

   b) Soit $\quad G_m=\left\{x+y\sqrt{m}\;\middle|\;(x,y)\in\mathbf{Z}^2,\ x+y\sqrt{m}>0,\ x^2-my^2=1\right\}$.

   Démontrer que G_m est soit réduit à $\{1\}$, soit de la forme $\{{\gamma_m}^n,\ n\in\mathbf{Z}\}$ pour un certain $\gamma_m\geqslant 1+\sqrt{m}$.

   On peut prouver que $G_m=\{1\}$ si et seulement si m est le carré d'un entier ; cette précision est inutile dans la suite.

3. Pour q dans Q, soit $\quad A_q=\left\{\lambda\in\mathbf{N}^*\;\middle|\;\exists n\in\mathbf{N}^*,\ n(n+1)=q\,\lambda^2\right\}$.

   Montrer que A_q est soit vide, soit de la forme : $\{\lambda_{j,q},\ j\geqslant 1\}$ où $(\lambda_{j,q})_{j\geqslant 1}$ est une suite d'éléments de $\mathbf{N}^*$ telle que :

$$\forall j\geqslant 1,\qquad \lambda_{j+1,q}\ \geqslant\ (1+2\sqrt{q})\ \lambda_{j,q}.$$

   Indication. La relation $n(n+1)=q\,\lambda^2$ équivaut à $(2n+1)^2-4q\,\lambda^2=1$.

B. Indépendance des racines carrées des entiers sans facteur carré et application

Si K est un sous-corps de $\mathbf{R}$, m un élément de $\mathbf{N}$, $a_1,\dots,a_m$ des réels, on note $K(a_1,\dots,a_m)$ le plus petit sous-corps de $\mathbf{R}$ contenant K et $a_1,\dots,a_m$; si $m=0$, ce corps est égal à K.

1. Soient K un sous-corps de $\mathbf{R}$, a et b dans $K\cap\mathbf{R}^{+*}$ tels que $\sqrt{a}$ et $\sqrt{b}$ n'appartiennent pas à K. Démontrer l'équivalence :

$$\sqrt{b}\ \in\ K(\sqrt{a})\quad\Leftrightarrow\quad\sqrt{ab}\ \in\ K.$$

2. a) Démontrer par récurrence sur $m\in\mathbf{N}$ l'assertion suivante :
   « Si $n\in\mathbf{N}^*$, si $p_1,\dots,p_m,q_1,\dots,q_n$ sont $m+n$ nombres premiers distincts, alors $\sqrt{q_1\cdots q_n}$ n'appartient pas à $\mathbf{Q}(\sqrt{p_1},\dots,\sqrt{p_m})$ ».

   b) Démontrer que la famille $(\sqrt{q})_{q\in Q}$ est $\mathbf{Q}$-libre.

3. Soit :

$$\Lambda=\left\{\sqrt{n(n+1)},\ n\in\mathbf{N}^*\right\}\cup\left\{-\sqrt{n(n+1)},\ n\in\mathbf{N}^*\right\}.$$

   Démontrer que Λ est un ensemble de Sidon réel et que $K'(\Lambda)\leqslant 2$.

IV. Polynômes trigonométriques aléatoires

Soient n dans $\mathbf{N}^*$, $(a_1, \ldots, a_n)$ dans $\mathbf{C}^n$ et p l'élément de $\mathscr{P}_{\mathbf{Z}}$ défini par :

$$\forall t \in \mathbf{R}, \qquad p(t) = \sum_{k=1}^{n} a_k \mathrm{e}^{\mathrm{i}kt}.$$

A. Inégalité de Bernstein faible

1. Établir la majoration :

$$\|p'\|_\infty \leqslant \frac{n(n+1)}{2} \|p\|_\infty.$$

On peut prouver l'inégalité optimale : $\|p'\|_\infty \leqslant n \|p\|_\infty$; ce raffinement est inutile ici.
On pose désormais $\alpha_n = n(n+1)/2$.

2. Démontrer qu'il existe un segment S de $\mathbf{R}$ de longueur $1/\alpha_n$ tel que :

$$\forall t \in S, \ |p(t)| \geqslant \frac{\|p\|_\infty}{2}.$$

Dans la suite de cette partie **IV**, Ω est l'ensemble des n-uplets $\omega = (\omega_1, \ldots, \omega_n)$ tels que :

$$\forall k \in \{1, \ldots, n\}, \qquad \omega_k \in \{-1, 1\}.$$

On munit Ω de la probabilité uniforme notée P. L'espérance d'une variable aléatoire réelle X définie sur Ω est notée $E(X)$.

Si $1 \leqslant k \leqslant n$, soit X_k la variable aléatoire définie sur Ω par :

$$X_k(\omega) = \omega_k \qquad \text{si} \quad \omega = (\omega_1, \ldots, \omega_n).$$

On rappelle que $X_1, \ldots, X_n$ sont des variables aléatoires indépendantes de loi donnée par :

$$\forall k \in \{1, \ldots, n\}, \qquad P(X_k = 1) = P(X_k = -1) = \frac{1}{2}.$$

On fixe λ dans $\mathbf{R}^{+*}$.

B. Majoration d'une espérance

1. Démontrer que, pour tout x réel, $\operatorname{ch} x \leqslant \mathrm{e}^{x^2/2}$.

Indication. On pourra utiliser un développement en série entière.

Soit $Z = \sum_{k=1}^{n} a_k \, X_k$.

2. Calculer $E\left(\mathrm{e}^{\operatorname{Re} Z}\right)$.

3. a) Démontrer l'inégalité : $E\left(\mathrm{e}^{\lambda|\operatorname{Re} Z|}\right) \leqslant 2 \exp\left(\dfrac{\lambda^2}{2} \sum_{k=1}^{n} (\operatorname{Re} a_k)^2\right)$.

b) Démontrer l'inégalité : $E\left(\mathrm{e}^{\lambda|Z|}\right) \leqslant 2 \exp\left(\lambda^2 \sum_{k=1}^{n} |a_k|^2\right)$.

C. Un résultat de Salem et Zygmund

Pour ω dans Ω, soit p_ω l'élément de $\mathscr{P}_{\mathbf{Z}}$ défini par :

$$\forall t \in \mathbf{R}, \qquad p_\omega(t) = \sum_{k=1}^{n} a_k \, X_k(\omega) \, \mathrm{e}^{\mathrm{i}kt}.$$

Pour t dans $\mathbf{R}$, soit Z_t la variable aléatoire définie par :

$$\forall w \in \Omega, \qquad Z_t(\omega) = p_\omega(t).$$

Soit enfin M la variable aléatoire donnée par :

$$\forall \omega \in \Omega, \qquad M(\omega) = \|p_\omega\|_\infty.$$

1. a) Pour ω dans Ω, démontrer l'inégalité :
$$\frac{1}{\alpha_n} \, \exp\left(\frac{\lambda M(\omega)}{2}\right) \leqslant \int_0^{2\pi} \exp\left(\lambda \, |Z_t(\omega)|\right) \, \mathrm{d}t.$$
b) Démontrer l'inégalité :
$$E\left(\exp\left(\frac{\lambda M}{2}\right)\right) \leqslant 4\pi\alpha_n \, \exp\left(\lambda^2 \sum_{k=1}^{n} |a_k|^2\right).$$
2. a) Démontrer qu'il existe ω dans Ω tel que :
$$M(\omega) \leqslant 2\left(\frac{\ln(4\pi\alpha_n)}{\lambda} + \lambda \sum_{k=1}^{n} |a_k|^2\right).$$
b) Conclure qu'il existe ω dans Ω tel que :
$$M(\omega) \leqslant 4\sqrt{\ln(4\pi\alpha_n) \sum_{k=1}^{n} |a_k|^2}.$$
En choisissant $(a_1, \ldots, a_n) = (1, \ldots, 1)$, on obtient ainsi $(\delta_1, \ldots, \delta_n)$ dans $\{\pm 1\}^n$ tel que :
$$\forall t \in \mathbf{R}, \qquad \left|\sum_{k=1}^{n} \delta_k \, \mathrm{e}^{\mathrm{i}kt}\right| \leqslant 4\sqrt{n \ln(4\pi\alpha_n)}.$$
C'est uniquement ce résultat qui sera utilisé dans la partie **V**.
3. Soit Λ un ensemble de Sidon contenu dans $\mathbf{Z}$. Montrer :
$$|\Lambda \cap \{1, \ldots, n\}| \leqslant 16 \, K(\Lambda)^2 \, \ln(4\pi\alpha_n).$$

V. Vibrations des sphères

Pour n dans $\mathbf{N}^*$, soit $(\delta_{k,n})_{1 \leqslant k \leqslant n}$ une suite d'éléments de $\{-1, 1\}$ possédant la propriété énoncée en **IV.**C.2 : « si $R_n = \sum_{k=1}^{n} \delta_{k,n} \, X^k$, alors $\sup\left\{\left|R_n(\mathrm{e}^{\mathrm{i}u})\right|, \, u \in \mathbf{R}\right\} \leqslant 4\sqrt{n \ln(4\pi\alpha_n)}$ ».

Pour t dans $\mathbf{R}$ et x dans $[-1, 1]$, soit : $u_n(t, x) = \dfrac{1}{n} \displaystyle\sum_{k=1}^{n} \delta_{k,n} \, L_k(x) \, \mathrm{e}^{\mathrm{i}\sqrt{k(k+1)}t}$.

D'après **I.**C.5, u_n appartient à $\mathscr{E}$. On se propose d'établir, pour n grand, certaines propriétés asymptotiques de u_n.

On fixe ε et T dans $\mathbf{R}^{+*}$, η dans $]0, 1[$; I_η a la même signification qu'en **I.**B.

1. Démontrer qu'il existe N dans $\mathbf{N}^*$ tel que :

$$(1) \qquad \forall n \geqslant N, \quad \forall (t,x) \in \mathbf{R} \times I_\eta, \qquad |u_n(t,x)| \leqslant \varepsilon.$$

2. Indiquer une constante absolue m appartenant à $\mathbf{R}^{+*}$ telle que :

$$(2) \qquad \sup\{|u_n(t,1)|,\ t \in \mathbf{R}\} \geqslant m \quad \text{et} \quad \sup\{|u_n(t,-1)|,\ t \in \mathbf{R}\} \geqslant m.$$

3. Pour t dans $\mathbf{R}$ et x dans $[-1,1]$, soit : $v_n(t,x) = \dfrac{1}{n} \displaystyle\sum_{k=1}^{n} \delta_{k,n}\, L_k(x)\, \mathrm{e}^{\mathrm{i}(2k+1)t/2}$.

   a) Démontrer la majoration : $\forall (t,x) \in \mathbf{R}\times[-1,1], \quad |v_n(t,x)| \leqslant \dfrac{1}{n} \sup\left\{|R_n(\mathrm{e}^{\mathrm{i}u})|,\ u \in \mathbf{R}\right\}$.

   b) Déduire de a) l'existence de N' dans $\mathbf{N}$ tel que :

$$(3) \qquad \forall n \geqslant N', \quad \forall (t,x) \in [-T,T] \times [-1,1], \qquad |u_n(t,x)| \leqslant \varepsilon.$$

On obtient ainsi des solutions de l'équation des ondes sur la sphère unité S^2 de $\mathbf{R}^3$, ne dépendant que d'une coordonnée, uniformément petites sur tout compact ne contenant pas les pôles (relation (1)), uniformément petites sur la sphère en temps fini (relation (3)), mais prenant de grandes valeurs aux pôles à certains instants (relation (2)).

Présentation de l'épreuve d'analyse et probabilités

1 But du problème

Le numéro 1 de "Astérisque" (1973, [8]) rassemble trois articles d'Yves Meyer. Chacun étudie un problème d'analyse harmonique dans lequel la théorie des nombres joue un rôle majeur. Le premier d'entre eux est consacré à la propagation des ondes sur une sphère euclidienne. Supposons $n \geqslant 3$, et notons $\Delta_{S^{n-1}}$ l'opérateur de Laplace-Beltrami sur la sphère S^{n-1} de $\mathbf{R}^n$. La détermination des éléments propres de $\Delta_{S^{n-1}}$ fournit des solutions explicites de :

$$(1) \qquad \frac{\partial^2 u}{\partial t^2} = \Delta_{S^{n-1}}(u),$$

à savoir les fonctions de la forme (2) :

$$u(t,m) = a_0(m) + \sum_{k=1}^{N} \left(a_k(m) \cos\left(\sqrt{k(k+n-2)}t\right) + b_k(m) \sin\left(\sqrt{k(k+n-2)}t\right)\right)$$

où, pour tout k, a_k et b_k sont des harmoniques sphériques de degré k. Meyer prouve que certaines de ces fonctions ont un comportement asymptotique étonnant. Précisément, si ω est un élement de S^{n-1}, si ϵ et T des réels > 0 et K compact de $S^{n-1} \setminus \{\pm\omega\}$, on obtient une fonction u de la forme (2) telle que :

- $\forall (t,m) \in \mathbf{R}^+ \times K,\ |u(t,m)| \leqslant \epsilon$,
- $\forall (t,m) \in [0,T] \times S^{n-1},\ |u(t,m)| \leqslant \epsilon$,
- $\overline{\lim_{t \to -\infty}} |u(t,m)| \geqslant 1$ et $\overline{\lim_{t \to +\infty}} |u(t,m)| \geqslant 1$.

Dans [1], Marcel Berger cite ce résultat et en suggère une illustration sismologique surprenante !

La construction nécessite trois ingrédients. Les deux premiers sont classiques : comportement asymptotique des fonctions zonales, construction d'un choix de signe $\pm$ tels que les polynômes $\sum_0^N \pm z^k$ pour N dans $\mathbf{N}$ aient une norme uniforme petite sur le cercle unité (dans la limite permise par l'égalité de Parseval). Le troisième, plus subtil, est que l'ensemble des fréquences :

$$\left\{ \pm\sqrt{k(k+n-2)},\ k \in \mathbf{N} \right\}$$

vérifie la propriété de Sidon ; c'est le coeur de l'article [8].

Le but du sujet est d'établir une forme un peu affaiblie de ce résultat pour $n = 3$, les $\overline{\lim}$ étant remplacés par des sup ; l'énoncé original n'est pas plus difficile mais sa mise en place aurait alourdi le texte. Le cas $n \geqslant 3$ se traite de façon analogue mais exige des préliminaires sensiblement plus lourds : l'étude des fonctions zonales générales (et pas seulement des polynômes de Legendre), la propriété de Sidon pour les parties q-lacunaires de $\mathbf{Z}$ (et pas seulement dans le cas dissocié $q \geqslant 3$), la structure des solutions de l'équation $x^2 - dy^2 = c$ (et pas le seul cas $d = 1$ – pour ce dernier point, la difficulté supplémentaire est négligeable).

2 Organisation du sujet

La partie I rassemble quelques généralités. On y détermine les solutions à variable séparable de (1) ne dépendant que d'une coordonnée, ce qui fait apparaître les fonctions (2). Les fonctions zonales sont ici les polynômes de Legendre dont on étudie sommairement le comportement asymptotique.

La partie II présente les deux exemples d'ensembles de Sidon utiles dans la suite : les parties dissociées de $\mathbf{Z}$ (dont les suites "3-lacunaires" à la Hadamard) et les parties $\mathbf{Q}$-libres de $\mathbf{R}$ (reformulation du classique théorème de Kronecker). Le cas des parties de $\mathbf{Z}$ est éclairé par la caractérisation des Sidon via les mesures d'interpolation. Ces mesures permettent notamment d'interpréter très agréablement les produits de Riesz ([5]) ; faute d'espace, ce point n'a pu être abordé dans le sujet.

La partie III combine les exemples de II pour établir que l'ensemble de fréquences $\{\pm\sqrt{k(k+1)},\ k \in \mathbf{N}\}$ est de Sidon. Ceci nécessite deux résultats arithmétiques : le b-a-ba sur l'équation de Pell-Fermat (sans l'existence de solutions non triviales) et la liberté de $(\sqrt{q})_{q\in\mathcal{Q}}$ où $\mathcal{Q}$ est l'ensemble des éléments "squarefree" de $\mathbf{N}^*$. Le premier se déduit du caractère monogène d'un sous-groupe discret de $(\mathbf{R}^{+*}, \times)$. Le second est prouvé dans [8] par un argument très rapide mais relativement sophistiqué (loi de réciprocité quadratique + théorème de la progression arithmétique) ; il s'agit en fait d'un cas particulier de la dualité de Kummer ([6]). Pour que le problème soit "self-contained", on en a proposé une démonstration un peu laborieuse mais élémentaire.

La partie IV est dévolue à un théorème prouvé en 1954 par Salem et Zygmund ([3]). Pondérant les coefficients d'un polynôme trigonométrique de degré n par des signes aléatoires, on établit l'existence de (beaucoup de) choix de signes tels que la norme uniforme des polynômes obtenus diffère de la norme quadratique d'un facteur multiplicatif de l'ordre de $\sqrt{\ln n}$. L'article [8] n'utilise pas ce résultat mais une construction élémentaire non probabiliste de Rudin-Shapiro ([4]), qui donne d'ailleurs un résultat meilleur dans le cas envisagé ici de coefficients valant ± 1. La rédaction retenue offre l'avantage de tester les candidats en probabilités (finies !) et en analyse d'une variable réelle ; elle permet en outre de montrer le caractère clairsemé des ensembles de Sidon ("condition de maille", cf [2] ou [7]).

Enfin, la partie V utilise une grande partie de ce qui précède pour construire les fonctions désirées.

3 Compléments

Outre [8], on trouvera de nombreux résultats reliant analyse harmonique et théorie des nombres algébrique des nombres dans [9]. Les références [10], [2] contiennent la théorie classique des ensembles de Sidon, [7] donne une preuve probabiliste du théorème de Drury sur les réunions finies d'ensembles de Sidon (dont [9] adapte la preuve classiques aux "Sidon topologiques" de $\mathbf{R}$). Enfin, [3] contient beaucoup d'applications des méthodes probabilistes à l'Analyse Harmonique.

Références

[1] M. BERGER *Cinq siècles de mathématiques en France*, ADPF,

[2] J.P. KAHANE, *Séries trigonométriques absolument convergentes*, Springer,

[3] J.P. KAHANE, *Some random series of functions*, Cambridge,

[4] J.P. KAHANE, R. SALEM, *Ensembles parfaits et séries trigonométriques*, Hermann,

[5] Y. KATZNELSON, *An introduction to harmonic analysis*, Cambridge,

[6] S. LANG, *Algebra*, Addison Wesley,

[7] D. LI, H. QUEFFELEC, *Introduction à l'étude des espaces de Banach*, SMF,

[8] Y. MEYER, *Trois problèmes sur les sommes trigonométriques* (Astérisque),

[9] Y. MEYER, *Algebraic Numbers and Harmonic Analysis* North Holland,

[10] A. ZYGMUND, *Trigonometric Series* Cambridge.

Corrigé de l'épreuve d'analyse et probabilités

Partie I

I.A.1.a) Pour μ dans $\mathbf{R}^*$:

$$\frac{1}{T}\int_0^T e_\mu = \left[\frac{e^{i\mu T}-1}{T}\right] \quad \underset{T\to+\infty}{\longrightarrow} \quad 0.$$

On en déduit :

$$\frac{1}{T}\int_0^T p\, e_{-\lambda_0} \quad \underset{T\to+\infty}{\longrightarrow} \quad c_{\lambda_0}.$$

b) Avec les notations de a), $p=0$ implique $c_{\lambda_0}=0$ pour tout réel λ_0, d'où le résultat.

2. a) Gardons les mêmes notations. Alors :

$$\text{Re } p = \sum_{\lambda\in\mathbf{R}} \frac{c_\lambda + \overline{c_{-\lambda}}}{2}\, e_\lambda \qquad \text{et} \qquad \text{Im } p = \sum_{\lambda\in\mathbf{R}} \frac{c_\lambda - \overline{c_{-\lambda}}}{2i}\, e_\lambda.$$

La symétrie de Λ montre que si $\lambda \notin \Lambda$, $c_\lambda = c_{-\lambda} = 0$ d'où l'on tire, avec les égalités précédentes, $\text{Re } p \in \mathcal{P}_\Lambda$ et $\text{Im } p \in \mathcal{P}_\Lambda$, puis le résultat voulu.

b) Supposons que Λ est un Sidon réel et fixons p dans $\mathcal{P}_\Lambda$. Le a) fournit $N(\text{Re}p) \leqslant K'(\Lambda)\ \sup\ \text{Re } p \leqslant K'(\Lambda)\ \|p\|_\infty$ et de même $N(\ \text{Im } p) \leqslant K'(\Lambda)\ \|p\|_\infty$. Par suite :

$$N(p) = N(\ \text{Re } p + i\ \text{Im } p) \leqslant N(\ \text{Re } p) + N(\ \text{Im } p) \leqslant 2K'(\Lambda)\ \|p\|_\infty.$$

Il s'ensuit que Λ est de Sidon avec $K(\Lambda) \leqslant 2K'(\Lambda)$.

