MINISTÈRE DE L'ÉDUCATION NATIONALE

DIRECTION GÉNÉRALE DES RESSOURCES HUMAINES

RAPPORT DE JURY DE CONCOURS

AGRÉGATION DE MATHÉMATIQUES

CONCOURS EXTERNE

Session 2008

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

Table des matières

Chapitre 1

Composition du jury

Directoire

Foulon Patrick, Président	Professeur des Universités
Bougé Luc, Vice-président	Professeur des Universités
Moisan Jacques, Vice-président	Inspecteur général
Torossian Charles, Vice-président	Chargé de recherches
Van der Oord Eric, Vice-président	Inspecteur général
Chevallier Jean-Marie, Secrétaire général	Maître de conférences
Boisson François, Directoire	Professeur de chaire supérieure
Goudon Thierry, Directoire	Professeur des Universités
Lévy Thierry, Directoire	Chargé de recherches
Mestre Jean François, Directoire	Professeur des Universités
Petazzoni Bruno, Directoire	Professeur de chaire supérieure
Quercia Michel, Directoire	Professeur de chaire supérieure

Abergel Luc	Professeur de chaire supérieure
Aymard Catherine	Professeure de chaire supérieure
Bachmann Florence	Professeure agrégée
Barbolosi Dominique	Maître de conférences
Barou Geneviève	Maître de conférences
Barral Julien	Maître de conférences
Baumann Pierre	Chargé de recherche
Bayle Lionel	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
Bertrand Pierre	Professeur des Universités
Blanloeil Vincent	Maître de conférences
Bonnaillie-Noel Virginie	Chargée de recherche
Bonnefont Claire	Professeure de chaire supérieure
Borel Agnès	Professeure de chaire supérieure
Boyer Franck	Chargé de recherche
Burban Anne	Professeure de chaire supérieure

Cabane Robert	Inspecteur général
Cadoret Anna	Maître de conférences
Caldero Philippe	Maître de conférences
Cerf-Danon Hélène	Professeure de chaire supérieure
Chafaï Djalil	Maître de conférences
Chevallier Marie-Elisabeth	Professeure de chaire supérieure
Chillès Alain	Professeur de chaire supérieure
Contejean Evelyne	Chargée de recherche
Cori René	Maître de conférences
Correia Hubert	Professeur agrégé
De la Bretèche Régis	Professeur des Universités
De Seguins Pazzis Clément	Professeur agrégé
Devie Hervé	Professeur de chaire supérieure
Domelevo Komla	Maître de conférences
Dozias Sandrine	Professeure agrégée
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
Fleurant Sandrine	Professeure agrégée
Fontaine Philippe	Professeur agrégé
Fontanez Françoise	Professeure agrégée
Fort Jean-Claude	Professeur des Universités
Fouquet Mireille	Maître de conférences
Furter Jean-Philippe	Maître de conférences
Gallois Mirentchu	Professeure agrégée
Gamboa Fabrice	Professeur des Universités
Gaudry Pierrick	Chargé de recherche
Godefroy Gilles	Directeur de recherche
Goldsztejn Emmanuel	Professeur agrégé
Guelfi Pascal	Professeur de chaire supérieure
Guibert Gil	Professeur agrégé
Haas Bénédicte	Maître de conférences
Hanrot Guillaume	Chargé de recherche
Harinck Pascale	Chargée de recherche
Hernandez David	Chargé de recherche
Hirsinger Odile	Professeure agrégée
Isaïa Jérôme	Professeur agrégé
Istas Jacques	Professeur des Universités
Julg Pierre	Professeur des Universités
Kostyra Marie-Laure	Professeure agrégée
Lafitte Pauline	Maître de conférences
Latrémolière-Quercia Evelyne	Professeure de chaire supérieure
Le Calvez Patrice	Professeur des Universités
Le Merdy Sylvie	Professeure agrégée
Le Nagard Eric	Professeur de chaire supérieure
Lefevre Pascal	Maître de conférences
Lévy Véhel Jacques	Directeur de recherche
Loiseau Bernard	Professeur de chaire supérieure
Maggi Pascale	Professeure de chaire supérieure

Mahieux Annick	Professeure de chaire supérieure
Maillot Vincent	Chargé de recherche
Marchal Philippe	Chargé de recherche
Martineau Catherine	Professeure de chaire supérieure
Méril Alex	Professeur des Universités
Méthou Edith	Professeure agrégée
Mézard Ariane	Professeure des Universités
Mitschi Claude	Maître de conférences
Mneimné Rached	Maître de conférences
Monier Marie	Professeure agrégée
Noble Pascal	Maître de conférences
Paoluzzi Luisa	Maître de conférences
Paradan Paul-Emile	Maître de conférences
Paroux Katy	Maître de conférences
Pennequin Denis	Maître de conférences
Peyre Emmanuel	Professeur des Universités
Philibert Bertrand	Professeur agrégé
Prieur Clémentine	Maître de conférences
Quentin de Gromard Thierry	Maître de conférences
Régnier Mireille	Directrice de recherche
Risler Jean-Jacques	Professeur des Universités
Samson Adeline	Maître de conférences
Sauloy Jacques	Maître de conférences
Sauvé Marie	Professeur agrégé
Seuret Stéphane	Maître de conférences
Sidaner Sophie	Professeure de chaire supérieure
Suffrin Frédéric	Professeur agrégé
Taieb Franck	Professeur de chaire supérieure
Tosel Emmanuelle	Professeure agrégée
Tosel Nicolas	Professeur de chaire supérieure
Vernier le Goff Claire	Professeure agrégée
Vincent Christiane	Professeure de chaire supérieure
Wagschal Claude	Professeur des Universités
Weil Jacques-Arthur	Maître de conférences
Zayana Karim	Professeur agrégé
Zeitoun Marc	Professeur des Universités
Zwald Laurent	Maître de conférences

Chapitre 2

Déroulement du concours et statistiques

2.1 Déroulement du concours

Les épreuves écrites se sont déroulées selon le calendrier suivant :

- Épreuve de mathématiques générales : jeudi 2 avril 2008 ;
- Épreuve d'analyse et probabilités : vendredi 3 avril 2008 .

La liste d'admissibilité a été publiée le mardi 3 juin 2008.

L'oral s'est déroulé du 24 juin au 13 juillet au lycée Marcelin-Berthelot de Saint-Maur-des-Fossés. La liste d'admission a été publiée le lundi 16 juillet 2008.

Depuis 2006 le concours propose quatre options qui se distinguent seulement pour les trois premières A, B, C, par les épreuves de modélisation et l'option D (informatique) avec trois épreuves orales spécifiques. En 2008 comme en 2007, 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.

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`

[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.

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.

2.2 Statistiques et commentaires généraux sur la session 2008

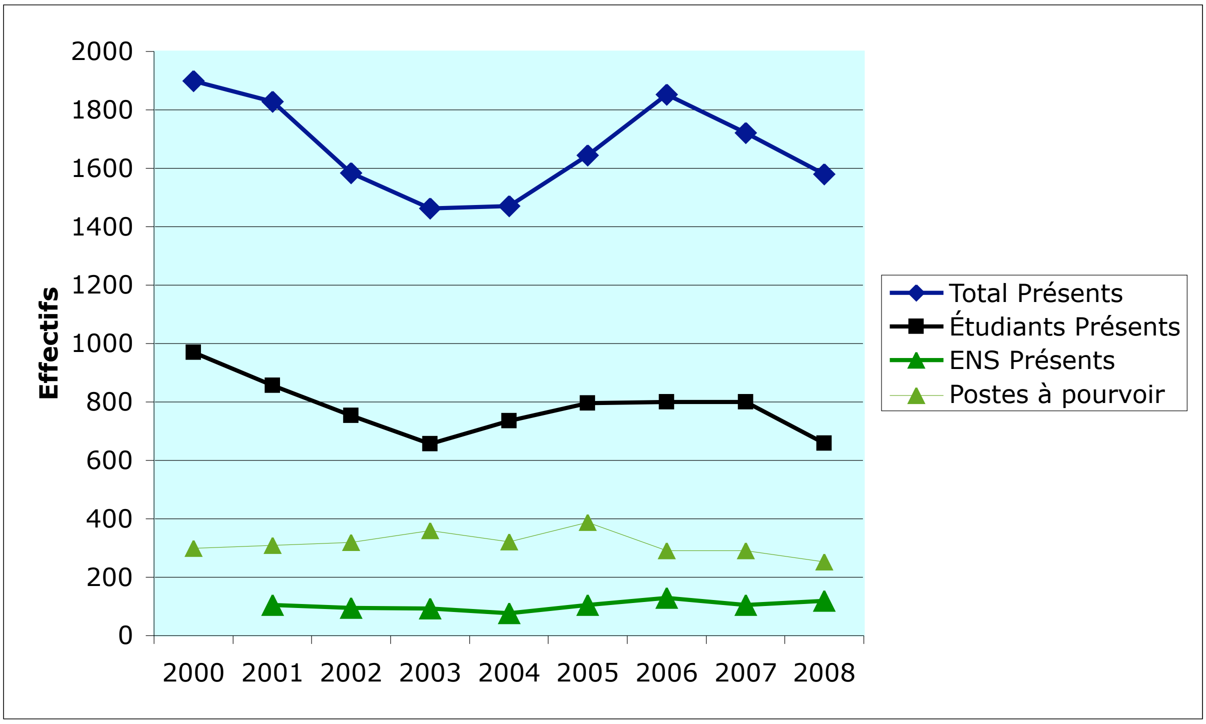
Après la diminution sensible du nombre de postes au concours 2006 (de 388 postes en 2005 à 290 postes en 2006 et 2007 soit une diminution de plus de 23 %), le nombre de postes proposés au concours 252 en 2008 subit une nouvelle baisse de 13 %.

L'augmentation régulière du nombre d'inscrits constatée depuis le concours 2004 a plafonné en 2006-07 . Le nombre d'inscrits et surtout le nombre de présents aux deux épreuves d'écrit en 2008 est en baisse sensible : c'est certainement la conséquence 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 des étudiants hors ENS.[3]

Année	Total Inscrits	Total Présents	Étudiants Présents	ENS Présents	Postes à pourvoir	Présents par poste
2000	**2875**	**1900**	970		300	**6,3**
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**
2008	**2491**	**1579**	659	119	252	**6,3**

Évolution du nombre de présents aux deux épreuves d'écrit



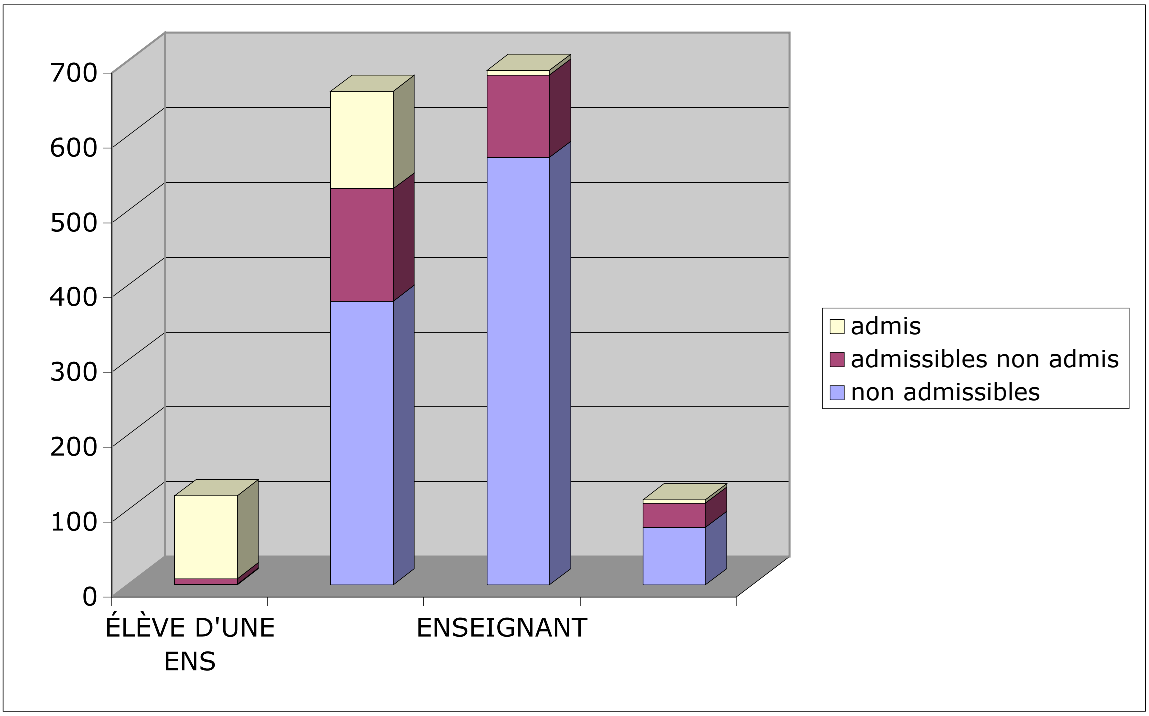
[3] dans cette population, sont regroupées les catégories « étudiant »et « élève de 1re année d'IUFM ».

À l'issue de la délibération d'écrit, 551 candidats ont été déclarés admissibles ; le premier admissible avait une moyenne de 20/20 et le dernier une moyenne de 8,375/20. Finalement, à l'issue des épreuves orales, les 252 postes offerts au concours ont été pourvus ; le premier admis a une moyenne de 19,6/20, le dernier admis une moyenne de 10,1/20.

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	162	110	22	8	20,0	7,3
ÉLÈVE D'UNE ENS	125	119	118	111	99,2	93,3
ÉTUDIANT	637	549	258	122	47,0	22,2
SALARIÉ SECTEUR PRIVÉ	93	31	12	1	38,7	3,2
SANS EMPLOI	110	50	21	4	42,0	8,0
ENSEIGNANT DU SUPÉRIEUR	28	16	6	2	37,5	12,5
AGRÉGÉ	2	1	0	0	0,0	0,0
CERTIFIÉ	851	455	76	1	16,7	0,2
PLP	37	12	3	0	25,0	0,0
AUTRE ENSEIGNANT 2nd DEGRÉ	357	201	30	3	14,9	1,5
ENSEIGNANT 1er DEGRÉ	9	2	1	0	50,0	0,0
AUTRE FONCTIONNAIRE	15	4	1	0	25,0	0,0
SURVEILLANT	22	10	1	0	10,0	0,0
AUTRE	43	19	2	0	10,5	0,0
TOTAL	**2491**	**1579**	**551**	**252**	**34,9**	**16,0**

Résultat du concours par catégories professionnelles[4]



Résultat du concours par grandes catégories

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

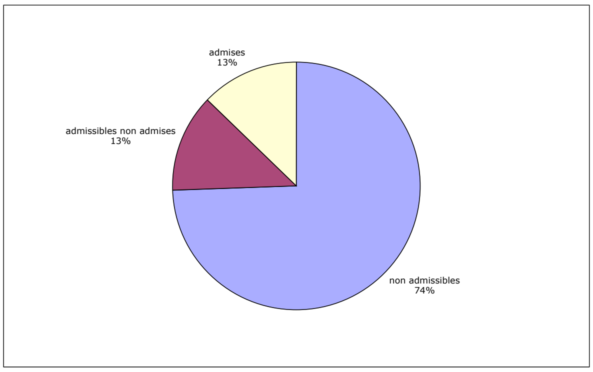
[4] Les catégories professionnelles listées ci-dessus correspondent aux déclarations des candidats lors de l'inscription : elles ne font l'objet d'aucune vérification et doivent être considérées avec prudence.

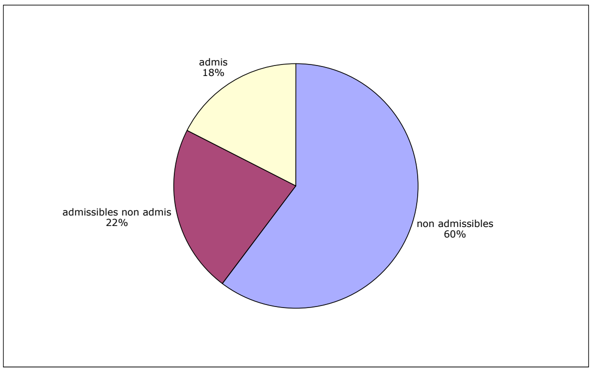
des étudiants (ENS et hors ENS) constitue en effet 92 % de l'effectif des admis (88 % en 2007).

Répartition selon le genre

GENRE	Inscrits	Présents	Admissibles	Admis	% Admissibles	% Admis
FEMMES	828	535	137	68	25,61	12,71
HOMMES	1663	1044	414	184	39,66	17,62
TOTAL	2491	1579	551	252	34,90	15,96

Résultat du concours par genres





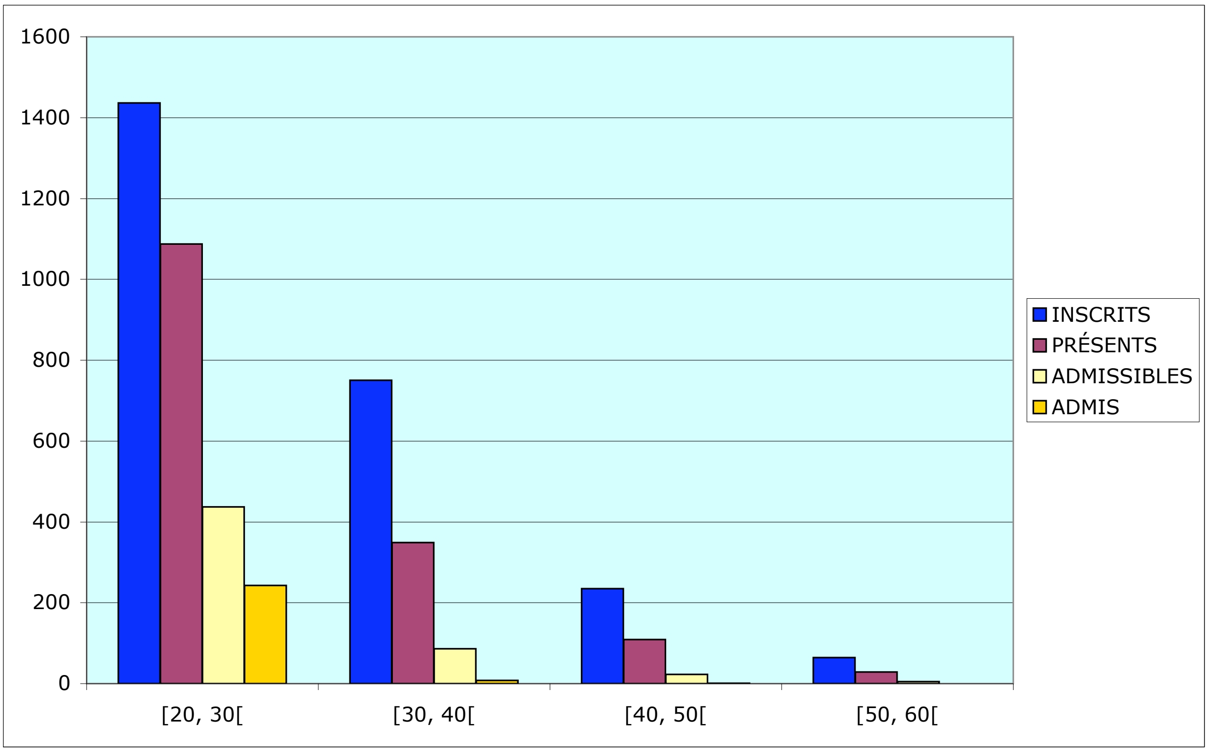
FEMMES HOMMES

On constate un léger rééquilibrage de la parité pour le succès au concours, par rapport aux pourcentages constatés en 2007 (19, 9 % d'admis pour 10, 9 % d'admises). Ceci fait suite à une baisse constatée en 2006 et 2007 alors que les taux de succès chez les femmes (23 %) et chez les hommes (24 %) étaient pratiquement identiques en 2005. Ces pourcentages sont à analyser en tenant compte du fait que 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 (16 % cette année, à comparer aux 10% de 2007). Dans cette catégorie, on trouve en effet, en 2007, 44 % des reçus au concours (contre 34, % en 2007). Si l'on regarde, en revanche, dans la catégorie des étudiants hors ENS, la parité est respectée dans les succès, puisqu'il y a 22 % d'admis chez les hommes et 23 % chez les femmes !

Répartition selon l'âge

TRANCHE D'ÂGE	INSCRITS	PRÉSENTS	ADMISSIBLES	ADMIS
[20, 30[	1436	1087	437	243
[30, 40[	750	349	86	8
[40, 50[	235	109	23	1
[50, 60[	64	29	5	0

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 96 % des reçus ont moins de 30 ans.

Répartition selon l'académie

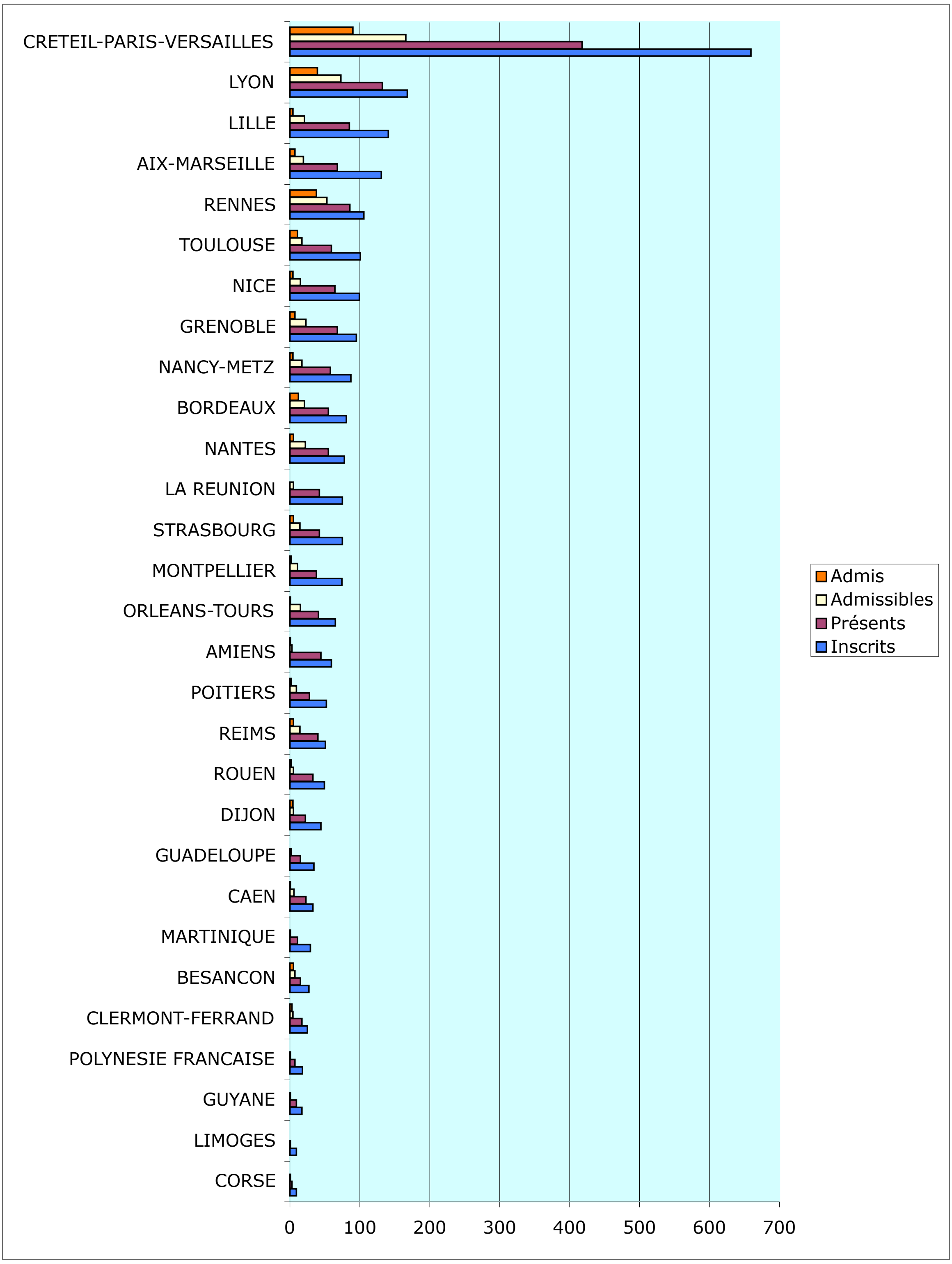
Académie	Inscrits	Présents	Admissibles	Admis
AIX-MARSEILLE	131	68	19	7
AMIENS	59	44	3	1
BESANCON	27	15	7	5
BORDEAUX	81	55	21	12
CAEN	33	23	6	1
CLERMONT-FERRAND	25	17	4	3
CORSE	9	3	1	0
DIJON	44	22	5	4
GRENOBLE	95	68	23	7
GUADELOUPE	34	15	2	0
GUYANE	17	9	1	0
LA RÉUNION	75	42	5	0
LILLE	141	85	21	4
LIMOGES	9	1	0	0
LYON	168	132	73	39
MARTINIQUE	29	11	1	0
MONTPELLIER	74	38	11	2
NANCY-METZ	87	58	17	4
NANTES	78	55	22	5
NICE	99	64	15	4
ORLÉANS-TOURS	65	41	15	1
POITIERS	52	28	9	2
REIMS	51	40	14	5
RENNES	106	86	53	38
ROUEN	49	33	5	2
STRASBOURG	75	42	14	5
TOULOUSE	101	59	17	11
POLYNESIE FRANCAISE	18	7	1	0
CRÉTEIL-PARIS-VERSAILLES	659	418	166	90
TOTAL	2491	1579	551	252

Résultat du concours par académies

Hors ENS	Inscrits	Présents	Admissibles	Admis
CRÉTEIL-PARIS-VERSAILLES	593	357	105	34
RENNES	75	55	23	9
LYON	141	105	46	13

ENS seulement	Inscrits	Présents	Admissibles	Admis
CRETEIL-PARIS-VERSAILLES	66	61	61	56
RENNES	31	31	30	29
LYON	27	27	27	26

Représentation des résultats par académies (y compris ENS)



Chapitre 3

Épreuve écrite de mathématiques générales

3.1 Énoncé

Préambule

Ce problème a pour objectif de démontrer le théorème de finitude sur les classes d'équivalence de groupes libres quadratiques en utilisant l'inégalité de Hermite-Minkovski. On étudie dans la partie I les sous-groupes finis de $GL_n(\mathbf{Z})$. La partie II est consacrée à l'étude des réseaux et en particulier la démonstration de l'inégalité de Hermite. On étudie dans la partie III les cristalloïdes. On démontre enfin le théorème de finitude dans la partie IV. Les deux premières parties sont indépendantes. La troisième n'utilise que les questions II-1 et II-3. Les parties III et IV sont indépendantes.

Notations

- Dans tout le problème, E est un espace vectoriel réel de dimension finie $n \geqslant 1$.
- On note $\mathbf{R}$ le corps des nombres réels, $\mathbf{C}$ le corps des nombres complexes, $\mathbf{Q}$ le corps des nombres rationnels, $\mathbf{Z}$ l'anneau des entiers relatifs et $\mathbf{N}$ l'ensemble des entiers naturels. On note $\mathbf{Z}^*$ l'ensemble des entiers relatifs privé de 0 et $\mathbf{N}^*$ l'ensemble des entiers naturels privé de 0.
- Si A et B sont deux ensembles, on note $A \setminus B$ l'ensemble des éléments de A qui n'appartiennent pas à B.
- Si F est un espace vectoriel réel, on note $L(E,F)$ l'ensemble des applications linéaires de E dans F et $GL(E)$ le groupe linéaire de E. Si f est un endomorphisme de E et e une base de E, on note $\mathrm{Mat}(f,e)$ la matrice de f dans la base e.
- Si $(e_1,..,e_p)$ est une famille de vecteurs de E, on note $< e_1,..,e_p >$ le sous-espace vectoriel de E engendré par la famille $(e_1,..,e_p)$.
- On note $M_n(\mathbf{Z})$ l'anneau des matrices à coefficients entiers de taille n et $GL_n(\mathbf{Z})$ le groupe des éléments inversibles de cet anneau. Si $k \in \mathbf{N}^*$ on note $kM_n(\mathbf{Z})$ l'ensemble des matrices de $M_n(\mathbf{Z})$ dont tous les coefficients sont des multiples de k.

Rappels

- On rappelle qu'une matrice de $M_n(\mathbf{Z})$ appartient à $GL_n(\mathbf{Z})$ si et seulement si son déterminant est égal à 1 ou -1. Si $\mathbf{K}$ est un corps, on note $M_n(\mathbf{K})$ l'ensemble des matrices de taille n à coefficients dans le corps $\mathbf{K}$ et I_n la matrice identité de taille n.
- Si p et q sont deux entiers naturels, on note $p \wedge q$ le plus grand commun diviseur de p et q, on note également $p|q$ si p divise q. Si m est un entier supérieur ou égal à 1, on note $\Phi_m(X)$ le polynôme cyclotomique d'ordre m. On rappelle que
$$\Phi_m(X) = \prod_{\{k \in \{1,..,m\} / k \wedge m = 1\}} (X - e^{2ik\pi/m}).$$

– On rappelle également que $\Phi_m(X)$ est un polynôme unitaire à coefficients entiers, irréductible dans $\mathbf{Q}[X]$. Le degré de $\Phi_m(X)$ est $\varphi(m)$ où φ est la fonction indicatrice d'Euler, définie de $\mathbf{N}^*$ dans $\mathbf{N}^*$ par : si p est un nombre premier et $r \in \mathbf{N}^*$ on a $\varphi(p^r) = p^r - p^{r-1}$ et si $p \in \mathbf{N}^*$ et $q \in \mathbf{N}^*$ sont premiers entre eux, alors $\varphi(pq) = \varphi(p)\varphi(q)$.
– On rappelle enfin que

$$X^m - 1 = \prod_{d|m} \Phi_d(X).$$

– Si $P = X^n + \sum_{i=0}^{n-1} a_i X^i$ est un polynôme unitaire de degré n à coefficients complexes, on note M_P la matrice compagnon de $M_n(\mathbf{C})$ dont le (i,j)-ième terme vaut 1 si $i = j+1$, vaut $-a_{i-1}$ si $j = n$, vaut 0 dans les autres cas. Ainsi pour le polynôme $P = X^3 + a_2X^2 + a_1X + a_0$, la matrice M_P est de la forme

$$M_P = \begin{pmatrix} 0 & 0 & -a_0 \\ 1 & 0 & -a_1 \\ 0 & 1 & -a_2 \end{pmatrix}.$$

Si $M \in M_n(\mathbf{C})$, on note $C_M(X) = \det(XI_n - M)$ le polynôme caractéristique de M.

I Sous-groupes finis de $GL_n(\mathbf{Z})$

1. Soit P un polynôme à coefficients complexes unitaire de degré n et M_P la matrice compagnon qui lui est associée. Démontrer que P est le polynôme caractéristique de la matrice M_P.
2. Soit $M \in GL_2(\mathbf{Z})$, d'ordre fini m.
   (a) Montrer que si z est une racine complexe du polynôme $C_M(X)$ alors z est racine du polynôme $X^m - 1$.
   (b) Montrer, en résolvant avec soin l'équation $\varphi(k) = 1$, qu'il y a exactement deux polynômes cyclotomiques de degré un.
   (c) Montrer de même qu'il y a exactement trois polynômes cyclotomiques de degré deux dont on donnera les expressions développées.
   (d) En déduire que le polynôme $C_M(X)$ appartient à l'ensemble
   $$\{X^2 + X + 1, X^2 + 1, X^2 - X + 1, X^2 - 1, (X-1)^2, (X+1)^2\}.$$
   (e) En déduire que $m \in \{1, 2, 3, 4, 6\}$.
   (f) Donner un élément de $GL_2(\mathbf{Z})$ d'ordre 6.
3. Soit $M \in GL_n(\mathbf{Z})$ d'ordre $m \geqslant 2$ et p un nombre premier, $p \geqslant 3$. On suppose que $M = I_n + p^r N$ avec $r \in \mathbf{N}^*$ et $N \in M_n(\mathbf{Z}) \setminus pM_n(\mathbf{Z})$.
   (a) Montrer que $mp^r N \in p^{2r} M_n(\mathbf{Z})$. En déduire que p divise m.
   On pose alors $m = pm'$ et $M' = M^p$.
   (b) Montrer que p divise m'.
   (c) Conclure à une contradiction.
4. Soit p un nombre premier, $p \geqslant 3$. Soit G un sous-groupe fini de $GL_n(\mathbf{Z})$. On note $\mathbf{F}_p$ un corps de cardinal p, unique à isomorphisme près. On rappelle que la surjection naturelle $\mathbf{Z} \to \mathbf{F}_p$ induit un morphisme de groupes
   $$GL_n(\mathbf{Z}) \to GL_n(\mathbf{F}_p).$$
   Montrer que G est isomorphe à un sous-groupe de $GL_n(\mathbf{F}_p)$.

5. Soit G un sous-groupe fini de $GL_2(\mathbf{Z})$.
   (a) Montrer que le cardinal de G est un diviseur de 48.
   (b) Montrer que le cardinal de G ne peut pas être égal à 48.

   (On pourra, éventuellement, étudier $\Phi_8(X)$ considéré comme un polynôme à coefficients dans $\mathbf{F}_3$.)

II Réseaux

On suppose dans la suite du problème que l'espace vectoriel E est muni d'un produit scalaire $(.,.)$ et de la norme $\| \ \|$ associée. Si F est un sous-espace vectoriel de E, on note $F^\perp$ son orthogonal. On rappelle qu'un réseau $\mathscr{R}$ de E est un ensemble de vecteurs de la forme

$$\{\sum_{i=1}^{n} a_i e_i \ / \ \forall i \in \{1,..,n\}\ ,\ a_i \in \mathbf{Z}\}.$$

où $e = (e_1,..,e_n)$ est une base de E. La famille e est dite $\mathbf{Z}$-base de $\mathscr{R}$. Un élément v de $\mathscr{R}$ est dit primitif s'il existe une $\mathbf{Z}$-base e de $\mathscr{R}$ telle que les coordonnées de v dans e sont premières entre elles dans leur ensemble. **On admet** le résultat suivant qui pourra être utilisé librement : si v est un vecteur primitif d'un réseau $\mathscr{R}$, il existe une $\mathbf{Z}$-base de $\mathscr{R}$ de la forme $(v, v_2,.., v_n)$.

Dans toute la suite du problème, $\mathscr{R}$ est un réseau de E.

1. Soit e une $\mathbf{Z}$-base de $\mathscr{R}$ et e' une famille de n vecteurs de E. Montrer que e' est une $\mathbf{Z}$-base de $\mathscr{R}$ si et seulement si e' est une base de E et la matrice de passage de e à e' appartient à $GL_n(\mathbf{Z})$.
2. Soit $e = (e_1,..,e_n)$ une $\mathbf{Z}$-base de $\mathscr{R}$. Montrer que le déterminant de la matrice de $M_n(\mathbf{R})$ dont le (i,j)-ième coefficient est égal à (e_i, e_j) est indépendant du choix de la $\mathbf{Z}$-base e de $\mathscr{R}$. C'est le discriminant du réseau $\mathscr{R}$, on le note $\Delta(\mathscr{R})$.
3. Soit r un réel strictement positif et a un élément de E. On note

   $$B(a,r) = \{x \in E \ / \ \|x - a\| \leqslant r\}.$$

   Montrer que $B(a,r) \cap \mathscr{R}$ est de cardinal fini.

   Si A est un sous-ensemble non vide minoré de $\mathbf{R}$, on note Inf A la borne inférieure de A. On note $m(\mathscr{R}) = \mathrm{Inf}\,\{\ \|x\| \ / \ x \in \mathscr{R} \setminus \{0\}\}$.

4. Montrer que le réel $m(\mathscr{R})$ est strictement positif et qu'il existe $v \in \mathscr{R} \setminus \{0\}$ vérifiant $\|v\| = m(\mathscr{R})$.
5. On suppose $n \geqslant 2$ dans les questions 5-a, 5-b et 5-c. Soit $k \in \{1,..,n-1\}$ et $(v_1,.., v_k, e_{k+1},..e_n)$ une $\mathbf{Z}$-base de $\mathscr{R}$. On pose $W_k =< v_1,.., v_k >$ et π_k la projection orthogonale sur $W_k^\perp$.
   (a) Montrer que $\pi_k(\mathscr{R})$ est un réseau de $W_k^\perp$ dont on précisera une $\mathbf{Z}$-base.
   (b) Montrer qu'il existe un vecteur v_{k+1} du réseau $\mathscr{R}$ vérifiant

   $$\|\pi_k(v_{k+1})\| = m(\pi_k(\mathscr{R})).$$

   (c) Montrer qu'il existe une famille $(f_{k+2},.., f_n)$ de E telle que la famille $(v_1,.., v_{k+1}, f_{k+2},.., f_n)$ est une $\mathbf{Z}$-base de $\mathscr{R}$.
   (On pourra montrer que $\pi_k(v_{k+1})$ est un vecteur primitif du réseau $\pi_k(\mathscr{R})$.)

(d) En déduire qu'il existe une $\mathbf{Z}$-base $(v_1,..,v_n)$ de $\mathscr{R}$ vérifiant $\|v_1\| = m(\mathscr{R})$ et

$$\forall k \in \{1,..,n-1\} \ \ \|\pi_k(v_{k+1})\| = m(\pi_k(\mathscr{R})),$$

où l'on note π_k la projection orthogonale sur $< v_1,..,v_k >^{\perp}$. Une telle base est appelée base réduite du réseau $\mathscr{R}$.

(e) On considère $\mathbf{R}^2$ muni de sa structure euclidienne usuelle. Soit $\mathscr{R}_1$ le réseau de $\mathbf{R}^2$ déterminé par la $\mathbf{Z}$-base $e = ((1,0),(-1/2,\sqrt{3}/2))$. Vérifier que e est une base réduite de $\mathscr{R}_1$.

6. On suppose $n \geqslant 2$ dans les questions 6-a, 6-b et 6-c. Soit $e = (e_1,..,e_n)$ une base réduite de $\mathscr{R}$. Soit π_1 la projection orthogonale sur l'hyperplan $< e_1 >^{\perp}$.

(a) Montrer que pour tout couple (j,k) appartenant à $\{2,..,n\}^2$ on a

$$(\pi_1(e_j),\pi_1(e_k)) = (e_j,e_k) - \frac{1}{m(\mathscr{R})^2}(e_1,e_j)(e_1,e_k).$$

(b) Montrer que $\Delta(\mathscr{R}) = m(\mathscr{R})^2\Delta(\pi_1(\mathscr{R}))$.

(c) Soit $v \in \mathscr{R}\setminus\{0\}$. On suppose que $v = te_1 + v'$ avec $t \in \mathbf{R}$ et $v' \in < e_1 >^{\perp}$. Vérifier que

$$m(\mathscr{R})^2 \leqslant t^2 m(\mathscr{R})^2 + \|v'\|^2.$$

(d) En déduire l'inégalité de Hermite :

$$m(\mathscr{R})^2 \leqslant (4/3)^{(n-1)/2}\Delta(\mathscr{R})^{1/n}.$$

7. On note H_n l'ensemble des réels $\rho \geqslant 0$ tels que pour tout réseau $\mathscr{R}$ de E on a $m(\mathscr{R})^2 \leqslant \rho\Delta(\mathscr{R})^{1/n}$. On note alors $\eta_n = \operatorname{Inf} H_n$.

(a) Montrer que $\eta_n \geqslant 1$.

(b) Montrer que $\eta_2 = 2/\sqrt{3}$.

III Cristalloïdes

On suppose dans cette partie $n \geqslant 2$. On note $O(E)$ le groupe orthogonal de E et $O(\mathscr{R})$ l'ensemble des isométries de E qui stabilisent $\mathscr{R}$ c'est à dire qui induisent une bijection de $\mathscr{R}$ sur $\mathscr{R}$. $O(\mathscr{R})$ est un sous-groupe de $O(E)$. Si e est une $\mathbf{Z}$-base de $\mathscr{R}$, l'application $\psi_e : g \to \mathrm{Mat}(g,e)$ est un morphisme injectif de groupes de $O(\mathscr{R})$ dans $GL_n(\mathbf{Z})$ qui permet d'identifier $O(\mathscr{R})$ à un sous-groupe de $GL_n(\mathbf{Z})$. Un cristalloïde de E est un couple $(\mathscr{R},\Gamma)$ où $\mathscr{R}$ est un réseau de E et Γ un sous-groupe de $O(\mathscr{R})$.

1. Montrer que $O(\mathscr{R})$ est de cardinal fini.

   On dit que deux cristalloïdes de E notés $(\mathscr{R},\Gamma)$ et $(\mathscr{R}',\Gamma')$ sont équivalents s'il existe $u \in GL(E)$ vérifiant $u(\mathscr{R}) = \mathscr{R}'$ et $u\Gamma u^{-1} = \Gamma'$. On définit ainsi une relation d'équivalence sur les cristalloïdes de E. Deux sous-groupes G et G' de $GL_n(\mathbf{Z})$ sont dits $\mathbf{Z}$-conjugués s'il existe $M \in GL_n(\mathbf{Z})$ vérifiant $MGM^{-1} = G'$. On définit ainsi une relation d'équivalence sur les sous-groupes de $GL_n(\mathbf{Z})$.

2. Soit $(\mathscr{R},\Gamma)$ un cristalloïde de E, e une $\mathbf{Z}$-base de $\mathscr{R}$ et G un sous-groupe de $GL_n(\mathbf{Z})$. Montrer que G est $\mathbf{Z}$-conjugué à $\psi_e(\Gamma)$ si et seulement s'il existe une $\mathbf{Z}$-base e' de $\mathscr{R}$ telle que $G = \psi_{e'}(\Gamma)$.

3. Soit $(\mathscr{R},\Gamma)$ et $(\mathscr{R}',\Gamma')$ deux cristalloïdes de E, e une $\mathbf{Z}$-base de $\mathscr{R}$ et e' une $\mathbf{Z}$-base de $\mathscr{R}'$. Montrer que $(\mathscr{R},\Gamma)$ est équivalent à $(\mathscr{R}',\Gamma')$ si et seulement si les groupes $\psi_e(\Gamma)$ et $\psi_{e'}(\Gamma')$ sont $\mathbf{Z}$-conjugués.

   On peut ainsi définir une application ψ qui à toute classe d'équivalence de cristalloïdes de E de représentant $(\mathscr{R},\Gamma)$ associe une classe de $\mathbf{Z}$-conjugaison de sous-groupes finis de $GL_n(\mathbf{Z})$ de représentant $\psi_e(\Gamma)$ où e est une $\mathbf{Z}$-base quelconque de $\mathscr{R}$.

4. Montrer que l'application ψ est une bijection de l'ensemble des classes d'équivalence de cristalloïdes de E sur l'ensemble des classes de $\mathbf{Z}$-conjugaison de sous-groupes finis de $GL_n(\mathbf{Z})$.
5. En déduire que $GL_2(\mathbf{Z})$ possède un sous-groupe isomorphe au groupe diédral D_6.

IV Groupes libres quadratiques

On suppose dans les questions 1,2 et 3 que E est muni d'une forme bilinéaire symétrique non dégénérée b de signature (p,q) avec $p \geqslant 1$. On suppose que la forme b vérifie

$$\forall (x,y) \in \mathscr{R}^2\ ,\ b(x,y) \in \mathbf{Q}.$$

Si F est un sous-espace vectoriel de E, on note $F^{\perp b}$ l'orthogonal de F pour la forme b. On note également

$$m_b(\mathscr{R}) = \mathrm{Inf}\,\{b(x,x)^{1/2}\ /\ x \in \mathscr{R}\ ,\ b(x,x) > 0\}.$$

De même que dans le cas euclidien, un élément v de $\mathscr{R}$ est dit primitif s'il existe une $\mathbf{Z}$-base e de $\mathscr{R}$ telle que les coordonnées de v dans e sont premières entre elles dans leur ensemble. On admet encore le résultat suivant : si v est un vecteur primitif d'un réseau $\mathscr{R}$, il existe une $\mathbf{Z}$-base de $\mathscr{R}$ de la forme $(v, v_2, .., v_n)$.

1. Montrer qu'il existe $v \in \mathscr{R} \setminus \{0\}$ tel que $m_b(\mathscr{R}) = b(v,v)^{1/2}$.

   On note $W = < v >^{\perp b}$ et b' la forme bilinéaire définie sur W par restriction de la forme b.

2. Déterminer la signature de b'.

   Soit $e = (e_1, .., e_n)$ une $\mathbf{Z}$-base de $\mathscr{R}$. Le déterminant de la matrice de $M_n(\mathbf{Q})$ de (i,j)-ième terme $b(e_i,e_j)$ est indépendant du choix de la $\mathbf{Z}$-base e. On le note $\Delta_b(\mathscr{R})$.

3. Démontrer l'inégalité de Hermite-Minkovski

   $$m_b(\mathscr{R})^2 \leqslant 3^{\frac{n-p}{n}} (4/3)^{\frac{n-1}{2}} |\Delta_b(\mathscr{R})|^{1/n}.$$

   (On pourra s'inspirer du raisonnement effectué dans la partie II pour démontrer l'inégalité de Hermite.)

   Un groupe libre quadratique est un couple $(\mathscr{R},b)$ où $\mathscr{R}$ est un réseau d'un espace vectoriel réel E de dimension n et b une forme bilinéaire symétrique sur E, non dégénérée, vérifiant

   $$\forall (x,y) \in \mathscr{R}^2\ ,\ b(x,y) \in \mathbf{Z}.$$

Le discriminant du groupe libre quadratique $(\mathscr{R}, b)$ est l'entier $\Delta_b(\mathscr{R})$, son rang est l'entier n. Deux groupes libres quadratiques $(\mathscr{R}, b)$ et $(\mathscr{R}', b')$, associés à des espaces vectoriels E et E' sont dits équivalents s'il existe $u \in L(E, E')$ qui induit une bijection de $\mathscr{R}$ sur $\mathscr{R}'$ vérifiant

$$\forall (x, y) \in \mathscr{R}^2\ ,\ b'(u(x), u(y)) = b(x, y).$$

On définit ainsi une relation d'équivalence sur l'ensemble des groupes libres quadratiques. Le but de cette partie est de démontrer le théorème suivant : pour tout couple $(\Delta, n) \in \mathbf{Z}^* \times \mathbf{N}^*$ il n'y a qu'un nombre fini de classes d'équivalence de groupes libres quadratiques de discriminant Δ et de rang n.