I.B.1.a) Si f est une fonction holomorphe au voisinage du disque fermé bordé par l'image de γ, z_0 un point intérieur à ce même disque, p un entier naturel, la formule de Cauchy donne :

$$f^{(p)}(z_0) = p! \int_\gamma \frac{f(z)}{(z-z_0)^{p+1}}\, \frac{\mathrm{d}z}{2i\pi}$$

Reste à appliquer ce résultat à $f = U_n$, $p = n$ et $z_0 = x$.

b) Prenons x dans $]-1,1[$ et $r = \sqrt{1-x^2}$. Il vient :

$$\begin{aligned}
\int_\gamma \frac{(z^2-1)^n}{(z-x)^{n+1}}\, \frac{\mathrm{d}z}{2i\pi} &= \frac{1}{2\pi}\int_{-\pi}^{\pi} \left(\frac{\left(x+re^{i\theta}\right)^2 - 1}{re^{i\theta}}\right)^n \mathrm{d}\theta \\
&= \frac{1}{2\pi}\int_{-\pi}^{\pi} \left(\frac{x^2-1}{re^{i\theta}} + 2x + re^{i\theta}\right)^n \mathrm{d}\theta \\
&= \frac{1}{2\pi}\int_{-\pi}^{\pi} \left(-\sqrt{1-x^2}e^{-i\theta} + 2x + \sqrt{1-x^2}e^{i\theta}\right)^n \mathrm{d}\theta \\
&= \frac{1}{2\pi}\int_{-\pi}^{\pi} \left(2\left(x + i\sqrt{1-x^2}\sin\theta\right)\right)^n \mathrm{d}\theta
\end{aligned}$$

Tenant compte de la définition de L_n et de a), on en déduit la formule demandée.
Il reste à étendre la formule à $x = \pm 1$. Il est clair que l'on peut trouver P dans $\mathbf{C}[X, Y]$ tel que :

$$\forall x \in [-1, 1], \qquad \int_{-\pi}^{\pi} \left(x + i\sqrt{1-x^2}\sin\theta\right)^n \, \mathrm{d}\theta = P\left(x, \sqrt{1-x^2}\right)$$

(il suffit de développer l'intégrale par la formule du binôme). Cette formule montre que les deux membres de l'égalité proposée sont fonctions continues de x sur $[-1, 1]$, et le résultat suit.

2. La question 1.b) donne : $L_n(1) = 1$ et $L_n(-1) = (-1)^n$.
Si $x \in [-1, 1]$ et $\theta \in \mathbf{R}$, on a :

$$\left|x + i\sqrt{1-x^2}\sin\theta\right|^2 = x^2 + (1-x^2)\sin^2\theta \leqslant x^2 + 1 - x^2 \leqslant 1$$

On en tire : $|L_n(x)| \leqslant 1$. Au total : $\sup\{|L_n(x)|\,,\ x \in [-1, 1]\} = 1$.

3. a) Pour $x \in I_\eta$ et $\theta \in R$, le calcul de la question 2 donne :

$$\begin{aligned}\left|x + i\sqrt{1-x^2}\sin\theta\right|^2 &= x^2 + (1-x^2)\sin^2\theta = \sin^2\theta + x^2\cos^2\theta \\ &\leqslant \sin^2\theta + (1-\eta)^2\cos^2\theta\end{aligned}$$

Or :

$$\sin^2\theta + (1-\eta)^2\cos^2\theta = 1 - 2\eta\cos^2\theta + \eta^2\cos^2\theta \leqslant 1 - \eta\cos^2\theta$$

car $\eta^2 \leqslant \eta$. L'inégalité demandée suit aisément.

b) Pour n dans $\mathbf{N}$, posons :

$$I_n = \int_{-\pi}^{\pi} \varphi_n \qquad \text{où} \quad \varphi_n(\theta) = \left(1 - \eta\cos^2\theta\right)^{n/2}.$$

Grâce à a), il suffit de montrer que $I_n \to 0$.
Mais (φ_n) converge simplement vers 0 sur $[-\pi, \pi] \setminus \{\pm\pi/2\}$, et est bornée par 1. La conclusion résulte du théorème de convergence dominée.

I.C.1.a) Puisque $U_n = (X^2-1)^n$, ${U_n}' = 2nX(X^2-1)^{n-1}$, d'où le résultat.

b) On dérive $n+1$ fois la relation de a) avec la formule de Leibniz. Il vient :

$$(X^2-1){U_n}^{(n+2)} + 2(n+1)X{U_n}^{(n+1)} + n(n+1){U_n}^{(n)} = 2nX\ {U_n}^{(n+1)} + 2n(n+1){U_n}^{(n)}.$$

C'est la relation voulue.

2. On remarque que :

$$D(f)(x) = \frac{d}{dx}\left((1-x^2)f'(x)\right).$$

On intégre par parties en observant que $(1-x^2)f'(x)$ et $(1-x^2)g'(x)$ s'annulent en ± 1, et il vient :

$$\begin{aligned}\int_{-1}^{1} D(f)\ g &= -\int_{-1}^{1}(1-x^2)\ f'(x)\ g'(x)\,\mathrm{d}x = -\int_{-1}^{1}(1-x^2)\ g'(x)\ f'(x)\,\mathrm{d}x \\ &= \int_{-1}^{1} D(g)\ f\end{aligned}$$

3. La question 1.b) montre que Σ contient $\{-n(n+1),\ n \in \mathbf{N}\}$. Inversement, soit λ dans $\mathbf{R} \setminus \{-n(n+1),\ n \in \mathbf{N}\}$. Montrons que $V_\lambda = \{0\}$, ce qui donnera le résultat demandé. En appliquant la question 2 avec f dans V_λ et $g = P_m$ où $m \in \mathbf{N}$, il vient :

$$\lambda \int_{-1}^{1} fP_m = -m(m+1) \int_{-1}^{1} fP_m, \qquad \text{d'où} \quad \int_{-1}^{1} fP_m = 0.$$

D'autre part, P_n étant de degré n pour tout n, $(P_n)_{n\in\mathbf{N}}$ est une base de $\mathbf{R}[X]$, et ce qui précède implique :

$$\int_{-1}^{1} fP = 0$$

pour tout P de $\mathbf{R}[X]$. Le théorème d'approximation de Weierstrass permet classiquement d'en déduire $f = 0$.

4. Le théorème de Cauchy-Lipschitz linéaire implique que l'espace des solutions de (E) sur $]-1,1[$ est de dimension 2. Soit donc u une fonction de classe C^2 sur $]-1,1[$ telle que (u, L_n) soit une base de l'espace précédent. Pour établir que $V_{-n(n+1)} = \mathbf{C}L_n$, il suffit de voir que u ne se prolonge pas en une fonction de classe C^2 sur $[-1,1]$. Soit $W = L_n u' - L_n{}' u$. Un calcul classique assure que :

$$\forall x \in]-1,1[, \qquad W'(x) = \frac{2x}{1-x^2}\, W(x).$$

Il s'ensuit que :

$$\forall x \in]-1,1[, \qquad W(x) = \frac{W(0)}{1-x^2}.$$

D'autre part, la liberté de (u, L_n) et les propriétés usuelles du wronskien montrent que $W(0) \neq 0$. Par suite :

$$|W(x)| \underset{x\to\pm1}{\longrightarrow} +\infty,$$

d'où la conclusion.

5. Si $u(t,x) = a(t)\, b(x)$, l'équation proposée s'écrit :

$$a''(t)\, b(x) = (1-x^2)b''(x) - 2xb'(x)\, a(t).$$

Supposons u non identiquement nulle. En choisissant t tel que $a(t) \neq 0$, on voit que b est fonction propre de D, donc colinéaire à L_n pour un certain n de $\mathbf{N}$. On a alors, en choisissant x n'annulant pas L_n, $a''(t) = -n(n+1)\, a(t)$ pour tout réel t. On en déduit que a est affine si $n = 0$, combinaison linéaire de $e_{-\sqrt{n(n+1)}}$ et $e_{\sqrt{n(n+1)}}$ si $n \geqslant 1$. En fin de compte, u est bien de la forme voulue. La réciproque est immédiate.

Partie II

A.1.a) Soit $(a_1, \ldots, a_n) \in \mathbf{Z}^n \setminus \{0\}$ tel que : $\sum_{i=1}^{n} a_i w_i = 0$. Soit l la forme linéaire sur $\mathbf{R}^n$ qui à $(x_1, \ldots, x_n)$ associe :

$$\frac{1}{2\pi} \sum_{i=1}^{n} a_i x_i.$$

On a $w \in \ker l$ et, si $v \in \mathbf{Z}^n$:

$$l(2\pi v) = \sum_{i=1}^{n} a_i v_i \ \in \ \mathbf{Z}.$$

Il s'ensuit que $l(G_w) \subset \mathbf{Z}$.

b) Puisque $\mathbf{R}^n$ est de dimension finie, l est continue d'où :

$$l\left(\overline{G_w}\right) \subset \overline{l(G_w)},$$

et, puisque $\mathbf{Z}$ est fermé dans $\mathbf{R}$, $l(\overline{G_w})) \subset \mathbf{Z}$. Si G_w était dense dans $\mathbf{R}^n$, $l(\overline{G_w})$ serait égal à $l(\mathbf{R}^n) = \mathbf{R}$ car une forme linéaire non nulle est surjective, ce qui donne la contradication désirée.

(Le a) assure en fait que G_w est contenu dans une réunion dénombrable d'hyperplans affines parallèles et régulièrement espacés de $\mathbf{R}^n$; cette réunion est trivialement un fermé de $\mathbf{R}^n$ négligeable et d'intérieur vide.)

2.a) L'application J_T est une forme n-linéaire sur $\mathcal{C}^n$, de sorte qu'il suffit de prouver le résultat quand les f_i sont des e_λ. Posons $f_i = e_{\lambda_i}$, $\lambda_i \in \mathbf{Z}$, de sorte que :

$$J_T(f_1, \ldots, f_n) = \frac{1}{T} \int_0^T e_{\sum_{i=1}^n \lambda_i w_i}.$$

D'après **I.A**.1.a), cette quantité tend vers $\delta_{0, \sum_{i=1}^n \lambda_i w_i}$ lorsque $T \to +\infty$. Mais la $\mathbf{Q}$-liberté de $(w_1, \ldots, w_n)$ assure que :

$$\sum_{i=1}^{n} \lambda_i w_i = 0 \quad \Leftrightarrow \quad (w_1, \ldots, w_n) = (0, \ldots, 0),$$

d'où le résultat.

b) Munissons $\mathcal{C}^n$ de la norme produit. Il est alors immédiat que les J_T sont toutes de norme subordonnée 1, donc forment une famille équicontinue de formes n-linéaires. Un raisonnement classique montre qu'il suffit d'établir le résultat pour $(f_1, \ldots, f_n)$ appartenant à une famille dense de $\mathcal{C}^n$. Or, gr,ce au théorème de Weierstrass trigonométrique, ${\mathcal{P}_{\mathbf{Z}}}^n$ est dense dans $\mathcal{C}^n$ pour la norme produit, et a) permet de conclure.

c) Fixons $(x_1, \ldots, x_n)$ dans $\mathbf{R}^n$ et ε dans $]0, \pi[$. Si $1 \leqslant j \leqslant n$, prenons pour f_j une fonction continue, 2π-périodique, strictement positive sur $]x_j - \varepsilon, x_j + \varepsilon[$, nulle sur $[x_j - \pi, x_j + \pi] \backslash]x_j - \varepsilon, x_j + \varepsilon[$. Le b) garantit :

$$J_T(f_1, \ldots, f_n) \quad \underset{T \to +\infty}{\longrightarrow} \quad \prod_{j=1}^{n} \left(\frac{1}{2\pi} \int_0^{2\pi} f_j \right).$$

Le membre de droite étant dans $\mathbf{R}^{+*}$, cette relation assure l'existence d'un réel t tel que :

$$\forall j \in \{1, \dots, n\}, \qquad f_j(w_j t) > 0.$$

On en déduit l'existence de $(m_1, \dots, m_n)$ dans $\mathbf{Z}^n$ tel que :

$$\forall j \in \{1, \dots, n\}, \qquad tw_j \in]2\pi m_j + x_j - \varepsilon, 2\pi m_j + x_j + \varepsilon[.$$

Pour la norme $\| \ \|_\infty$ sur $\mathbf{R}^n$, le vecteur $(x_1, \dots, x_n)$ est donc à une distance au plus ε du vecteur $t(w_1, \dots, w_n) - 2\pi(m_1, \dots, m_n)$ de G_w, d'où la densité désirée.

3. Il est clair que :

$$\sup g \leqslant \sum_{j=1}^{n} \sup g_j.$$

Pour établir la réciproque, on considère, si $1 \leqslant j \leqslant n$, un réel x_j tel que $\sup g_j = g_j(x_j)$ (qui existe par continuité et périodicité de g_j). La question 2 donne une suite (t_k) de réels et n suites $(m_{j,k})$ pour $1 \leqslant j \leqslant n$ d'entiers telles que :

$$t_k(w_1, \dots, w_n) + 2\pi(m_{1,k}, \dots, m_{n,k}) \underset{k \to +\infty}{\longrightarrow} (x_1, \dots, x_n).$$

Il s'ensuit que :

$$\forall j \in \{1, \dots n\}, \qquad g_j(w_j t_k) \underset{k \to +\infty}{\longrightarrow} g_j(x_j),$$

donc que :

$$g(t_k) \underset{k \to +\infty}{\longrightarrow} \sum_{j=1}^{n} \sup g_j,$$

ce qui achève la preuve.

4. La symétrie de Λ est immédiate. Puisque Λ_γ est contenue dans $\mathbf{Z}$ et $\mathbf{Q}$-libre, les $\gamma\Lambda_\gamma$ pour γ dans Γ sont deux à deux disjoints. On pose, si $\gamma \in \Gamma$ et si $f = \sum_{\lambda \in \mathbf{R}} a_\lambda e_\lambda$:

$$f_\gamma = \sum_{\lambda \in \gamma\Lambda_\gamma} a_\lambda e_\lambda.$$

On a déjà : $N(f) = \sum_{\gamma \in \Gamma} N(f_\gamma)$. D'autre part, f_γ est de la forme $x \mapsto g_\gamma(\gamma_x)$ où g_γ appartient à $\mathcal{P}^{\mathbf{R}}_{\Lambda_\gamma}$. La question 3 entraîne alors :

$$\sup f = \sum_{\gamma \in \Gamma} \sup g_\gamma = \sum_{\gamma \in \Gamma} \sup f_\gamma.$$

Reste à écrire $N(f_\gamma) \leqslant K'(\Lambda) \sup f_\gamma$ et à sommer sur $\gamma \in \Gamma$ pour obtenir, compte-tenu de ce qui précède : $N(f) \leqslant K'(\Lambda) \sup f$.

B.I.1.a) Ecrivons d'abord :

$$\begin{aligned} R_k^\varphi &= \prod_{j=1}^{k} \left(1 + \frac{e^{i\varphi_j} e_{\lambda_j} + e^{-i\varphi_j} e_{-\lambda j}}{2}\right) \\ &= \sum_{(\varepsilon_1, \dots, \varepsilon_k) \in \{-1,0,1\}^k} \frac{e^{i\left(\sum_{j=1}^k \varepsilon_j \varphi_j\right)}}{2^{|\varepsilon_1| + \dots + |\varepsilon_k|}} \, e_{\sum_{j=1}^k \varepsilon_j \varphi_j} \end{aligned}$$

L'hypothèse de dissociation montre que le seul $(\varepsilon_1, \ldots, \varepsilon_k)$ de $\{-1,0,1\}^k$ tel que $\sum_{j=1}^{k} \varepsilon_j \lambda_j = 0$ est $(0,\ldots,0)$, d'où : $\widehat{R_k^\varphi}(0) = 1$. Elle implique de même que le seul k-uplet $(\varepsilon_1, \ldots, \varepsilon_k)$ de $\{-1,0,1\}^k$ tel que $\sum_{j=1}^{k} \varepsilon_j \lambda_j = \lambda_m$ est :

$$\Big(0,\ldots,0,\underset{m\text{ième place}}{1},0,\ldots,0\Big)$$

d'où : $\widehat{R_k^\varphi}(\lambda_m) = e^{i\varphi_m}/2$. De même $\widehat{R_k^\varphi}(-\lambda_m) = e^{-i\varphi_m}/2$.

b) La formule de Parseval assure :

$$\frac{1}{2\pi}\int_{-\pi}^{\pi} p\, R_k^\varphi = \sum_{n\in\mathbf{Z}} \hat{p}(n)\, \widehat{R_k^\varphi}(-n).$$

Vu que p est dans $\mathcal{P}_\Lambda$, a) implique alors :

$$\frac{1}{2\pi}\int_{-\pi}^{\pi} pR_k^\varphi = \sum_{n\in\mathbf{Z}} \left(e^{-i\varphi_n}\hat{p}(\lambda_n) + e^{i\varphi_n}\hat{p}(-\lambda_n)\right).$$

Mais p étant à valeurs réelles : $\hat{p}(-\lambda_m) = \overline{\hat{p}(\lambda_m)}$ si $m \in \mathbf{Z}$ et, en choisissant k pour que λ_k soit supérieur ou égal au degré du polynôme trigonométrique p :

$$\frac{1}{2\pi}\int_{-\pi}^{\pi} p\, R_k^\varphi = \sum_{m\geqslant 1} \text{Re}\ \left(e^{-i\varphi_m}\hat{p}(\lambda_m)\right).$$

En prenant, pour tout $m \geqslant 1$, φ_m dans $\mathbf{R}$ tel que $e^{-i\varphi_m}\hat{p}(\lambda_m) \in \mathbf{R}^+$, on a le résultat désiré.

c) Avec les notations de b) et en tenant compte de la positivité de R_k^φ, il vient :

$$\sum_{m=1}^{k} |\hat{p}(\lambda_m)| \ \leqslant\ \frac{\sup p}{2\pi}\int_{-\pi}^{\pi} R_k^\varphi \ \leqslant\ \sup p$$

car $\widehat{R_k^\varphi}(0) = 1$. Puisque p est à valeurs réelles, on en tire aussitôt :

$$\sum_{m=1}^{k} |\hat{p}(-\lambda_m)| \ \leqslant\ \sup p,$$

d'où, en sommant : $N(p) \leqslant 2\sup p$. C'est le résultat voulu.

2. Soient $\varepsilon = (\varepsilon_j)_{j\geqslant 1}$ et $\varepsilon' = (\varepsilon'_j)_{j\geqslant 1}$ deux suites presque nulles d'éléments de $\{-1,0,1\}$ telles que :

$$\sum_{j\geqslant 1} \varepsilon_j\lambda_j = \sum_{j\geqslant 1} \varepsilon'_j\lambda_j.$$

Supposons par l'absurde $\varepsilon \neq \varepsilon'$, et notons $N = \max\left\{j \geqslant 1,\ \varepsilon_j \neq \varepsilon'_j\right\}$. On a alors :

$$(\varepsilon'_N - \varepsilon_N)\lambda_N = \sum_{j=1}^{N-1}(\varepsilon_j - \varepsilon'_j)\lambda_j \quad \text{d'où} \quad \lambda_N \geqslant \sum_{j=1}^{N-1} 2\lambda_j$$

vu que $|\varepsilon_j - \varepsilon'_j| \leqslant 2$ si $1 \leqslant j \leqslant N-1$ et $|\varepsilon'_N - \varepsilon_N| \geqslant 1$. Or, si $j \leqslant N-1$:

$$\lambda_j \leqslant \frac{\lambda_N}{3^{N-j}} \quad \text{d'où} \quad \sum_{j=1}^{N-1} \lambda_j \leqslant \lambda_N \sum_{j=1}^{N-1} \frac{1}{3^{N-j}} \cdot$$

La contradiction résulte alors de :

$$\sum_{j=1}^{N-1} \frac{1}{3^{N-j}} < \sum_{k=1}^{+\infty} \frac{1}{3^k} = \frac{1}{2} \cdot$$

Partie III

A.1.a) Si $G = \{0\}$, le résultat est trivial. Supposons $G \neq \{0\}$ de sorte que $G \cap \mathbf{R}^{+*} \neq \{0\}$ gr,ce à la stabilité de G par passage à l'opposé. L'hypothèse donne l'existence de $c = \min(G \cap \mathbf{R}^{+*})$. Montrons alors que $G = c\mathbf{Z}$. Puisque G contient c, il contient $c\mathbf{Z}$. Soit inversement g dans G. On écrit $g = qc + r$ avec $q \in \mathbf{Z}$ et $0 \leqslant r < c$. Il vient $r = g - qc$ d'où $r \in G$ et, par définition de c : $r = 0$, $g = \lambda c$ et $g \in c\mathbf{Z}$.

b) L'exponentielle est un isomorphisme strictement croissant et bicontinu de $(\mathbf{R}, +)$ sur $(\mathbf{R}^{+*}, \times)$. La question a) montre alors que les sous-groupes de $(\mathbf{R}^{+*}, \times)$ dont l'intersection avec $[1, +\infty[$ admet 1 comme point isolé sont les $c^{\mathbf{Z}} = \{c^n,\ n \in \mathbf{Z}\}$ avec $c \in [1, +\infty[$.

2.a) Déjà :

$$x - y\sqrt{m} = \frac{1}{x + y\sqrt{m}}$$

est dans $]0, 1[$ donc $-x + y\sqrt{m}$ est dans $]-1, 0[$. Ainsi : $x + y\sqrt{m} > x - y\sqrt{m} > -x + y\sqrt{m}$. On en déduit $x > 0$, $y > 0$, d'où : $(x, y) \in (\mathbf{N}^*)^2$ et $x + y\sqrt{m} \geqslant 1 + \sqrt{m}$.

b) Le a) montre que 1 est point isolé de $G_m \cap [1, +\infty[$. Il suffit de vérifier que G_m est un sous-groupe de $(\mathbf{R}^{+*}, \times)$ pour conclure via la question 1.b).