4. Soit $(\mathscr{R}, b)$ un groupe libre quadratique. On suppose b de signature (p, q) avec $p \geqslant 1$. On reprend les notations v, W et b' introduites à la question IV-1. On note π la projection sur W parallèlement à $< v >$ et $\mathscr{R}' = \pi(\mathscr{R})$. On sait que $\mathscr{R}'$ est un réseau de W. On pose enfin

$$\mathscr{R}'' = m_b(\mathscr{R})^2 \mathscr{R}' = \{m_b(\mathscr{R})^2 v \ /\ v \in \mathscr{R}'\}.$$

   (a) Montrer que $\mathscr{R}'' \subset \mathscr{R}$ et que
   $$\forall (x, y) \in \mathscr{R}''^2\ ,\ b'(x, y) \in \mathbf{Z}.$$
   (b) Montrer que $\Delta_{b'}(\mathscr{R}'')$ ne peut prendre qu'un nombre fini de valeurs, le discriminant $\Delta_b(\mathscr{R})$ étant fixé.

5. Soit $(\mathscr{R}_1, b_1)$ un groupe libre quadratique. On appelle extension de $(\mathscr{R}_1, b_1)$ tout groupe libre quadratique de la forme $(\mathscr{R}_2, b_1)$ avec $\mathscr{R}_1 \subset \mathscr{R}_2$. On appelle réseau complémentaire de $\mathscr{R}_1$ l'ensemble

$$C(\mathscr{R}_1) = \{y \in E\ /\ \forall x \in \mathscr{R}_1\ ,\ b_1(x, y) \in \mathbf{Z}\}.$$

   (a) Montrer que $C(\mathscr{R}_1)$ est un réseau de E et que pour toute extension $(\mathscr{R}_2, b_1)$ de $(\mathscr{R}_1, b_1)$ on a $\mathscr{R}_2 \subset C(\mathscr{R}_1)$.
   (b) Montrer que le cardinal du groupe quotient $C(\mathscr{R}_1)/\mathscr{R}_1$ est fini.

6. Démontrer le théorème de finitude : pour tout couple $(\Delta, n) \in \mathbf{Z}^* \times \mathbf{N}^*$ il n'y a qu'un nombre fini de classes d'équivalence de groupes libres quadratiques de discriminant Δ et de rang n.

7. Exemples.
   (a) Montrer qu'il y a exactement une classe d'équivalence de groupes libres quadratiques de rang 2 et de discriminant -2.
   (On pourra montrer, si $(\mathscr{R}, b)$ est un groupe libre quadratique de rang 2 et de discriminant -2, qu'il existe $v \in \mathscr{R}$, primitif, vérifiant $b(v, v) \in \{1, 2\}$.)
   (b) Montrer qu'il y a exactement deux classes d'équivalence de groupes libres quadratiques de rang 2 et de discriminant -1.

3.2 Corrigé

I. - Sous-groupes finis de $GL_n(\mathbf{Z})$

1. Il s'agit d'un résultat classique : montrons le par récurrence sur le degré $n \in \mathbf{N}^*$ du polynôme P.
Pour $n = 1$, P est de la forme $X + a_0$, $M_P = (-a_0)$ et $C_{M_P}(X) = |X + a_0| = X + a_0 = P$. Pour $n \geqslant 2$, supposons avoir établi le résultat au rang $n-1$. Un polynôme P à coefficients complexes unitaire de degré n est de la forme $P = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 = XQ + a_0$, où
$Q = X^{n-1} + a_{n-1}X^{n-2} + \ldots + a_2X + a_1$.
Or, $C_{M_P}(X) = \det(XI_n - M_P) = \begin{vmatrix} X & 0 & \ldots & \ldots & \ldots & 0 & a_0 \\ -1 & X & 0 & \ldots & \ldots & 0 & a_1 \\ 0 & -1 & X & 0 & \ldots & 0 & a_2 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & \ldots & 0 & -1 & X & 0 & a_{n-3} \\ 0 & \ldots & \ldots & 0 & -1 & X & a_{n-2} \\ 0 & \ldots & \ldots & \ldots & 0 & -1 & X + a_{n-1} \end{vmatrix}$.
En développant ce déterminant par rapport à la première ligne, il vient :
$C_{M_P}(X) = X\det(XI_{n-1} - M_Q) + a_0(-1)^{n+1}(-1)^{n-1} = XC_{M_Q}(X) + a_0$.
Or, par hypothèse de récurrence, $C_{M_Q}(X) = Q$; d'où $C_{M_P}(X) = XQ + a_0 = P$.
Par conséquent, pour tout polynôme P à coefficients complexes unitaire de degré n, le polynôme caractéristique de la matrice compagnon qui lui est associée est le polynôme P lui-même.

2. (a) Soit $M \in GL_2(\mathbf{Z})$ d'ordre fini $m \in \mathbf{N}^*$. Le complexe z étant racine de $C_M(X)$ est valeur propre de la matrice M, donc racine de tout polynôme annulateur de M. La matrice M étant d'ordre m, le polynôme $X^m - 1$ est annulateur pour M, donc z est racine de ce polynôme.

   (b) Le nombre de polynômes cyclotomiques de degré 1 est égal au nombre de solutions de l'équation $\varphi(k) = 1$ d'inconnue $k \in \mathbf{N}^*$. Soit p un nombre premier et r un entier strictement positif tel que $\varphi(p^r) \leqslant 1$. On obtient donc
$$p^{r-1}(p-1) \leqslant 1.$$
On en déduit que $p - 1 \leqslant 1$ donc p est égal à 2. Si $p = 2$ on a alors $r \leqslant 1$ (la fonction $r \to 2^{r-1}$ est strictement croissante sur $\mathbf{N}^*$). Donc une solution k n'admet comme facteur premier que le nombre 2 avec exposant inférieur ou égal à 1. L'équation n'admet donc que deux solutions, $k = 1$ ou $k = 2$. Il y a donc exactement deux polynômes cyclotomiques de degré 1, les polynômes $\Phi_1(X) = X - 1$ et $\Phi_2(X) = X + 1$.

   (c) Le nombre de polynômes cyclotomiques de degré 2 est égal au nombre de solutions de l'équation $\varphi(k) = 2$ d'inconnue $k \in \mathbf{N}^*$. Soit p un nombre premier et r un entier strictement positif tel que $\varphi(p^r) \leqslant 2$. On obtient donc
$$p^{r-1}(p-1) \leqslant 2.$$
Par conséquent, $p - 1 \leqslant 2$. Si $p = 2$ on a $r = 1$ ou $r = 2$, et si $p = 3$ alors $r = 1$. Donc le nombre k n'admet dans sa décomposition en facteurs irréductibles que les nombres premiers 2 avec exposant possible inférieur à 2 et 3 avec exposant possible inférieur à 1. On obtient alors aisément $\varphi(k) = 2$ si et seulement si $k = 3, 4$ ou 6. Par conséquent les polynômes cyclotomiques de degré 2 sont $\Phi_3(X) = (X - j)(X - j^2) = X^2 + X + 1$, $\Phi_4(X) = (X - i)(X + i) = X^2 + 1$ et
$\Phi_6(X) = (X + j)(X + j^2) = X^2 - X + 1$.

   (d) Soit P un facteur irréductible dans $\mathbf{Q}[X]$ de $C_M(X)$. D'après la question (a), toute racine complexe z de P est racine de $C_M(X)$, donc de $X^m - 1$: c'est donc une racine m-ième de l'unité. Comme P est scindé sur $\mathbf{C}$, il divise donc $X^m - 1$ dans $\mathbf{C}[X]$, mais aussi dans $\mathbf{Q}[X]$. Par unicité de la décomposition du polynôme $X^m - 1$ en produit de polynômes irréductibles dans $\mathbf{Q}[X]$, et connaissant la décomposition $X^m - 1 = \prod_{d|m} \Phi_d(X)$, P est nécessairement un polynôme cyclotomique.

$C_M(X)$ étant unitaire, c'est donc un produit de polynômes cyclotomiques. Comme il est de degré 2, on déduit, d'après les questions (b) et (c), que :

- ou bien c'est un polynôme cyclotomique de degré 2, c'est-à -dire : Φ_3, Φ_4 ou Φ_6 ;
- ou bien c'est le produit de deux polynômes cyclotomiques de degré 1, c'est-à-dire : $\Phi_1^2, \Phi_1\Phi_2$ ou Φ_2^2.

Ainsi, $C_M(X)$ est l'un des six polynômes unitaires suivant : X^2+X+1, X^2+1, X^2-X+1, $(X-1)^2$, $(X-1)(X+1)$ ou $(X+1)^2$.

(e) La matrice M est d'ordre m, donc admet le polynôme X^m-1 comme polynôme annulateur. Ce polynôme étant scindé à racines simples dans $\mathbf{C}$, la matrice M est diagonalisable dans $\mathbf{C}$. Son ordre est donc le PPCM des ordres de ses valeurs propres (vues comme éléments du goupe $(\mathbf{C}^*,*)$). Si $C_M(X)=\Phi_4(X)$, les valeurs propres de M sont i et $-i$ donc $m=4$. Dans tous les autres cas, les valeurs propres sont des racines sixièmes de l'unité, donc m est un diviseur de 6, d'où le résultat.

(f) $M=\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ appartient à $GL_2(\mathbf{Z})$ car $\det(M)=1$.

De plus, $C_M(X)=X^2-X+1$ (c'est une matrice compagnon), donc M est diagonalisable dans $\mathbf{C}$ avec deux valeurs propres qui sont des racines primitives sixième de l'unité, donc M est d'ordre 6.

3. (a)
- $M^m=I_n$ donc, par application de la formule du binôme de Newton (valide ici puisque N permute avec I_n), il vient :
$I_n=\sum_{k=0}^{m}\begin{pmatrix} m \\ k \end{pmatrix}p^{rk}N^k=I_n+mp^rN+p^{2r}\sum_{k=2}^{m}\begin{pmatrix} m \\ k \end{pmatrix}p^{(k-2)r}N^k.$
Ainsi : $mp^rN=p^{2r}A$, avec $A=-\sum_{k=2}^{m}\begin{pmatrix} m \\ k \end{pmatrix}p^{(k-2)r}N^k\in M_n(\mathbf{Z})$; d'où $mp^rN\in p^{2r}M_n(\mathbf{Z})$.
- Par conséquent mN appartient à $p^rM_n(\mathbf{Z})$ et, comme $r\in\mathbf{N}^*$, p divise chaque coefficient de la matrice mN. Or, comme N appartient à $M_n(\mathbf{Z})\backslash pM_n(\mathbf{Z})$, il existe un coefficient $n_{i,j}$ de N que p ne divise pas. Comme p est premier et qu'il divise $mn_{i,j}$, il divise m ou $n_{i,j}$: donc nécessairement p divise m.

(b) Par une nouvelle application de la formule du binôme,

$$\begin{aligned} M'=M^p=(I_n+p^rN)^p &= I_n+p^r\sum_{k=1}^{p}\begin{pmatrix} p \\ k \end{pmatrix}p^{r(k-1)}N^k \\ &= I_n+p^r(pN+p^r\sum_{k=2}^{p}\begin{pmatrix} p \\ k \end{pmatrix}p^{r(k-2)}N^k) \\ &= I_n+p^{r+1}N', \end{aligned}$$

en posant $N'=N+p^{r-1}\sum_{k=2}^{p}\begin{pmatrix} p \\ k \end{pmatrix}p^{r(k-2)}N^k$.

On a $N\in M_n(\mathbf{Z})\backslash pM_n(\mathbf{Z})$. Montrons que $p^{r-1}\sum_{k=2}^{p}\begin{pmatrix} p \\ k \end{pmatrix}p^{r(k-2)}N^k\in pM_n(\mathbf{Z})$. En effet,

- Si $k=p$, l'entier $\begin{pmatrix} p \\ k \end{pmatrix}p^{r(k-2)}$ devient $p^{r(p-2)}$ divisible par p car $p\geqslant 3$ (**c'est ici que l'on utilise l'hypothèse** $p\neq 2$).
- Si $k\in\{2,\dots,p-1\}$ le coefficient binômial $\begin{pmatrix} p \\ k \end{pmatrix}$ est divisible par le nombre premier p.

Dans tous les cas les entiers $\begin{pmatrix} p \\ k \end{pmatrix}p^{r(k-2)}$ qui apparaissent dans la définition de N' sont divisibles par p, donc $p^{r-1}\sum_{k=2}^{p}\begin{pmatrix} p \\ k \end{pmatrix}p^{r(k-2)}N^k\in pM_n(\mathbf{Z})$ et l'on déduit $N'\in M_n(\mathbf{Z})\backslash pM_n(\mathbf{Z})$.

Ainsi $M'=I_n+p^{r+1}N'$, avec $r+1\in\mathbf{N}^*$ et $N'\in M_n(\mathbf{Z})\backslash pM_n(\mathbf{Z})$, M' est d'ordre m' (puisque $M'=M^p$ et que M est d'ordre pm') et $m'\geqslant 2$ car $N'\neq 0$; donc, par le même raisonnement qu'à la question (a), on obtient que p divise m'.

(c) Si les hypothèses faites au début de la question 3 étaient valides, en réitérant le processus précédent k fois, on obtiendrait que m s'écrive sous la forme $m = p^k m_k$, avec $m_k \in \mathbf{N}^*$ ($m_k \neq 0$ car $m \neq 0$), d'où $m \geqslant p^k \geqslant 3^k$ pour tout $k \in \mathbf{N}$. Ceci est bien sûr impossible puisque la suite (3^k) diverge vers $+\infty$.
Par conséquent, aucune matrice $M \in GL_n(\mathbf{Z})$ d'ordre $m \geqslant 2$ ne peut s'écrire sous la forme énoncée au début de la question 3 pour aucun nombre premier $p \geqslant 3$. Autrement dit, toute matrice $M \in GL_n(\mathbf{Z})$ d'ordre $m \geqslant 2$ est de la forme $M = I_n + N$, où le PGCD des coefficients de $N \in M_n(\mathbf{Z})$ est une puissance de 2.

4. Notons ω le morphisme de groupes de $GL_n(\mathbf{Z})$ dans $GL_n(\mathbf{F}_p)$ introduit par l'énoncé. Etant induit par la surjection naturelle de $\mathbf{Z}$ sur $\mathbf{F}_p$, ω est surjectif.
Soit G un sous-groupe fini de $GL_n(\mathbf{Z})$ d'ordre $m \geqslant 2$ (on écarte le cas trivial où $G = \{I_n\}$).
$\omega(G)$ est un sous-groupe fini de $GL_n(\mathbf{F}_p)$ et la restriction $\omega_{|G}$ de ω à G induit un morphisme surjectif de G sur $\omega(G)$.
Montrons que $\omega_{|G}$ est injective, c'est-à-dire que $\mathrm{Ker}(\omega_{|G}) = \{I_n\}$.
Soit $M \in G \cap \mathrm{Ker}(\omega)$. Alors $\omega(M) = I_n$, d'où $M = I_n + pN_1$ avec $N_1 \in M_n(\mathbf{Z})$. En factorisant au maximum par p l'ensemble des coefficients de la matrice N_1, M s'écrit alors sous la forme $M = I_n + p^r N$ avec $r \in \mathbf{N}^*$ et $N \in M_n(\mathbf{Z}) \setminus pM_n(\mathbf{Z})$. D'après la question 3, M ne peut donc pas être d'ordre $m \geqslant 2$. Or M est bien d'ordre fini, puisqu'elle appartient à un groupe G fini : donc M est d'ordre 1, c'est-à-dire que $M = I_n$. Ainsi $\mathrm{Ker}(\omega_{|G}) = G \cap \mathrm{Ker}(\omega) = \{I_n\}$: $\omega_{|G}$ est injective.
$\omega_{|G}$ est donc un isomorphisme de G sur $\omega(G)$: G est donc bien isomorphe à un sous-groupe de $GL_n(\mathbf{F}_p)$.

5. (a) Soit G un sous-groupe fini de $GL_2(\mathbf{Z})$. D'après la question 4, G est isomorphe à un sous-groupe de $GL_2(\mathbf{F}_3)$. Or le cardinal de $GL_2(\mathbf{F}_3)$ est $(3^2-1) \times (3^2-3) = 8 \times 6 = 48$ (ce résultat s'obtient en comptant les bases de $\mathbf{F}_3^2$).
Donc, d'après le théorème de Lagrange, le cardinal de G divise 48.

(b) Si le cardinal de G est égal à 48, alors G est isomorphe à $GL_2(\mathbf{F}_3)$. Or on sait que G ne contient pas d'élément d'ordre 8 ; en exhibant un élément d'ordre 8 dans $GL_2(\mathbf{F}_3)$, on montre ainsi qu'il n'est pas possible que G soit de cardinal 48.
Deux méthodes sont possibles pour exhiber un tel élément :

- soit directement, par tâtonnement sur les éléments de $GL_2(\mathbf{F}_3)$: on vérifie facilement que la matrice $\begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix}$, par exemple, est un élément de $GL_2(\mathbf{F}_3)$ d'ordre 8 ;
- soit en considérant le polynôme cyclotomique

$$\Phi_8(X) = (X - e^{i\pi/4})(X - e^{-i\pi/4})(X - e^{3i\pi/4})(X - e^{-3i\pi/4}) = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1) = X^4 + 1$$

qui apparaît dans la décomposition de $X^8 - 1$: dans $\mathbf{F}_3[X]$, $X^4 + 1 = (X^2 + X + 2)(X^2 + 2X + 2)$ et la matrice compagnon associée au polynôme $X^2 + X + 2$ est la matrice $M = \begin{pmatrix} 0 & -2 \\ 1 & -1 \end{pmatrix}$, elle appartient à $GL_2(\mathbf{F}_3)$ car son déterminant est non nul. Elle est annulée par le polynôme $X^2 + X + 2$, donc par le polynôme $X^4 + 1$. Donc $M^4 = -I_2$ et $M^8 = I_2$, ce qui montre que la matrice M est d'ordre 8.

II. - Réseaux

1. • Supposons que $e' = (e'_1, \ldots, e'_n)$ soit une $\mathbf{Z}$-base de $\mathscr{R}$.
Alors $\mathscr{R} = \{\sum_{i=1}^{n} a'_i e'_i \ / \ \forall\, i \in \{1, \ldots, n\}, a'_i \in \mathbf{Z}\}$.
Or, pour tout $j \in [[1, n]]$, $e_j \in \mathscr{R}$, donc il existe $(p'_{1,j}, \ldots, p'_{n,j}) \in \mathbf{Z}^n$ tel que $e_j = \sum_{i=1}^{n} p'_{i,j} e'_i$. Par conséquent, e étant une famille génératrice de E, e' l'est aussi.

Comme e' est de cardinal égal à $n = \dim(E)$, e' est donc une base de E.
De plus, la matrice de passage de e' à e est la matrice des $p'_{i,j}$: elle appartient à $M_n(\mathbf{Z})$ et est inversible. Par un raisonnement symétrique son inverse appartient à $M_n(\mathbf{Z})$. Cette matrice de passage est donc dans $GL_n(\mathbf{Z})$.
Une implication est ainsi établie.

- Réciproquement, supposons que e' soit une base de E et que la matrice de passage de e à e' appartienne à $GL_n(\mathbf{Z})$. Notons $P = (p_{i,j})$ cette matrice et $P^{-1} = (p'_{i,j})$ sa matrice inverse.
  Pour tout $j \in [[1,n]]$, $e'_j = \sum_{i=1}^{n} p_{i,j} e_i$, donc $e'_j \in \mathscr{R}$.
  De plus :
  – $\forall\, (a'_1,\dots,a'_n) \in \mathbf{Z}^n$, $\sum_{j=1}^{n} a'_j e'_j = \sum_{j=1}^{n} a'_j \left(\sum_{i=1}^{n} p_{i,j} e_i\right) = \sum_{i=1}^{n} \left(\sum_{j=1}^{n} a'_{i,j} p_{i,j}\right) e_i.$
  Or $\forall\, i \in [[1,n]]$, $\sum_{j=1}^{n} a'_{i,j} p_{i,j} \in \mathbf{Z}$, donc $\sum_{j=1}^{n} a'_j e'_j \in \mathscr{R}$.
  Ainsi : $\{\sum_{j=1}^{n} a'_j e'_j \ /\ \forall\, j \in \{1,\dots,n\}, a'_j \in \mathbf{Z}\} \subset \mathscr{R}$.
  – Réciproquement, soit $x \in \mathscr{R}$. Il existe alors $(a_1,\dots,a_n) \in \mathbf{Z}^n$ tel que
  $x = \sum_{j=1}^{n} a_j e_j = \sum_{j=1}^{n} a_j \left(\sum_{i=1}^{n} p'_{i,j} e'_i\right) = \sum_{i=1}^{n} \left(\sum_{j=1}^{n} a_j p'_{i,j}\right) e'_i$, avec $\sum_{j=1}^{n} a_j p'_{i,j} \in \mathbf{Z}$ pour tout $i \in [[1,n]]$, donc $\mathscr{R} \subset \{\sum_{i=1}^{n} a'_i e'_i \ /\ \forall\, i \in \{1,\dots,n\}, a'_i \in \mathbf{Z}\}$.
  Donc $\mathscr{R} = \{\sum_{i=1}^{n} a'_i e'_i \ /\ \forall\, i \in \{1,\dots,n\}, a'_i \in \mathbf{Z}\}$, où e' est une base de E, si bien que e' est une $\mathbf{Z}$-base de $\mathscr{R}$.

2. Considérons deux $\mathbf{Z}$-bases $e = (e_1,\dots,e_n)$ et $e' = (e'_1,\dots,e'_n)$ de $\mathscr{R}$.
   Notons M (resp. M') la matrice de $M_n(\mathbf{R})$ dont le coefficient d'indice (i,j) est égal au produit scalaire (e_i,e_j) (resp. (e'_i,e'_j)), et P la matrice de passage de e à e'.
   Les matrices M et M' sont alors congruentes, et plus précisément : $M' = {}^tPMP$. En effet, il s'agit de la formule de changement de base pour une forme bilinéaire symétrique appliquée au produit scalaire avec les deux bases e et e'.
   Par conséquent, $\det(M') = \det({}^tP)\det(M)\det(P) = \det(M)(\det(P))^2$.
   Or $\det(P) = \pm 1$ donc $\det(M') = \det(M)$.
   Ceci prouve le résultat demandé et justifie la définition du discriminant du réseau $\mathscr{R}$: $\Delta(\mathscr{R}) = \det(M)$, où M est la matrice dont le coefficient d'indice (i,j) est (e_i,e_j), pour n'importe quelle $\mathbf{Z}$-base $e = (e_1,\dots,e_n)$ de $\mathscr{R}$.