Soient donc g et g' dans G_m : $g = x + y\sqrt{m}$, $g' = x' + y'\sqrt{m}$ avec $(x, y, x', y') \in \mathbf{Z}^4$, $g > 0$, $g' > 0$ et $x^2 - my^2 = x'^2 - my'^2 = 1$. Alors $gg' = xx' + myy' + \sqrt{m}\,(xy' + x'y)$ est bien de la forme $u + v\sqrt{m}$ avec $(u, v) \in \mathbf{Z}^2$ et $u^2 - mv^2 = 1$ vu que :

$$\begin{aligned} (xx' + myy')^2 - m\,(x'y + xy')^2 &= x^2x'^2 + m^2y^2y'^2 - mx'^2y^2 - mx^2y'^2 \\ &= \left(x^2 - my^2\right)\left(x'^2 - my'^2\right) = 1 \end{aligned}$$

D'autre part, $1/g = x - y\sqrt{m}$ est clairement dans G_m. Enfin G_m contient 1.

3. L'indication proposée montre, si $n(n+1) = q\lambda^2$, que $2n + 1 + \lambda\sqrt{4q}$ est dans G_{4q}.

Si $G_{4q} = \{1\}$ ceci implique $2n+1+\lambda\sqrt{4q} = 1$, ce qui est incompatible avec $(n, \lambda) \in (\mathbf{N}^*)^2$, d'où la vacuité de A_q. Notons que tel est le cas si $q = 1$ car $x^2 - 4y^2 = 1$ s'écrit $(x - 2y)(x + 2y) = 1$ d'où, si $x + 2y \in \mathbf{N}^*$, $x + 2y = 1$.

Si $G_{4q} \neq \{1\}$, la question 2.b) donne $\gamma_{4q} = \gamma$ dans $[1 + 2\sqrt{q}, +\infty[$ tel que $G_{4q} = \{\gamma^n,\ n \in \mathbf{Z}\}$. Avec les notations de la question, on obtient donc $m \in \mathbf{N}^*$ tel que $(2n + 1) + \lambda\sqrt{4q} = \gamma^m$. On en déduit $(2n + 1) - \lambda\sqrt{4q} = \gamma^{-m}$, puis par soustraction :

$$\lambda = \frac{1}{4\sqrt{q}} \left(\gamma^m - \frac{1}{\gamma^m}\right).$$

Posons donc, si $j \geqslant 1$:

$$\lambda_{j,q} = \frac{1}{4\sqrt{q}} \left(\gamma^j - \frac{1}{\gamma^j} \right).$$

On a, si $j \in \mathbf{N}^*$: $\lambda_{j+1,q} \geqslant \gamma \lambda_{j,q}$, et le résultat désiré s'ensuit.

B.1. On a d'abord : $K(\sqrt{a}) = \left\{ x + y\sqrt{a},\ (x,y) \in K^2 \right\}$. Si $\sqrt{b} \in K(\sqrt{a})$, on a donc $\sqrt{b} = x + y\sqrt{a}$ où $(x,y) \in K^2$ et $b = x^2 + ay^2 + 2xy\sqrt{a}$. Puisque $\sqrt{a} \notin K$, ceci implique $xy = 0$. L'égalité $y = 0$ implique $b = x^2$, $\sqrt{b} \in K$, ce qui est exclu. Il en résulte que $\sqrt{b/a} \in K$, puis que $\sqrt{ab} \in K$. Réciproquement, supposons $\sqrt{ab} \in K$. Alors $\sqrt{b} = \sqrt{ab}/\sqrt{a}$ est dans $K(\sqrt{a})$.

2.a) Pour $m = 0$, l'assertion proposée revient à : $\sqrt{q_1 \cdots q_m} \notin \mathbf{Q}$. Ceci est vrai car les q_i sont des nombres premiers deux à deux distincts, donc $q_1 \cdots q_m$ n'est pas un carré dans $\mathbf{Q}$.

Supposons l'assertion vraie au rang $m-1$ avec $m \in \mathbf{N}^*$, et soient $p_1, \ldots, p_m,\ q_1, \ldots, q_n$ comme dans le texte. On veut montrer que $\sqrt{q_1 \cdots q_n}$ n'appartient pas à $K(\sqrt{p_m})$ où $K = \mathbf{Q}\left(\sqrt{p_1}, \ldots, \sqrt{p_{m-1}}\right)$. Dans le cas contraire, a) impliquerait $\sqrt{q_1 \cdots q_n p_m} \in K$, et l'hypothèse de récurrence donnerait une contradiction car $q_1, \cdots, q_n, p_m, p_1, \ldots, p_{m-1}$ sont des nombres premiers deux à deux distincts. Le résultat suit.

b) Rangeons les nombres premiers en une suite strictement croissante $(p_i)_{i \geqslant 1}$ et posons, pour $n \in \mathbf{N}$:

$$Q_n = \left\{ \prod_{i=1}^{n} {p_i}^{\alpha_i},\ (\alpha_1, \ldots, \alpha_n) \in \mathbf{N}^n \right\}$$

(en convenant que $Q_0 = \{1\}$) de sorte que $(Q_n)_{n \geqslant 0}$ est croissante pour l'inclusion et que $Q = \bigcup_{n \in \mathbf{N}} Q_n$. Supposons $(\sqrt{q})_{q \in Q}$ liée. On dispose alors de $n = \min\{m \in \mathbf{N},\ (\sqrt{q})_{q \in Q_m} \text{ liée}\}$. Cette définition de n donne a et b dans $\mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})$ non nuls tels que $a + b\sqrt{p_n} = 0$. Il s'ensuit que $\sqrt{p_n}$ appartient à $\mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})$, ce qui contredit a).

3. Par définition :

$$\Lambda = \{ \varepsilon \lambda_{j,q} \sqrt{q} \mid \varepsilon \in \{\pm 1\},\ q \in Q,\ j \in \mathbf{N}^* \} = \bigcup_{q \in Q} \sqrt{q} B_q$$

avec $B_q = A_q \cup (-A_q)$. Puisque $1 + 2\sqrt{q} \geqslant 3$, B_q est, d'après **II.B**.2, une partie dissociée de $\mathbf{Z}$ donc, grâce à **II.B**.1.c), un ensemble de Sidon réel avec de plus $K'(B_q) \leqslant 2$. Le résultat de **III.B**.2 permet alors d'appliquer **II.A**.4, qui amène la conclusion désirée.

Partie IV

A.1. On a, si $k \in \{1, \dots, n\}$:

$$a_k = \frac{1}{2\pi} \int_{-\pi}^{\pi} p(t)\, e^{-ikt}\, \mathrm{d}t$$

d'où $|a_k| \leqslant \|p\|_\infty$. Mais $p' = \sum_{k=1}^{n} ika_k e_k$ est borné par $\sum_{k=1}^{n} k|a_k|$, d'où le résultat voulu.

2. Par continuité et périodicité, il existe t_0 dans $\mathbf{R}$ tel que $|p(t_0)| = \|p\|_\infty$. Soit δ dans $\mathbf{R}^{+*}$. Si $\delta\alpha_n\|p\|_\infty \leqslant \|p\|_\infty/2$, i.e. si $\delta\alpha_n \leqslant 1/2$, le théorème des accroissements finis assure que $|p|$ est minoré par $\|p\|_\infty/2$ sur $[t_0 - \delta, t_0 + \delta]$, d'où le résultat demandé.

B.1. On a, pour x dans $\mathbf{R}$:

$$\operatorname{ch} x = \sum_{k=0}^{+\infty} \frac{x^{2k}}{(2k)!} \quad \text{et} \quad e^{x^2/2} = \sum_{k=0}^{+\infty} \frac{x^{2k}}{k!\, 2^k}\,.$$

Compte-tenu de la positivité de x^{2k}, il suffit pour conclure de vérifier que, pour tout k de $\mathbf{N}$: $k!\, 2^k \leqslant (2k)!$. Or :

$$\frac{(2k)!}{k!\, 2^k} = \frac{(k+1)(k+2)\cdots 2k}{2^k}\,.$$

Si $k \geqslant 1$, les k entiers $k+1, k+2, \dots, 2k$ sont minorés par 2, et le résultat est clair ; le cas $k = 0$ est trivial.

2. On a :

$$E\left(\exp\left(\lambda \text{ Re } Z\right)\right) = E\left(\exp\left(\lambda \sum_{k=1}^{n} (\text{ Re } a_k)\, X_k\right)\right).$$

L'indépendance des X_k entraîne :

$$E\left(\exp\left(\lambda \text{ Re } Z\right)\right) = \prod_{k=1}^{n} E\left(\exp\left(\lambda(\text{ Re } a_k)\, X_k\right)\right).$$

Or $E\left(\exp\left(\lambda(\text{ Re } a_k)\, X_k\right)\right) = \operatorname{ch}\,(\lambda \text{ Re } a_k)$. Au total :

$$E\left(\exp\left(\lambda \text{ Re } Z\right)\right) = \prod_{k=1}^{n} \operatorname{ch}\,(\lambda \text{ Re } a_k)\,.$$

3.a) On a de même :

$$E\left(\exp\left(-\lambda \text{ Re } Z\right)\right) = \prod_{k=1}^{n} \operatorname{ch}\,(\lambda \text{ Re } a_k)\,.$$

Mais :

$$e^{\lambda|\text{ Re } z|} \leqslant e^{\lambda \text{ Re } z} + e^{-\lambda \text{ Re } z} \qquad \text{d'où} \quad E\left(e^{\lambda|\text{ Re } z|}\right) \leqslant 2\prod_{k=1}^{n} \operatorname{ch}\,(\lambda \text{ Re } a_k)\,.$$

Or, par 1 :

$$\operatorname{ch}\left(\lambda \text{ Re } a_k\right) \leqslant \exp\left(\frac{\lambda^2}{2} \mid \text{Re } a_k\mid^2\right).$$

Le résultat s'en déduit.

b) Une preuve tout à fait analogue donne :

$$E\left(e^{\lambda|\ \mathrm{Im}\ z|}\right) \leqslant 2\exp\left(\frac{\lambda^2}{2}\sum_{k=1}^{n}|\ \mathrm{Im}\ a_k|^2\right).$$

D'autre part, l'inégalité triangulaire et l'inégalité de Cauchy-Schwarz impliquent :

$$E\left(e^{\lambda|Z|}\right) \leqslant E\left(e^{\lambda|\ \mathrm{Re}\ z|}e^{\lambda|\ \mathrm{Im}\ z|}\right) \leqslant \sqrt{E\left(e^{2\lambda|\ \mathrm{Re}\ z|}\right)\ E\left(e^{2\lambda|\ \mathrm{Im}\ z|}\right)},$$

d'où le résultat.

C.1.a) On a :

$$\int_0^{2\pi}\exp\left(\lambda\,|Z_t(\omega)|\right)\,\mathrm{d}t = \int_0^{2\pi}\exp\left(\lambda|p_\omega(t)|\right)\,\mathrm{d}t.$$

D'après **IV.A**.3 et par périodicité de p_ω, il existe une partie de $[0,2\pi]$ constituée d'un ou deux segments, de mesure $1/\alpha_n$, sur laquelle $|p_\omega|$ est minoré par $M(\omega)/2$. Le résultat suit alors par positivité de exp.

b) Gr,ce à a) :

$$\frac{1}{\alpha_n}E_\omega\left(e^{\lambda M/2}\right) \leqslant E_\omega\left(\int_0^{2\pi}e^{\lambda|Z_t(\omega)|}\,\mathrm{d}t\right).$$

Mais le théorème de Fubini (qui revient dans ce cas à permuter une somme finie et une intégrale) donne :

$$E_\omega\left(\int_0^{2\pi}e^{\lambda|Z_\omega(t)|}\,\mathrm{d}t\right) = \int_0^{2\pi}E_\omega\left(e^{\lambda|Z_t(\omega)|}\right)\,\mathrm{d}t.$$

Or, gr,ce à la question **IV.B**.3.b) :

$$E_\omega\left(e^{\lambda|Z_t(\omega|}\right) \leqslant 2\exp\left(\lambda^2\sum_{k=1}^{n}|a_k|^2\right).$$

On en déduit la majoration annoncée.

2.a) Il existe ω dans Ω tel que :

$$\exp\left(\frac{\lambda M(\omega)}{2}\right) \leqslant E\left(e^{\lambda M/2}\right)$$

donc tel que :

$$\frac{\lambda M(\omega)}{2} \leqslant \ln\left(4\pi\alpha_n\right) + \lambda^2\sum_{k=1}^{n}|a_k|^2.$$

Le résultat suit.

b) Le résultat de a) s'applique pour tout $\lambda > 0$. On l'optimise en prenant :

$$\lambda = \sqrt{\frac{\ln(4\pi\alpha_n)}{\sum_{k=1}^{n}|a_k|^2}},$$

et on obtient l'inégalité de Salem-Zygmund.

(La conséquence de l'inégalité de Salem-Zygmund utilisée dans la partie **V** pourrait être remplacée par la construction de la suite de polynômes de Rudin-Shapiro, plus élémentaire mais n'utilisant pas d'arguments probabilistes.)

3. Prenons :

$$a_k = \begin{cases} 1 & \text{si} \quad k \in \Lambda \\ 0 & \text{si} \quad k \notin \Lambda \end{cases},$$

et appliquons 2.b) pour obtenir ω dans Ω tel que :

$$\left\| \sum_{k=1}^{n} a_k X_k(\omega)\ e_k \right\|_\infty \leqslant 4\sqrt{\ln(4\pi\alpha_n)\,|\Lambda \cap \{1,\ldots,n\}|}.$$

Puisque Λ est de Sidon, on a aussi :

$$K(\Lambda)\ \left\| \sum_{k=1}^{n} a_k X_k(\omega) e_k \right\|_\infty \geqslant \sum_{k=1}^{n} |a_k X_k(\omega|\,.$$

Or $\displaystyle\sum_{k=1}^{n} |a_k X_k(\omega| = |\Lambda \cap \{1,\ldots,n\}|$. On en déduit le résultat demandé.

Partie V

1. La question **I.B**.3.b) assure que (L_k) converge uniformément vers 0 sur I_η. Gr,ce au théorème de Cesàro, on en déduit :

$$\frac{1}{n}\sum_{k=1}^{n} \sup\{|L_k(x)|,\ x \in I_\eta\} \quad \to \quad 0.$$

Mais, si $(t,x) \in \mathbf{R} \times I_\eta$:

$$|u_n(t,x)| \leqslant \frac{1}{n}\sum_{k=1}^{n} \sup\{|L_k(x)|\,,\ x \in I_\eta\}\,,$$

d'où le résultat.

2. Gr,ce à **I.B**.2, on a :

$$u_n(t,1) = \frac{1}{n}\sum_{k=1}^{n} \delta_{k,n} e^{i\sqrt{k(k+1)}t}.$$

Les résultats de **III.B**.3 et **I.A**.2.b) montrent que $\Lambda = \left\{\sqrt{k(k+1)},\ k \in \mathbf{N}^*\right\}$ est un ensemble de Sidon avec $K(\Lambda) \leqslant 4$. Il s'ensuit que $\sup_{t\in\mathbf{R}} |u(t,1)| \geqslant 1/4$. On montre de même : $\sup_{t\in\mathbf{R}} |u_n(t,-1)| \geqslant 1/4$.

3.a) Ecrivons, avec **I.B**.1.b) :

$$\begin{aligned} v_n(t,x) &= \frac{1}{n}\sum_{k=1}^{n}\frac{\delta_{k,n}}{2\pi}\int_{-\pi}^{\pi}\left(x+i\sqrt{1-x^2}\sin\theta\right)^k \mathrm{d}\theta\, e^{i(2k+1)t/2} \\ &= \frac{1}{2\pi}\int_{-\pi}^{\pi}\frac{1}{n}\sum_{k=1}^{n}\delta_{k,n}\left(\left(x+i\sqrt{1-x^2}\sin\theta\right)e^{i(2k+1)t/2}\right)^k \mathrm{d}\theta \\ &= \frac{1}{2\pi n}\int_{-\pi}^{\pi} R_n\left(\left(x+i\sqrt{1-x^2}\sin\theta\right)e^{i(2k+1)t/2}\right)\mathrm{d}\theta \end{aligned}$$

On a :

$$\left|\left(x+i\sqrt{1-x^2}\in\theta\right)e^{i(2k+1)t/2}\right|^2 = x^2+(1-x^2)\sin^2\theta \leqslant 1.$$

Le principe du maximum entraîne, pour tout (t,x,θ) de $\mathbf{R}\times[-1,1]\times[-\pi,\pi]$:

$$\left|R_n\left(\left(x+i\sqrt{1-x^2}\sin\theta\right)e^{i(2k+1)t/2}\right)\right| \leqslant \sup_{u\in\mathbf{R}}\left|R_n(e^{iu})\right|.$$

Le résultat suit.

b) La question précédente et le choix de R_n assurent :

$$\forall (t,x)\in\mathbf{R}\times[-1,1], \qquad |v_n(t,x)| \leqslant 4\sqrt{\frac{\ln(4\pi\alpha_n)}{n}} \underset{n\to+\infty}{=} O\left(\frac{\ln n}{\sqrt{n}}\right).$$

Il reste à montrer que $(v_n - u_n)$ converge uniformément vers 0 sur $[-T,T]\times[-1,1]$ pour conclure. Or :

$$\begin{aligned} |v_n(t,x)-u_n(t,x)| &= \frac{1}{n}\left|\sum_{k=1}^{n}\delta_{k,n}L_k(x)\left(e^{i(k+1/2)t}-e^{i\sqrt{k(k+1)}t}\right)\right| \\ &\leqslant \frac{1}{n}\sum_{k=1}^{n}\left|e^{i(k+1/2)t}-e^{i\sqrt{k(k+1)}t}\right| \end{aligned}$$

car $|L_k|$ est majoré par 1 sur $[-1,1]$ gr,ce à **I.B**.2. Vu que $\varphi\mapsto e^{i\varphi}$ est 1-lipschitzienne sur $\mathbf{R}$, on a, si $t\in[-T,T]$:

$$\begin{aligned} \left|e^{i(k+1/2)t}-e^{i\sqrt{k(k+1)}t}\right| &\leqslant \left|(k+1/2)-\sqrt{k(k+1)}\right|.|t| \\ &\leqslant \left|k+1/2-\sqrt{k(k+1)}\right| T. \end{aligned}$$

La conclusion résulte du développement limité :

$$\sqrt{k(k+1)} = k\sqrt{1+1/k} = k\left(1+\frac{1}{2k}+O\left(\frac{1}{k^2}\right)\right) = k+\frac{1}{2}+O\left(\frac{1}{k}\right).$$

Rapport des correcteurs

Remarques générales sur les copies

Le problème était long. Il demandait de l'aisance dans les calculs, un certain recul sur les programmes des trois premières années de l'enseignement supérieur et la capacité de passer vite d'un domaine à un autre. Quelques candidats remarquables ont traité environ quatre parties. Beaucoup d'autres ont montré de réelles qualités mathématiques, soit en traitant quasi-complètement entre deux et trois parties soit en profitant de la variété des thèmes abordés pour résoudre un nombre très significatif de questions. Le nombre de copies faibles demeure cependant important. Souvent, ce ne sont pas tant les connaissances qui font défaut que la pratique. Ainsi, par exemple, la formule de Cauchy est connue mais beaucoup de candidats sont incapables de l'expliciter pour le chemin particulier proposé par l'énoncé, la définition du wronskien est donnée mais le calcul n'est pas fait, la structure des sous-groupes additifs de $\mathbf{R}$ est familière mais sa transposition aux sous-groupes multiplicatifs de $\mathbf{R}^{+*}$ pose problème... Les questions où il est demandé en un certain sens d'estimer une expression, qu'il s'agisse d'établir une inégalité (**I.B**.2), d'étudier une suite d'intégrales (**I.B**.3) ou d'appliquer le théorème des accroissements finis pour contrôler la taille d'une fonction sur un intervalle (**IV.A**.2) sont particulièrement révélatrices. Conseillons donc aux candidats de consacrer une partie de leur préparation à acquérir, par la pratique d'exercices ou de problèmes, ces réflexes de base que sont – pour citer J. Dieudonné – majorer, minorer encadrer.

Remarques sur les questions

I.A. Le 1.a) a parfois donné lieu à des précautions bien inutiles pour justifier l'existence de l'intégrale proposée ; certains candidats ne dominent pas la notion de partie presque nulle ! La question 2.a) a souvent mal été traitée à cause d'une mauvaise lecture de l'énoncé. Il ne s'agissait évidemment pas de montrer que la partie réelle d'une fonction bornée est bornée, mais d'utiliser la symétrie des cofficients pour établir une stabilité par conjugaison.

I.B. Dans la question 1.a), la formule de Cauchy est rarement citée avec précision. Beaucoup de copies oublient de considérer les cas limites $x = \pm 1$ dans 1.b). La détermination du maximum de L_n sur $[-1, 1]$ est rarement menée à bien : réponses fausses par suite de majorations trop grossières, voire aberrantes (résultat non réel). Parmi les candidats qui traitent 3, beaucoup utilisent un découpage et des majorations laborieuses plutôt que le théorème de convergence dominée, d'application immédiate ici.

I.C. La question 1.b) a été traitée par les candidats ayant eu le courage d'appliquer la formule de Leibniz. La question 2 a en général été correctement résolue. Il n'en va pas de même de 3 et 4, plus sélectives. Quelques candidats ont cependant indiqué une élégante solution de 4 ne suivant pas l'indication de l'énoncé mais faisant appel à un argument d'orthogonalité. Enfin, la question 5 a souvent été rédigée de façon approximative.