3. L'idée consiste à prouver qu'un réseau $\mathscr{R}$ de E n'est pas dense dans E, la raison intuitive étant que $\mathbf{Z}$ n'est pas dense dans $\mathbf{R}$.
   Considérons un réel r strictement positif, un vecteur a de E et une $\mathbf{Z}$-base $e = (e_1,\dots,e_n)$ de $\mathscr{R}$. Raisonnons par l'absurde : supposons que l'ensemble $B(a,r) \cap \mathscr{R}$ soit de cardinal infini. Il contient donc un sous-ensemble infini dénombrable et on peut alors construire une suite (x_p) de vecteurs deux à deux distincts de $B(a,r) \cap \mathscr{R}$. Cette suite étant bornée dans un espace vectoriel isomorphe à $\mathbf{R}^n$, elle admet, d'après le théorème de Bolzano-Weierstrass, une suite extraite (y_p) convergente. Or, pour tout $n \in \mathbf{N}$, $y_p \neq y_{p+1}$ donc, comme les systèmes de coordonnées de y_p et y_{p+1} dans la base e sont deux n-uplets distincts d'entiers, on a nécessairement $||y_p - y_{p+1}||_\infty \geqslant 1$ (où $||\ ||_\infty$ désigne la norme infinie). Comme la norme euclidienne majore la norme infinie (ou comme toutes les normes sont équivalentes en dimension finie), l'inégalité ci-dessus obtenue pour tout $p \in \mathbf{N}$ contredit la convergence de la suite (y_p).
   Par conséquent, la supposition est fausse : $B(a,r) \cap \mathscr{R}$ est bien de cardinal fini.

4. L'ensemble $\{||x|| \ /\ x \in \mathscr{R}\backslash\{0\}\}$ est bien une partie de $\mathbf{R}$ non vide et minorée par 0, donc la quantité

$m(\mathscr{R})$ est bien définie, du fait que **R** vérifie l'axiome de la borne inférieure.
De plus, soit e un vecteur quelconque non nul de $\mathscr{R}$. D'après la question précédente, l'ensemble $A = B(0, ||e||) \cap \mathscr{R}$ est non vide et de cardinal fini, on peut donc considérer un vecteur v de plus petite norme de cet ensemble : v est donc un vecteur non nul de $\mathscr{R}$ et

$$||v|| = \mathrm{Inf}\{||x|| \ / \ x \in A\} = \mathrm{Inf}\{||x|| \ / \ x \in \mathscr{R}\backslash\{0\}\} = m(\mathscr{R})$$

Ainsi $m(\mathscr{R}) = ||v||$ pour un vecteur $v \in \mathscr{R}\backslash\{0\}$; cette borne inférieure est atteinte : c'est un plus petit élément.

5. (a) L'image par π_k de la base $(v_1, \ldots, v_k, e_{k+1}, \ldots, e_n)$ de E est une famille génératrice de $\pi_k(E)$. Or, comme π_k est surjective de E sur $W_k^\perp$, $\pi_k(E) = W_k^\perp$; et, comme $\pi_k(v_1) = \ldots \pi_k(v_k) = 0$, $(\pi_k(e_{k+1}), \ldots, \pi_k(e_n))$ est une famille génératrice de $W_k^\perp$. Étant de cardinal $n-k = \dim(W_k^\perp)$, c'est donc une base de $W_k^\perp$. De plus,

$$\begin{aligned}
\pi_k(\mathscr{R}) &= \left\{\pi_k\left(\sum_{i=1}^k a_i v_i + \sum_{i=k+1}^n a_i e_i\right) \ / \ \forall\, i \in \{1, \ldots, n\}, a_i \in \mathbf{Z}\right\} \\
&= \left\{\sum_{i=1}^k a_i \pi_k(v_i) + \sum_{i=k+1}^n a_i \pi_k(e_i) \ / \ \forall\, i \in \{1, \ldots, n\}, a_i \in \mathbf{Z}\right\} \\
&= \left\{\sum_{i=k+1}^n a_i \pi_k(e_i) \ / \ \forall\, i \in \{k+1, \ldots, n\}, a_i \in \mathbf{Z}\right\}.
\end{aligned}$$

On a ainsi prouvé que $\pi_k(\mathscr{R})$ est un réseau de $W_k^\perp$ de **Z**-base $(\pi_k(e_{k+1}), \ldots, \pi_k(e_n))$.

(b) Comme $e_{k+1} \notin W_k$, $||\pi_k(e_{k+1})|| > 0$.
Comme à la question 4, l'ensemble $A = B(0, ||\pi_k(e_{k+1})||) \cap \pi_k(\mathscr{R})\backslash\{0\}$ est un ensemble non vide (car il contient $\pi_k(e_{k+1})$) de cardinal fini ; on peut donc considérer un vecteur u de plus petite norme de A. Alors $||u|| > 0$ et comme $u \in \pi_k(\mathscr{R})$, il existe $v_{k+1} \in \mathscr{R}$ tel que $u = \pi_k(v_{k+1})$.
Alors $||\pi_k(v_{k+1})|| = \inf\{||u|| \ / \ u \in A\} = \inf\{||u|| \ / \ u \in \pi_k(\mathscr{R})\backslash\{0\}\} = m(\pi_k(\mathscr{R}))$.

(c)
- D'après ce qui précède, il existe $(n-k)$ entiers $a_{k+1}, \ldots, a_n$ tels que $\pi_k(v_{k+1}) = a_{k+1}\pi_k(e_{k+1}) + \ldots + a_n\pi_k(e_n)$. Notons d le PGCD de $a_{k+1}, \ldots, a_n$. Il existe alors $(a'_{k+1}, \ldots, a'_n) \in \mathbf{Z}^{n-k}$ tel que $a_i = d a'_i$ pour tout $i \in [[k+1, n]]$ et $a'_{k+1}, \ldots, a'_n$ sont premiers entre eux dans leur ensemble. Posons $v'_{k+1} = \dfrac{1}{d} v_{k+1}$. Alors $\pi_k(v'_{k+1}) \in \pi_k(\mathscr{R})\backslash\{0\}$. Si $d > 1$, alors $||\pi_k(v'_{k+1})|| = \dfrac{1}{d}||\pi_k(v_{k+1})|| < ||\pi_k(v_{k+1})||$, ce qui contredit le fait que $||\pi_k(v_{k+1})|| = m(\pi_k(\mathscr{R}))$. Donc $d = 1$, ce qui prouve que $\pi_k(v_{k+1})$ est un vecteur primitif du réseau $\pi_k(\mathscr{R})$.
- D'après le résultat admis par l'énoncé, il existe une famille $(f'_{k+2}, \ldots, f'_n)$ de vecteurs de E telle que $(\pi_k(v_{k+1}), f'_{k+2}, \ldots, f'_n)$ soit une **Z**-base de $\pi_k(\mathscr{R})$. Il existe alors une famille $(f_{k+2}, \ldots, f_n)$ de vecteurs de $\mathscr{R}$ vérifiant pour tout $i \in \{k+2, \ldots, n\}$, $\pi_k(f_i) = f'_i$. Nous allons montrer que $(v_1, \ldots, v_k, v_{k+1}, f_{k+2}, \ldots, f_n)$ est une base de E. La famille étant de cardinal n, il suffit de montrer qu'elle est libre. Supposons que l'on ait une relation de la forme

$$\sum_{i=1}^{k+1} a_i v_i + \sum_{i=k+2}^n a_i f_i = 0.$$

En appliquant π_k nous obtenons

$$a_{k+1}\pi_k(v_{k+1}) + \sum_{i=k+2}^n a_i f'_i = 0.$$

La famille $(\pi_k(v_{k+1}), f'_{k+2}, \ldots, f'_n)$ étant une **Z**-base de $\mathscr{R}$ est une famille libre, donc les a_i sont nuls pour $i \in \{k+1, \ldots, n\}$. On conclut alors à la nullité des autres a_i en remarquant que la famille $(v_1, \ldots, v_k)$ est libre. Donc la famille $(v_1, \ldots, v_k, v_{k+1}, f_{k+2}, \ldots, f_n)$ est une base de E.

- Nous allons montrer que cette famille est une $\mathbf{Z}$-base de $\mathscr{R}$. Tous les éléments de cette famille étant des éléments de $\mathscr{R}$, nous avons l'inclusion
$$\{\sum_{i=1}^{k+1} a_i v_i + \sum_{i=k+2}^{n} a_i f_i \ / \ \forall i \in \{1,\dots,n\} \ \ a_i \in \mathbf{Z}\} \subset \mathscr{R}.$$
Soit alors $x \in \mathscr{R}$. Par construction il existe une famille $(a_{k+1},\dots,a_n)$ d'entiers tels que $\pi_k(x) = a_{k+1}\pi_k(v_{k+1}) + \sum_{i=k+2}^{n} a_i f_i'$. Donc le vecteur $y = x - a_{k+1}v_{k+1} - \sum_{i=k+2}^{n} a_i f_i$ appartient au noyau de π_k et à $\mathscr{R}$. Il existe donc une famille d'entiers $(b_1,\dots,b_n)$ telle que $y = \sum_{i=1}^{k} b_i v_i + \sum_{i=k+1}^{n} b_i e_i$. La famille $(v_1,\dots,v_k)$ forme une base du noyau de π_k et la famille $(e_{k+1},\dots,e_n)$ forme une base d'un supplémentaire de ce noyau. Le vecteur y appartenant au noyau de π_k, nous obtenons $y = \sum_{i=1}^{k} b_i v_i$. D'où
$$x = \sum_{i=1}^{k} b_i v_i + a_{k+1}v_{k+1} + \sum_{i=k+2}^{n} a_i f_i.$$
Nous avons donc montré l'inclusion
$$\mathscr{R} \subset \{\sum_{i=1}^{k+1} a_i v_i + \sum_{i=k+2}^{n} a_i f_i \ / \ \forall i \in \{1,\dots,n\} \ \ a_i \in \mathbf{Z}\}.$$
Il résulte de tout cela que $(v_1,\dots,v_{k+1},f_{k+2},\dots,f_n)$ est une $\mathbf{Z}$-base de $\mathscr{R}$.

(d) Ce résultat s'obtient par récurrence limitée sur $l \in [[1,n]]$ dans laquelle il suffit d'utiliser correctement les résultats des questions (a), (b) et (c). Considérons l'hypothèse de récurrence suivante $\mathscr{H}_l$: « il existe une $\mathbf{Z}$-base $(v_1,\dots,v_l,e_{l+1},\dots,e_n)$ de $\mathscr{R}$ vérifiant $||v_1|| = m(\mathscr{R})$ et $\forall k \in [[1,l-1]]$, $||\pi_k(v_{k+1})|| = m(\pi_k(\mathscr{R}))$, où π_k est la projection orthogonale sur $< v_1,\dots,v_k >^{\perp}$. »

- Pour $l = 1$, d'après la question 4, il existe un vecteur $v_1 \in \mathscr{R}\backslash\{0\}$ tel que $||v_1|| = m(\mathscr{R})$. v_1 est nécessairement un vecteur primitif de $\mathscr{R}$ (par une argumentation analogue à celle faite à la question (c)), donc il existe une $\mathbf{Z}$-base de $\mathscr{R}$ de la forme $(v_1,e_2,\dots,e_n)$ et $\mathscr{H}_1$ est vérifiée.
- Supposons avoir établi $\mathscr{H}_l$ pour une valeur $l \leqslant n-1$: il existe alors une $\mathbf{Z}$-base $(v_1,\dots,v_l,e_{l+1},\dots,e_n)$ de $\mathscr{R}$ vérifiant $||v_1|| = m(\mathscr{R})$ et $\forall k \in [[1,l-1]]$, $||\pi_k(v_{k+1})|| = m(\pi_k(\mathscr{R}))$. Cette base vérifie donc les hypothèses du début de la question 4 : on en déduit donc successivement que :
  - $\pi_l(\mathscr{R})$ est un réseau de $< v_1,\dots,v_l >^{\perp}$ (question (a)) ;
  - il existe un vecteur v_{l+1} de $\mathscr{R}$ vérifiant $||\pi_l(v_{l+1})|| = m(\pi_l(\mathscr{R}))$ (question (b)) ;
  - il existe une $\mathbf{Z}$-base de $\mathscr{R}$ de la forme $(v_1,\dots,v_l,v_{l+1},f_{l+2},\dots,f_n)$ (question (c)).

  Ceci prouve bien que $\mathscr{H}_{l+1}$ est aussi vérifiée.

D'après le principe de récurrence, $\mathscr{H}_l$ est donc vraie pour tout entier $l \in [[1,n]]$; donc $\mathscr{H}_n$ est vérifiée, ce qui répond à la question.

(e) Le réseau $\mathscr{R}_1$ considéré ici est le réseau plan constitué par un maillage de triangles équilatéraux de côté égal à 1. Posons $e_1 = (1,0)$ et $e_2 = (-1/2,\sqrt{3}/2)$. Il est manifeste que $m(\mathscr{R}_1) = 1 = ||e_1||$. Avec les notations de l'énoncé, π_1 est donc la projection orthogonale sur $< e_1' >$, avec $e_1' = (0,1)$. D'après la question (a), $\pi_1(\mathscr{R}_1)$ est un réseau de $< e_1' >$ de $\mathbf{Z}$-base $(\pi_1(e_2))$. Il est alors manifeste également que $||\pi_1(e_2)|| = m(\pi_1(\mathscr{R}_1))$ (un calcul très simple aboutit d'ailleurs à $||\pi_1(e_2)|| = ||(e_2,e_1')e_1'|| = \sqrt{3}/2||e_1'|| = \sqrt{3}/2$). Ainsi, e est une base réduite de $\mathscr{R}_1$.

6. (a) Soit $(j,k) \in [[2,n]]^2$.
$\pi_1(e_j) = e_j - \lambda e_1$ où λ est un réel tel que $(e_1,\pi_1(e_j)) = 0$. Or $(e_1,\pi_1(e_j)) = (e_1,e_j) - \lambda||e_1||^2$, avec $||e_1|| = m(\mathscr{R})$; donc $\lambda = \dfrac{(e_1,e_j)}{m(\mathscr{R})^2}$ et $\pi_1(e_j) = e_j - \dfrac{(e_1,e_j)}{m(\mathscr{R})^2}e_1$.
De même, $\pi_1(e_k) = e_k - \dfrac{(e_1,e_k)}{m(\mathscr{R})^2}e_1$. Ainsi :
$$\begin{aligned}(\pi_1(e_j),\pi_1(e_k)) &= (e_j - \frac{(e_1,e_j)}{m(\mathscr{R})^2}e_1, e_k - \frac{(e_1,e_k)}{m(\mathscr{R})^2}e_1)\\ &= (e_j,e_k) - 2\frac{(e_1,e_j)(e_1,e_k)}{m(\mathscr{R})^2} + \frac{(e_1,e_j)(e_1,e_k)}{m(\mathscr{R})^4}||e_1||^2\\ &= (e_j,e_k) - \frac{1}{m(\mathscr{R})^2}(e_1,e_j)(e_1,e_k).\end{aligned}$$

(b) Notons $A = (a_{i,j})$ la matrice de $M_n(\mathbf{R})$ dont le coefficient d'indice (i,j) (pour $1 \leqslant i, j \leqslant n$) est égal à $a_{i,j} = (e_i, e_j)$ et A_1 la matrice de $M_{n-1}(\mathbf{R})$ dont le coefficient d'indice (i,j) (pour $2 \leqslant i, j \leqslant n$) est égal à $(\pi_1(e_i), \pi_1(e_j))$.

Pour $j \in [[2, n]]$, effectuons successivement les transvections $L_j \leftarrow L_j - \dfrac{a_{j,1}}{a_{1,1}} L_1$ à partir des lignes de la matrice A. La matrice A' ainsi obtenue se déduit donc de A par multiplications à gauche par $(n-1)$ matrices de tranvection. Or, comme une matrice de tranvection est de déterminant égal à 1, il vient : $\det(A) = \det(A')$.

De plus, les lignes L'_j de A' pour $j \in [[2, n]]$ ont pour coefficients 0 en première colonne et, en colonne $k \in [[2, n]]$:

$a_{j,k} - \dfrac{a_{j,1}}{a_{1,1}} a_{1,k} = (e_j, e_k) - \dfrac{(e_j, e_1)}{(e_1, e_1)}(e_1, e_k) = (e_j, e_k) - \dfrac{1}{m(\mathscr{R})^2}(e_1, e_j)(e_1, e_k) = (\pi_1(e_j), \pi_1(e_k))$.

A' a donc pour première ligne la première ligne L_1 de A et le reste de A' est constitué d'une colonne de zéros juxtaposée à la matrice A_1. Par un calcul de déterminant par blocs on a $\det(A') = (e_1, e_1)\det(A_1)$ (car (e_1, e_1) est le coefficient en première ligne et première colonne de A'). Or, d'après la question 4, $(e_1, e_1) = m(\mathscr{R})^2$ et, d'après la question 2, $\det(A) = \Delta(\mathscr{R})$ et $\det(A_1) = \Delta(\pi_1(\mathscr{R}))$.

Ainsi : $\Delta(\mathscr{R}) = m(\mathscr{R})^2 \Delta(\pi_1(\mathscr{R}))$.

(c) D'après le théorème de Pythagore, puisque e_1 et v' sont orthogonaux, on a :
$||v||^2 = ||te_1 + v'||^2 = t^2||e_1||^2 + ||v'||^2 = t^2 m(\mathscr{R})^2 + ||v'||^2$.
Or $v \neq 0$ donc $m(\mathscr{R}) \leqslant ||v||$.
Ainsi : $m(\mathscr{R})^2 \leqslant t^2 m(\mathscr{R})^2 + ||v'||^2$.

(d) Nous allons montrer l'égalité de Hermite en raisonnant par récurrence sur n. Pour $n = 1$, l'inégalité est clairement vérifiée : si (e_1) est une $\mathbf{Z}$-base de $\mathscr{R}$, nous avons $m(\mathscr{R})^2 = (e_1, e_1) = \Delta(\mathscr{R})$. Cela donne le résultat.

Supposons donc $n \geqslant 2$ et l'inégalité vérifiée à l'ordre $n-1$. Choisissons $(e_1, \ldots, e_n)$ une base réduite de $\mathscr{R}$. Il existe, par hypothèse de récurrence, un vecteur v' du réseau $\pi_1(\mathscr{R})$ vérifiant la relation (*)

$$||v'||^2 \leqslant (4/3)^{(n-2)/2} \Delta(\pi_1(\mathscr{R}))^{1/(n-1)}.$$

Soit alors $v \in \mathscr{R}$ tel que $\pi_1(v) = v'$. Il existe un réel t tel que $v = te_1 + v'$ et l'on peut choisir v de manière à ce que $|t| \leqslant 1/2$ (quitte à remplacer v par $v - ke_1$ où l'entier k est tel que $|t - k| \leqslant 1/2$). En appliquant la question 6-c nous obtenons

$$m(\mathscr{R})^2 \leqslant ||v'||^2/(1 - t^2) \leqslant (4/3)||v'||^2.$$

Nous avons donc par (*)

$$m(\mathscr{R})^2 \leqslant (4/3)^{n/2} \Delta(\pi_1(\mathscr{R}))^{1/(n-1)}.$$

D'après la question 6-b $\Delta(\pi_1(\mathscr{R})) = \Delta(\mathscr{R})/m(\mathscr{R})^2$, ce qui permet de conclure à la véracité de l'inégalité à l'ordre n.

7. H_n est une partie de $\mathbf{R}^+$ non vide (car d'après l'inégalité de Hermite, $(4/3)^{(n-1)/2} \in H_n$), donc elle admet une borne inférieure η_n qui vérifie alors $m(\mathscr{R})^2 \leqslant \eta_n \Delta(\mathscr{R})^{1/n}$.

(a) Considérons le réseau $\mathbf{Z}^n$ de $\mathbf{R}^n$ euclidien usuel. La base canonique $e = (e_1, \ldots, e_n)$ de $\mathbf{R}^n$ est orthonormale et c'est de manière immédiate une base réduite de $\mathbf{Z}^n$, avec $m(\mathscr{R})^2 = ||e_1||^2 = 1$ et $\Delta(\mathscr{R}) = \det(I_n) = 1$.
Ainsi $m(\mathscr{R})^2 = \Delta(\mathscr{R})^{1/n}$, et comme $m(\mathscr{R})^2 \leqslant \eta_n \Delta(\mathscr{R})^{1/n}$, on en déduit que $\eta_n \geqslant 1$.

(b)
- D'une part, l'inégalité de Hermite s'écrit, pour $n = 2$: $m(\mathscr{R})^2 \leqslant (2/\sqrt{3})\Delta(\mathscr{R})^{1/2}$; donc $2/\sqrt{3} \in H_2$, d'où $\eta_2 \leqslant 2/\sqrt{3}$.
- D'autre part, le réseau $\mathscr{R}_1$ étudié à la question 5.(e) vérifie : $m(\mathscr{R}_1)^2 = ||e_1||^2 = 1$ et $\Delta(\mathscr{R}_1) = \begin{vmatrix} 1 & -1/2 \\ -1/2 & 1 \end{vmatrix} = 3/4$; donc $m(\mathscr{R}_1)^2 = (2/\sqrt{3})\Delta(\mathscr{R}_1)^{1/2}$; or $m(\mathscr{R}_1)^2 \leqslant \eta_2 \Delta(\mathscr{R}_1)^{1/2}$; d'où $\eta_2 \geqslant 2/\sqrt{3}$.

Finalement : $\eta_2 = 2/\sqrt{3}$.
Ceci prouve que l'inégalité d'Hermite ne peut pas être améliorée pour tout $n \geqslant 2$ puisque la valeur $(4/3)^{(n-1)/2}$ est atteinte pour $n = 2$.

III. - Cristalloïdes

1. Soit g un élément de $O(\mathscr{R})$, où $\mathscr{R}$ est un réseau de E de $\mathbf{Z}$-base $e = (e_1, \ldots, e_n)$. L'application g est entièrement déterminée par la donnée des vecteurs $g(e_1), \ldots, g(e_n)$.
Soit $k \in [[1, n]]$. D'après la question II.3, $B(0, \|e_k\|) \cap \mathscr{R}$ est de cardinal fini. Or $g(e_k)$ appartient à $B(0, \|e_k\|) \cap \mathscr{R}$ (puisque $g(e_k) \in \mathscr{R}$ et $\|g(e_k)\| = \|e_k\|$). Il n'y a donc qu'un nombre fini α_k de vecteurs $g(e_k)$ possibles. D'où au total un nombre fini d'éléments $g \in O(\mathscr{R})$ possibles, inférieur à $\prod_{k=1}^{n} \alpha_k$. Par conséquent, $O(\mathscr{R})$ est de cardinal fini.
2. • Supposons que G est $\mathbf{Z}$-conjugué à $\psi_e(\Gamma)$. Alors il existe une matrice $M \in GL_n(\mathbf{Z})$ telle que $MGM^{-1} = \psi_e(\Gamma)$. Notons e' la base de E telle que M soit la matrice de passage de e à e'. D'après la question II.1, e' est une $\mathbf{Z}$-base de $\mathscr{R}$.
De plus, pour toute matrice $P \in M_n(\mathbf{R})$, on a :
$$\begin{aligned} P \in G \Leftrightarrow MPM^{-1} \in \psi_e(\Gamma) \quad &\Leftrightarrow \exists\, g \in \Gamma,\ MPM^{-1} = \mathrm{Mat}(g, e) \\ &\Leftrightarrow \exists\, g \in \Gamma,\ P = M^{-1} \times \mathrm{Mat}(g, e) \times M = \mathrm{Mat}(g, e') \\ &\Leftrightarrow P \in \psi_{e'}(\Gamma) \end{aligned}$$
Donc $G = \psi_{e'}(\Gamma)$.
   • Réciproquement, supposons qu'il existe une $\mathbf{Z}$-base e' de $\mathscr{R}$ telle que $G = \psi_{e'}(\Gamma)$. Notons M la matrice de passage de e à e'.
Pour toute matrice $P \in M_n(\mathbf{R})$, on a :
$$\begin{aligned} P \in MGM^{-1} \Leftrightarrow P \in M\psi_{e'}(\Gamma)M^{-1} \quad &\Leftrightarrow \exists\, g \in \Gamma,\ P = M \times \mathrm{Mat}(g, e') \times M^{-1} = \mathrm{Mat}(g, e') \\ &\Leftrightarrow P \in \psi_e(\Gamma) \end{aligned}$$
Donc $MGM^{-1} = \psi_e(\Gamma)$: G et $\psi_e(\Gamma)$ sont $\mathbf{Z}$-conjugués.