II.A. Un grand nombre de candidats ne voient pas que 1.b) est conséquence directe de 1.a). Dans la question 2.b), l'argument central (approximation pour se ramener à 2.a)) est souvent compris, mais rares sont les copies qui le mettent en forme de façon convaincante (l'équicontinuité des formes J_T est essentielle). Les questions 3 et 4 ont rarement été bien résolues.

II.B. Cette partie s'est révélée très sélective. La question 1 nécessitait de comprendre comment la dissociation se réflétait dans les coefficients d'un produit de Riesz et la question 2.a) ne pouvait être résolue qu'à l'aide du résultat de 1. Beaucoup de candidats ont préféré passer directement à la partie **III**.

III.A. En général 1.a) n'a pas posé de problème mais 1.b) qui s'en déduisait par le passage à l'exponentielle n'a pas été bien traité. Beaucoup de candidats ont résolu la question 2.a) ; 2.b) a souvent été comprise, les vérifications n'étant pas toutes faites en général. La question 3, en revanche, a été peu abordée.

III.B. Partie purement algébrique, dont les questions 1 et 2 ont été bien résolues par un nombre significatif de candidats. Il n'en est pas de même de 3, aboutissement de **II** et **III** nécessitant un recul important face au sujet.

IV.A. Très peu de bonnes réponses en 1 mais beaucoup d'inégalités fantaisistes ; un candidat brillant a amélioré le facteur quadratique $n(n+1)/2$ en utilisant Parseval pour p'. La question 2 était facile et son très faible succés a surpris les correcteurs.

IV.B. Cette partie établissait une inégalité probabiliste classique de Chernoff. Un certain nombre de candidats l'ont bien traitée.

IV.C. Après une application de Fubini (dans un cadre trivial) cette partie ne nécessitait que des calculs élémentaires. Mais elle arrivait tard dans le problème et peu de candidats l'ont abordée.

V. Cette partie n'a été abordée que par une poignée de candidats.

Épreuves orales d'algèbre et d'analyse

Organisation des épreuves

Les modalités, mises en place au concours 2001, ont cette année encore donné entière satisfaction et sont reconduites pour la session 2008. Elles sont décrites ci-après de manière détaillée, prenant en compte l'expérience acquise.

À l'issue de la période de préparation, le jury fait procéder à la photocopie des plans préparés par les candidats. Ces derniers sont manuscrits, comportent 3 pages A4 *au maximum* et possèdent une marge de 1 cm sur tous les côtés afin d'éviter tout problème lors de la photocopie. Il est conseillé de ne pas utiliser de stylos de couleurs, car les couleurs ne passent pas à la photocopie. Il est en revanche conseillé de soigner la présentation du plan écrit, de mettre des titres, d'encadrer les formules, etc. pour qu'il soit le plus lisible possible.
Les plans peuvent être complétés par des planches de figures.

Le candidat *peut utiliser sa copie du plan pendant l'épreuve* et pourra utiliser les notes manuscrites produites durant la préparation, pendant la première phase de l'interrogation dite « argumentation et présentation du plan ».

L'épreuve s'organise en trois temps, prévus pour une durée totale d'un maximum de 50 minutes : une présentation du plan éventuellement suivie d'une brève discussion, un développement de 15 minutes et enfin une partie consacrée au dialogue et aux questions.

Première partie : le plan

Le candidat est convié à utiliser son temps de parole, 8 minutes maximum, pour présenter, argumenter et mettre en valeur son plan.

Le plan écrit n'est ni une énumération de paragraphes, ni un exposé complet avec développement des démonstrations. Il définit avec précision les notions introduites, donne les *énoncés complets* des résultats fondamentaux, cite des exemples et des applications. *Le plan doit être maîtrisé*, c'est à dire que les résultats exposés doivent être compris ainsi que l'organisation d'ensemble. Il est souhaitable que le candidat connaisse dans leurs grandes lignes les démonstrations des résultats figurant au programme du concours : le jury pourra appliquer ce critère pour évaluer la maîtrise du plan. C'est au candidat de circonscrire son plan, notamment en ce qui concerne les énoncés débordant largement le cadre du programme.

Il s'agit d'une épreuve orale, il est donc inutile de recopier le plan au tableau, dans la mesure où le jury possède une copie du texte. Il est souhaitable que le candidat utilise son temps de parole pour expliquer de façon systématique les articulations principales de son plan. Les détails techniques, s'ils sont clairement écrits dans le plan, pourront ne pas être repris oralement. Le candidat peut faire un bref exposé introductif et commenter utilement ensuite ses résultats principaux, les outils développés, l'organisation d'ensemble et mettre en perspective

les méthodes utilisées. Il peut être utile de consacrer du temps à un exemple pertinent qui éclaire la problématique de la leçon, à faire usage du tableau pour illustrer ses propos. La présentation et la justification orale du plan sont des points importants d'appréciation.

Quelques rares candidats prennent des libertés quant au libellé de la leçon ; les titres des leçons définissent un champ clair qu'il faut traiter entièrement. Le hors sujet est lourdement sanctionné.

Le plan est rarement commenté. Le candidat se contente trop souvent d'une présentation linéaire du plan, sans en expliquer ou en mettre en valeur les articulations, ni faire ressortir les méthodes ou les résultats importants. Il en résulte parfois de (graves) incohérences dans l'ordre logique de présentation du plan.

Insistons sur le fait, encore une fois, que la recopie de plans, disponibles sur Internet ou dans des livres spécialisés, ne constitue pas un travail suffisant. L'exposé oral ne peut être maîtrisé s'il ressemble à une récitation. La solidité de la maîtrise du plan, y compris dans les résultats simples, constitue un point essentiel de l'évaluation. Le jury veille à la cohérence du plan et des développements eu égard le niveau du candidat. Moins mais mieux ! En quelque sorte, les candidats en surchauffe ne seront pas avantagés. La compréhension profonde des notions présentées, leur assimilation personnelle et le rendu lors de l'exposé oral sont des éléments de notation. Si les plans sont en général d'un bon niveau, rappelons que la maîtrise du plan, c'est-à-dire la compréhension des notions présentées et des principaux théorèmes, est un élément essentiel dont le jury tient le plus grand compte.

Il faut faire effort de formalisation. Les candidats doivent maîtriser les quantificateurs et donner un énoncé mathématique entièrement correct (exemple : c'est le centre d'un p-groupe non trivial qui est non trivial).

À la fin de cette présentation, le jury peut questionner brièvement le candidat. Ce temps de dialogue permet au candidat de préciser certains aspects du plan, de développer l'argumentation et de justifier certains choix. On peut aborder quelques points techniques sans entrer dans des détails qui retarderaient le début du développement. Le jury ne cherche pas à déstabiliser le candidat.

Deuxième partie : le développement

Le candidat soumet au jury une liste de plusieurs points (deux au minimum, mais trois sont appréciés) qu'il propose de développer. Ceux-ci peuvent être soit la démonstration d'un théorème, soit la présentation d'un exemple significatif, soit le développement détaillé d'une partie délimitée du plan.

La pertinence de tous les développements proposés, *leur adéquation au sujet* et leur niveau de difficulté sont des éléments essentiels de la notation. Les candidats veilleront à proposer des développements qui permettent de mettre en valeur leur maîtrise technique, sans excéder leur capacité, à en faire un exposé clair et complet dans le temps imparti. Les développements manifestement hors sujet ou en dessous du niveau exigible de l'agrégation sont pénalisés par le jury.

Le jury choisit, parmi les propositions du candidat, le thème d'un exposé. Le jury refusera d'avantager par son choix de développement le candidat qui a concentré sa préparation sur un seul développement substantiel et intéressant, par rapport à ceux qui ont réellement préparé les deux ou trois développements demandés.

Le candidat dispose d'au plus 15 minutes pour ce développement détaillé, qui doit comprendre toutes les explications nécessaires à la compréhension du jury. Le candidat peut adopter un

rythme plus ou moins rapide, mais ne doit pas perdre sciemment son temps. On s'attend à ce que ***le candidat expose sans le support de ses notes*** (sauf exception éventuelle sur un énoncé très technique, pour lequel le candidat sera convié par le jury à consulter ses notes si le besoin s'en fait sentir). La clarté de cet exposé, l'aisance et la sûreté avec lesquelles il est présenté constituent un facteur important d'appréciation

L'exposé doit être complet, sans suppression d'étapes intermédiaires, ni report d'argumentation techniques dans des résultats *ad hoc* admis. En particulier la technique qui consiste à admettre un « lemme préliminaire » qui contient toute la difficulté de la preuve, est sanctionnée. Le jury peut intervenir durant le développement pour une précision, une correction ou une justification. L'intervention éventuelle du jury ne donne pas lieu à une extension de la durée totale de l'exposé.

Au terme du développement le jury peut poser des questions sur l'exposé pour s'assurer de la maîtrise et de la compréhension du sujet abordé.

Lors du développement le jury attend du candidat des explications sur le déroulement de la preuve et l'intervention pertinente des notions développées durant l'exposé oral ; il peut être opportun lors du développement de se référer explicitement au plan présenté. Rappelons que le développement doit être en rapport avec le sujet traité, la leçon présentée et le plan écrit. Le jury ne serait d'ailleurs pas mécontent de voir proposer plus fréquemment la démonstration de théorèmes importants. Par ailleurs les idées doivent être expliquées clairement. La récitation d'un développement est lourdement sanctionnée ; le jury veille à ce que les futurs enseignants comprennent ce qu'ils exposent et sachent exposer ce qu'ils comprennent. C'est une qualité essentielle d'un futur agrégé.

On ne saurait trop conseiller aux candidats d'illustrer leur développement (et éventuellement leur plan) par un ou plusieurs dessins : l'exposé y gagne en clarté pour le jury, le candidat peut ainsi montrer un souci louable de pédagogie et cela lui permet de mieux comprendre les notions exposées : on a vu, par exemple, cette année un développement sur la fonction de Cantor – sans un dessin – où la candidate s'est avérée n'avoir aucune intuition de ce qui se passait dans sa démonstration.

Trop peu de candidats commencent leur développement par une rapide exposition des grandes idées ou étapes de ce dernier. Le jury aimerait avoir une petite explication de la démarche au début du développement. De cette absence d'explications préalables, il résulte parfois que le développement ressemble à une succession plus ou moins convaincante de résultats intermédiaires.

Dans le cas d'un développement ambitieux, il ne faut pas négliger les cas élémentaires. Certains candidats se sentent agressés ou déstabilisés quand on demande une précision d'un niveau qu'ils jugent trop faible : ils doivent répondre à la question simplement (sans dire que c'est trop simple), le jury s'assurant parfois seulement que les bases sont solides ; par exemple s'il y a un dénombrement à faire en début de développement il faut savoir justifier ses affirmations par une explication rapide orale et pas seulement énoncer brutalement : « Cet ensemble contient 24 éléments ».

Troisième partie : questions et dialogue

L'exposé est suivi d'une discussion au cours de laquelle le jury s'assure de la solidité des connaissances du candidat sur les questions précédemment abordées (plan, exposé) ou sur tout autre point en rapport avec le sujet et figurant au programme de l'oral. Un ou plusieurs exercices peuvent être proposés par le jury. Le jury peut à son gré poser des questions dans des champs connexes aux thèmes de la leçon, voire plus éloignés.

Durant cette partie, les exercices et questions posés permettent d'évaluer les réactions et les capacités techniques des candidats dans un champ vierge. Le candidat doit donc s'attendre à ce qu'un dialogue s'établisse, lui permettant de profiter de suggestions si le besoin apparaît au jury. Il peut adopter un style moins formalisé que dans le développement, s'appuyer sur le plan : la priorité est ici à l'élaboration des idées, à la méthode d'appréhension des problèmes mathématiques. Le jury peut parfois poser des questions difficiles pour lesquelles il n'attend pas de réponses immédiates ; cela lui permet d'évaluer les capacités de réflexion du candidat et de tester son esprit de méthode.

Pendant cette discussion le jury veille à laisser un temps raisonnable au candidat pour réfléchir, sans le submerger de questions.

Le candidat doit être conscient que s'il met un énoncé dans son plan il s'expose à des questions élémentaires et à des calculs éventuels sur ce point. Par exemple si l'on montre que la dimension d'un SETIM est un invariant pour une forme quadratique (indice), il faut savoir le calculer pour la forme quadratique $q(x,y) = x^2 + y^2$ dans $\mathbb{C}$; si l'on utilise les polynômes cyclotomiques, il faut pouvoir calculer Φ_6.

Une fois de plus, insistons sur le fait qu'il est essentiel de bien maîtriser ce que l'on propose. Encore trop de candidats proposent des résultats et des développements de très haut niveau sans pour autant maîtriser les bases. Par exemple, un candidat a proposé, dans une leçon sur les séries entières, le théorème d'Hadamard sur les séries lacunaires mais n'a pas su calculer $\sum_{n\geqslant 1} \frac{(-1)^{n-1}}{n}$.

Certains candidats, heureusement peu nombreux, ne sont pas assez combatifs et sollicitent le jury pour avoir de l'aide plutôt que de réfléchir par eux-mêmes. D'autres ne savent pas utiliser les théorèmes présents dans leur plan même sur des cas simples.

Oral d'Algèbre et géométrie

1. **Groupe opérant sur un ensemble :** Cette leçon est transversale. Les exemples doivent venir aussi de la géométrie et de l'algèbre linéaire, comme l'action à gauche de $GL(n)$ sur $Mat(n,p)$: savoir décrire les orbites des actions de groupes présentées.
2. **Sous-groupes distingués :** Il faut bien connaître le cas du groupe Σ_4, notamment $V_4 \hookrightarrow A_4 \hookrightarrow \Sigma_4$ et faire le lien avec le tétraèdre. En général le stabilisateur d'un élément n'est pas un sous-groupe distingué, contrairement à ce que le jury a pu entendre.
3. **Groupes finis de petit cardinal :** Après avoir cité les théorèmes fondamentaux sur les groupes, la leçon doit se concentrer sur les exemples. Les développements ne peuvent pas porter sur les théorèmes généraux. C'est une leçon bien distincte de le leçon "Groupes finis". Une bonne référence reste les exercices du chapitre 1 du livre de Perrin.
4. **Groupe des permutations d'un ensemble fini :** Les différentes formules pour la signature doivent être connues ; proposer comme développement que la signature est un morphisme n'est pas un développement substantiel au niveau de l'agrégation. Les candidats doivent faire le lien entre un sous-groupe d'ordre deux de Σ_n et le groupe A_n. Le lien entre le déterminant et la signature doit figurer dans cette leçon. Les éléments d'ordre 2 doivent être connus.
5. **Groupe linéaire $GL(E)$ et sous-groupes :** Cette leçon peut être traitée, ou comprise de plusieurs façons. En général on attend que le candidat précise à chaque instant quelle

structure il considère sur l'espace vectoriel E ; au départ E n'a pas de structure et on peut parler de $SL(E)$, k^*Id, des sous-groupes finis, du groupe dérivé en fonction du corps. Quand le corps est **R** on peut interpréter $SL(E)$ comme transformation conservant le volume et l'orientation. On peut ensuite considérer ce qui se passe si on choisit une base, un drapeau, une structure euclidienne, un produit hermitien. On peut traiter aussi le cas des sous-groupes finis de $SO(3)$.

6. **Anneaux $\mathbb{Z}/n\mathbb{Z}$:**
   On attend la description des sous-groupes additifs de $\mathbb{Z}/n\mathbb{Z}$. Attention en général si $d|n$, $\mathbb{Z}/d\mathbb{Z}$ n'est pas un sous-ensemble de $\mathbb{Z}/n\mathbb{Z}$. La description des éléments inversibles pour la structure multiplicative doit être connue. La structure des groupes abéliens de type fini doit être connue, il y a deux présentations distinctes (diviseurs élémentaires ou via les p-Sylow) ; il faut savoir passer de l'une à l'autre.
7. **Nombres premiers :** Cette leçon est classique et bien balisée, encore faut-il l'organiser de façon cohérente. Il est absurde de vouloir déduire que l'ensemble des nombres premiers est infini de la divergence de la série $\sum \frac{1}{p}$. Il peut être intéressant de consacrer une section à la répartition des nombres premiers, à des exemples de nombres premiers, à la recherche de nombres premiers, aux applications en algèbre, en géométrie. Par contre le choix du développement doit être bien réfléchi ; le candidat ne peut se contenter de proposer un théorème de Sylow sous prétexte qu'un nombre premier apparaît en cours de route, ou le critère d'Eisenstein.
8. **Anneaux principaux :** Bien mettre en évidence l'arithmétique sous-jacente. Les applications en algèbre linéaire sont appréciées. Il faudrait savoir pourquoi $A[X]$ est principal si et seulement si A est un corps. Il faut savoir aussi que $\mathbb{R}[X,Y]$ est factoriel et non principal et exhibant un idéal non principal. Connaître les théorèmes de transfert peut être utile.
9. **Corps finis :** Comprendre les sous-corps de $\mathbb{F}_{64}$ est un bon exercice, en particulier $\mathbb{F}_{16}$ n'est pas un sous-corps de $\mathbb{F}_{64}$.
10. **Groupe des nombres complexes de module 1 :** Il y a trois réalisations de ce groupe, $SO(2)$, $U(1)$ et $\mathbb{R}/\mathbb{Z}$. Chacune est reliée à un aspect géométrique, algébrique, arithmétique. C'est l'occasion de s'interroger sur l'exponentielle complexe, ce qu'est le nombre π, la mesure des angles. Quelle place trouve la suite exacte $2\pi\mathbb{Z} \hookrightarrow \mathbb{R} \underset{t\mapsto\exp(it)}{\longrightarrow} U(1)$? Y-a-t-il une section continue ?
11. **Corps des fractions rationnelles :** La décomposition en éléments simples sur $\mathbb{R}$ ou $\mathbb{C}$ doit être maîtrisée. On fera attention au point suivant, souvent mal compris : la décomposition sur $\mathbb{R}$ ne résulte pas de celle sur $\mathbb{C}$ par regroupement comme le jury l'a entendu à maintes reprises. On pourra s'en convaincre en étudiant le cas $\frac{1}{(X^2+X+1)^3}$.
    Le lien avec les développements limités doit être compris. Les développements de cette leçon doivent éviter l'écueil du hors sujet.
12. **Polynômes irréductibles :** Des informations sur le degré du corps de rupture et du corps de décomposition d'un polynôme irréductible de degré d sont utiles : d dans le premier cas, $d!$ dans le second. Le candidat peuvent réfléchir à l'exercice suivant : exhiber un isomorphisme entre $\mathbb{R}[X]/(X^2+X+1)$ et $\mathbb{R}[X]/(X^2+1)$.
13. **Algèbre des polynômes à n indéterminées, polynômes symétriques :** Le théorème principal sur la structure de l'algèbre des polynômes symétriques et l'algorithme qui va

avec doivent être connus et pratiqués sur des exemples. Trop peu d'applications sont proposées par les candidats.

14. **Dimension d'un espace vectoriel, rang :** Contrairement aux apparences, cette leçon classique présente des difficultés sur la logique de présentation, la cohérence du plan et le traitement intégral du sujet ! Les exemples doivent mettre en évidence la notion de rang ou dimension, par exemple en dualité, dans les formes quadratiques et bien-sûr sur les matrices. Le jury accepte que soit proposé en développement le traitement précis de points du cours, par exemple on peut proposer "Théorème de la dimension + base incomplète + dimension d'un sous-espace". Ne proposer que le théorème de la base incomplète n'est pas suffisant au niveau de l'agrégation.
15. **Matrices équivalentes. Matrices semblables, Opérations sur les lignes et les colonnes :** Bien distinguer les opérations à gauche des opérations à droite. L'une opère sur les lignes, l'autre sur les colonnes. L'une permet de trouver les équations de l'image et l'autre une base du noyau. La notion de matrice échelonnée pourra être introduite. Rappelons que $A = PB$ avec A, B des matrices de $Mat(n, p, \mathbb{K})$ est équivalent au fait que on peut passer des A vers B par manipulation des lignes et est équivalent au fait que A et B ont même noyau.
16. **Déterminant :** On reprend le commentaire du rapport 2006 qui reste d'actualité.

    Les candidats ont recopié de mauvais plans sur Internet en oubliant les propriétés importantes du déterminant ; volume, orientation, discussion du rang grace aux bordantes. Le jury ne peut se contenter d'un Vandermonde ou d'un déterminant circulant dans un plan !

    Signalons que les candidats qui ont proposé comme développement des thèmes trop éloignés de la leçon ont tous été sanctionnés. Par exemple le calcul de la distance à un sous-espace vectoriel ne peut pas constituer un développement substantiel. On ne peut pas présenter le théorème de Müntz sans présenter le calcul du déterminant de Cauchy préalablement. D'une manière générale on attend pendant le développement l'illustration d'un calcul ou la manipulation de déterminants non triviaux et pas uniquement l'extraction d'un résultat du plan.
17. **Réduction d'un endomorphisme en dimension finie :** Cette leçon ne peut se réduire à la diagonalisation. Dans la décomposition de Dunford $f = d + n$, le fait que d et n sont des polynômes en f doit être signalé. L'utilisation des polynômes d'endomorphisme est certainement utile dans cette leçon. On doit savoir que 0 est une racine simple du polynôme minimal si $\{0\} \neq \ker(A) = \ker(A^2)$. On pourra s'interroger sur les classes de similitudes de matrices parmi les matrices ayant un polynôme caractéristique donné.
18. **Sous-espaces stables :** On constate une amélioration dans le traitement de cette leçon. Les conseils des années précédentes commencent à être compris. Toutefois les candidats mal préparés confondent cette leçon avec la leçon de réduction. Il est bien évident que cette leçon est difficile. Les candidats doivent savoir déterminer tous les sous-espaces stables d'une matrice 3×3 ou d'une matrice diagonalisable ou d'une matrice réduite à un seul bloc de Jordan.
19. **Exponentielle de matrices :** La notion de groupe à un paramètre peut être introduite. On fera attention aux choix des développements qui ne peuvent aller trop vers l'analyse. Dans le cas diagonalisable, les projecteurs sont utiles pour le calcul de l'exponentielle. On

pourra par exemple essayer de calculer l'exponentielle de la matrice

$$\begin{pmatrix} 1 & * & * & * \\ 0 & 2 & * & * \\ 0 & 0 & 3 & * \\ 0 & 0 & 0 & 4 \end{pmatrix}.$$

On pourra par exemple étudier, pour $A \in Mat(n, \mathbb{C})$ l'application exponentielle de $\mathbb{C}[A]$ dans $\mathbb{C}[A]$ et montrer comment les notions topologiques peuvent intervenir utilement pour montrer que l'exponentielle est surjective de $Mat(n, \mathbb{C})$ sur $GL(n, \mathbb{C})$.

20. **Endomorphismes nilpotents :** Il y a un nombre fini de classes de conjugaison. On peut avantageusement étudier l'application exponentielle sur le cône des matrices nilpotentes. Attention à ne pas se perdre dans les détails inutiles concernant le logarithme d'une matrice unipotente ou l'exponentielle d'une matrice nilpotente. L'utilisation des séries formelles ou des développements limités sont bien utiles. Les matrices nilpotentes de rang r ne sont pas toutes conjuguées entre elles.
21. **Polynômes d'endomorphismes :** Ils ne sont pas tous nuls ! Les candidats doivent connaître sans hésiter la dimension de l'algèbre $\mathbb{K}[f]$. La notion de commutant d'un endomorphisme doit être comprise par les meilleurs. Les polynômes d'endomorphismes permettent de calculer les puissances d'un endomorphisme. On fera le lien avec les suites récurrentes linéaires ou les équations différentielles linéaires d'ordre n. On n'exige pas le théorème du bicommutant.
22. **Formes quadratiques. Orthogonalité. Isotropie :** Le cône isotrope est un aspect important de cette leçon. Il existe des formes quadratiques sur $\mathbb{C}$, contrairement à ce que beaucoup de candidats affirment et il y a une différence entre formes quadratiques sur $\mathbb{C}$ et formes hermitiennes !

    Il peut être utile de faire le lien, même de manière élémentaire, avec la géométrie (coniques, calcul de tangentes, polaires, étude locale des fonctions etc.).

    L'algorithme de Gauss doit être énoncé et pouvoir être appliqué sur une forme de $\mathbb{R}^3$. Le lien avec la signature doit être clairement énoncé. Il est important d'illustrer cette leçon d'exemples.
23. **Formes linéaires et hyperplans :** Savoir calculer la dimension d'une intersection d'hyperplans est au cœur de la leçon. L'utilisation des opérations élémentaires sur les lignes et les colonnes permet facilement d'obtenir les équations d'un sous-espace vectoriel ou d'exhiber une base d'une intersection d'hyperplans. Cette leçon peut être traitée transversalement : géométrie algèbre et topologie.
24. **Méthodes combinatoires**

    Il est essentiel que des méthodes soient dégagées et illustrées : principe de récurrence, principe d'inclusion-exclusion, principe des bergers, le tout est la somme des parties, utilisation de séries entières (génératrices), etc. Chaque méthode doit être illustrée par des exemples.

    La partie élémentaire de cette leçon ne doit pas être oubliée. Notamment le jury s'attend à ce que les candidats sachent calculer des cardinaux classiques.

25. **Isométries d'un espace affine euclidien de dimension 2 ou 3 :** La classification doit être parfaitement connue. Théorème de décomposition commutative. En dimension 3 : déplacements (translation, rotations, vissage) ; antidéplacements (symétries planes,

symétries glissées, et isométrie négative à point fixe unique).

Leçons de géométrie : commentaire global

En général les leçons de géométrie n'ont eu que peu de succès comme souvent : c'est un tort. Il semble impossible d'obtenir un dessin de la part des candidats. C'est encore une fois un non sens mathématique, pédagogique et historique de ne pas vouloir illustrer la géométrie ou les mathématiques par le dessin.

Pour certains candidats, il serait plus profitable de travailler des leçons de géométrie, même à un niveau élémentaire, plutôt que de choisir des sujets d'algèbre générale qu'ils ne maîtrisent pas.

Ces leçons ont été pauvres, montrant un manque flagrant de préparation alors que ces thématiques sont enseignées au niveau des lycées et des classes préparatoires.

26. **Coniques :** Bien distinguer les notions affines, métriques (projectives). Le centre est une notion affine, le foyer est une notion euclidienne. Il faut savoir trouver le centre d'une ellipse, situer le paramètre, les asymptotes d'une hyperbole et connaître quelques formules célèbres et élémentaires.
27. **Barycentres. Convexité :**

    Il faut noter que de nombreux candidats sont pénalisés par des notations assez lourdes et un cadre théorique peu commode. Ne pas déséquilibrer la leçon.
28. **Utilisation des groupes en géométrie :** C'est une leçon transversale et difficile. On ne peut prétendre avoir une bonne note si elle n'est pas préparée.
29. **Angles, définition et utilisation en géométrie :**

    Le minimum est exigible sur l'exponentielle complexe et le calcul d'un argument. Bien soigner la présentation de la mesure des angles. Savoir donner une condition nécessaire et suffisante pour que la somme de trois vecteurs unitaires soit nulle en utilisant les nombres complexes.
30. **Homographies de la droite complexe.** Les applications aux suites homographiques sont les bienvenues. L'utilisation du birapport en géométrie est indispensable.
31. **Problèmes d'angles et distance en dimension 2 et 3 :** On fera attention à ne pas confondre cette leçon avec une leçon de géométrie globale. Les problèmes affines déguisés en problèmes euclidiens ne peuvent prétendre constituer l'essentiel de la leçon.

Oral d'analyse et probabilités

1. **Espaces de fonctions. Exemples et applications :** Leçon de synthèse qui a permis à de très bons candidats de faire un exposé parfois brillant. Bien entendu, l'exhaustivité est à proscrire, le candidat doit choisir les thèmes et les espaces fonctionnels dont il souhaite présenter les propriétés.

   Voici quelques remarques ponctuelles. Le théorème d'Ascoli est souvent présenté pour l'espace $\mathcal{C}(X;Y)$ où X et Y sont des espaces métriques compacts et les candidats sont bien embarrassés lorsqu'on leur demande ce qu'il en est de l'espace $\mathcal{C}(X;\mathbb{R})$. Il est bon également de citer des applications de ce théorème fondamental, par exemple concernant les opérateurs intégraux à noyau continu, le théorème de Peano, etc. Pour la caractérisation du dual des espaces L^p, les candidats se contentent du cas $1 \leqslant p \leqslant 2$, on ne peut ignorer le cas $2 \leqslant p < \infty$.

2. **Utilisation de la notion de compacité :** Dans cette leçon, il est souhaitable de présenter un théorème utilisant la méthode diagonale ; les candidats n'ont que l'embarras du choix : théorèmes d'Ascoli, de Montel, compacité faible séquentielle de la boule unité d'un espace de Hilbert, etc.
3. **Théorèmes de point fixe. Exemples et applications :** Le théorème de Peano est parfois présenté comme application du théorème de Schauder. Présenter un tel développement lorsqu'on n'a aucune idée de la démonstration des théorèmes d'Ascoli, Brouwer et Schauder est quelque peu gênant. Signalons que la méthode très ingénieuse (et simple !) de Carathéodory permet d'obtenir le résultat à l'aide du seul théorème d'Ascoli.
4. **Prolongement de fonctions. Exemples et applications :** En ce qui concerne le théorème de prolongement des applications uniformément continues, on ignore bien souvent la version linéaire, alors qu'elle peut être l'objet de développement intéressant, tel que le théorème de Plancherel, par exemple. Quant au prolongement de la fonction Γ en une fonction méromorphe dans tout le plan complexe, il serait bon de savoir que la relation fonctionnelle $\Gamma(z+1) = z\,\Gamma(z)$ permet de le faire en quelques lignes.
5. **Applications linéaires continues entre espaces vectoriels normés. Exemples et applications :** Lister tous les théorémes de Banach ne constitue pas un test très probant, il serait plus intéressant de se limiter à quelques énoncés en les illustrant par des exemples significatifs, par exemple dans la théorie des séries de Fourier.
6. **Utilisation de la dimension finie en analyse :** Les candidats devraient s'interroger sur l'intérêt de disposer d'une caractérisation topologique de la dimension finie.
7. **Bases hilbertiennes. Exemples et applications :** Cette leçon permet de parler de polynômes orthogonaux et de donner des exemples de bases hilbertiennes dans des espaces L^2, mais les candidats ont bien du mal à en déduire des bases hilbertiennes de $L^2(\mathbb{R})$.
8. **Différentiabilité :** Les leçons concernant les applications différentiables restent parfois extrêmement formelles. Des théorèmes, tel que le théorème des fonctions implicites, doivent être illustrés par des exemples géométriques. Il est également surprenant de voir un candidat incapable de déterminer l'espace tangent à une courbe paramétrée.
9. **Suites et séries :** Le jury a constaté que ces leçons, apparemment élémentaires, pouvaient être l'objet d'exposés originaux et fort intéressants. La leçon sur les développements asymptotiques doit comporter des méthodes générales, par exemple la méthode de Laplace, avec des exemples significatifs (fonctions spéciales).
10. **Fonctions monotones. Fonctions convexes. Exemples et applications :** Les propriétés de dérivabilité des fonctions convexes sont en général mal connues. Il est d'autre part indispensable d'expliquer clairement les relations entre la monotonie et la convexité. Un développement souvent proposé concerne les inégalités de Hölder et de Minkowski pour des familles finies de réels, alors qu'il est plus simple (et plus général) de traiter le cas des fonctions mesurables positives. La signification topologique de ces inégalités est rarement expliquée, ceci est regrettable. Ce développement, relativement modeste, pourrait être étoffé en montrant comment ces inégalités permettent d'exhiber d'autres fonctions convexes, par exemple la convexité logarithmique de la fonction Γ .
11. **Intégration :** Les candidats choisissant ces leçons ont en général de bonnes connaissances sur le sujet. Certains éprouvent le besoin de parler de l'intégrale de Riemann, ceci n'a qu'un intérêt limité si on se contente des résultats les plus élémentaires reposant sur la convergence uniforme.

12. **Fonctions holomorphes :** Dans ce domaine, les leçons sont en général d'un bon niveau. Le théorème de Cauchy est souvent énoncé sous une forme particulière en prenant l'intégrale le long du bord d'un disque, alors que, pour le théorème des résidus, on considère des compacts à bord régulier ; ceci est assez incohérent. La définition d'une fonction méromorphe est parfois erronée l'ensemble des pôles doit être une partie fermée et discrète.

Compléments

On conseille la lecture des rapports 2005 et 2006 sur les épreuves d'oral d'algèbre, d'analyse et de probabilité, les conseils qui y sont prodigués restent d'actualité.

Épreuve orale de modélisation

Organisation de l'épreuve de modélisation

Depuis la session 2006 incluse, deux textes au choix sont proposés à l'épreuve de modélisation. Le jury souhaite rappeler ce qu'il attend des candidats dans cette épreuve. Les remarques concernant l'organisation de l'épreuve de modélisation s'appliquent à toutes les options, y compris à l'épreuve d'« analyse des systèmes informatiques » qui en est la version pour l'option D (informatique). Des remarques supplémentaires, spécifiques à cette épreuve, seront données plus loin, dans le cadre de la partie du rapport consacrée à l'option informatique.

Les textes sont surmontés du bandeau suivant :

> *Il est rappelé que le jury n'exige pas une compréhension exhaustive du texte. Vous êtes laissé(e) libre d'organiser votre discussion comme vous l'entendez. Des suggestions de développement, largement indépendantes les unes des autres, vous sont proposées en fin de texte. Vous n'êtes pas tenu(e) de les suivre. Il vous est conseillé de mettre en lumière vos connaissances à partir du fil conducteur constitué par le texte. Le jury appréciera que la discussion soit accompagnée d'exemples traités sur ordinateur. Le jury aura le texte sous les yeux, mais vous devez considérer qu'il ne l'a pas lu.*

Plus précisément, le jury s'attend à ce que le candidat dégage une problématique, en s'inspirant du texte, pour mettre en valeur sa maturité mathématique et ses connaissances. L'interrogation dure une heure, pendant laquelle le candidat gère comme il le désire le tableau et les illustrations informatiques qu'il entend présenter (le jury dispose d'écrans de contrôle reproduisant celui du candidat). Le candidat doit préparer un exposé d'environ 3/4 d'heure, le quart d'heure restant étant occupé par les questions du jury.

Le texte est court, environ 5 pages, motivé par un problème concret. Il peut présenter des arguments rapides, voire heuristiques (signalés comme tels). Il ne contient pas d'assertion délibérément trompeuse et se conclut par une liste de suggestions.

Il appartient au candidat de discuter la mathématisation du problème, en particulier d'expliquer les hypothèses faites lors de la modélisation ou du traitement du modèle, de critiquer ou d'améliorer le modèle, du point de vue de l'adéquation à la réalité, de la généralité, de la rigueur, de la simplicité du traitement mathématique subséquent...

Le jury n'ayant *a priori* pas lu le texte, le candidat commencera par présenter celui-ci. Un plan en début d'exposé est apprécié, annonçant en particulier les propriétés du modèle que le candidat va dégager. Il est important d'expliquer le problème et le modèle, de l'illustrer, ainsi que d'y revenir en fin d'exposé. Le modèle mathématique a-t-il les propriétés attendues ? Des propriétés parasites surprenantes ? A-t-on résolu le problème posé ?

Le candidat dispose pendant sa préparation et l'interrogation d'un ordinateur dont la configuration est décrite sur le site de l'agrégation de mathématiques, à l'adresse `http://www.agreg.org`.

Il est vivement souhaité que des illustrations informatiques (simulation, résolution numérique ou formelle, cas particuliers éclairants...) soient présentées, mais *il ne s'agit pas d'une épreuve*

de programmation. Un programme qui ne fonctionne pas n'est en rien rédhibitoire et le jury appréciera un regard critique du candidat sur une tentative non aboutie. Une utilisation raisonnée des fonctions des logiciels disponibles est plus appréciée qu'une reprogrammation d'algorithmes standards. Bien intégré dans l'exposé, un tel travail peut en revanche devenir pertinent pour illustrer les insuffisances d'une méthode naïve.

Les suggestions sont facultatives et ne sont là que pour guider la réflexion du candidat sur des points significatifs du texte, ou des exemples utilisables. Certaines d'entre elles sont conçues pour permettre au candidat de comprendre le problème, de «rentrer» dans le modèle.

S'il est exclu de plaquer une démonstration d'un théorème du programme dans l'exposé, les démonstrations mathématiques de certaines assertions du textes sont très appréciées. Le candidat peut, tout comme le texte, utiliser des arguments heuristiques s'il les signale comme tels.

Un travers à éviter à tout prix : la paraphrase linéaire du texte sans aucun apport personnel du candidat, ni mise en perspective, agrémentée de la recopie de toutes les formules rencontrées.

Recommandations du jury

Le jury attache un intérêt particulier à l'effort de modélisation (qu'on peut définir comme le passage du « concret » aux mathématiques), à la mise en perspective des applications présentées, ainsi qu'aux illustrations permises par les moyens informatiques mis à disposition des candidats.

Le principal travers observé chez les candidats est la répétition linéaire du texte, y compris des passages non compris en espérant que le jury ne demandera pas de détails. Rappelons qu'utiliser des notions que l'on ne comprend pas, dans cette épreuve comme dans les autres, est une faute lourdement sanctionnée. Enfin, rappelons qu'*aucun développement n'est attendu.* Le candidat est libre de proposer des démonstrations de résultats utilisés, mais le jury peut les refuser, ou demander au candidat d'en donner seulement les grandes lignes.

Quelques qualités appréciées : prise de distance et d'initiative par rapport au texte, étude d'un exemple ou d'un cas simple pour comprendre le texte et le faire comprendre au jury, simplification ou, à l'inverse, généralisation du problème proposé, étude qualitative ou heuristique, critique du modèle.

Option A : probabilités et statistiques

Sur le plan

Il est demandé aux candidats de présenter un plan *succint* de leur exposé, sachant que le jury ne connait a priori pas le détail du texte choisi, mais qu'il en a une copie sous les yeux. Bien que ce fait soit indiqué aux candidats à leur arrivée, beaucoup d'entre eux se lancent dans de *longues paraphrases* du texte, sans mettre clairement en évidence la problématique et les points qu'ils ont traités ou abordés. Il en résulte souvent une mauvaise gestion du temps imparti.

Sur la présentation

Nombre de candidats semblent oublier que l'agrégation est un concours visant à recruter des *enseignants*.

Gestion anarchique du tableau, fautes linguistiques, voix à peine audible, manque de clarté syntaxique, écarts par rapport au plan annoncé, sont autant de phénomènes encore trop fréquents auxquels le jury est évidemment sensible. De surcroît, trop de candidats peinent à effectuer des calculs analytiques clairs, corrects et lisibles.

L'exposé doit être un dosage dynamique entre preuves mathématiques, illustrations informatiques, critiques éventuelles du texte, réponse aux questions et mise en lumière de connaissances.

Connaissance du progamme

Les jurys notent, hélas, encore trop de lacunes sur des *points fondamentaux* du programme. On peut parfois avoir l'impression que certains candidats (heureusement peu nombreux) se sont fourvoyés dans le choix de leur option et se présentent en ignorant totalement le calcul des probabilités et les statistiques. Ainsi, parmi les florilèges, on a pu voir plusieurs candidats prétendre que l'espérance d'une somme de variables aléatoires est égale à la somme des espérances à condition que ces variables soient indépendantes. D'autre part, lors de la discussion avec le candidat, le jury ne s'interdit pas de poser des questions de nature statistique pour des textes à coloration probabiliste et inversement. Un nombre croissant de textes mêlent d'ailleurs les deux aspects. Le jury encourage donc les candidats et les préparateurs à tenir compte de l'ensemble du programme.

Probabilités

- L'énoncé correct de la loi des grands nombres est ignoré de beaucoup de candidats, lesquels confondent allégrement les convergences presque sûre et en loi !
- Les inégalités de base de type Markov ou Tchebitchev sont quelquefois ignorées.
- Les propriétés fondamentales des chaînes de Markov sont souvent mal connues : classification des états, conditions de convergence vers la loi stationnaire (apériodicité), etc. L'équation de base satisfaite par la mesure invariante est fréquemment écrite de façon erronée. De nombreux candidats sont incapables d'expliquer la manière d'exploiter une trajectoire d'une chaîne de Markov.
- Les propriétés spectrales des matrices de transitions sont souvent ignorées, notamment l'égalité entre le nombre de valeurs propres sur le cercle unité et la période dans le cas irréductible. Trop de candidats n'arrivent pas à faire la liaison avec les théorèmes de Perron-Frobénius.
- La notion d'espérance conditionnelle est mal maîtrisée, tant dans sa définition que dans son utilisation, et certains candidats hésitent quant à l'interprétation en terme de projecteur orthogonal. D'autre part, il ne suffit pas de pouvoir calculer la loi de X_{n+1} sachant X_n pour en déduire que X_n est une chaîne de Markov.
- La définition des martingales est très souvent imprécise. Les théorèmes du programme sur la convergence des surmartingales positives ne sont pratiquement jamais employés, alors qu'ils permettent des démonstrations convaincantes et simples dans de nombreux modèles.

Statistiques.

- Les notions élémentaires de statistique paramétrique ne sont pas toujours clairement définies. Certains candidats confondent souvent *l'estimation* d'un paramètre et *un test* sur un paramètre.
- Nombre de candidats ne savent pas les principes de construction d'un intervalle de confiance.

- Les estimateurs de la moyenne, de la variance, ainsi que la notion de biais sont quelquefois totalement ignorés.
- Certains candidats n'ont pas assimilé les bases du modèle linéaire gaussien. À ce propos, il faut noter que les estimés via les moindres carrés ne sont pas correctement compris : les tentatives pour les retrouver conduisent souvent les candidats à des calculs imprécis, voire surréalistes.
- Certains candidats confondent les théorèmes de Glivenko-Cantelli et de Kolmogorov-Smirnov, se montrant incapables d'expliquer leur utilité combinée pour la mise en place d'un test statistique. L'hypothèse de continuité de la fonction de répartition est assez souvent oubliée.

Utilisation de l'outil informatique

Certains candidats utilisent des logiciels non adaptés au problème traité. Par exemple Maple pour des calculs numériques ou matriciels classiques, alors que Matlab ou Scilab seraient plus efficaces.

Le jury incite les candidats à mettre en valeur leurs programmes informatiques, notamment en traçant des courbes et des graphiques pertinents. De trop nombreux candidats se bornent à coder des fonctions, sans les exploiter de manière parlante. Lors du commentaire d'un graphique, il est souhaitable de préciser la nature du tracé, des axes, des échelles, puis d'expliquer les aspects illustratifs et éventuellement prédictifs.

Option B : calcul scientifique

Remarque préliminaire :

comme pour les autres épreuves du concours, il est attendu à l'épreuve de modélisation que le candidat fasse la démonstration

- de ses connaissances mathématiques,
- de ses qualités pédagogiques.

En effet, l'épreuve s'appuie avant tout sur le socle des connaissances du programme d'analyse et d'algèbre.