   L'équivalence à prouver est ainsi établie.
3. • Supposons que les deux cristalloïdes $(\mathscr{R}, \Gamma)$ et $(\mathscr{R}', \Gamma')$ sont équivalents. Alors il existe $u \in GL(E)$ tel que $u(\mathscr{R}) = \mathscr{R}'$ et $u\Gamma u^{-1} = \Gamma'$.
Comme e est une base de E et que u est un isomorphisme, $e'' = u(e)$ est une base de E. De plus :
$$\begin{aligned} \mathscr{R}' = u(\mathscr{R}) \quad &= \left\{ u\left(\sum_{i=1}^{n} a_i e_i\right) \ /\ \forall\, i \in \{1, \ldots, n\}, a_i \in \mathbf{Z} \right\} \\ &= \left\{ \sum_{i=1}^{n} a_i e''_i \ /\ \forall\, i \in \{1, \ldots, n\}, a_i \in \mathbf{Z} \right\} \end{aligned}$$
donc e'' est une $\mathbf{Z}$-base de $\mathscr{R}'$.
Posons $G = \psi_e(\Gamma)$, $G' = \psi_{e'}(\Gamma')$ et $G'' = \psi_{e''}(\Gamma')$. D'après la question 2, G' et G'' sont $\mathbf{Z}$-conjugués.
Notons $U = \mathrm{Mat}(u, e)$: U est aussi la matrice de passage de e à e''.
Pour tout $g' \in \Gamma'$, il existe $g \in \Gamma$ tel que $g' = ugu^{-1}$, si bien que :
$\mathrm{Mat}(g', e'') = \mathrm{Mat}(g', u(e)) = U^{-1} \times \mathrm{Mat}(g', e) \times U = U^{-1} \times \mathrm{Mat}(ugu^{-1}, e) \times U = U^{-1}U \times \mathrm{Mat}(g, e) \times U^{-1}U = \mathrm{Mat}(g, e)$.
Ainsi, pour toute matrice $P \in M_n(\mathbf{R})$, on a :
$P \in G'' \Leftrightarrow \exists\, g' \in \Gamma',\ P = \mathrm{Mat}(g', e'') \Leftrightarrow \exists\, g \in \Gamma,\ P = \mathrm{Mat}(g, e) \Leftrightarrow P \in G$.
Donc $G'' = G$. Par conséquent, $G = \psi_e(\Gamma)$ et $G' = \psi_{e'}(\Gamma')$ sont $\mathbf{Z}$-conjugués.
   • Réciproquement, supposons que $G = \psi_e(\Gamma)$ et $G' = \psi_{e'}(\Gamma')$ sont $\mathbf{Z}$-conjugués. Alors il existe $M \in GL_n(\mathbf{Z})$ vérifiant $MGM^{-1} = G'$.
Notons $v \in GL(E)$ tel que $\mathrm{Mat}(v, e) = M^{-1}$ et $e'' = v(e)$. e'' est une base de E et $M \in GL_n(\mathbf{Z})$ est la matrice de passage de e à e'' donc e'' est une $\mathbf{Z}$-base de $\mathscr{R}$, d'après la question II.1.
Notons aussi $M' \in GL_n(\mathbf{R})$ la matrice de passage de e à e'' et $u \in GL(E)$ l'automorphisme tel que $\mathrm{Mat}(u, e'') = M'$, si bien que $e' = u(e'')$.

– D'une part : comme $e'' = v(e)$ est une base de E et que la matrice M^{-1} de passage de e à e'' appartient à $GL_n(\mathbf{Z})$, e'' est une $\mathbf{Z}$-base de $\mathscr{R}$ (toujours d'après la question II.1). Ainsi, comme $e' = u(e'')$ et que e'' et e' sont des $\mathbf{Z}$-bases respectives des réseaux $\mathscr{R}$ et $\mathscr{R}'$, on a $u(\mathscr{R}) = \mathscr{R}'$ (1).

– D'autre part, pour tout $g \in \Gamma$, on a :
$\mathrm{Mat}(ugu^{-1}, e') = \mathrm{Mat}(ugu^{-1}, u(e'')) = M'^{-1} \times \mathrm{Mat}(ugu^{-1}, e'') \times M' = M'^{-1} M' \times \mathrm{Mat}(g, e'') \times M'^{-1} M' = \mathrm{Mat}(g, e'') = \mathrm{Mat}(g, v(e)) = M \times \mathrm{Mat}(g, e) \times M^{-1}$.
Or $\mathrm{Mat}(g, e) \in G$, donc $\mathrm{Mat}(ugu^{-1}, e') \in MGM^{-1} = G'$. Ainsi $ugu^{-1} \in \Gamma'$, ce qui prouve que $u\Gamma u^{-1} \subset \Gamma'$.
On montre de la même manière que $u^{-1}\Gamma' u \subset \Gamma$, d'où $\Gamma' \subset u\Gamma u^{-1}$.
Finalement : $u\Gamma u^{-1} = \Gamma'$ (2).

Les relations (1) et (2) obtenues ci-dessus établissent que les cristalloïdes $(\mathscr{R}, \Gamma)$ et $(\mathscr{R}', \Gamma')$ sont équivalents.

L'équivalence à prouver dans cette question est donc établie.

4. Montrons que ψ est injective et surjective.
   - Considérons deux cristalloïdes $(\mathscr{R}, \Gamma)$ et $(\mathscr{R}', \Gamma')$ de E, de $\mathbf{Z}$-bases respectives e et e'. Supposons que les classes d'équivalence de cristalloïdes de $(\mathscr{R}, \Gamma)$ et $(\mathscr{R}', \Gamma')$ aient la même image par ψ. Alors $\psi_e(\Gamma)$ et $\psi_{e'}(\Gamma')$ sont $\mathbf{Z}$-conjugués ; donc, d'après la question 3, $(\mathscr{R}, \Gamma)$ et $(\mathscr{R}', \Gamma')$ sont équivalents, c'est-à-dire que leurs classes d'équivalence sont égales : ceci prouve l'injectivité de ψ.
   - Considérons une classe d'équivalence de sous-groupe de $GL_n(\mathbf{Z})$ de représentant G'. Considérons $\mathbf{R}^n$ muni de sa base canonique $e = (e_1, \ldots, e_n)$ et le réseau $\mathscr{R}$ de $\mathbf{Z}$-base e. Le groupe G' s'identifie par choix de la base e à un sous-groupe fini G de $GL(\mathbf{R}^n)$. Les matrices des éléments de G dans la base e étant des éléments de $GL_n(\mathbf{Z})$, les éléments de G stabilisent $\mathscr{R}$. Nous allons construire un produit scalaire sur $\mathbf{R}^n$ qui fait de G un sous-groupe du groupe orthogonal. Notons $(.,.)$ le produit scalaire usuel de $\mathbf{R}^n$ et $|G|$ le cardinal de G. La forme bilinéaire $(.,.)_G$ définie pour tout couple $(u, v) \in (\mathbf{R}^n)^2$ par
$$(u, v)_G = \frac{1}{|G|} \sum_{g \in G} (g(u), g(v))$$
est clairement un produit scalaire sur $\mathbf{R}^n$. De plus, si $g' \in G$, on a
$$\begin{aligned}(g'(u), g'(v))_G &= \frac{1}{|G|} \sum_{g \in G} (g(g'(u)), g(g'(v))) \\ &= \frac{1}{|G|} \sum_{g'' \in G} (g''(u), g''(v)) \\ &= (u, v)_G\end{aligned}$$
Donc, si l'on munit $\mathbf{R}^n$ du produit scalaire $(.,.)_G$, le groupe G est un sous-groupe du groupe orthogonal qui stabilise $\mathscr{R}$. Le couple $(\mathscr{R}, G)$ est donc un cristalloïde de l'espace euclidien $(\mathbf{R}^n, (.,.)_G)$. Les deux espaces euclidiens $(\mathbf{R}^n, (.,.)_G)$ et E étant de même dimension, il existe une isométrie $u : \mathbf{R}^n \longrightarrow E$. Le couple $(u(\mathscr{R}), uGu^{-1})$ est alors clairement un cristalloïde de E vérifiant $\psi_{u(e)}(uGu^{-1}) = G'$. Ceci montre la surjectivité de l'application ψ.

   L'application ψ est donc une bijection de l'ensemble des classes d'équivalence de cristalloïdes de E sur l'ensemble des classes de $\mathbf{Z}$-conjugaison de sous-groupes finis de $GL_n(\mathbf{Z})$.

5. Le groupe diédral D_6 est le groupe des isométries du plan euclidien conservant un hexagone régulier ; c'est un sous-groupe de $O(\mathscr{R}_1)$, où $\mathscr{R}_1$ est le réseau de $\mathbf{R}^2$ étudié à la question II.5.e qui contient l'hexagone régulier centré en l'origine 0 et de sommet le point de coordonnées $(0, 1)$. En effet, le groupe D_6 est engendré par deux éléments, la rotation d'angle $\pi/3$ et la symétrie de droite d'angle $\pi/6$. On vérifie que ces deux isométries sont dans $\mathscr{O}(\mathscr{R}_1)$ par exemple en vérifiant que les matrices de ces isométries dans la $\mathbf{Z}$-base e de la question II-5-e sont dans $GL_2(\mathbf{Z})$: on a respectivement $\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$. On peut alors identifier D_6 à un sous-groupe de $\mathscr{O}(\mathscr{R}_1)$ (en fait on a égalité : une isométrie qui conserve

$\mathscr{R}_1$ permute les six vecteurs de norme 1 de $\mathscr{R}_1$, donc conserve l'hexagone). $(\mathscr{R}_1, D_6)$ est donc un cristalloïde de $\mathbf{R}^2$ et $\psi_e(D_6)$ est un sous-groupe de $GL_2(\mathbf{Z})$. Le groupe diédral D_6 est donc isomorphe à un sous-groupe de $GL_2(\mathbf{Z})$.

IV. - Groupes libres quadratiques

1. Considérons une $\mathbf{Z}$-base $e = (e_1, \ldots, e_n)$ de $\mathscr{R}$. Notons $b(e_i, e_j) = p_{i,j}/q_{i,j}$ avec $p_{i,j} \wedge q_{i,j} = 1$. Notons alors q le ppcm des $q_{i,j}$ (pour i et j variant dans l'ensemble $\{1, \ldots, n\}$). Pour tout couple $(x, y) \in \mathscr{R}^2$, on a $b(x, y) \in \frac{1}{q}\mathbf{Z}$. L'ensemble $\{b(x,x)^{1/2} \ / \ x \in \mathscr{R} \ , \ b(x,x) > 0\}$ est donc un sous-ensemble de $\frac{1}{\sqrt{q}}\mathbf{N}^*$. D'autre part c'est un ensemble non vide. En effet, puisque $p \geqslant 1$, il existe un vecteur a de E tel que $b(a, a) > 0$. Par continuité de la forme b, celle-ci est strictement positive sur une boule ouverte centrée en a de rayon $r > 0$. Par équivalence des normes en dimension fini, on peut choisir la norme infinie associée à la base e, et par homothétie, la forme b est strictement positive sur les boules centrée en λa et de rayon λr. Si l'on choisi le réel λ de manière à avoir $\lambda r > 1$, la boule considérée contient un élément du réseau $\mathscr{R}$. L'ensemble $\{b(x,x)^{1/2} \ / \ x \in \mathscr{R} \ , \ b(x,x) > 0\}$ est donc un sous-ensemble non vide de $\frac{1}{\sqrt{q}}\mathbf{N}^*$, il admet par conséquent un plus petit élément atteint en un vecteur v qui est non nul puisque $b(v, v) > 0$. D'où l'existence de v.
2. Puisque $b(v, v) > 0$ la restriction de b à la droite $< v >$ est non dégénérée. Nous avons donc une somme directe, orthogonale au sens de b, $E = W \oplus < v >$. Par additivité de la signature, la signature de b' est $(p-1, q)$.
3. Si $p = n$, l'inégalité de Hermite-Minkovski devient l'inégalité de Hermite, démontrée dans la partie II. Soit donc $n \geqslant 2$ et $1 \leqslant p < n$. Nous allons montrer l'inégalité par récurrence sur p. Pour simplifier les notations, nous notons $m = m_b(\mathscr{R})$, π la projection sur W parallèlement à $< v >$ et $\mathscr{R}' = \pi(\mathscr{R})$.
   - Supposons $p = 1$. La forme b' est définie négative, donc $-b'$ est définie positive. Notons $m' = m_{-b'}(\mathscr{R}')$. D'après IV-1 il existe $w' \in \mathscr{R}'$ tel que $-b'(w', w') = m'^2$ et $w \in \mathscr{R}$ tel que $\pi(w) = w'$. Par conséquent, $w = tv + w'$ et l'on peut choisir le réel t pour avoir $1/2 \leqslant |t| \leqslant 1$ (même technique qu'en II-6). On a alors $b(w, w) = t^2 m^2 + b(w', w') < m^2$ car $b(w', w') < 0$. Par minimalité de m^2 on en déduit $b(w, w) \leqslant 0$, donc
   $$t^2 m^2 \leqslant -b(w', w') = m'^2$$
   puis
   $$m^2/4 \leqslant m'^2.$$
   D'autre part, en appliquant l'inégalité de Hermite au réseau $\mathscr{R}'$ avec le produit scalaire $-b'$ nous obtenons l'inégalité
   $$m'^2 \leqslant (4/3)^{(n-2)/2} \Delta_{-b'}(\mathscr{R}')^{1/(n-1)}.$$
   Les deux inégalités précédentes combinées montrent alors que
   $$m^2 \leqslant 4(4/3)^{(n-2)/2} \Delta_{-b'}(\mathscr{R}')^{1/(n-1)}.$$
   Un raisonnement similaire à celui de la question II-6-b montre que
   $$|\Delta_b(\mathscr{R})| = m^2 |\Delta_{-b'}(\mathscr{R}')|.$$
   On en déduit
   $$m^2 \leqslant 4(4/3)^{(n-2)/2} m^{-2/(n-1)} |\Delta_b(\mathscr{R})|^{1/n-1}$$
   soit encore après simplification
   $$m^2 \leqslant 3^{(n-1)/n} (4/3)^{(n-1)/2} |\Delta_b(\mathscr{R})|^{1/n-1},$$
   ce qui est l'inégalité de Hermite-Minkovski dans le cas $p = 1$.

- Supposons maintenant $1 < p < n$ et l'inégalité vérifiée à l'ordre $p-1$. La forme b' est de signature $(p-1, q)$ avec $p-1 \geqslant 1$. Notons $m' = m_{b'}(\mathscr{R}')$. D'après IV-1 il existe $w' \in \mathscr{R}'$ tel que $b'(w', w') = m'^2$ et $w \in \mathscr{R}$ tel que $\pi(w) = w'$. Par conséquent, $w = tv + w'$ et l'on peut choisir le réel t pour avoir $|t| \leqslant 1/2$. On a
$$b(w, w) = t^2 m^2 + b(w', w') = t^2 m^2 + m'^2 > 0.$$
On en déduit par minimalité de m, $b(w, w) \geqslant m^2$, soit encore
$$m^2 \leqslant t^2 m^2 + m'^2 \leqslant m^2/4 + m'^2,$$
d'où l'on déduit $\frac{3}{4} m^2 \leqslant m'^2$. Par hypothèse de récurrence on a
$$m'^2 \leqslant 3^{\frac{n-p}{n-1}} (4/3)^{\frac{n-2}{2}} |\Delta_{b'}(\mathscr{R}')|^{1/(n-1)}.$$
On en déduit
$$m^2 \leqslant (4/3) 3^{\frac{n-p}{n-1}} (4/3)^{\frac{n-2}{2}} |\Delta_{b'}(\mathscr{R}')|^{1/(n-1)}.$$
Un raisonnement similaire à celui de la question II-6-b montre encore que
$$|\Delta_b(\mathscr{R})| = m^2 |\Delta_{-b'}(\mathscr{R}')|.$$
On en déduit
$$m^2 \leqslant (4/3) 3^{\frac{n-p}{n-1}} (4/3)^{\frac{n-2}{2}} m^{\frac{-2}{n-1}} |\Delta_b(\mathscr{R})|^{1/(n-1)}.$$
Après simplification on trouve exactement l'inégalité de Hermite-Minkovski à l'ordre p, ce qui conclut la démonstration.

4. (a) Soit $x \in \mathscr{R}''$. Il existe $y \in \mathscr{R}$ tel que $m_b(\mathscr{R})^2 \pi(y) = x$, et l'on a $m_b(\mathscr{R})^2 y = tv + x$ où $t \in \mathbf{R}$. En appliquant $b(., v)$ à cette égalité, on trouve $m_b(\mathscr{R})^2 b(y, v) = t b(v, v)$ (car $b(v, x) = 0$) soit encore $t = b(y, v) \in \mathbf{Z}$. On déduit alors de $x = m_b(\mathscr{R})^2 y - tv$ que x appartient au réseau $\mathscr{R}$ ce qui montre l'inclusion $\mathscr{R}'' \subset \mathscr{R}$. La forme b' est restriction de la forme b qui est à valeurs entières sur $\mathscr{R}$ et $\mathscr{R}'' \subset \mathscr{R}$, on en déduit que b' est à valeurs entières sur $\mathscr{R}''$.

   (b) On suppose le discriminant $\Delta_b(\mathscr{R})$ fixé. D'après la question IV-3 l'entier $m_b(\mathscr{R})$ est borné donc ne peut prendre qu'un nombre fini de valeurs. On sait d'autre part que
$$|\Delta_b(\mathscr{R})| = m_b(\mathscr{R})^2 |\Delta_{b'}(\mathscr{R}')|,$$
et
$$|\Delta_{b'}(\mathscr{R}'')| = m_b(\mathscr{R})^{2(n-1)} |\Delta_{b'}(\mathscr{R}')| = m_b(\mathscr{R})^{2(n-2)} |\Delta_b(\mathscr{R})|.$$
On en déduit que le discriminant $|\Delta_{b'}(\mathscr{R}'')|$ ne peut prendre qu'un nombre fini de valeurs.

5. (a) Soit $e = (e_1, \ldots, e_n)$ une $\mathbf{Z}$-base de $\mathscr{R}_1$. Dire qu'un vecteur $y \in E$ appartient à $\mathscr{C}(\mathscr{R}_1)$ équivaut à dire
$$\forall i \in \{1, \ldots, n\} \ \ b_1(y, e_i) \in \mathbf{Z}.$$
La forme b_1 étant non dégénérée, l'application $\psi' : x \longrightarrow b_1(., x)$ est un isomorphisme de E sur son dual E^*. Notons $e_i^* = b_1(., e_i)$. La famille $(e_1^*, \ldots, e_n^*)$ est une base de E^*. L'application $\psi : x \longrightarrow (e_1^*(x), \ldots, e_n^*(x))$ est un isomorphisme entre les espaces vectoriels E et $\mathbf{R}^n$. Notons $\mathscr{R}^*$ le réseau de $\mathbf{R}^n$ de $\mathbf{Z}$-base la base canonique $(c_1, \ldots, c_n)$ de $\mathbf{R}^n$. L'ensemble $\mathscr{C}(\mathscr{R}_1)$ est l'image réciproque de $\mathscr{R}^*$ par ψ, c'est donc un réseau de E de $\mathbf{Z}$-base $(\psi^{-1}(c_1), \ldots, \psi^{-1}(c_n))$ (c'est la base antéduale de la base $(e_1^*, \ldots, e_n^*)$). On remarque que $\mathscr{R}_1 \subset \mathscr{C}(\mathscr{R}_1)$).
   Si $\mathscr{R}_2$ est une extension de $\mathscr{R}_1$, la forme b_1 étant à valeurs entières sur $\mathscr{R}_2$, on a pour tout $x \in \mathscr{R}_2$ et tout $i \in \{1, \ldots, n\}$, $b_1(x, e_i) \in \mathbf{Z}$. Cela montre que $\psi(\mathscr{R}_2) \subset \mathscr{R}^*$, soit $\mathscr{R}_2 \subset \mathscr{C}(\mathscr{R}_1)$.

   (b) Soit $e = (e_1, \ldots, e_n)$ une $\mathbf{Z}$-base de $\mathscr{R}_1$. Tout élément de $\mathscr{C}(\mathscr{R}_1)/\mathscr{R}_1$ admet un unique représentant dans $\mathscr{C}(\mathscr{R}_1)$ de la forme $\sum_{i=1}^n x_i e_i$ où les réels x_i appartiennent à l'intervalle $[0, 1[$. Le pavé construit sur la famille e est un ensemble borné de E, donc d'après la question II-3 ne contient qu'un nombre fini d'éléments de $\mathscr{C}(\mathscr{R}_1)$. Donc le cardinal du groupe quotient $\mathscr{C}(\mathscr{R}_1)/\mathscr{R}_1$ est fini.

6. On démontre le théorème par récurrence sur n. Quitte à prendre la forme $-b$, on se ramène au cas $p \geqslant 1$.
   - Si $n=1$, la forme b est donnée par une matrice à un coefficient dans une base quelconque, donc est fixée par le choix du discriminant : il n'y a qu'une classe d'équivalence de groupe libre quadratique de rang 1 et de discriminant fixé.
   - Supposons le théorème vérifié à l'ordre $n-1$ et démontrons-le à l'ordre n. Fixons le discriminant Δ et considérons un groupe $(\mathscr{R}, b)$ de rang n et de discriminant Δ. D'après la question IV-3, il n'y a qu'un nombre fini de possibilités pour $m_b(\mathscr{R})$. Donc le groupe libre quadratique G_1 de rang 1, de $\mathbf{Z}$-base (v), et de forme la restriction de b à $<v>$ appartient à un nombre fini de classes d'équivalence. Le groupe libre quadratique $G_2 = (\mathscr{R}'', b')$ est de rang $n-1$ et son discriminant ne peut prendre qu'un nombre fini de valeurs d'après la question IV-4-b. Par hypothèse de récurrence, ce groupe n'appartient qu'à un nombre fini de classes d'équivalence. Le groupe libre quadratique G_3 obtenu par somme directe de G_1 et G_2 n'appartient donc qu'à un nombre fini de classes d'équivalence. D'après la question IV-4-a, le groupe $(\mathscr{R}, b)$ est une extension de G_3 et d'après la question IV-5, il n'y a qu'un nombre fini d'extensions d'un groupe libre quadratique. Cela conclut la démonstration du théorème.

7. (a) Soit e la base canonique de $\mathbf{R}^2$ et le groupe libre quadratique $G = (\mathscr{R}, b)$ tel que e est une $\mathbf{Z}$-base de $\mathscr{R}$ et la matrice de b dans e est $\begin{pmatrix}1 & 0\\ 0 & -2\end{pmatrix}$. Ce groupe est bien un groupe libre quadratique de rang 2 et de dicriminant -2 et nous allons montrer que tout groupe libre quadratique de rang 2 et de discriminant -2 est équivalent à celui-ci.. Soit $(\mathscr{R}, b)$ un groupe libre quadratique de rang 2 et de discriminant -2. Le discriminant étant strictement négatif, la signature de la forme b est $(1,1)$. D'après la question IV-3, on a $m_b(\mathscr{R})^2 \leqslant 3^{1/2}(4/3)^{1/2}2^{1/2} = 2\sqrt{2} < 3$. D'après la question IV-1, il existe un vecteur $v \in \mathscr{R}$ vérifiant $b(v,v) = m_b(\mathscr{R})^2$, donc étant obligatoirement primitif par minimalité de $m_b(\mathscr{R})$ et vérifiant $b(v,v) \in \{1,2\}$.
   - Supposons $b(v,v)=1$. Le vecteur v étant primitif, on peut le compléter en une $\mathbf{Z}$-base (v, e_2) de $\mathscr{R}$. La matrice de b dans cette base est de la forme $\begin{pmatrix}1 & \alpha\\ \alpha & \beta\end{pmatrix}$. Considérons la famille $e' = (v, -\alpha v + e_2)$. C'est une $\mathbf{Z}$-base de $\mathscr{R}$ car la matrice de passage appartient à $GL_2(\mathbf{Z})$ et dans cette base la forme b a pour matrice $\begin{pmatrix}1 & 0\\ 0 & -2\end{pmatrix}$. Le groupe est équivalent à G
   - Supposons $b(v,v)=2$. Le vecteur v étant primitif, on peut le compléter en une $\mathbf{Z}$-base (v, e_2) de $\mathscr{R}$. La matrice de b dans cette base est de la forme $\begin{pmatrix}2 & \alpha\\ \alpha & \beta\end{pmatrix}$ avec $2\beta - \alpha^2 = -2$. Considérons la famille $e' = (v, e_2 - tv)$ où l'entier t est choisi de manière à ce que $\alpha - 2t \in \{0,1\}$. La famille e' est une $\mathbf{Z}$-base de $\mathscr{R}$ car la matrice de passage appartient à $GL_2(\mathbf{Z})$ et dans cette base la forme b a pour matrice $\begin{pmatrix}2 & \alpha'\\ \alpha' & \beta'\end{pmatrix}$ avec $\alpha' \in \{0,1\}$ et $2\beta' - \alpha'^2 = -2$. Cela impose $\alpha' = 0$ et $\beta' = -1$. Le vecteur $v' = e'_1 - e'_2$ vérifie alors $b(v', v') = 1$ ce qui contredit l'hypothèse faite sur $m_b(\mathscr{R})$. Ce cas est impossible.

   (b) Soit e la base canonique de $\mathbf{R}^2$ et les groupes libres quadratiques $G_i = (\mathscr{R}, b_i)$ tel que e est une $\mathbf{Z}$-base de $\mathscr{R}$, la matrice de b_1 dans e est $\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$ et la matrice de b_2 dans e est $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$. Ces groupes sont bien des groupes libres quadratiques de rang 2 et de discriminant -1. Ils ne sont pas équivalents car la forme b_2 ne prend que des valeurs paires alors que la forme b_1 prend des valeurs impaires. Nous allons montrer que tout groupe libre quadratique de rang 2 et de discriminant -1 est équivalent à l'un de ces deux groupes.
   Soit $(\mathscr{R}, b)$ un groupe libre quadratique de rang 2 et de discriminant -1. Le discriminant étant strictement négatif, la signature de la forme b est $(1,1)$. D'après la question IV-3, on a $m_b(\mathscr{R})^2 \leqslant 3^{1/2}(4/3)^{1/2}1^{1/2} = 2$. D'après la question IV-1, il existe un vecteur $v \in \mathscr{R}$ vérifiant $b(v,v) = m_b(\mathscr{R})^2$, donc étant obligatoirement primitif par minimalité de $m_b(\mathscr{R})$ et vérifiant

$b(v,v) \in \{1,2\}$.

- Supposons $b(v,v)=1$. Le vecteur v étant primitif, on peut le compléter en une $\mathbf{Z}$-base (v,e_2) de $\mathscr{R}$. La matrice de b dans cette base est de la forme $\begin{pmatrix}1 & \alpha\\ \alpha & \beta\end{pmatrix}$. Considérons la famille $e'=(v,-\alpha v+e_2)$. C'est une $\mathbf{Z}$-base de $\mathscr{R}$ car la matrice de passage appartient à $GL_2(\mathbf{Z})$ et dans cette base la forme b a pour matrice $\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$. Le groupe est équivalent à G_1
- Supposons $b(v,v)=2$. Le vecteur v étant primitif, on peut le compléter en une $\mathbf{Z}$-base (v,e_2) de $\mathscr{R}$. La matrice de b dans cette base est de la forme $\begin{pmatrix}2 & \alpha\\ \alpha & \beta\end{pmatrix}$ avec $2\beta-\alpha^2=-1$. Considérons la famille $e'=(v,e_2-tv)$ où l'entier t est choisi de manière à ce que $\alpha-2t\in\{0,1\}$. La famille e' est une $\mathbf{Z}$-base de $\mathscr{R}$ car la matrice de passage appartient à $GL_2(\mathbf{Z})$ et dans cette base la forme b a pour matrice $\begin{pmatrix}2 & \alpha'\\ \alpha' & \beta'\end{pmatrix}$ avec $\alpha'\in\{0,1\}$ et $2\beta'-\alpha'^2=-1$. Cela impose $\alpha'=1$ et $\beta'=0$. Soit alors la famille $e''=(e'_1-e'_2,e'_2)$. C'est une $\mathbf{Z}$-base de $\mathscr{R}$ car la matrice de passage appartient à $GL_2(\mathbf{Z})$ et dans cette base la forme b a pour matrice $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$. Le groupe est donc équivalent à G_2.

3.3 Rapport sur l'épreuve écrite de mathématiques générales

Rapport des correcteurs

Remarques sur le problème

L'idée directrice du problème de mathématiques générales est un beau théorème de finitude sur les classes d'équivalence de groupes libres quadratiques. La démonstration s'appuie sur l'inégalité de Hermite-Minkovski, généralisation au cas quadratique de l'inégalité de Hermite. La première partie est centrée sur l'étude des sous-groupe finis de $GL_n(\mathbf{Z})$ et avait pour but principal de tester les capacités des candidats sur différents points du programme : algèbre linéaire, arithmétique de $\mathbf{Z}$ et $K[X]$, groupes,... La deuxième partie introduit les réseaux en démontrant quelques résultats classiques (en particulier l'existence de bases réduites) et en préparant la partie IV par la démonstration de l'inégalité de Hermite. La partie III met en oeuvre des techniques différentes du reste du problème en ouvrant une parenthèse sur la cristallographie, toujours dans le souci de permettre aux candidats de mettre en valeur leurs capacités. La partie IV démontre enfin l'inégalité de Hermite-Minkovski puis le théorème de finitude. On y combine dans une même structure les notions, souvent peu familières aux candidats, de réseaux et de formes quadratiques. Les candidats souhaitant approfondir les notions développées dans le problème pourront, par exemple, consulter l'ouvrage de J.M. Arnaudiès et J. Bertin, Groupes, algèbres et géométrie T2, où ils trouveront de nombreux exemples et développements ainsi qu'une bibliographie détaillée.

Remarques générales sur les copies

La plupart des remarques des années précédentes restent valables et peuvent être lues avec profit par les candidats. Nous développerons cependant les points qui nous semblent plus particulièrement utiles pour les futurs candidats.

La clarté, la rigueur, la précision et la concision de la rédaction sont des éléments importants d'appréciation des copies. De nombreux candidats perdent des points précieux dans les questions les plus accessibles du problème par des défauts de rédaction. Une première catégorie de défauts consiste en des démonstrations qui, bien que mathématiquement justes, sont maladroites, confuses, excessivement longues par multiplication inutiles des disjonctions de cas, utilisent des notations ou des notions qui ne font pas parties de l'énoncé et que le candidat n'a pas cru bon de définir (ou de définir avec précision),... Une deuxième catégorie de défauts, nettement plus graves et donc fortement sanctionnés, consiste en des démonstrations où manquent un ou plusieurs éléments essentiels dans l'enchaînement logique des arguments de la preuve : non initialisation d'une récurrence, utilisation du binôme de Newton dans un anneau non commutatif sans préciser que les éléments considérés commutent, oubli d'un argument crucial d'irréductibilité ou de non dégénérescence,... Il faut que les futurs candidats soient persuadés qu'ils ne perdront pas de temps ni de points, bien au contraire, en proposant une rédaction complète et rigoureuse des questions qu'ils auront résolues (tout en sachant rester concis...).

Il est par ailleurs indispensable que les candidats vérifient lors de leur préparation du concours qu'ils maîtrisent les bases de chaque chapitre du programme de l'agrégation et qu'ils savent mettre en oeuvre les théorèmes étudiés dans des situations concrètes de difficulté raisonnable : ce qui fait le plus souvent défaut aux candidats est moins la connaissance de résultats théoriques que leur assimilation par la pratique. C'est un entraînement extrêmement profitable pour la préparation des épreuves écrites et orales.

D'autre part, les problèmes d'agrégation sont volontairement de difficulté progressive et découpés en parties largement indépendantes pour permettre aux candidats de mettre en valeur leurs capacités. Si le grapillage est déconseillé, il est tout à fait possible qu'un candidat se sente peu à l'aise sur les notions développées dans une partie ou soit bloqué après une recherche sérieuse, lorsque la difficulté devient trop élevée. Le candidat a alors tout intérêt soit à regarder si les dernières questions de la partie, qui consistent souvent en une mise en application des résultats théoriques de la partie sur un exemple et sont abordables en admettant les résultats en question, lui semblent accessibles, soit à regarder si il se sent plus habile sur les parties suivantes : malgré la progressivité du problème, les premières questions des parties sont à priori toujours de difficulté mesurée et peuvent être l'occasion pour un candidat de montrer ses capacités.

Signalons enfin qu'une copie a traité tout le problème parfaitement mais que la grande majorité des candidats n'a abordé de manière sérieuse que les parties I et II qui ont donc été les parties discriminantes.

Remarques sur les questions

I.1. La plupart des candidats ont traité cette question, avec pour nombre d'entre eux une rédaction qui manque de rigueur. Dans le cas d'un raisonnement par récurrence, la récurrence n'est pas toujours initialisée ou le passage de n à $n+1$ n'est pas clairement explicité. De même la méthode consistant à développer le déterminant donnant le polynôme caractéristique par rapport à la dernière colonne a souvent été sanctionnée par manque, parfois total, de détails sur les calculs menés.

I.2.a. La question a été particulièrement discriminante. Il suffisait de remarquer qu'une valeur propre d'un endomorphisme est racine d'un polynôme annulateur de cet endomorphisme. De nombreuses erreurs portant sur les liens entre polynôme caractéristique, polynôme annulateur et polynôme minimal annulateur d'un endomomorphisme ont été relevées, la plus fréquente consistant à affirmer que le polynôme $C_M(X)$ était un diviseur de $X^m - 1$.

I.2.b-c. Les deux questions ont été traitées par la plupart des copies, avec un réel effort de rédaction. Les solutions proposées manquaient souvent de concision.

I.2.d. La question n'a été traité correctement que très rarement, les candidats n'utilisant pas (ou mal) l'irréductibilité des polynômes cyclotomiques et ayant des difficultés avec la notion de racine multiple.

I.2.e. Les solutions proposées par les candidats sont souvent longues ou incomplètes faute d'avoir remarqué que la matrice M était diagonalisable.

I.2.f. De nombreuses copies donnent une matrice d'ordre 6. Il était attendu une justification du fait que la matrice proposée était bien d'ordre 6. Rappelons que la vérification $M^6 = I_2$ prouve uniquement que l'ordre de M est un diviseur de 6.

I.3.b. Question plutôt bien traitée mis à part la difficulté technique qui imposait $p > 2$ qui n'a été traitée que de manière rarissime.

I.3.c. Dans cette question qui consistait essentiellement à réutiliser les deux questions précédentes, la rédaction manquait généralement de rigueur, ce qui a été sanctionné.

I.5.a. Il était attendu une justification pour le cardinal de $GL_2(\mathbf{F}_3)$.

I.5.b. La question n'a été traitée correctement que très rarement.

II.1. La question a été abordée dans la plupart des copies, la totalité des vérifications nécessaires n'étant que rarement faites.

II.2. L'erreur la plus fréquente a été de donner comme formule de changement de base $P^{-1}MP$.

II.3. La question a souvent été mal traitée. De nombreux candidats n'ont tenté de résoudre la question que dans un cas de norme particulière. D'autre ont voulu utiliser le fait que le réseau $\mathscr{R}$ était discret, sans démontrer cette propriété et en ne l'utilisant pas toujours à bon escient (rappelons en particulier que l'intersection d'un compact et d'un ensemble discret de $\mathbf{R}^n$ n'est pas obligatoirement un ensemble fini).

II.5.b. Il était suffisant de se ramener à la question 4.

II.5.d. La rédaction a été particulièrement discriminante dans cette question : il était nécessaire d'expliciter clairement le raisonnement par récurrence.

II.5.e. Seules les rares copies où étaient effectuées avec rigueur toutes les vérifications ont obtenues la totalité des points.

II.6.d. La question, délicate, n'a été que très rarement traitée.

II.7. Les deux questions ont souvent été abordées. Un nombre non négligeable de candidats perdent des points par manque de rigueur dans la rédaction ou mauvaise gestion des inégalités.

III.1. La question a été traitée par un nombre trop restreint de candidats au vu de sa difficulté, l'argument essentiel consistant à utiliser II.3.

III.2-3-4. Les questions 2-3-4 ont souvent donné lieu à une rédaction confuse. La principale difficulté consistait à comprendre la nature des objets manipulés.

III.5. La question 5 n'a été que très rarement abordée alors qu'elle proposait une application des résultats précédents, indépendante de leur démonstration. Elle devait permettre aux candidats de mettre en valeur leur connaissance du groupe diédral.

IV. La partie IV n'a été abordée que par une poignée d'excellents candidats. Les questions traitées sont alors le plus souvent très bien rédigées. Il est à remarquer que plusieurs questions de cette partie étaient de difficulté raisonnable et auraient pu être abordées par un nombre non négligeable de candidats.

Chapitre 4

Épreuve écrite d'analyse et probabilités

4.1 Énoncé

Notations et définitions

- Soit p un entier supérieur ou égal à 1. Soit Ω un ouvert de $\mathbf{R}^p$, on note C_Ω l'espace vectoriel des fonctions de Ω dans $\mathbf{R}$ qui sont de classe $\mathscr{C}^\infty$.
- Dans tout le problème, on appellera *difféomorphisme* entre deux ouverts de $\mathbf{R}^p$ une bijection entre ces deux ouverts qui est de classe $\mathscr{C}^\infty$ ainsi que sa réciproque.
- Si I est un intervalle on note I^2 le carré $I \times I$ de $\mathbf{R}^2$.
- Soit I un intervalle ouvert et f un élément de C_I . On dit que $x_0 \in I$ est un *point critique* de f si $f'(x_0) = 0$. Une *valeur critique* de f est un réel de la forme $f(x_0)$ où x_0 est un point critique. On dit qu'un point critique x_0 est *non dégénéré* si $f''(x_0)$ est non nul.
- Si A et B sont deux parties du plan $\mathbf{R}^2$ on dira que A et B sont *de même type* s'il existe deux intervalles ouverts I et J et un difféomorphisme ϕ de I^2 sur J^2 tels que :

$$A \subset I^2, \qquad B \subset J^2, \qquad \phi(A) = B$$

Objet du problème

Soit I un intervalle ouvert non vide de $\mathbf{R}$. Pour toute fonction f élément de C_I, et pour tout réel λ on définit la partie de $\mathbf{R}^2$:

$$E_\lambda(f) = \{(x, y) \in I^2, f(x) + f(y) = \lambda\}$$

Le problème se propose d'étudier quelques propriétés des ensembles $E_\lambda(f)$.

I. Préliminaires et exemples

I.A. Généralités

1. Soit I un intervalle ouvert quelconque de $\mathbf{R}$, et f un élément de C_I.

   (a) Déterminer $E_\lambda(f) \cap E_\mu(f)$ (pour λ, μ distincts) et $\cup_{\lambda\in\mathbf{R}} E_\lambda(f)$.

   (b) Démontrer que pour tout λ, $E_\lambda(f)$ est un fermé de I^2, et trouver une symétrie commune à tous les $E_\lambda(f)$.

(c) Soit $x_0 \neq 0$. On pose $g(x) = f(x + x_0)$. Préciser l'intervalle de définition de g. Quelle transformation géométrique envoie $E_\lambda(g)$ sur $E_\lambda(f)$?

2. Déterminer selon la valeur de λ, l'ensemble $E_\lambda(f)$ lorsque la fonction f est définie sur $\mathbf{R}$ par $f(x) = x^2$.
3. On prend dans cette question la fonction f définie sur $\mathbf{R}$ par $f(x) = x - x^3$. Démontrer que $E_0(f)$ est la réunion d'une droite et d'une ellipse.
4. On prend dans cette question la fonction f définie sur $\mathbf{R}$ par $f(x) = x^2 - x^3$.
   Démontrer que $E_0(f)$ est la réunion du point $(0,0)$ et d'une courbe dont on donnera une équation polaire et qu'on tracera sommairement, par exemple à l'aide d'une calculatrice graphique.

I.B. Racine carrée d'une fonction positive

5. Dans cette question, on note $I =]a, b[$ un intervalle contenant 0 ($a, b \in \overline{\mathbf{R}}$). On suppose de plus que la fonction $f \in C_I$ vérifie l'hypothèse suivante :

   (H) 0 est l'unique point critique de f et il est non dégénéré ; on a $f(0) = 0$ et $f''(0) > 0$.

   (a) Expliciter les variations de f.
   (b) On pose $g(x) = \int_0^1 (1-u) f''(xu)\,du$.
   Établir l'égalité $f(x) = x^2 g(x)$.
   (c) Démontrer que g est de classe $\mathscr{C}^\infty$ et strictement positive sur $]a, b[$.
   (d) Construire une fonction h croissante et de classe $\mathscr{C}^\infty$ sur I telle que pour tout x on ait $f(x) = h(x)^2$. Justifier que h est un difféomorphisme de I sur un intervalle J qu'on précisera en fonction de f.

Définition : *la fonction h ainsi définie sera appelée racine carrée de f.*

I.C. Ovales du plan

On reprend les notations de la question **5.** en supposant toujours que f vérifie l'hypothèse **(H)**.

6. En utilisant la racine carrée de f, démontrer que pour $\lambda > 0$ l'ensemble $E_\lambda(f)$ est de même type que l'intersection du cercle d'équation $x^2 + y^2 = \lambda$ et du carré J^2.

Définition : *dans la suite du problème, on appellera **ovale** toute partie du plan qui est de même type qu'un cercle.*

7. Une application

On considère le système différentiel (S) suivant :

$$\begin{cases} x'(t) & = & x(t) - x(t)y(t) \\ y'(t) & = & -y(t) + x(t)y(t) \end{cases}$$

où x et y sont deux fonctions inconnues de la variable t. Soit $(x_0, y_0) \in (\mathbf{R}_+^*)^2, (x_0, y_0) \neq (1,1)$.

On note : $t \to (x(t), y(t))$ l'unique solution maximale de (S) vérifiant $x(0) = x_0, y(0) = y_0$.

(a) Établir que les fonctions x et y ne peuvent pas s'annuler.
(b) Démontrer que le support de l'arc paramétré $t \mapsto (x(t), y(t))$ est inclus dans un ovale que l'on caractérisera à l'aide de x_0, y_0 et de la fonction g définie pour $x > 0$ par $g(x) = x - 1 - \ln(x)$.

II. Un problème de dénombrement

On rappelle le résultat suivant : *si $z \to g(z)$ est une fonction d'une variable complexe holomorphe sur le disque ouvert de centre* 0 *et de rayon r, alors elle est somme sur ce disque ouvert d'une série entière convergente.*

1. On pose, pour tout $z \in \mathbf{C}, \cos(z) = \frac{e^{iz}+e^{-iz}}{2}$ et $\sin(z) = \frac{e^{iz}-e^{-iz}}{2i}$.
   (a) Résoudre l'équation $\cos(z) = 0$.
   (b) Établir l'existence d'une suite $(b_n)_{n\in\mathbf{N}}$ de nombres **réels** tels que pour tout complexe z de module assez petit on ait :
   $$\frac{\sin(z)+1}{\cos(z)} = \sum_{n=0}^{\infty} \frac{b_n}{n!} z^n$$
   (il n'est pas demandé de calculer les coefficients b_n).
   (c) Démontrer que la fonction H définie sur $\mathbf{C} \setminus \{z, \cos(z) = 0\}$ par $H(z) = \frac{\sin(z)+1}{\cos(z)} + \frac{4}{2z-\pi}$ possède un prolongement holomorphe sur le disque ouvert $\left\{z, |z| < \frac{3\pi}{2}\right\}$.
   (d) En déduire que $b_n \sim \frac{2^{n+2} n!}{\pi^{n+1}}$.

2. Permutations alternantes
On donne $a_0, \ldots, a_{n-1}$, n nombres réels distincts rangés par ordre croissant : $a_0 < \ldots < a_{n-1}$. Soit σ une permutation de l'ensemble $\{a_0, \ldots, a_{n-1}\}$. On dit que σ est *alternante* si elle vérifie les deux propriétés suivantes :

$\sigma(a_{2i}) < \sigma(a_{2i+1})$ pour tout i tel que $0 < 2i+1 \leqslant n-1$
$\sigma(a_{2i-1}) > \sigma(a_{2i})$ pour tout i tel que $0 < 2i \leqslant n-1$

On dit que σ est *antialternante* si elle vérifie les inégalités inverses. On note e_n le nombre de permutations alternantes (par convention $e_0 = e_1 = 1$).
   (a) Déterminer toutes les permutations alternantes ainsi que l'entier e_n lorsque $n = 2, 3$ ou 4.
   (b) Démontrer qu'il y a (pour $n \geqslant 2$) autant de permutations alternantes que de permutations antialternantes.
   (c) Démontrer que pour tout $n \geqslant 1$ on a :
   $$2e_{n+1} = \sum_{i=0}^{n} \binom{n}{i} e_i e_{n-i}$$

Indication : *pour une permutation σ de $\{a_0, \ldots a_n\}$,on pourra considérer l'indice j tel que $\sigma(a_j) = a_0$.*
   (d) En conclure que pour tout n, $e_n = b_n$.

III. Les serpents d'Arnold

Dans cette partie, $I = \mathbf{R}$.