Une des difficultés consiste bien sûr à faire appel à une très large palette d'outils mathématiques pour illustrer un propos scientifique donné. Le fait que les textes s'appuient le plus souvent sur un contexte hors du strict champ mathématique ne saurait en aucun cas être un prétexte à réduire la rigueur de l'argumentation. Les connaissances mathématiques du candidat peuvent notamment se manifester par sa capacité à détailler certains des points techniques évoqués succinctement dans le corps du texte, sans qu'il soit nécessaire que ces développements figurent d'emblée dans l'exposé du candidat. Ils pourront en revanche être demandés durant la phase de dialogue avec le jury.

La compréhension du texte

Le jury est agréablement surpris par les candidats capables d'appliquer un théorème compliqué qu'ils viennent de démontrer, à la situation simple proposée dans le texte, ou encore à même de proposer des exemples d'applications, pertinents et intéressants de ces mêmes résultats.

Le jury ne se contente pas d'une paraphrase pure et simple du texte. Le candidat est appelé à faire la preuve de sa compréhension des enjeux de modélisation du texte et de sa culture mathématique en développant les aspects du texte qui lui paraissent les plus intéressants.

Rappelons à ce propos qu'il n'est pas exigé de traiter ce dernier dans son intégralité et que les suggestions de développement placées en fin de texte ne sont nullement une liste de questions à traiter dans l'ordre ou exhaustivement.

L'exposition

Le jury est sensible à la clarté de l'exposition, à la qualité de l'organisation de l'exposé, à la gestion du temps de l'exposé et à l'exploitation conjointe du tableau et de l'ordinateur. Les candidats sont notamment invités à présenter brièvement au début de l'épreuve le plan suivant lequel leur propos est organisé.

Les connaissances mathématiques

L'épreuve de l'option B réclame en particulier des connaissances solides sur les éléments suivants qui ne sont pas toujours assez bien maîtrisés :

- Analyse des équations différentielles ordinaires et calcul différentiel : résultats d'existence-unicité, locale ou globale, du problème de Cauchy, comportement qualitatif des solutions, résolution complète d'équations différentielles simples, dérivation de fonctions de $\mathbb{R}^n$ dans $\mathbb{R}^m$, en particulier les fonctions composées.

- Schémas numériques pour les équations différentielles ordinaires : un point manifestement délicat du programme réside dans les notions de stabilité, consistance et convergence de schémas numériques sur lesquelles la grande majorité des candidats fait des confusions importantes.

- Notions de base en algèbre linéaire et résolution de systèmes linéaires : théorème du rang, conditionnement, méthodes directes et itératives, décomposition spectrale et recherche des éléments propres.

- Optimisation : existence d'extrema, méthodes de descente, gradient conjugué, convexité.

- Résolution approchée d'équations du type f (x) = 0, méthode de Newton.
- Notions élémentaires sur les équations aux dérivées partielles classiques (ondes, chaleur, transport, équations elliptiques en dimension 1...). Le candidat doit être capable d'évoquer les caractéristiques propres à ces équations, le comportement qualitatif de leurs solutions et doit connaître des méthodes de résolution, exactes et approchées, de ces problèmes.

En revanche, l'épreuve ne requiert pas d'expérience sur les notions de solutions faibles, ni de dextérité sur les espaces fonctionnels liés à la théorie des distributions.

En comparaison avec un passé pas si lointain, le jury se réjouit du fait que la grande majorité des candidats joue dorénavant le jeu du texte. Seule une très petite minorité persiste à ne voir dans les textes qu'un prétexte à replacer une leçon d'oral « classique » , attitude que le jury est contraint de sanctionner en espérant la voir totalement disparaître un jour.

L'outil informatique

Dans l'ensemble, le jury note avec satisfation que très peu de candidats esquivent toute illustration informatique ; d'ailleurs toute impasse en la matière est systématiquement sanctionnée. L'épreuve ne saurait être une épreuve de dextérité de programmation informatique ; de nombreux candidats présentent des simulations de qualité qui exploitent les routines standards des outils mis à leur disposition, sans les reprogrammer de A à Z. Les éléments valorisés sont :

- la pertinence de l'illustration choisie en rapport avec le propos du texte,
- la capacité à agrémenter les résultats numériques de commentaires et de critiques pertinentes,
- l'intuition, appuyée sur les notions du programme, sur les limites de la méthode numérique développée.

Les candidats dont l'illustration informatique n'est pas aboutie sont invités à présenter la démarche numérique qu'ils prévoyaient de mettre en œuvre : une démarche cohérente, avec des objectifs précis en rapport avec le texte, est aussi valorisée par le jury. Par ailleurs des erreurs bénignes de programmation peuvent être corrigées durant l'épreuve et ne sont pas pénalisantes.

À propos des équations différentielles

Les théorèmes de Cauchy-Lipschitz ou d'échappement font encore des ravages. Peu de candidats sont capables de montrer l'existence locale de solutions d'une équation différentielle ordinaire concrète : certains veulent l'appliquer à un problème d'ordre deux, d'autres à des espaces fonctionnels (en voyant, dans une équation $y' = f(y,t)$, la fonction f comme une distribution sur $C^1(\mathbb{R}) \times \mathbb{R}$ (?)), d'autres enfin introduisent des notions fines (cylindres de sécurité, fonctions localement lipschitziennes) sans être capables de les exploiter ni de les définir. Le jeu d'écriture permettant de réduire une équation d'ordre supérieur à un système d'ordre un est souvent mal compris. Très peu de candidats réalisent qu'une solution locale n'est pas nécessairement globale.

Algèbre et calcul formel

Quelques défauts généraux signalés

- Il est regrettable que des candidats s'appuyent sur les exemples donnés dans le texte sans essayer d'en produire d'autres de leur propre mouvement.
- Manque de regard critique des candidats sur les résultats obtenus (principalement par eux-mêmes).
- Manque de regard critique sur le texte : les textes sont « volontairement allusifs » et plutot que de reproduire les allusions, il vaut mieux, de loin, relever les points qu'il faudrait démontrer meme si on n'a pas obtenu de démonstration.
- Dans une épreuve de calcul formel, plutôt que de voir des candidats se lancer dans de longs et délicats calculs au tableau, on souhaiterait qu'ils sachent s'appuyer sur les logiciels à leur disposition, surtout quand le texte le leur suggère.

Les lacunes importantes

- L'algèbre linéaire est toujours mal maîtrisée, y compris dans les aspects les plus élémentaires de discussion de systèmes linéaires. Les candidats ne sont que rarement capables de remarquer

qu'un système homogène comportant plus d'inconnues que d'équations a une solution non triviale. La dimension de l'espace des solutions est rarement reliée au rang.

- Des candidats pensent souvent que l'algorithme du pivot de Gauss est de complexité quadratique en la dimension. Plus généralement, certaines complexités (division euclidienne de deux entiers, algorithme d'Euclide) ne sont pas connues. Il serait souhaitable que les candidats aient quelques idées sur les ordres de grandeur de nombre d'opérations élémentaires "faisables" (par exemple, un algorithme nécessitant de l'ordre de 10^{100} opérations ne terminera jamais en pratique).
- Concernant l'algorithme d'Euclide étendu, il serait souhaitable que les candidats sachent le formaliser un minimum. L'absence de formalisation a pour conséquence que les relations intermédiaires, utiles en pratique (reconstruction rationnelle) sont ignorées.
- En géométrie, le lien du résultant avec les questions d'élimination est mal compris. Bien des candidats, s'appuyant sur la présentation classique, considèrent le résultant comme un outil s'appliquant à des polynômes univariés à coefficients réels ou complexes. En outre, la géométrie affine n'est pas appréciée des candidats, qui tendent à l'éviter et ne sont par exemple pas à l'aise avec des notions élémentaires comme l'associativité du barycentre. Bien que n'étant pas explicitement au programme, la paramétrisation rationnelle d'une conique devrait faire partie de la culture d'un candidat.
- Même dans le cadre d'une épreuve d'algèbre et calcul formel, un candidat ne devrait pas être surpris de se voir suggérer d'approcher des quantités exactes d'une façon ou d'une autre (lemme chinois, méthodes d'évaluation-interpolation, $\mathbb{Z}/p^k\mathbb{Z}$, calcul flottant...).
- Si les candidats savent généralement donner une description abstraite des corps finis non premiers, il est rare d'en obtenir une réalisation concrète comme $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2+X+1)$. Au mieux parviendra-t-on au corps de décomposition de $X^{2^2} - X$ sur $\mathbb{F}_2$, dans une clôture algébrique fixée mais bien mystérieuse.
- La complexité des opérations arithmétiques sur les grands entiers (ou les polynômes) n'est pas connue, et les candidats ont du mal à la retrouver. Il n'y a pas grand sens à estimer le nombre d'itérations de l'algorithme d'Euclide si on n'estime pas le coût de chaque étape, même grossièrement. Ni à décrire RSA pour affirmer finalement que le coût de chiffrement (resp. déchiffrement) est de e (resp. d) multiplications.
- Quand on introduit l'algorithme de Berlekamp pour construire des codes correcteurs, il est bon de savoir exhiber quelques codes simples (code de répétition, code de parité...), et de pouvoir expliquer comment on réalise l'étape de codage sur un exemple.

Épreuves orales de l'option informatique

L'option informatique a été ouverte pour la première fois en 2006. Des préparations se sont organisées à l'ENS Cachan (rassemblant les candidats de l'ENS Cachan, de l'ENS Ulm, de l'Université Paris 7 et de l'Université Paris 11), à l'ENS Lyon, à l'antenne de Bretagne de l'ENS Cachan (Rennes/Ker Lann) et à l'Université Joseph Fourier de Grenoble. Au total, ces préparations regroupaient une quinzaine d'étudiants, donc une toute petite partie des candidats.

De nombreux candidats (233) se sont inscrits à l'option informatique pour le concours 2007, mais seuls 107 d'entre eux se sont présentés aux épreuves écrites. La proportion de désistement entre l'inscription et l'écrit (54 %) est significativement plus importante que dans les autres options (globalement elle est de 39 %). Elle peut s'expliquer par une confusion sur le terme même d'option informatique, certains candidats potentiels s'apercevant après coup – à la lecture du programme, par exemple – que cette option nécessite des connaissances approfondies dans le domaine de la science informatique, ce qui n'a pas grand chose à voir avec l'utilisation d'outils logiciels en mathématiques !

Remarques sur les résultats des candidats

Sur les 598 admissibles aux épreuves écrites, 37 étaient inscrits dans l'option informatique et, parmi eux, 24 ont été reçus. Les candidats de l'option se répartissent à peu près uniformément dans le classement global.

> *Il est important de rappeler qu'il n'y a pas de quota prédéfini : tous les candidats reçus sont agrégés de mathématiques, quelle que soit l'option choisie pour le concours et tous sont gérés ensuite selon des procédures identiques.*

Les candidats admissibles de l'option informatique ont une moyenne d'écrit légèrement supérieure à celle de l'ensemble des candidats admissibles (+0,8/20), avec un écart-type comparable. Au concours 2006, c'était le contraire (−0,6/20). En ce qui concerne les épreuves orales, spécifiques à l'option informatique, on note une amélioration légère du rang des candidats reçus entre l'admissibilité et l'admission, qui est cette année comparable à ce qu'elle est pour les autres options.

De même, on note, en 2007, pour les candidats (présents à l'oral) de l'option informatique une meilleure adéquation qu'en 2006 entre leurs résultats à l'épreuve de mathématiques (moyenne 10,4/20) et à l'épreuve d'informatique fondamentale (moyenne 10,2/20), ces résultats étant comparables à ceux des candidats inscrits aux autres options.

En résumé, le concours 2007 semble montrer que les candidats de l'option informatique sont plus proches qu'en 2006 des candidats des autres options. Leurs résultats dans les épreuves de mathématiques écrites et orales ont bien progressé d'une année sur l'autre et sont, en moyenne, au niveau de ceux des autres candidats. Leur double compétence et le travail qu'implique sa construction, leur permet de réussir globalement mieux que dans les autres options.[6]

[6] Il faut dire aussi que dans cette option, les élèves d'une ENS sont sensiblement plus nombreux (16 % des candidats présents à l'écrit, alors qu'ils sont globalement moins de 6 %) et représentent les 2/3 des admis.

Une remarque sur l'épreuve orale de mathématiques

Il y a, dans cette option, à côté de candidats de grande qualité, une proportion anormalement élevée de candidats qui n'ont visiblement pas préparé l'oral de mathématiques. Sur le sujet qu'ils ont « choisi », ils n'ont donc à proposer qu'un plan banal et des développements triviaux, car les 3 heures de préparation ne permettent pas de préparer un oral correct *ex nihilo*. Dans cette option comme dans les autres, il faut que les candidats préparent sérieusement pendant l'année la plupart des leçons sous peine de compromettre leur chance de réussite.

Remarques sur l'épreuve d'informatique fondamentale

L'épreuve de leçon d'informatique a été organisée exactement sur le modèle de celles de mathématiques. L'épreuve dure 45 minutes. Un ensemble de 25 titres de leçons ayant été diffusé à l'avance, le candidat tire un couplage de deux titres parmi ces 25 et choisit l'un des deux. Après 3 heures de préparation, il expose son plan de leçon au jury pendant une petite dizaine de minutes, ainsi que deux propositions de développement. Le jury choisit l'une des propositions, le candidat expose ce développement pendant une quinzaine de minutes, puis une discussion libre s'engage avec le jury pendant le reste du temps.

Le jury a noté que la plupart des candidats ont choisi un sujet d'algorithmique quand le couplage le leur proposait. Ceci a été le cas pour les deux tiers des candidats. Cependant, un tiers des candidats a traité des leçons moins classiques comme *Machine de Turing* ou *Classes P et NP, NP-complétude*.

De manière générale, le jury a plutôt été heureusement surpris par la qualité de certaines leçons présentées, notamment parmi les leçons les plus avancées, ce qui confirme le bon travail des préparations spécifiques en amont du concours. Ceci se traduit par une moyenne légèrement supérieure pour cette épreuve à celle de leçon d'algèbre des autres options. En revanche, le niveau est aussi un peu plus hétérogène, ce qui donne un écart-type lui aussi un peu plus grand.

Contrairement à l'an passé, nous n'avons pas cette année observé de confusion importantes à propos des notions de base, comme par exemple entre l'*interface* d'une structure de données (pile, file, etc.) et son *implémentation* (par un tableau, par exemple). Ceci est sûrement un résultat du bon travail accompli par les préparateurs.

Comme l'an passé, une tentation bien compréhensible est de mathématiser les sujets de leçons en oubliant l'aspect informatique. Ainsi, sur le sujet *Classes P et NP, NP-complétude*, il était tentant de faire une leçon complètement centrée sur un résultat majeur, par exemple la NP-complétude du problème SAT, en oubliant complètement les aspects plus concrets de ce domaine et ses multiples applications.

Le jury tient donc à rappeler qu'il s'agit bien d'une épreuve d'*informatique fondamentale*, et non pas d'outils mathématiques pour l'informatique. Il appartient au candidat de montrer la pertinence des outils mathématiques qu'il développe vis-à-vis des objectifs du thème informatique développé dans la leçon, que ce thème soit d'intérêt scientifique ou technologique.

La présentation d'outils mathématiques pour eux-mêmes, en particulier lorsqu'il s'agit d'outils sophistiqués comme ceux de la théorie de la calculabilité ou de la théorie des types, s'apparente donc à un « hors-sujet ». Les deux questions-clés de cette épreuve sont toujours :

- À quoi cet outil mathématique sert-il dans le cadre informatique considéré ?
- La complexité ou le coût de son utilisation est-elle bien compensée par la qualité supplémentaire d'information qu'il permet d'obtenir ?

Le jury invite tout particulièrement les candidats à se préparer à gérer ce type de questions, centrales dans la pédagogie de l'informatique au niveau des lycées et des classes préparatoires. On trouvera dans le rapport 2006 une discussion précise de quelques leçons à titre d'exemple.

Remarques sur l'épreuve de modélisation : « analyse de systèmes informatiques »

Les candidats ont en général compris la différence entre l'épreuve de modélisation et la leçon. Le candidat doit montrer qu'il comprend la modélisation. Cependant, une compréhension exhaustive du texte n'est pas attendue. Il expose le résultat de sa réflexion en proposant un développement personnel. Un élément d'appréciation est le niveau des développements et la qualité des preuves qu'il choisit d'établir et de présenter.

Le déroulement de l'épreuve de modélisation est très variable du fait des textes eux-mêmes. Une grande latitude est laissée au candidat dans ses développements, avec cependant la nécessité de présenter l'exercice d'informatique. Nous décrivons ci-dessous un schéma-type et les attentes du jury, notamment en ce qui concerne l'exercice d'informatique.

Un schéma possible. Le candidat dispose de 40-45 minutes pour décrire le problème, développer sa modélisation et présenter l'exercice d'informatique. La description du problème, à l'intention d'un jury qui ne connaît pas nécessairement le problème en profondeur, dure environ 10 minutes. Elle peut s'appuyer sur un exemple concret, soit une donnée du texte, soit une construction personnelle. L'exercice est généralement présenté immédiatement après l'exposé des notions à implémenter. Le candidat présente un ou plusieurs développements dans les 20-25 minutes restantes.

Les développements. Certains candidats s'efforcent de présenter la plus grande partie possible du texte, au détriment d'une compréhension en profondeur. Leur exposé tend alors à ressembler à un résumé, voire une paraphrase du texte. D'autres, ou les mêmes, détaillent des preuves simples et n'ont pas le temps de présenter des développements plus intéressants et originaux qu'ils ont pourtant préparés. La gestion du temps peut être facilitée par la présentation systématique d'un plan *succinct* en début d'épreuve. Le jury pourra ainsi s'appuyer sur ce plan pour accélérer la présentation afin de permettre l'exposé des développements intéressants que la candidat a lui-même proposés.

Le jury rappelle qu'il n'attend pas, dans les développements, un exposé, même brillant, d'une démonstration classique connue... et relue durant le temps de préparation ! Par exemple, montrer que le Voyageur de Commerce est NP-complet en le ramenant à 3-SAT est hors sujet. Montrer que le problème du texte se ramène à une recherche d'arbre couvrant minimum (ou pas) et énoncer correctement et rigoureusement sa complexité en fonction des contraintes spécifiques du problème est par contre dans le sujet.

Plusieurs candidats ont suggéré un algorithme qui n'était pas dans le texte proposé. Il est recommandé que celui-ci représente soit une préparation pédagogique à la présentation des autres algorithmes soit une amélioration manifeste. Enfin, il ne doit pas réduire exagérément la présentation du texte lui-même.

L'exercice d'informatique. Cette partie de l'épreuve a été globalement satisfaisante, les candidats ayant généralement bien compris l'importance qui y est attachée. Elle dure environ 10 minutes. Le candidat choisit librement, dans les 40 premières minutes, le moment de présenter son exercice d'informatique, de façon qu'il s'intègre au mieux dans son exposé. Le plus souvent, les candidats le placent dès que les notions nécessaires ont été introduites dans l'exposé. Cette introduction doit être soignée et complète, afin d'éviter tant les allers-retours du terminal au tableau que les discours « avec les mains » devant l'écran.

D'une manière générale, le candidat doit proposer un code lisible et mettre en valeur ses connaissances en programmation. Par exemple, il peut justifier, dans la présentation du programme, ses choix informatiques (structures de données, algorithmique, etc.) Par contre, il faut éviter de descendre dans les détails les plus triviaux du code, que le jury lit lui-même à l'écran. On pourra lui demander d'évaluer la complexité de son implémentation ou de discuter de choix alternatifs.

Cette présentation au jury *doit être faite que le programme « tourne » – ce que l'on espère – ou pas*. Ensuite, le candidat lance une exécution. La possibilité de modification au vol d'un paramètre est appréciée pour la vérification de la correction. Si le programme « ne tourne pas », le jury évalue la qualité générale du code réalisé. Cette évaluation interactive permet à un candidat réactif de repérer l'erreur, voire de la corriger, de recompiler et de relancer l'exécution.

Le candidat choisit son langage. Les trois langages ont été utilisés avec une petite prédominance de Caml, et un léger retrait de C. Ce choix peut orienter les questions, car l'implémentation du problème est plus facile dans certains langages. Par exemple, la différence ensembliste entre deux listes étant prédéfinie dans les bibliothèques de Caml, on attend du candidat qui l'utiliserait qu'il puisse expliquer l'implémentation d'une liste et la complexité des opérations concernées.

De nombreux candidats programment plus que l'exercice demandé. Ces extensions sont alors considérées et évaluées comme des développements au choix du candidat. Par exemple, des simulations simples ont pu servir à exposer un développement. Elles doivent mettre en valeur d'autres capacités du candidat.

Ouvrages autorisés

Les candidats peuvent utiliser librement les ouvrages de la bibliothèque de l'agrégation dont la composition, pour la session 2007, est rappelée en annexe 3. Ils peuvent aussi emprunter les ouvrages mis à la disposition de tous les candidats par les centres de préparation à l'agrégation. Ces ouvrages sont rangés dans une des deux salles de la bibliothèque. Le nombre d'exemplaires de chaque titre étant limité, un ouvrage emprunté par un ou plusieurs candidats peut être indisponible.

Un candidat peut aussi utiliser tout ouvrage qu'il a apporté à la condition :

- qu'il soit en vente dans le commerce, ce qui se manifeste par la présence d'un numéro d'identification ISBN ;
- qu'il soit rédigé en langue française ou en langue anglaise ;
- qu'il soit vierge de toute annotation ;
- qu'il ne comporte pas des plans ou des développements tous faits, spécifiquement rédigés pour la préparation de l'agrégation : à cet égard une liste d'ouvrages interdits est affichée sur la porte de la bibliothèque.