On se propose d'étudier la topologie de $E_\lambda(f)$ pour une famille de fonctions appelées *serpents d'Arnold*. Un entier $n > 0$ étant donné, on fixe n réels $a_0 < \ldots < a_{n-1}$ tels que les sommes $a_i + a_j$ pour $i \leqslant j$ soient toutes distinctes.

On note $\mathscr{A}_n$ l'ensemble des fonctions f de $\mathbf{R}$ dans lui même qui vérifient les propriétés suivantes :

– f est de classe $\mathscr{C}^\infty$;

– f possède exactement n points critiques, $x_0(f) < \ldots < x_{n-1}(f)$ et ils sont tous non dégénérés ;
– Les valeurs critiques de f sont $a_0, \ldots, a_{n-1}$.
Autrement dit, il existe une permutation σ_f de $a_0, \ldots, a_{n-1}$ telle que, pour tout i, $f\big(x_i(f)\big) = \sigma_f(a_i)$. La permutation σ_f s'appelle permutation associée à f ;
– $f(x)$ tend vers $+\infty$ quand x tend vers $-\infty$;
– $f(x)$ tend vers $+\infty$ ou vers $-\infty$ quand x tend vers $+\infty$.

Définition : *un élément f de $\mathscr{A}_n$ s'appelle un serpent à n points critiques.*

Remarque : pour alléger les notations, lorsqu'il n'y a pas d'ambiguïté, on note $x_0, \ldots, x_{n-1}$ les points critiques de f. De même, la notation $\mathscr{A}_n$ est en réalité une abréviation pour $\mathscr{A}_n(a_0, \ldots, a_{n-1})$.

Classes d'équivalence de serpents

1. Soit $f \in \mathscr{A}_n$. Préciser les variations de f selon la parité de n.
2. (a) Démontrer que la relation $\sim$ définie par « $f \sim g$ si et seulement s'il existe un difféomorphisme croissant h de $\mathbf{R}$ tel que $f = g \circ h$ » est une relation d'équivalence sur $\mathscr{A}_n$.
   (b) Démontrer que si $f \sim g$ alors pour tout λ, $E_\lambda(f)$ et $E_\lambda(g)$ sont de même type.
3. Soit h un difféomorphisme croissant de $\mathbf{R}$. Démontrer que $f \in \mathscr{A}_n \Leftrightarrow f \circ h \in \mathscr{A}_n$, et qu'alors $\sigma_f = \sigma_{f\circ h}$.
4. Réciproquement on suppose que f et g sont deux éléments de $\mathscr{A}_n$ qui vérifient $\sigma_f = \sigma_g$.
   (a) Démontrer qu'il existe une unique bijection h croissante de $\mathbf{R}$ dans $\mathbf{R}$ telle que $f = g \circ h$ et $h(x_k(f)) = x_k(g)$.
   (b) En utilisant la partie I, démontrer que h est un difféomorphisme.
5. (a) Démontrer que le nombre de classes d'équivalence de $\sim$ est majoré par l'entier b_n défini dans la partie **II**.
   (b) On admet que si $[\lambda, \mu]$ ne contient aucun élément $a_i + a_j$, les ensembles $E_\lambda(f)$ et $E_\mu(f)$ sont de même type. En déduire un majorant du nombre de types des $E_\lambda(f)$, lorsque λ parcourt $\mathbf{R}$ et f parcourt $\mathscr{A}_n$.

Topologie de $E_\lambda(f)$ dans le cas non critique

On se propose dans les questions qui suivent de décrire la topologie de $E_\lambda(f)$ lorsque f est un élément de $\mathscr{A}_n$ et que le réel λ n'est pas de la forme $a_i + a_j$.

On note $I_0 =]-\infty, x_0]$, $I_n = [x_{n-1}, \infty[$, et pour k variant de 1 à $n-1$, $I_k = [x_{k-1}, x_k]$.

6. Sous-graphes
   (a) Vérifier que $E_\lambda(f) \cap (I_i \times I_j)$ est, pour tout (i, j), l'ensemble vide ou le graphe d'une fonction strictement monotone continue définie sur un intervalle fermé inclus dans I_i.

Définition : *lorsque l'intersection $E_\lambda(f) \cap (I_i \times I_j)$ est non vide, on convient de l'appeler un* ***sous-graphe*** *de $E_\lambda(f)$.*

   (b) Démontrer que les extrémités du sous-graphe $E_\lambda(f) \cap (I_i \times I_j)$ sont sur la frontière du rectangle $I_i \times I_j$.
   (c) Démontrer que chaque extrémité d'un sous-graphe appartient à exactement un autre sous-graphe et que deux sous-graphes ne peuvent avoir d'autre point commun qu'une extrémité.
   (d) Démontrer que, si n est impair, tous les sous-graphes sont bornés et que si n est pair il y en a exactement 2 qui sont non bornés.

7. Composantes connexes de $E_\lambda(f)$
   (a) Démontrer que toute composante connexe est une union $\cup_{i=1}^{p} S_i$ de sous-graphes tels que S_i et S_{i+1} (pour i variant de 1 à $p-1$) ont une extrémité commune.
   (b) En déduire que lorsque n est pair il y a exactement une composante connexe non bornée.
   (c) Lorsque C est une composante connexe bornée, construire une bijection continue du cercle unité S^1 sur C

On peut alors démontrer, mais nous ne le ferons pas, que C est un ovale.

8. Démontrer que le nombre d'ovales est inférieur ou égal à $\left[\frac{n+1}{2}\right]^2$ (où $[\,.\,]$ désigne la partie entière).
9. Dans cette question on choisit $n = 2$.
   (a) Illustrer le fait que les composantes ne sont pas forcément des ovales lorsque λ est l'un des $a_i + a_j$
   (b) Démontrer qu'il y a au maximum 4 ensembles $E_\lambda(f)$ de types différents quand λ décrit $\mathbf{R}$.

IV. Réalisation polynomiale des serpents

On garde les notations de la partie précédente. L'entier n est supposé supérieur ou égal à 2. On souhaite démontrer le théorème **(*T*)** suivant, dû au mathématicien René Thom :

(*T*) *Pour toute $f \in \mathscr{A}_n$ il existe un polynôme P de degré $n+1$ tel que $f \sim P$.*

Il en résulte que les différents ensembles $E_\lambda(f)$ vus ci-dessus sont tous de même type qu'une courbe algébrique.

Notations

On note Ω_1 et Ω_2 les deux ouverts de $\mathbf{R}^{n-1}$ définis par :

$$\begin{aligned}
\Omega_1 &= \left\{(x_1,\dots,x_{n-1}) \in \mathbf{R}^{n-1},\ 0 < x_1 < x_2 < \cdots < x_{n-1}\right\},\\
\Omega_2 &= \left\{(y_1,\dots,y_{n-1}) \in \mathbf{R}^{n-1},\ 0 < y_1,\ \text{et pour tout } i > 0,\ y_{2i-1} > y_{2i} \text{ et } y_{2i} < y_{2i+1}\right\}.
\end{aligned}$$

Si $x = (x_1,\dots,x_{n-1})$ est un élément de Ω_1, on note P_x le polynôme de degré n défini par

$$P_x(t) = t(x_1 - t)\cdots(x_{n-1} - t)$$

Enfin, pour tout $i \in \{1,\dots,n-1\}$, on définit un polynôme $Q_{i,x}$ en posant $Q_{i,x}(t) = \frac{1}{t^2}\int_0^t \frac{P_x(u)}{x_i - u}\,du$.

A. Deux lemmes de topologie et un d'algèbre

1. Soient U et V deux ouverts connexes de $\mathbf{R}^{n-1}$ et ϕ une application continue de U dans V. On fait les deux hypothèses suivantes :
   H1 : l'image par ϕ de tout ouvert de U est un ouvert de V ;
   H2 : l'image réciproque par ϕ de tout compact de V est un compact de U.
   Démontrer que ϕ est surjective.
2. Soit E_n l'ensemble des polynômes unitaires (c'est-à-dire de coefficient dominant égal à 1) de degré n à coefficients réels. Démontrer que $\inf_{P\in E_n} \int_0^1 |P(t)|\,dt$ est un réel **strictement** positif.
   Dans la suite, on notera $C = \inf_{P\in E_n} \int_0^1 |P(t)|\,dt$.

3. Soient $R_1, \dots, R_{n-1}$, $n-1$ polynômes de degré inférieur ou égal à $n-2$, linéairement indépendants et $(t_1, \dots, t_{n-1})$, $n-1$ réels distincts. Démontrer que le déterminant $\det(R_i(t_j))$ est non nul.

B. Le théorème (T)

Soit Φ l'application :

$$\begin{array}{ccc} \Omega_1 & \to & \Omega_2 \\ x & \mapsto & \left(\int_0^{x_1} P_x(t)\,dt, \dots, \int_0^{x_{n-1}} P_x(t)\,dt\right) \end{array}$$

Afin d'alléger les notations, le vecteur $\Phi(x)$ sera noté $(y_1, \dots, y_{n-1})$.

4. Justifier que cette application est bien définie, exprimer ses dérivées partielles en fonction des polynômes $Q_{i,x}$ et en déduire que Φ vérifie l'hypothèse **H1**.
5. Pour $x \in \Omega_1$ démontrer l'inégalité :

$$\left| y_1 + \sum_{i=1}^{n-2} (-1)^i (y_{i+1} - y_i) \right| \geqslant C(x_{n-1})^{n+1}.$$

6. Démontrer que Φ vérifie l'hypothèse **H2** et en déduire le théorème ***(T)***.

4.2 Corrigé

Corrigé AP08

I.

I.A. Généralités et exemples.

1. (a) $E_\lambda(f)\bigcap E_\mu(f)$ est vide pour λ,μ distincts et $\bigcup\limits_{\lambda\in\mathbf{R}} E_\lambda(f)=I^2$

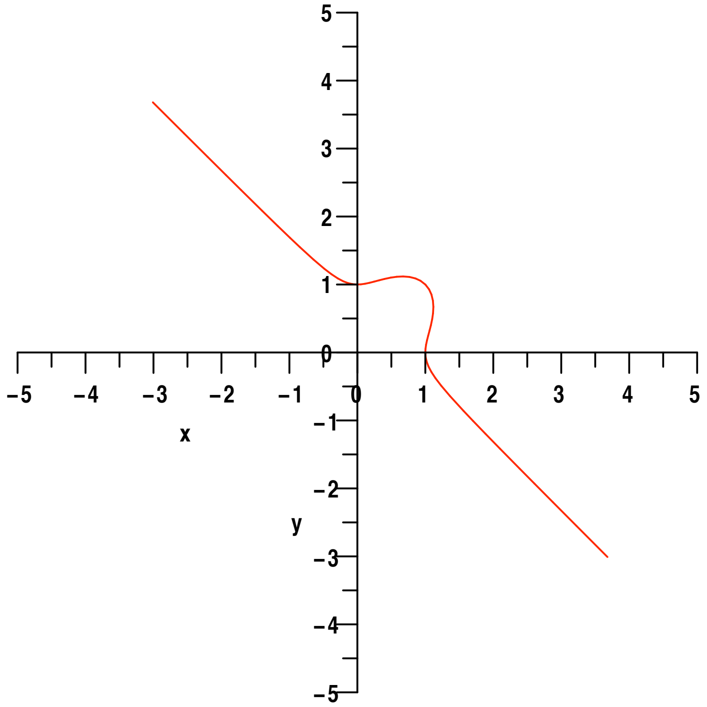
   (b) $E_\lambda(f)$ est l'image réciproque du fermé $\{\lambda\}$ par l'application continue $(x,y)\to f(x)+f(y)$. C'est donc un fermé de I^2. Tous les $E_\lambda(f)$ sont invariants par la transformation $(x,y)\to(y,x)$ donc sont symétriques par rapport à la première bissectrice.

   (c) g est définie sur l'intervalle J obtenu par translation de $-x_0$ à partir de I. $E_\lambda(f)$ est l'image de $E_\lambda(g)$ par la translation de vecteur $\overrightarrow{T}=(x_0,x_0)$

2. $E_\lambda(f)$ est l'ensemble d'équation $x^2+y^2=\lambda$. Donc :
   si $\lambda<0$, $E_\lambda(f)$ est vide
   si $\lambda=0$, $E_\lambda(f)$ est le point $(0,0)$
   si $\lambda>0$, $E_\lambda(f)$ est le cercle de centre $(0,0)$ et de rayon $\sqrt{\lambda}$.

3. $E_0(f)$ a pour équation $x-x^3+y-y^3=0$ soit $(x+y)(x^2-xy+y^2-1)=0$; C'est donc la réunion de la droite **D** d'équation $x+y=0$ et de la conique **C** d'équation $x^2-xy+y^2=1$. Cette conique est bien une ellipse car la forme quadratique $(x,y)\to x^2+xy+y^2$ est définie positive.

4. Cette fois ci $E_0(f)$ a pour équation $x^2+y^2=x^3+y^3$, ce qui donne, en écrivant $x=\rho\cos t, y=\rho\sin t$, $\rho^2(1-\rho(\cos^3 t+\sin^3 t))=0$. $E_0(f)$ est donc la réunion du point $(0,0)$ et de la courbe γ d'équation polaire $\rho(t)=\dfrac{1}{\cos^3 t+\sin^3 t}$.



I.B.Racine carrée d'une fonction positive.

5. (a) $f''(0) > 0$ donc puisque $f'(0) = 0$, f' est du signe de x au voisinage de zéro. Comme f' ne s'annule qu'en zéro on en déduit qu'elle est du signe de x sur $\mathbf{R}$ tout entier. f est donc décroissante sur $\mathbf{R}_-$ et croissante sur $\mathbf{R}_+$.

   (b) La formule de Taylor donne $f(x) = f(0) + xf'(0) + \int_0^x (x-t)f''(t)dt = \int_0^x (x-t)f''(t)dt$. Pour x non nul on fait dans cette intégrale le changement de variable $u = \dfrac{t}{x}$ et on obtient le résultat voulu. pour x nul le résultat demandé est évident.

   (c) la fonction g est de classe infinie par application du théorème de dérivation sous le signe intégrale dont toutes les hypothèses sont satisfaites. On a $g(0) = \dfrac{f''(0)}{2} > 0$. Par ailleurs pour x non nul $g(x) = \dfrac{f(x)}{x^2}$ est non nul et positif d'après l'étude des variations de f.

   (d) Puisque g est <u>strictement</u> positive la fonction $\sqrt{g}$ est également de classe infinie. On pose alors $h(x) = x\sqrt{g(x)}$. On a bien $f = h^2$ et h de classe infinie. Pour x non nul $h(x)$ est du signe de x, de même que$f'(x)$. l'égalité $2h(x)h'(x) = f'(x)$ assure alors $h'(x) > 0$. De plus on a
   $h'(0) = \lim\limits_0 \dfrac{h(x)}{x} = \sqrt{g(0)} > 0$. h' est positive et ne s'annule pas, donc h est un difféomorphisme de I sur $J =]-\sqrt{\lim\limits_a f(x)}, \sqrt{\lim\limits_b f(x)}[$

I.C. Ovales du plan.

6. Notons $\mathscr{C}_\lambda$ le cercle d'équation $x^2 + y^2 = \lambda$ et introduisons l'application

$$\phi : (x, y) \longmapsto (h(x), h(y))$$

   ϕest un difféomorphisme de I^2 sur J^2 puisque elle est bijective de classe $\mathscr{C}^\infty$ et que son jacobien au point (x, y) vaut $h'(x)h'(y) \neq 0$.
   Comme $E_\lambda(f) = \{(x, y), h^2(x) + h^2(y) = \lambda\}$ on a $E_\lambda(f) = \phi^{-1}(\mathscr{C}_\lambda \bigcap J^2)$ et donc le résultat voulu.

7. L'existence et l'unicité de la solution maximale sont assurées par le théorème de Cauchy. Notons s cette solution et $\mathscr{I}_s$ son intervalle de définition.

   (a) Supposons par exemple qu'il existe t_0 tel que $x(t_0) = 0$ alors la fonction $t \longmapsto (0, y(t_0)e^{-t+t_0})$ est solution de (S) et vaut $(x(t_0), y(t_0))$ en $t = t_0$. Pourtant en $t = 0$ elle vaut $(0, y(t_0)e^{t_0}) \neq (x_0, y_0)$. Il y a donc deux solutions différentes au même problème de Cauchy en t_0. C'est impossible. S'il existe t_0 tel que $y(t_0) = 0$ on aboutit à la même contradiction avec la fonction $t \longmapsto (x(t_0)e^{t-t_0}, 0)$.

   (b) Commençons par remarquer que $g(x(t)) + g(y(t))$ est bien défini et se dérive en
   $x'(t)(1 - \dfrac{1}{x(t)}) + y'(t)(1 - \dfrac{1}{y(t)}) = (1 - y(t))(x(t) - 1) + (-1 + x(t))(y(t) - 1) = 0$
   Par conséquent $g(x(t)) + g(y(t)) = g(x_0) + g(y_0)$ pour tout t ce qui prouve que le support de la solution est inclus dans $E_\lambda(g)$ pour $\lambda = g(x_0) + g(y_0)$.

   Reste à voir que c'est un ovale : comme $g'(x) = 1 - \dfrac{1}{x}$ et $g''(x) = \dfrac{1}{x^2} > 0$, 1 est l'unique point critique de g et il est non dégénéré. De plus $g(1) = 0$. Donc l'hypothèse **(H)** est vérifiée pour la fonction f telle que $f(x-1) = g(x)$ (nous savons d'après la question 1.c qu'une translation de la variable ne change pas le type). Comme ici on a $g(]0, 1[) = g(]1, +\infty[) = \mathbf{R}^+$, le carré J^2 est égal au plan tout entier. Enfin, comme $(x_0, y_0) \neq (1, 1)$ on a $\lambda > 0$. La question 6. s'applique donc, et $E_\lambda(g)$ est un ovale.

II.

1. (a) $\cos z = 0 \Leftrightarrow e^{iz} = -e^{-iz} \Leftrightarrow e^{2iz} = -1 \Leftrightarrow z \in \frac{\pi}{2} + \pi\mathbf{Z}$

   (b) la fonction cos est homomorphe et ne s'annule par sur le disque ouvert de centre 0 de rayon $\frac{\pi}{2}$ donc $z \mapsto \frac{1+\sin z}{\cos z}$ est holomorphe sur ce même disque, ce qui assure l'existence (et l'unicité) de la série. Les coefficients b_n sont réels car ce sont les dérivées successives en 0 de $\frac{1+\sin z}{\cos z}$ qui est réel pour z réel.

   (c) La fonction H est déjà holomorphe sur le disque ouvert $\left\{z, |z| < \frac{3\pi}{2}\right\}$ privé des points $\frac{\pi}{2}, \frac{-\pi}{2}$.
   Lorsque deux fonctions holomorphes g_1, g_2 s'annulent en z_0, le quotient $\frac{g_1}{g_2}$ se prolonge en une fonction holomorphe au voisinage de z_0 si et seulement si l'ordre du zéro z_0 pour g_1 est supérieur ou égal à son ordre pour g_2.
   or $z_0 = -\frac{\pi}{2}$ est un zéro d'ordre 1 des fonctions $g_1(z) = \sin z + 1$ et $g_2(z) = \cos z$, puisque les deux fonctions s'annulent en z_0 et pas leurs dérivées. Ceci prouve que H se prolonge en $-\frac{\pi}{2}$.
   Pour $z_0 = \frac{\pi}{2}$ on peut écrire $H(z) = \frac{(z-\frac{\pi}{2})(1+\sin z) + 2\cos z}{(z-\frac{\pi}{2})\cos z} = \frac{g_1(z)}{g_2(z)}$. z_0 est zéro d'ordre 2 pour g_2 et comme $g_1(z_0) = g_1'(z_0) = 0$ il est d'ordre au moins 2 pour g_1. Donc par le même argument, H se prolonge en $\frac{\pi}{2}$.

   (d) Pour z voisin de zéro on a $\frac{4}{2z-\pi} = \sum_0^\infty \frac{-2^{n+2}}{\pi^{n+1}} z^n$, donc $H(z) = \sum_0^\infty (\frac{b_n}{n!} - \frac{2^{n+2}}{\pi^{n+1}}) z^n$. Comme H est holomorphe sur $\{z, |z| < \frac{3\pi}{2}\}$, le rayon de convergence de cette série est au moins égal à $\frac{3\pi}{2}$. La série converge pour $z = \frac{\pi}{2}$ donc en particulier $(\frac{b_n}{n!} - \frac{2^{n+2}}{\pi^{n+1}})(\frac{\pi}{2})^n = o(1)$ ce qui donne directement l'équivalent voulu.

2. (a) Une permutation σ étant représentée par le n-uplet $(\sigma(a_0), \dots, \sigma(a_{n-1}))$ on a :

   pour $n = 2$, une seule permutation alternante : (a_0, a_1)

   pour $n = 3$, deux permutations alternantes : (a_0, a_2, a_1) et (a_1, a_2, a_0)

   pour $n = 4$, cinq permutations alternantes : $(a_0, a_2, a_1, a_3), (a_0, a_3, a_1, a_2), (a_1, a_2, a_0, a_3), (a_1, a_3, a_0, a_2)$ et (a_2, a_3, a_0, a_1)

   (b) Notons $\mathscr{AL}$ (resp. $\mathscr{AAL}$) l'ensemble des permutations alternantes (resp. antialternantes). Soit τ la permutation qui inverse les a_i : $\tau = (a_{n-1}, \dots, a_1, a_0)$. Alors l'application $\sigma \mapsto \tau \circ \sigma$ est une bijection de $\mathscr{AL}$ sur $\mathscr{AAL}$. Les deux ensembles ont donc le même cardinal.

   (c) Comptons de deux façons différentes le nombre de permutations de $n+1$ éléments $a_0, \dots, a_n$ qui sont alternantes ou antialternantes.
   D'une part ce nombre vaut $2e_{n+1}$ d'après la question précédente et le fait que les ensembles $\mathscr{AL}$ et $\mathscr{AAL}$ sont disjoints.
   D'autre part, choisir un élément σ de $\mathscr{AL} \bigcup \mathscr{AAL}$ c'est successivement :
   – Choisir parmi $\{0, .., n\}$ l'indice i tel que $\sigma(a_i) = a_0$ (noter que la parité de cet indice détermine si σ est alternante ou antialternante).
   – Choisir parmi $\{a_1, .., a_n\}$ le sous ensemble S_i des images par σ de $\{a_0, \dots, a_{i-1}\}$. Il y a $\binom{n}{i}$ choix pour cet ensemble ; ce choix détermine l'ensemble T_i des images de $\{a_{i+1}, .., a_n\}$.