Le président du jury, ou l'un des membres du jury, a toute autorité pour refuser l'utilisation d'un ouvrage ne remplissant pas l'ensemble de ces conditions.

À titre indicatif, on trouvera ci-après la liste des ouvrages non autorisés pour le concours 2007 :

AVEZ A. Analyse pour l'agrégation [Masson]

AVEZ A. La leçon d'analyse à l'Oral de l'agrégation [Masson]

AVEZ A. La leçon de géométrie à l'Oral de l'agrégation [Masson]

CHAMBERT-LOIR A. Exercices de mathématiques pour l'agrégation, tome I, 1re édition [Masson]

CORTIER J.P. Exercices corrigés d'algèbre et géométrie [CRDP de Champagne Ardenne]

DUMAS L. Modélisation à l'oral de l'agégation. Calcul Scientifique [Ellipses]

GUÉNARD F. Vademecum de l'oral d'analyse, agrégation de mathématiques [Eska]

MADERÈ K. Préparation à l'oral de l'agrégation. Leçon d'algèbre [Ellipses]

MADÈRE K. Préparation à l'oral de l'agrégation. Leçon d'analyse [Ellipses]

MADÈRE K. Développement pour leçon d'analyse, agrégation de mathématiques [Ellipses]

MADÈRE K. Développement pour leçon d'algèbre, agrégation de mathématiques [Ellipses]

MEUNIER P. Exercices pour l'agrégation interne de mathématiques [PUF]

MEUNIER P. Préparation à l'agrégation interne, IREM de Montpellier [PUF]

TOULOUSE P.S. Thèmes de probabilités et statistiques, agrégation de mathématiques [Dunod]

ANNEXE 1 :
Leçons d'oral 2007 (options A, B et C)

Algèbre et géométrie

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

102 - Sous-groupes discrets de $\mathbb{R}^n$. Réseaux. Exemples.

103 - Exemples et applications des notions de sous-groupes distingué et de groupe quotient.

104 - Groupes finis. Exemples et applications.

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

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

107 - Sous-groupes finis de $\mathrm{O}(2,\mathbb{R})$, de $\mathrm{O}(3,\mathbb{R})$. Applications.

108 - Exemples de parties génératrices d'un groupe.

109 - Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.

110 - Nombres premiers. Applications.

111 - Exemples d'applications des idéaux d'un anneau commutatif unitaire.

112 - Corps finis. Applications.

113 - Groupe des nombres complexes de module 1. Applications.

114 - Équations diophantiennes du premier degré $ax+by=c$. Autres exemples d'équations diophantiennes.

115 - Corps des fractions rationnelles à une indéterminée sur un corps commutatif. Applications.

116 - Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

117 - Algèbre des polynômes à n indéterminées ($n \geqslant 2$). Polynômes symétriques. Applications.

118 - Racines des polynômes à une indéterminée. Relations entre les coefficients et les racines d'un polynôme. Exemples et applications.

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

121 - Matrices équivalentes. Matrices semblables. Applications.

122 - Opérations élémentaires sur les lignes et les colonnes d'une matrice. Résolution d'un système d'équations linéaires. Exemples et applications.

123 - Déterminant. Exemples et applications.

124 - Réduction d'un endomorphisme en dimension finie. Applications.

125 - Sous-espaces stables d'un endomorphisme d'un espace vectoriel de dimension finie. Applications.

126 - Endomorphismes diagonalisables.

127 - Exponentielle de matrices. Applications.

128 - Endomorphismes nilpotents.

129 - Polynômes d'endomorphismes. Polynômes annulateurs. Applications.

130 - Exemples de décompositions remarquables dans le groupe linéaire. Applications.

131 - Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.

132 - Formes linéaires et hyperplans en dimension finie. Exemples et applications.

133 - Endomorphismes remarquables d'un espace vectoriel euclidien de dimension finie.

134 - Endomorphismes remarquables d'un espace vectoriel hermitien de dimension finie.

135 - Isométries d'un espace affine euclidien de dimension finie. Formes réduites. Applications en dimensions 2 et 3.

136 - Coniques. Applications

137 - Barycentres dans un espace affine réel de dimension finie ; convexité. Applications.

138 - Homographies de la droite complexe. Applications.

139 - Applications des nombres complexes à la géométrie.

140 - Angles : définitions et utilisation en géométrie.

141 - Utilisation des groupes en géométrie.

142 - Exemples d'utilisation de la géométrie projective.

143 - Constructions à la règle et au compas.

144 - Problèmes d'angles et de distances en dimension 2 ou 3.

145 - Méthodes combinatoires, problèmes de dénombrement.

146 - Anneaux principaux.

147 - Applications affines. Groupe affine.

148 - Groupe orthogonal d'une forme quadratique. Générateurs. Exemples.

149 - Groupes finis de petit cardinal.

Analyse et probabilités

201 - Espaces de fonctions. Exemples et applications.

202 - Exemples de parties denses et applications.

203 - Utilisation de la notion de compacité.

204 - Connexité. Exemples et applications.

205 - Espaces complets. Exemples et applications.

206 - Théorèmes de point fixe. Exemples et applications.

207 - Prolongement de fonctions. Exemples et applications.

208 - Utilisation de la continuité uniforme en analyse.

209 - Utilisation de la dénombrabilité en analyse et en probabilités.

210 - Applications linéaires continues entre espaces vectoriels normés. Exemples et applications.

211 - Utilisation de la dimension finie en analyse.

212 - Méthodes hilbertiennes.

213 - Bases hilbertiennes. Exemples et applications.

214 - Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications.

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

216 - Exemples d'études affines ou métriques de courbes.

217 - Étude locale de surfaces. Exemples.

218 - Applications des formules de Taylor.

219 - Problèmes d'extremums.

220 - Équations différentielles $X' = f(t, X)$; exemples d'études qualitatives des solutions.

221 - Équations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications.

222 - Exemples d'équations différentielles. Solutions exactes ou approchées.

223 - Convergence des suites numériques. Exemples et applications.

224 - Comportement asymptotique des suites numériques. Rapidité de convergence. Exemples.

226 - Comportement d'une suite réelle ou vectorielle définie par une itération $u_{n+1} = f(u_n)$. Exemples.

227 - Exemples de développement asymptotique de fonctions d'une variable réelle.

228 - Continuité et dérivabilité des fonctions réelles d'une variable réelle. Exemples et contre-exemples.

229 - Fonctions monotones. Fonctions convexes. Exemples et applications.

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

231 - Illustrer par des exemples et des contre-exemples la théorie des séries numériques.

232 - Méthodes d'approximation des solutions d'une équation $F(X) = 0$. Exemples.

233 - Intégration des fonctions d'une variable réelle. Suites de fonctions intégrables.

234 - Espaces L^p, $1 \leqslant p \leqslant +\infty$.

235 - Interversion d'une limite et d'une intégrale. Exemples et applications.

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

237 - Exemples d'intégrales impropres sur un intervalle de $\mathbb{R}$.

238 - Méthodes de calcul approché d'intégrales.

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

240 - Transformation de Fourier, produit de convolution. Applications.

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

242 - Exemples d'utilisation de fonctions définies par des séries.

243 - Convergence des séries entières, propriétés de la somme. Exemples et applications.

244 - Fonctions d'une variable complexe, holomorphie. Exemples et applications.

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

246 - Développement d'une fonction périodique en série de Fourier. Exemples et applications.

247 - Exemples de problèmes d'interversion de limites.

248 - Approximation des fonctions numériques par des fonctions polynomiales ou polynomiales par morceaux. Exemples.

249 - Le jeu de pile ou face (suites de variables de Bernoulli indépendantes).

250 - Loi binomiale, loi de Poisson. Applications.

251 - Indépendance d'événements et de variables aléatoires. Exemples.

252 - Parties convexes, fonctions convexes (d'une ou plusieurs variables). Applications.

253 - Variables gaussiennes. Applications.

ANNEXE 2 :
Leçons d'oral pour l'option D

Leçons de mathématiques

Algèbre et géométrie

104 - Groupes finis. Exemples et applications.

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

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

109 - Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.

110 - Nombres premiers. Applications.

112 - Corps finis. Applications.

116 - Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

118 - Racines des polynômes à une indéterminée. Relations entre les coefficients et les racines d'un polynôme. Exemples et applications.

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

121 - Matrices équivalentes. Matrices semblables. Applications.

122 - Opérations élémentaires sur les lignes et les colonnes d'une matrice. Résolution d'un système d'équations linéaires. Exemples et applications.

123 - Déterminant. Exemples et applications.

124 - Réduction d'un endomorphisme en dimension finie. Applications.

128 - Endomorphismes nilpotents.

129 - Polynômes d'endomorphismes. Polynômes annulateurs. Applications.

131 - Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.

132 - Formes linéaires et hyperplans en dimension finie. Exemples et applications.

133 - Endomorphismes remarquables d'un espace vectoriel euclidien de dimension finie.

135 - Isométries d'un espace affine euclidien de dimension finie. Formes réduites. Applications en dimensions 2 et 3.

136 - Coniques. Applications

137 - Barycentres dans un espace affine réel de dimension finie ; convexité. Applications.

139 - Applications des nombres complexes à la géométrie.

141 - Utilisation des groupes en géométrie.

144 - Problèmes d'angles et de distances en dimension 2 ou 3.

145 - Méthodes combinatoires, problèmes de dénombrement.

Analyse et probabilités

203 - Utilisation de la notion de compacité.

206 - Théorèmes de point fixe. Exemples et applications.

210 - Applications linéaires continues entre espaces vectoriels normés. Exemples et applications.

214 - Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications.

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

216 - Exemples d'études affines ou métriques de courbes.

218 - Applications des formules de Taylor.

221 - Équations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications.

222 - Exemples d'équations différentielles. Solutions exactes ou approchées.

224 - Comportement asymptotique des suites numériques. Rapidité de convergence. Exemples.

226 - Comportement d'une suite réelle ou vectorielle définie par une itération $u_{n+1} = f(u_n)$. Exemples.

227 - Exemples de développement asymptotique de fonctions d'une variable réelle.

229 - Fonctions monotones. Fonctions convexes. Exemples et applications.

231 - Illustrer par des exemples et des contre-exemples la théorie des séries numériques.

232 - Méthodes d'approximation des solutions d'une équation $F(X) = 0$. Exemples.

233 - Intégration des fonctions d'une variable réelle. Suites de fonctions intégrables.

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

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

240 - Transformation de Fourier, produit de convolution. Applications.

243 - Convergence des séries entières, propriétés de la somme. Exemples et applications.

244 - Fonctions d'une variable complexe, holomorphie. Exemples et applications.

246 - Développement d'une fonction périodique en série de Fourier. Exemples et applications.

248 - Approximation des fonctions numériques par des fonctions polynomiales ou polynomiales par morceaux. Exemples.

250 - Loi binomiale, loi de Poisson. Applications.

253 - Variables gaussiennes. Applications.

Leçons d'informatique fondamentale

901 - Exemples de structures de données et de leurs applications.
902 - Diviser pour régner : exemples et applications.
903 - Exemples d'algorithmes de tri : complexité.
904 - Arbres binaires de recherche. Applications.
905 - Parcours de graphes : exemples et applications.
906 - Programmation dynamique : exemples et applications.
907 - Algorithmique du texte : exemples et applications.
908 - Automates finis. Exemples et applications.
909 - Langages rationnels. Exemples et applications.
910 - Langages algébriques. Exemples et applications.
911 - Automates à pile ; puissance et limites.
912 - Fonctions récursives primitives et non primitives.
913 - Machines de Turing.
914 - Décidabilité et indécidabilité.
915 - Classes P et NP, NP-complétude. Exemples.
916 - Formules booléennes. Représentation et satisfiabilité.
917 - Logique du premier ordre : syntaxe et sémantique.
918 - Méthode de résolution, programmation logique.
919 - Unification : algorithmes et applications.
920 - Réécriture et formes normales.
921 - Langages typés : objectifs, mise en œuvre, applications.
922 - Descriptions sémantiques des langages de programmation.
923 - Analyses lexicale et syntaxique : principes, mise en œuvre, applications.
924 - Typage statique : objectifs, mise en œuvre, applications.
925 - Génération de code pour une machine à pile : principes, mise en œuvre, applications.

ANNEXE 3 :
La bibliothèque de l'agrégation

AABELSON H. **SUSSMAN G. J.** **SUSSMAN J.**	Structure and interpretation of computer programs	MIT Press
AHUÉS M. **CHATELIN F.**	Exercices de valeurs propres de matrices	Masson
ALBERT L. **Collectif**	Cours et exercices d'informatique	Vuibert
ALESSANDRI M.	Thèmes de géométrie	Dunod
ALLOUCHE J. P. **SHALLIT J.**	Automatic sequences theory, applications, generalizations	Cambridge
AMAR E. **MATHERON É.**	Analyse complexe	Cassini
ANDLER M. **BLOCH J. D.** **MAILLARD B.**	Exercices corrigés de Mathématiques • Tome 1A - Topologie • Tome 1B - Fonctions numériques • Tome 2 - Suites et séries numériques • Tome 3 - Analyse fonctionnelle • Tome 5 - Algèbre générale, polynômes • Tome 6 - Algèbre linéaire, première partie • Tome 7 - Algèbre linéaire, deuxième partie	Ellipses
ANDREWS G.	Number Theory	Dover
APPLE A.W.	Modern compiler implementation • in C • in Java • in ML	Cambrigde
ARIBAUD F. **VAUTHIER J.**	Mathématiques. Première année de DEUG	ESKA

ARNAUDIES J-M. **BERTIN J.**	Groupes, Algèbres et Géométrie • Tome I • Tome II	Ellipses
ARNAUDIES J-M. **DELEZOIDE P.** **FRAYSSE H.**	Exercices résolus d'analyse	Dunod
ARNAUDIES J-M. **DELEZOIDE P.** **FRAYSSE H.**	Exercices résolus d'algèbre bilinéaire et géométrie du cours de Mathématiques tome 4	Dunod
ARNAUDIES J-M. **FRAYSSE H.**	Cours de Mathématiques • 1. Algèbre • 2. Analyse • 3. Compléments d'analyse • 4. Algèbre bilinéaire et géométrie	Dunod
ARNOLD V.	Chapitre supplémentaire de la théorie des équations différentielles ordinaires	MIR
ARNOLD V.	Équations différentielles ordinaires	MIR
ARTIN E.	Algèbre géométrique	Gauthier-Villars
ARTIN E.	Algèbre géométrique	Gabay
ARTIN M.	Algebra	Prentice Hall
AUBIN J.P.	Analyse fonctionnelle appliquée • Tome 1 • Tome 2	PUF
AUTEBERT J. M.	Calculabilité et décidabilité	Masson
AUTEBERT J. M.	Théorie des langages et des automates	Masson
AUDIN M.	Géométrie de la licence à l'agrégation	Belin

AVANISSIAN V.	Initiation à l'analyse fonctionnelle	PUF
AVEZ A.	Calcul différentiel	Masson
BAASE S. **VAN GELDER A.**	Computer algorithms Introduction to design & analysis	Addison Wesley
BADOUEL E. **BOUCHERON S.** **DICKY A., PETIT A.** **SANTHA M., WEIL P.,** **ZEITOUN M.**	Problèmes d'informatique fondamentale	Springer
BAKHVALOV N.	Méthodes numériques	MIR
BARANGER J.	Analyse numérique	Hermann
BARBE Ph. **LEDOUX M.**	Probabilité (De la licence à l'agrégation)	Belin
BARRET M. **BENIDIR M.**	Stabilité des filtres et des systèmes linéaires	Dunod
BASILI B. **PESKINE C.**	Algèbre	Diderot, éditeur Arts et Sciences
BASS J.	Cours de Mathématiques • Tome 1 • Tome 2	Masson
BAUER F. L.	Decrypted secrets. Methods and maxims of cryptology	Springer
BENDER C. **ORSZAG S.**	Advanced mathematical methods for scientists and engineers	Mc Graw Hill
BERGER M. **GOSTIAUX B.**	Géométrie différentielle	Armand Colin

BERGER M. **BERRY J-P.** **PANSU P.** **SAINT RAYMOND X.**	Problèmes de géométrie commentés et rédigés	Cédic/Nathan
BERGER M.	Géométrie • Index • 1. Action de groupes, espaces affines et projectifs • 2. Espaces euclidiens, triangles, cercles et sphères • 3. Convexes et polytopes, polyèdres réguliers, aires et volumes • 4. Formes quadratiques, quadriques et coniques • 5. La sphère pour elle-même, géométrie hyperbolique, l'espace des sphères	Cédic/Nathan
BERGER M.	Géométrie tome 2	Nathan
BICKEL P.J. **DOKSUM K.A.**	Mathematical statistics	Prentice Hall
BIDEGARAY B. **MOISAN L.**	Petits problèmes de mathématiques appliquées et de modélisation	Springer
BIGGS NORMAN L.	Discrete mathematics	Oxford Science Publications
BLANCHARD A.	Les corps non commutatifs	PUF
BOAS R.	A primer of real functions	Mathematical association of America
BON J.L.	Fiabilité des systèmes	Masson
BONNANS J.F. **GILBERT J.C.** **LEMARECHAL C.** **SAGASTIZABAL C.**	Optimisation numérique	Springer

BOURBAKI N.	Éléments de Mathématique • Topologie générale, chapitres V à X • Fonctions d'une variable réelle, chapitres I à VII • Fonctions d'une variable réelle, chapitres I à III • Fascicule XIII Intégration, chapitres I à IV	HERMANN
BOUVIER A. **RICHARD D.**	Groupes	HERMANN
BREMAUD P.	Introduction aux probabilités	SPRINGER
BREZIS H.	Analyse fonctionnelle, théorie et applications	MASSON
BRIANE M. **PAGES G.**	Théorie de l'intégration Cours et exercices, 3ème édition	VUIBERT
BROUSSE P.	Mécanique MP - PC.- Spéciales A. A'. B. B'.	ARMAND COLIN
BRUCE J.W. **GIBLIN P.J.** **RIPPON P.J.**	Microcomputers and Mathematics	CAMBRIDGE
CABANE R. **LEBOEUF C.**	Algèbre linéaire • 1. Espaces vectoriels , Polynômes • 2. Matrices et réduction	ELLIPSES
CABANNES H.	Cours de Mécanique générale	DUNOD
CALAIS J.	Éléments de théorie des anneaux	PUF
CALAIS J.	Éléments de théorie des groupes	PUF
CARREGA J.C.	Théorie des corps	HERMANN
CARTAN H.	Calcul différentiel (1971)	HERMANN

CARTAN H.	Cours de calcul différentiel (1977)	Hermann
CARTAN H.	Formes différentielles	Hermann
CARTAN H.	Théorie élémentaire des fonctions analytiques	Hermann
CARTIER P. **KAHANE J.P.** **ARNOLD V. et al.**	Leçons de mathématiques d'aujourd'hui	Cassini
CASTLEMAN K.R.	Digital image processing	Prentice Hall
CHAMBERT-LOIR A. **FERMIGER S.** **MAILLOT V.**	Exercices de mathématiques pour l'agrégation Analyse 1 (seconde édition revue et corrigée)	Masson
CHAMBERT-LOIR A. **FERMIGER S.**	Exercices de mathématiques pour l'agrégation • Analyse 2 • Analyse 3	Masson
CHATELIN F.	Valeurs propres de matrices	Masson
CHILDS L.	A concrete introduction to Higher Algebra	Springer Verlag
CHOQUET G.	Cours d'analyse Tome II : Topologie	Masson
CHOQUET G.	L'enseignement de la géométrie	Hermann
CHRISTOL G. **PILIBOSSIAN P.** **YAMMINE S.**	• Algèbre 1 • Algèbre 2	Ellipses
CIARLET P.G.	Introduction à l'analyse numérique matricielle et à l'optimisation	Masson
COGIS O. **ROBERT C.**	Au-delà des ponts de Könisberg. Théorie des graphes. Problèmes, théorie, algorithmes	Vuibert

COHN P.M.	Algebra Volume 1	John Wiley
COLLET P.	Modeling binary data	Chapman and Hall
COMBROUZE A.	Probabilités et statistiques	PUF
CORI R. **LASCAR D.**	Logique mathématique • 1. Calcul propositionnel, algèbre de Boole, calcul des prédicats • 2. Fonctions récursives, théorème de Gödel, théorie des ensembles, théorie des modèles	Dunod
CORMEN T. H. **LEISERSON C. E.** **RIVEST R. L.** **STEIN C.**	Introduction à l'algorithmique	Dunod
COTRELL M. **GENON-CATALOT V.** **DUHAMEL C.** **MEYRE T.**	Exercices de probabilités	Cassini
COURANT R. **HILBERT D.**	Methods of Mathematical Physics • Volume 1 • Volume 2	John Wiley
COUSINEAU G. **MAUNY M.**	Approche fonctionnelle de la programmation	Ediscience
COXETER H.S.M.	Introduction to Geometry	John Wiley
CVITANOVIC P.	Universality in Chaos	Institute of Physics Publishing
DACUNHA-CASTELLE D. **DUFLO M.**	• Probabilités et Statistiques 1. Problèmes à temps fixe • Exercices de Probabilités et Statistiques 1. Problèmes à temps fixe	Masson
DACUNHA-CASTELLE D. **REVUZ D.** **SCHREIBER M.**	Recueil de problèmes de calcul des probabilités	Masson

DARTE A. **VAUDENAY S.**	Algorithmique et optimisation	Dunod
DAVID R. **NOUR K.** **RAFFALI C.**	Introduction à la logique Théorie de la démonstration	Dunod
DEHEUVELS P.	L'intégrale	PUF
DEHEUVELS P.	L'intégrale	Que-sais-je ? PUF
DEHEUVELS R.	Formes quadratiques et groupes classiques	PUF
DEHORNOY P.	Mathématiques de l'informatique	Dunod
DEHORNOY P.	Complexité et décidabilité	Springer
DELTHEIL R. **CAIRE D.**	Géométrie et compléments	Jacques Gabay
DEMAILLY J.P.	Analyse numérique et équations différentielles	PU Grenoble
DEMAZURE M.	Catastrophes et bifurcations	Ellipses
DEMAZURE M.	Cours d'algèbre : primalité, divisibilité, codes	Cassini
DEMBO A. **ZEITOUNI O.**	Large deviations techniques and applications	Springer
DESCOMBES R.	Éléments de théorie des nombres	PUF
DESCHAMPS **WARUSFEL** **MOULIN, RUAUD** **MIQUEL, SIFRE**	Mathématiques, cours et exercices corrigés • 1ère année MPSI, PCSI, PTSI • 2ème année MP, PC, PSI	Dunod

DEVANZ C. **ELHODAIBI M.**	Exercices corrigés de Mathématiques posés à l'oral des Ensi, Tome 2	Ellipses
DIEUDONNÉ J.	Algèbre linéaire et géométrie élémentaire	Hermann
DIEUDONNÉ J.	Calcul infinitésimal	Hermann
DIEUDONNÉ J.	Sur les groupes classiques	Hermann
DIEUDONNÉ J.	Éléments d'Analyse. • Fondements de l'analyse moderne • Éléments d'Analyse Tome 2.	Gauthier-Villars
DIXMIER J.	Cours de Mathématiques du premier cycle • Première année • Deuxième année	Gauthier-Villars
DUBUC S.	Géométrie plane	PUF
DUCROCQ A. **WARUSFEL A.**	Les Mathématiques, plaisir et nécessité Un parcours guidé dans l'univers des mathématiques	Vuibert
DUGAC P.	Histoire de l'analyse. Autour de la notion de limite et de ses voisinages	Vuibert
DYM H. **Mac KEAN H.P.**	Fouriers series and integrals	Academics Press
EBBINGHAUS, HERMES **HIRZEBRUCH** **KOECHER** **LAMOTKE, MAINZER** **NEUKIRSCH, PRESTEL,** **REMMERT**	Les Nombres	Vuibert
EL HAJ LAAMRI	Mesures, intégration et transformée de Fourier des fonctions	Dunod

EL KACIMI ALAOUI A. **QUEFFÉLEC H.** **SACRÉ C.** **VASSALLO V.**	Quelques aspects des mathématiques actuelles	Ellipses
EPISTEMON L. **(OVAERT J.L.** **VERLEY J.L.)**	Exercices et problèmes • Analyse. Volume 1 • Algèbre.	Cédic/Nathan
EXBRAYAT J.M. **MAZET P.**	Notions modernes de mathématiques • Algèbre 1 : Notions fondamentales de la théorie des ensembles • Analyse 1 : Construction des espaces fondamentaux de l'analyse • Analyse 2 : Éléments de topologie générale	Hatier
FADDEEV D. **SOMINSKI I.**	Recueil d'exercices d'Algèbre Supérieure	MIR
FAIRBANK X. **BEEF C.**	POX - Exercices posés au petit oral de l'X	Ellipses
FARAUT J.	Analyse sur les groupes de Lie	Calvage et Mounet
FARAUT J. **KHALILI E.**	Arithmétique Cours, Exercices et Travaux Pratiques sur Micro-Ordinateur	Ellipses
FELLER W.	An introduction to probability theory and its applications • Volume 1 • Volume 2	John Wiley
FERRIER J.P.	Mathématiques pour la licence	Masson
FLORY G.	Exercices de topologie et analyse avec solutions • Tome 1 - Topologie • Tome 2 - Fonctions d'une variable réelle • Tome 3 - Fonctions différentiables, intégrales multiples • Tome 4 - Séries, équations différentielles	Vuibert

FRANCHINI J. **JACQUENS J-C.**	Mathématiques Spéciales • Algèbre • Analyse 1 • Analyse 2	Ellipses
FRANCINOU S. **GIANELLA H.** **NICOLAS S.**	Exercices de mathématiques Oraux X-ens Algèbre 1	Cassini
FRANCINOU S. **GIANELLA H.**	Exercices de Mathématiques Algèbre 1	Masson
FRENKEL J.	Géométrie pour l'élève-professeur	Hermann
FRESNEL J.	Géométrie algébrique	UFR Maths Bordeaux
FRESNEL J.	Géométrie	IREM de Bordeaux
FRESNEL J.	Anneaux	Hermann
FRESNEL J.	Groupes	Hermann
FRESNEL J.	Méthodes modernes en géométrie	Hermann
FUHRMANN P.	A polynomial approach to linear algebra	Springer
GABRIEL P.	Matrices, géométrie, algèbre linéaire	Cassini
GANTMACHER F.R.	Théorie des matrices • Tome 1 • Tome 2	Dunod
GENET J.	Mesure et intégration. Théorie élémentaire. Cours et exercices résolus	Vuibert
GHIDAGLIA J.M.	Petits problèmes d'analyse	Springer

GOBLOT R.	Algèbre commutative	Masson
GOBLOT R.	Thèmes de géométrie	Masson
GODEMENT R.	Analyse • Tome 1 • Tome 2 • Tome 3	Springer
GODEMENT R.	Cours d'Algèbre	Hermann
GOLUB G.H. **VAN LOAN C.F.**	Matrix computations	Wiley
GONNORD S. **TOSEL N.**	Thèmes d'Analyse pour l'agrégation • Topologie et Analyse fonctionnelle • Calcul différentiel	Ellipses
GOSTIAUX B.	Cours de mathématiques spéciales • Tome 1 - Algèbre • Tome 2 - Topologie et analyse réelle • Tome 3 - Analyse fonctionnelle et calcul différentiel • Tome 4 - Géométrie affine et métrique • Tome 5 - Géométrie : arcs et nappes	PUF
GOURDON X.	Les maths en tête, mathématiques pour M' • Algèbre • Analyse	Ellipses
GRAMAIN A.	Géométrie élémentaire	Hermann
GRAMAIN A.	Intégration	Hermann
GRIMMET G. **WELSH D.**	Probability (an introduction)	Oxford
GUJARATI D. N.	Basic Econometrics	Wiley
HABSIEGER L. **MARTEL V.**	Exercices corrigés posés à l'oral des ENSI Tome 1 Analyse	Ellipses

HALMOS P.	Problèmes de mathématiciens petits et grands	Cassini
HAMMAD P.	Cours de probabilités	Cujas
HAMMAD P. **TARANCO A.**	Exercices de probabilités	Cujas
HAMMER R. **HOCKS M.** **KULISH U.** **RATZ D.**	C++ toolbox for verified computing	Springer
HARDY G.H. **WRIGH E.M.**	An introduction to the theory of numbers	Oxford
HAREL D.	Computer LTD. What they really can't do	Oxford
HAREL D. **FELDMAN Y.**	Algorithmics. The spirit of computing	Addison Wesley
HENNEQUIN P.L. **TORTRAT A.**	Théorie des probabilités et quelques applications	Masson
HENRICI P.	Applied and Computational Complex Analysis • Volume 1 • Volume 2 • Volume 3	Wiley-Interscience
HERVE M.	Les fonctions analytiques	PUF
HIRSCH F. **LACOMBE G.**	Eléments d'analyse fonctionnelle	Masson
HOPCROFT J.E. **MOTWANI R.** **ULLMAN J. D.**	Introduction to automata theory, Languages and Computation	Addison Wesley
HOUZEL C.	Analyse mathématique : cours et exercices	Belin

IRELAND K. **ROSEN M.**	A Classical Introduction to Modern Numbers Theory	Springer Verlag
ISAAC R.	Une initiation aux probabilités (Trad. R. Mansuy)	Vuibert-Springer
ITARD J.	Les nombres premiers	Que sais-je ? PUF
JACOBSON N.	Basic Algebra • Tome I • Tome II	Freeman and Co
KAHANE J.P. **GILLES P.**	Séries de Fourier et ondelettes	Cassini
KATZNELSON Y.	An Introduction to Harmonic Analysis	Dover
KERBRAT Y. **BRAEMER J-M.**	Géométrie des courbes et des surfaces	Hermann
KNUTH D.E.	The art of computer programming • Volume 1 : Fundamental algorithms • Volume 2 : Seminumerical algorithms • Volume 3 : Sorting and Searching	Addison-Wesley
KOLMOGOROV A. **FOMINE S.**	Eléments de la théorie des fonctions et de l'analyse fonctionnelle	Ellipses
de KONNINCK J.M. **MERCIER A.**	Introduction à la théorie des nombres	Modulo
KÖRNER T.W.	Fourier analysis	Cambridge
KÖRNER T.W.	Exercises for Fourier analysis	Cambridge
KREE P.	Introduction aux Mathématiques et à leurs applications fondamentales M.P.2	Dunod
KRIVINE H.	Exercices de Mathématiques pour physiciens	Casssini

KRIVINE J.L.	Théorie axiomatique des ensembles	PUF
LAFONTAINE J.	Introduction aux variétés différentielles	PUF
LALEMENT R.	Logique, réduction, résolution	Masson
LANG S.	Algèbre linéaire • Tome 1 • Tome 2	InterEditions
LANG S.	Algebra	Addison-Wesley
LANG S.	Linear Algebra	Addison-Wesley
LAVILLE G.	Courbes et surfaces	Ellipses
LAVILLE G.	Géométrie pour le CAPES et l'Agrégation	Ellipses
LAX P. D.	Linear Algebra	Wiley
LEBORGNE D.	Calcul différentiel et géométrie	PUF
LEBOSSÉ C. **HÉMERY C.**	Géométrie. Classe de Mathématiques	Jacques Gabay
LEHNING H. **JAKUBOWICZ D.**	Mathématiques supérieures et spéciales 2 : Dérivation	Masson
LEHNING H.	Mathématiques supérieures et spéciales • Tome 1 : Topologie • Tome 3 : Intégration et sommation • Tome 4 : Analyse en dimension finie • Tome 5 : Analyse fonctionnelle	Masson

LEICHTNAM E. **SCHAUER X.**	Exercices corrigés de mathématiques posés aux oraux X-ENS • Tome I - Algèbre 1 • Tome 2 - Algèbre et géométrie • Tome 3 - Analyse 1 • Tome 4 - Analyse 2	Ellipses
LELONG-FERRAND J. **ARNAUDIES J.M.**	Cours de Mathématiques • Tome 1 pour M-M' : Algèbre • Tome 1 pour A-A' : Algèbre • Tome 2 : Analyse • Tome 3 : Géométrie et cinématique • Tome 4 : Equations différentielles, intégrales multiples	Dunod
LELONG-FERRAND J.	Géométrie différentielle	Masson
LELONG-FERRAND J.	Les fondements de la géométrie	PUF
LESIEUR L. **MEYER Y.** **JOULAIN C.** **LEFEBVRE J.**	Algèbre linéaire, géométrie	Armand Colin
LION G.	Algèbre pour la licence Cours et exercices (2ème édition)	Vuibert
LION G.	Géométrie du plan Cours complet avec 600 exercices résolus	Vuibert
LOTHAIRE M.	Algebraic combinatorics on words	Cambridge
MAC LANE S. **BIRKHOFF G.**	Algèbre • 1 : Structures fondamentales • 2 : Les grands théorèmes	Gauthier-Villars
MACKI J. **STRAUSS A.**	Introduction to optimal control theory	Springer
MALLIAVIN M. P. **WARUSFEL A.**	Algèbre linéaire et géométrie classique. Exercices	Masson

MALLIAVIN M. P.	Les groupes finis et leurs représentations complexes	Masson
MALLIAVIN P.	Géométrie différentielle intrinsèque	Hermann
Manuels Matlab	• Using Matlab version 5 • Using Matlab version 6 • Statistics Toolbox	
MARCE S. **DEVAL-GUILLY E.**	Problèmes corrigés des ENSI	Ellipses
MASCART H. **STOKA M.**	Fonctions d'une variable réelle • Tome 2 : Exercices et corrigés • Tome 3 : Exercices et corrigés • Tome 4 : Exercices et corrigés	PUF
MAWHIN J.	Analyse : fondements, technique, évolutions	De Boeck Université
MAZET P.	Algèbre et géométrie pour le CAPES et l'Agrégation	Ellipses
MERKIN D.	Introduction to the theory of stability	Springer
MÉTIVIER M.	Notions fondamentales de la théorie des probabilités	Dunod
MÉTIVIER M.	Probabilités : dix leçons d'introduction. École Polytechnique	Ellipses
MEUNIER	Agrégation interne de Mathématiques Exercices d'oral corrigés et commentés • Tome 2	PUF
MIGNOTTE M.	Algèbre concrète, cours et exercices	Ellipses
MIGNOTTE M.	Mathématiques pour le calcul formel	PUF
MITCHELL J. C.	Concepts in programming languages	Cambridge

MNEIMNÉ R.	Eléments de géométrie : action de groupes	Cassini
MNEIMNÉ R.	Réduction des endomorphismes	Calvage et Mounet
MNEIMNÉ R. **TESTARD F.**	Introduction à la théorie des groupes de Lie classiques	Hermann
MOISAN J. **VERNOTTE A.** **TOSEL N.**	Exercices corrigés de mathématiques spéciales Analyse : suites et séries de fonctions	Ellipses
MOISAN J. **VERNOTTE A.**	Exercices corrigés de mathématiques spéciales Analyse : topologie et séries	Ellipses
MONIER J.M.	Cours de mathématiques • Analyse 1 MPSI, PCSI, PTSI • Analyse 2 MPSI, PCSI, PTSI • Analyse 3 MP, PSI, PC, PT • Analyse 4 MP, PSI, PC, PT • Algèbre 1 MPSI, PCSI, PTSI • Algèbre 2 MP, PSI, PC, PT • Exercices d'analyse MPSI • Exercices d'analyse MP • Exercice d'algèbre et géométrie MP	Dunod
MUTAFIAN C.	Le défi algébrique • Tome 1 • Tome 2	Vuibert
NAGEL E. **NEWMAN J. R.** **GÖDEL K.** **GIRARD J. Y.**	Le théorème de Gödel	Seuil
NAUDIN P. **QUITTE C.**	Algorithmique algébrique avec exercices corrigés	Masson
NEVEU J.	Base mathématique du calcul des probabilités	Masson

NIVEN I.	Irrational numbers	Mathematical Association of America
NORRIS J.R.	Markov chains	Cambridge
OPREA J.	Differential geometry	Prentice hall
OUVRARD J.Y.	• Probabilités 1 (capes, agrégation) • Probabilités 2 (maîtrise, agrégation)	Cassini
PAGES G. **BOUZITAT C.**	En passant par hasard ... Les probabilités de tous les jours	Vuibert
PAPINI O. **WOLFMANN J.**	Algèbre discrète et codes correcteurs	Springer
PEDOE D.	Geometry- A comprehensive course	Dover
PERKO L.	Differential equation and dynamical systems	Springer
PERRIN D.	Cours d'Algèbre	Ellipses
PERRIN D.	Cours d'Algèbre	ENSJF
PERRIN-RIOU B.	Algèbre, arithmétique et MAPLE	Cassini
PETAZZZONI B.	Seize problèmes d'informatique	Springer
PÓLYA G. **SZEGÖ G.**	Problems and Theorems in Analysis • Volume I • Volume II	Springer Verlag
POMMELLET A.	Agrégation de Mathématiques. Cours d'Analyse	Ellipses

QUEFFELEC H. **ZUILY C.**	Éléments d'analyse	Dunod
RALSTON A. **RABINOWITCH P**	A first curse in numerical analysis	Internatinal Student Edition
RAMIS E. **DESCHAMPS C.** **ODOUX J.**	Cours de Mathématiques spéciales • 1- Algèbre • 2- Algèbre et applications à la géométrie • 3- Topologie et éléments d'analyse • 4- Séries et équations différentielles • 5- Applications de l'analyse à la géométrie	Masson
RAMIS E. **DESCHAMPS C.** **ODOUX J.**	Exercices avec solutions • Algèbre • Analyse 1 • Analyse 2	Masson
RAO C.R.	Linear statistical inference and its application	Wiley
REINHARDT F. **SOEDER H.**	Atlas des mathématiques	Livre de Poche
RIDEAU F.	Exercices de calcul différentiel	Hermann
RIO E.	Théorie asymptotique des processus aléatoires faiblement dépendants	Springer
ROBERT C.	Contes et décomptes de la statistique - Une initiation par l'exemple	Vuibert
ROLLAND R.	Théorie des séries 2- Séries entières	Cédic/Nathan
ROMBALDI J.E.	Thèmes pour l'agrégation de mathématiques	EDP Sciences
ROMBALDI J.E.	Analyse matricielle	EDP Sciences
ROMBALDI J.E.	Interpolation, approximation Analyse pour l'agrégation	Vuibert

RUAUD J.F. **WARUSFEL A.**	Exercices de Mathématiques Algèbre 3	Masson
RUDIN W.	Analyse réelle et complexe	Masson
RUDIN W.	Functional analysis	Mc Graw Hill
RUDIN W.	Real and complex analysis	Mc Graw Hill
SAKS S. **ZYGMUND A.**	Fonctions analytiques	Masson
SAMUEL P.	Géométrie projective	PUF
SAMUEL P.	Théorie algébrique des nombres	Hermann
SARMANT M.C. **MERLIER T.** **PILIBOSSIAN Ph.** **YAMMINE S.**	Analyse 1	Ellipses
SAUVAGEOT F.	Petits problèmes de géométrie et d'algèbre	Springer
SAUX PICARD P.	Cours de calcul formel - Algorithmes fondamentaux	Ellipses
SAVIOZ J.C.	Algèbre linéaire, cours et exercices	Vuibert
SCHWARTZ L.	Analyse • I Topologie générale et analyse fonctionnelle • II Calcul différentiel et équations différentielles	Hermann
SCHWARTZ L.	Cours d'Analyse	Hermann
SEDGEWICK R.	Algorithms	Addison Wesley

SEDGEWICK R.	Algorithmes en Java	Pearson Education
SEDGEWICK R.	Algorithmes en langage C	Dunod
SELBERHERR S. **STIPPEL H.** **STRASSER E.**	Simulation of semi-conductor devices and processes	Springer
SERRE J.P.	Cours d'arithmétique	PUF
SERVIEN Cl.	• Analyse 3 • Analyse 4	Ellipses
SIDLER J.C.	Géométrie Projective	Dunod
SIPSER M.	Introduction to the theory of computation	Thomson C. T.
SKANDALIS G.	Topologie et analyse	Dunod
STANLEY R.P.	Enumerative combinatorics Volume I	Waddworth and Brooks
SZPIRGLAS A.	Exercices d'algèbre	Cassini
TAUVEL P.	Cours de Géométrie	Dunod
TAUVEL P.	Mathématiques générales pour l'agrégation	Masson
TAUVEL P.	Exercices de mathématiques pour l'agrégation Algèbre 2	Masson
TENENBAUM G. **WU J.**	Exercices corrigés de théorie analytique et probabiliste des nombres T 2	S. M. F.
TENENBAUM G.	Introduction à la théorie analytique et probabiliste des nombres T 1	S. M. F.

TENENBAUM G.	Introduction à la théorie analytique et probabiliste des nombres	Institut Elie Cartan
TENENBAUM G. **MENDÈS-FRANCE M.**	Les nombres premiers	Que sais-je ? PUF
TISSERON C.	Géométries affine, projective et euclidienne	Hermann
TISSIER A.	Mathématiques générales : exercices avec solutions	Bréal
TITCHMARSH E.C.	The theory of functions	Oxford
TORTRAT A.	Calcul des probabilités et introduction aux processus aléatoires	Masson
TRIGNAN J.	Constructions géométriques et courbes remarquables	Vuibert
TRUFFAULT B.	Exercices de géométrie élémentaires	IREM des Pays de Loire
TURING A **GIRARD J. Y.**	La Machine de Turing	Seuil
VALIRON G.	Cours d'analyse mathématique • I Théorie des fonctions • II Équations fonctionnelles - Applications	Masson
VAUQUOIS B.	Outils Mathématiques. Probabilités	Hermann
VAUTHIER J. **PRAT J-J.**	Cours d'Analyse Mathématique de l'Agrégation	Masson
WAGSCHAL C.	Fonctions holomorphes Équations différentielles	Hermann
WARUSFEL A.	Structures algébriques finies	Classiques Hachette

WARUSFEL, ATTALI COLLET, GAUTIER NICOLAS	Mathématiques • Analyse • Arithmétique • Géométrie • Probabilités	Vuibert
WEST D. B.	Introduction to graph theory	Prentice Hell
WHITTAKER E.T. WATSON G.N.	A course of modern analysis	Cambridge
WILF H.	Generatingfunctionology	Academic Press
WILLEM M.	Analyse fonctionnelle élémentaire	Cassini
WINSKEL G.	The formal semantics of programming languages	MIT Press
YALE P.B.	Geometry and Symmetry	Dover
YOUNG D.M. GREGORY R.T.	A survey of numerical mathematics	Dover
ZÉMOR G.	Cours de cryptographie	Cassini
ZUILY Cl. QUEFFELEC H.	Éléments d'analyse pour l'agrégation	Masson