– Choisir les deux restrictions de σ :
$\sigma_1 : \{a_0, ..., a_{i-1}\} \mapsto S_i$
$\sigma_2 : \{a_{i+1}, ..., a_n\} \mapsto T_i$
Si i est pair, la condition $\sigma \in \mathscr{AL} \bigcup \mathscr{AAL} \Leftrightarrow \sigma \in \mathscr{AL}$ est réalisé si et seulement si σ_1 est alternante et σ_2 antialternante (cette définition a bien un sens même si ce ne sont pas des permutations)
Si i est impair on a $\sigma \in \mathscr{AL} \bigcup \mathscr{AAL} \Leftrightarrow \sigma \in \mathscr{AAL}$ si et seulement si σ_1 et σ_2 sont antialternantes.
Dans les deux cas il y a $e_i e_{n-i}$ choix pour σ. Finalement on a bien

$$2e_{n+1} = \sum_{i=0}^{n} \left(\begin{array}{c} n \\ i \end{array} \right) e_i e_{n-i}$$

(d) Posons $f(x) = \sum_0^\infty \frac{e_n}{n!} x^n$. Cette série est définie au moins sur $]-1, 1[$ puisque $e_n \leqslant n!$ On a :

$$\begin{aligned} f^2(x) &= \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} \frac{e_i}{i!} \frac{e_{n-i}}{(n-i)!} \right) x^n \\ &= 1 + \sum_{n=1}^{\infty} \left(\sum_{i=0}^{n} \frac{e_i}{i!} \frac{e_{n-i}}{(n-i)!} \right) x^n \\ &= 1 + 2 \sum_1^\infty \frac{e_{n+1}}{n!} x^n \\ &= 1 + 2 (\sum_0^\infty \frac{e_{n+1}}{n!} x^n - 1) \\ &= 1 + 2(f'(x) - 1) \end{aligned}$$

Un calcul direct prouve que la fonction $x \mapsto \dfrac{1 + \sin x}{\cos x}$ vérifie la même équation différentielle. Comme les deux fonctions prennent la valeur 1 en zéro, elles sont égales au voisinage de zéro d'après le théorème de Cauchy. Par unicité des coefficients d'une série entière, on en déduit pour tout n $e_n = b_n$.

III.

1. Sur $]x_i, x_{i+1}[$ f croit pour tout i pair et décroit pour tout i impair. Elle décroit sur $]-\infty, x_0[$. Sur le dernier intervalle $]x_{n-1}, +\infty[$ f croit si n impair et décroit si n pair.
2. (a) $f = f \circ Id$ donne la réflexivité. Pour la symétrie, $f = g \circ h \Rightarrow g = f \circ h^{-1}$ et h^{-1} est un difféomorphisme croissant si h l'est. $f = g \circ h, g = g' \circ h' \Rightarrow f = g' \circ (h' \circ h)$ et puisque $h' \circ h$ est aussi un difféomorphisme croissant, $\sim$ est transitive.

   (b) Si $f = g \circ h$, introduisons l'application

   $$\phi : (x, y) \mapsto (h(x), h(y))$$

   Comme à la question **I.6**, ϕ est un difféomorphisme de $\mathbf{R}^2$ et $E_\lambda(f) = \phi^{-1}(E_\lambda(g))$
3. -h étant un difféomorphisme croissant les limites de f et de $g = f \circ h$ sont les mêmes.
   -$f'(x) = h'(x) g'(h(x))$ prouve, puisque h' ne s'annule pas que les points critiques de f sont exactement les $x_k(f) = h(x_k(g))$. Il y en a bien le même nombre et ils sont rangés dans le même sens par croissance de h. Les valeurs critiques sont bien les mêmes.
   -Enfin $f'' = h'' g' \circ h + h'^2 g'' \circ h$ donne $f''(x_k(f)) = h'^2(x_k(f)) g''(x_k(g))$ et les points critiques de f sont non dégénérés si et seulement si ceux de g le sont. Comme $f(x_k(f)) = g(x_k(g))$ les permutations σ_f et σ_g sont égales.

4. (a) Pour tout k les restrictions f_k et g_k des applications f et g à $[x_k(f), x_{k+1}(f)]$ et $[x_k(g), x_{k+1}(g)]$ sont des homéomorphismes sur leur image (et même des difféomorphismes si l'on restreint aux intervalles ouverts). Comme $\sigma_f = \sigma_g$ ces images sont toutes les deux $[\sigma_f(a_k), \sigma_f(a_{k+1})]$. On peut définir $h_k = g_k^{-1} \circ f_k$ sur $[x_k(f), x_{k+1}(f)]$. Cette application h est continue et strictement croissante car f_k et g_k ont la même monotonie. Enfin les égalités $h_k(x_k(f)) = x_k(g), h_k(x_{k+1}(f)) = x_{k+1}(g)$ assurent que h_k et h_{k+1} se raccordent en une fonction h continue et strictement croissante, donc bijective. On traiterait de même le cas des intervalles $]-\infty, x_0]$ et $[x_{n-1}, +\infty[$. De plus, vues les limites de f et g on a $h(\mathbf{R}) = \mathbf{R}$.

   Pour l'unicité, notons que l'égalité $f = g \circ h$ restreinte à $[x_k(f), x_{k+1}(f)]$ devient $f_k = g_k \circ h$ puisque, étant données les conditions imposées à h, on a forcément $h([x_k(f), x_{k+1}(f)]) = [x_k(g), x_{k+1}(g)]$, et donc $h_{|[x_k(f), x_{k+1}(f)]} = h_k$.

   (b) Soit $k \in \{0, ..., n-1\}$ Soit un intervalle I contenant $x_k(f)$ et aucun autre point critique de f. Alors d'après la première partie on peut écrire sur $I, f(x) = f(x_k(f)) + \epsilon\phi(x)^2$, où ϕ est un difféomorphisme croissant et ϵ est le signe de $f''(x_k(f))$. Avec des notations analogues on a $g(x) = g(x_k(g)) + \epsilon\psi(x)^2$ sur tout J contenant $x_k(g)$ et aucun autre point critique de g(ϵ est le même dans les deux cas). De $f = g \circ h$ on déduit sur I que $\phi^2(x) = \psi^2(h(x))$, d'où par croissance $\phi(x) = \psi(h(x))$ soit encore $h(x) = \psi^{-1}(\phi(x))$ ce qui prouve que h est un difféomorphisme sur I. Comme les intervalles I où cette construction est possible recouvrent $\mathbf{R}$, h est bien un difféomorphisme.

5. (a) D'après ce qui précède pour chaque permutation σ_f il y a au plus une classe de $\sim$. les variations de f étudiées à la question **1.** prouvent que σ_f est alternante. Il y a donc au maximum b_n classes pour $\sim$.

   (b) Il y a $\dfrac{n(n+1)}{2}$ rÈels $a_i + a_j$ qui délimitent $\dfrac{n(n+1)}{2} + 1$ intervalles ouverts. f étant fixée, lorsque λ parcourt $\mathbf{R}$ le nombre de types possibles pour $E_\lambda(f)$ est donc majoré par $n(n+1)+1$. Compte tenu de la question précédente, lorsqu'on fait varier f le nombre total de types possible est majoré par $(n(n+1)+1)b_n$.

6. (a) Avec les notations de la question **4.** $E_\lambda(f) \cap (I_i \times I_j) = \{(x, y), y = f_j^{-1}(\lambda - f_i(x))\}$ C'est donc le graphe d'une fonction strictement monotone définie sur l'intervalle fermé $f_i^{-1}(\lambda - f_j(I_j))$.

   (b) Pour tout $(a, b) \in E_\lambda(f)$ on a a ou b qui n'est pas un point critique de f vu que $\lambda \neq a_i + a_j$. Par conséquent, l'une des deux dérivées partielles de $(x, y) \mapsto f(x) + f(y)$ est non nulle en (a, b). Par le théorème des fonctions implicites, $E_\lambda(f)$ est localement un graphe en chacun de ses points. Il en que résulte que $E_\lambda(f) \cap (I_i \times I_j)$ n'est pas réduit à un point (il possède donc deux extrémités si son intervalle de définition est un segment et une seule si son intervalle de définition est non borné) et que ses extrémités sont sur la frontière du rectangle.

   (c) Comme $\lambda \neq a_i + a_j$ un sous graphe ne contient aucun (a_i, a_j). Or un point du plan autre que les (a_i, a_j) ne peut appartenir qu'à deux rectangles $I_i \times I_j$ distincts et alors il est sur leur frontière commune.

   (d) Commençons par noter que si n est impair, f est minorée d'après ses variations. Soit M sa borne inférieure, alors pour $(x, y) \in E_\lambda(f)$ on a $M \leqslant f(x) \leqslant \lambda - M$ et $M \leqslant f(y) \leqslant \lambda - M$. Comme les limites de f sont infinies, ceci prouve que $E_\lambda(f)$ est borné, donc tous ses sous graphes aussi.

   Lorsque n est pair, compte tenu des variations de f les seuls sous graphes pouvant être non bornés sont $E_\lambda(f) \cap (I_0 \times I_n)$ et $E_\lambda(f) \cap (I_n \times I_0)$. Le premier est le graphe d'une fonction définie sur $f_0^{-1}(\lambda - f(I_n)) = f_0^{-1}([\lambda - f(x_{n-1}), +\infty[)$ qui est un intervalle de la forme $]-\infty, b]$, donc il est non borné. le second est symétrique du premier par rapport à la droite $x = y$.

7. (a) Considérons une famille maximale $\{S_1, ..., S_p\}$ de sous-graphes distincts ayant la propriété de l'énoncé. alors $C = S_1 \cup ... \cup S_p$ est une composante connexe. En effet :

   C est connexe car les S_i sont tous connexes et $S_i \cap S_{i+1} \neq \emptyset$.

   C ne rencontre aucun sous graphe autre que les S_i par maximalité et d'après la question **6.c.**. Donc toute partie C' contenant strictement C n'est pas connexe.

De plus, toutes les composantes connexes sont de ce type puisque chaque élément de $E_\lambda(f)$ est dans un sous graphe et que tout sous graphe est dans une famille maximale du type précédent.

(b) Supposons que S_1 soit borné : il possède deux extrémités. Alors l'une n'est pas commune à S_2 car deux sous graphes ne peuvent avoir les deux mêmes extrémités. Cette extrémité est dans un sous-graphe par **6.c** donc dans un des S_i par maximalité, et donc forcément dans S_p vu qu'un sous-graphe n'a que 2 extrémités. il en résulte que S_p est borné. Le même raisonnement vaut dans l'autre sens et par conséquent les deux sous graphes non bornés du cas pair sont dans la même composante. Il y a donc dans ce cas une unique composante connexe non bornée.

(c) Gardons la notation $C = S_1 \cup \ldots \cup S_p$. Puisque S_1 et S_p ont une extrémité commune on pourra aussi noter S_0 pour S_p et S_{p+1} pour S_1. Comme S_i est un graphe d'une fonction continue sur un segment il possède un paramétrage de la forme

$$\begin{aligned} [a,b] &\to \mathbf{R}^2 \\ x &\mapsto (x,\phi(x)) \end{aligned}$$

En faisant le changement de variable affine $t = \dfrac{i-1}{p} + \dfrac{(x-a)}{p(b-a)}$ on obtient un paramétrage :

$$\begin{aligned} [\frac{i-1}{p},\frac{i}{p}] &\to \mathbf{R}^2 \\ t &\mapsto M(t) = (x(t),y(t)) \end{aligned}$$

Les deux extrémités de S_i sont alors les points $M(\frac{i-1}{p}), M(\frac{i}{p})$. Quitte à refaire un changement affine, on peut supposer que $S_i \cap S_{i-1} = M(\frac{i-1}{p})$ et $S_i \cap S_{i+1} = M(\frac{i}{p})$

de sorte que les fonctions M définies séparément sur chaque $[\frac{i-1}{p},\frac{i}{p}]$ se raccordent en une fonction continue sur $[0,1]$. Comme de plus $M(0) = M(1)$ (ce sont les extrémités communes de S_1 et S_p), l'application

$$\begin{aligned} S^1 &\to \mathbf{R}^2 \\ e^{2\pi i t} &\mapsto M(t) \end{aligned}$$

est définie, continue et réalise une bijection de S^1 sur C.

8. Dans une composante connexe, deux sous-graphes consécutifs correspondent à des paires d'indices $(i,j),(i',j')$ telles que $|i-i'|+|j-j'| = 1.(*)$

   Dans le cas où n est pair, la composante connexe non bornée contient les sous-graphes relatifs aux indices $(i,j) = (n,0)$ et $(i',j') = (0,n)$. Cette composante connexe contient donc au minimum $1+|n-0|+|0-n| = 2n+1$ sous graphes.

   Pour les composantes bornées la relation $(*)$ assure que le nombre de sous-graphes est pair différent de 2, donc au moins égal à 4.

   Comme il y a au maximum $(n+1)^2$ sous-graphes le nombre d'ovales est majoré par

   $\dfrac{(n+1)^2}{4}$ si n impair

   $\dfrac{(n+1)^2-(2n+1)}{4} = \dfrac{n^2}{4}$ si n est pair.

9. (a) Les deux exemples des questions **I.3** et **I.4** n' ont pas d'ovales bien que la fonction f soit un serpent à 2 points critiques. dans le premier cas on a deux valeurs critiques opposées a_1, a_2 et $\lambda = a_1 + a_2 = 0$, dans le second cas, $a_1 = 0$ est valeur critique et on a $\lambda = a_1 + a_1 = 0$.

   (b) Dans le cas particulier $n = 2$ il y a au maximum un ovale. De plus le type de $E_\lambda(f)$ ne dépend pas des valeurs de a_0, a_1. En effet on peut composer f à gauche par une transformation affine T qui envoie (a_0,a_1) sur $(-1,1)$ (par exemple) et $E_\lambda(T\circ f)$ est égal à $E_\mu(f)$ pour $\mu = T(\lambda)+T(0)$.

Or dans le cas de l'exemple du **I.A.3** la fonction f est impaire et possède deux points critiques opposés, et donc $E_\lambda(f)$ et $E_{-\lambda}(f)$ sont de même type. Il en résulte qu'il n'y a que 4 types possibles :

1. $\lambda = 0$
2. $\lambda \in]0, 2a_1[$
3. $\lambda = 2a_1$
4. $\lambda > 2a_1$

Les types 1. et 3. sont ceux mis en évidence à la question précédente, le type 2. et le type 4. (qui sont effectivement différents, même si on ne l'a pas prouvé) correspondent au cas où l'on a respectivement 1 et 0 ovale.

IV.

1. Soit (x_n) une suite de l' image de Φ qui converge dans V vers x. Notons y_n un antécédent de x_n. La suite (y_n) est dans $\phi^{-1}(K)$ où K est le compact $\{x_n, n \in \mathbf{N}\} \cup \{x\}$. Vu l'hypothèse sur Φ, (y_n) possède une valeur d'adhérence l et on a par continuité $\Phi(l) = x$. Donc x est dans l'image de Φ

   L'image de Φ est ouverte et fermée, donc c'est V par connexité.
2. C est la distance pour la norme 1 de l'origine au sous espace affine E_n. Comme ce dernier est de dimension finie, cette distance est atteinte, en particulier elle est non nulle.
3. Il est classique que l'appli cation $P \mapsto (P(t_1), ..., P(t_{n-1}))$ est un isomorphisme de $\mathbf{R}_{n-2}[X]$ sur $\mathbf{R}^{n-1}$. L'image d'une base $(R_1, ..., R_{n-1})$ est une base. D'où le résultat.
4. Il s'agit de montrer que Φ est bien à valeurs dans Ω_2. On a $y_1 > 0$ puisque P_x est positif sur l'intervalle $[0, x_1]$. De plus pour tout i, sur $[x_i, x_{i+1}]$ P_x est du signe de $t(x_1 - t)...(x_i - t)$ c'est à dire du signe de $(-1)^i$. Donc $y_{i+1} - y_i$ est du signe de $(-1)^i$ ce qui est exactement la propriété voulue.

   On a $\dfrac{\partial}{\partial x_i}\displaystyle\int_0^{x_j} P_x(t)dt = \int_0^{x_j} \dfrac{\partial}{\partial x_i} P_x(t)dt$pour tout (i, j) tel que $i \neq j$ par dérivation sous le signe intégrale. Lorsque j vaut i, il faut en plus dériver la borne et l'on obtient

   $$\frac{\partial}{\partial x_i}\int_0^{x_i} P_x(t)dt = \int_0^{x_i} \frac{\partial}{\partial x_i} P_x(t)dt + P_x(x_i)$$

   ce qui donne le même résultat vu que x_i est racine de P_x.
   Or $\dfrac{\partial}{\partial x_i} P_x = \dfrac{P_x}{x_i - x}$ donc $\dfrac{\partial}{\partial x_i}\displaystyle\int_0^{x_j} P_x(t)dt = x_j^2 Q_{i,x}(x_j)$.
   Soit J la matrice jacobienne de Φ. $\det J = \det(x_j^2 Q_{i,x}(x_j)) = \prod_j (x_j)^2 \det(Q_{i,x}(x_j))$. Ce déterminant est non nul d'après le résultat **3** sous réserve que les polynômes $Q_{i,x}$ qui sont bien de degré $n-2$ forment une famille libre.
   Mais si l'on suppose $\sum \lambda_i Q_{i,x} = 0$ alors en multipliant par x^2 puis en dérivant et en divisant par P_x il vient $\sum \lambda_i \dfrac{1}{x_i - x} = 0$ et finalement les λ_i sont nuls par unicité de la décomposition en éléments simples.
   J est inversible, donc d'après le théorème d'inversion locale Φ est ouverte.
5. On a déjà vu que $(-1)^i(y_{i+1} - y_i) = \displaystyle\int_{x_i}^{x_{i+1}} (-1)^i P_x(t)dt = \int_{x_i}^{x_{i+1}} |P_x(t)|dt$.

   La somme S proposée vaut donc $S = \displaystyle\int_0^{x_{n-1}} |P_x(t)|dt = \int_0^1 x_{n-1}|P_x(ux_{n-1})|du$ (on a posé $t = u.x_{n-1}$).
   Or $P_x(u.x_{n-1})$ est un polynôme de la forme $(x_{n-1})^n R(u)$ avec R polynôme unitaire de degré n. Donc d'après la question **2** on a $S \geqslant C(x_{n-1})^{n+1}$.

6. Ω_1 et Ω_2 sont bien des ouverts connexes puisque ce sont des intersections de demi-espaces vectoriels (donc convexes) ouverts. Soit K_2 un compact de Ω_2. Posons $K_1 = \Phi^{-1}(K_2)$. K_1 est fermé car Φ est continue, et borné en raison de la question précédente puisque $\sup_i |x_i| = x_{n-1}$ est borné si les y_i le sont (rappelons que C est stritement positive).

   Notons maintenant que l'application Φ est également définie sur $\overline{\Omega_1}$. Pour montrer que K_1 est compact il suffit de montrer qu'il est fermé dans $\overline{\Omega_1}$ car un fermé borné est un compact dans $\mathbf{R}^{n-1}$. Soit $X = (x_1, ..., x_{n-1})$ un point adhérent à K_1. S'il n'est pas dans K_1 alors il existe i tel que $x_i = x_{i+1}$ (ou bien $x_1 = 0$, qui se traite de la même façon). X est la limite d'une suite (X_n) d'éléments de K_1 donc puisque Φ est continue sur $\overline{\Omega_1}$, $\Phi(X)$ est la limite d'une suite de K_2, et par suite $\Phi(X) \in K_2 \subset \Omega_2$. Or manifestement, si $x_i = x_{i+1}$ on a $y_i = y_{i+1}$ ce qui fournit une contradiction.

   Toutes les hypothèses sont réunies pour appliquer la question **1.** : Φ est surjective.

   Soit alors $(a_0 < a_1 < ... < a_{n-1})$ et σ une permutation alternante. Posons $y_i = \sigma(a_i) - \sigma(a_0)$ pour $i = 1..n-1$. Posons $x_0 = 0$. Soit $(x_1, ..., x_{n-1})$ un antécédent de $(y_1, ..., y_{n-1})$ par Φ et soit enfin P le polynôme défini par l'égalité :$P(X) = \sigma(a_0) + \int_0^X P_x(t)\,dt$. Alors par construction $P(x_i) = \sigma(a_i)$ et $P'(x_i) = P_x(x_i) = 0$ pour tout i. De plus les zéros de $P' = P_x$ sont simples donc $P''(x_i) \neq 0$. Enfin P étant un polynôme ses limites sont infinies en $\pm\infty$ et vu son coefficient dominant $(-1)^{n-1} X^{n+1}$ il tend vers $+\infty$ en $-\infty$.

   P est donc bien un élément de $\mathscr{A}_n$.

.

4.3 Rapport sur l'épreuve écrite d'analyse et de probabilités

Rapport des correcteurs

Remarques générales

Le problème étudiait les lignes de niveau de fonctions de deux variables réelles. Il était construit en quatre parties relativement indépendantes permettant de balayer une large partie du programme (fonctions d'une variable réelle, équations différentielles, fonctions d'une variable complexe, topologie et calcul différentiel...). Les trois premières parties commençaient par des questions faciles ce qui a permis à tous les candidats, même les plus modestes, de mettre en évidence leurs connaissances.

La première partie d'analyse élémentaire établissait le lemme de Morse en dimension 1 et en donnait une application au système de Lokta Volterra. Elle permettait d'évaluer les candidats sur des notions dont la maîtrise est indispensable pour un enseignant de Terminale. Elle a été traitée de façon convenable par une grande partie d'entre eux. Les trois autres parties ont connu un succès plus mitigé. Un nombre significatif de candidats a abordé les quatres parties. Certains ont fait avec succès le choix de renoncer à la fin (difficile) du **III** et de traiter le **IV** qui était plus abordable. Cependant si quelques très bons candidats ont traité le problème quasiment dans sa totalité, bien trop nombreux sont ceux qui ont été arrêtés dès les premières véritables difficultés.

Le jury a déploré que certaines erreurs élémentaires apparaissent de façon récurrente. Par exemple (ici lors de la question **I.5**) trop de candidats utilisent un argument local pour prouver un résultat qui ne l'est pas; car le comportement au voisinage de zéro de f ne permet pas à lui seul de justifier les variations de f sur son intervalle de définition. Il est décevant de constater que peu de candidats sont à l'aise avec la signification et l'usage des quantificateurs. Nous avons noté (par exemple au **I.A** et au **I.C**) beaucoup de confusion sur le nombre de variables, l'importance de ce nombre (une ou deux) n'apparaît pas clairement à certains. Et bien des erreurs sont venues de négligences sur le domaine de définition. Nous invitons les candidats à se demander d'abord "Où sont les variables? Combien sont elles?". Trop de candidats s'en remettent aux formules automatiques d'égalité d'ensembles (simples jeux d'écritures); mieux vaut essayer d'avoir un contrôle géométrique *a priori* (par exemple en faisant un petit dessin). Nous insistons également sur la nécessité de travailler la notion de fonction composée qui n'est pas parfaitement maîtrisée (erreur dans le sens de la composition, dérivation, changement de variables). Signalons que la grande majorité des candidats ne sait pas faire la différence entre une bijection indéfiniment dérivable et un difféomorphisme.

En ce qui concerne les notions et théorème fondamentaux, les connaissances des candidats sont souvent soit imprécises (on invoque le théorème de dérivation des intégrales dépendant d'un paramètre sans connaître les hypothèses) soit trop formelles (on connaît les hypothèses de ce même théorème mais on se révèle incapable en pratique de dominer la fonction figurant sous le signe intégrale). La notion de fonction holomorphe n'est pas toujours comprise, le théorème de Cauchy-Lipschitz non plus et l'unicité y est souvent une propriété mystérieuse voire magique, ce qui n'empêche pas de l'appliquer dès qu'apparaît une équation différentielle. Quant au théorème d'inversion locale, rares sont ceux qui l'utilisent à bon escient.

Le jury a été étonné de constater l'absence fréquente du graphe de l'ensemble $E_0(f)$ à la question **I.4**. Rappelons que l'usage de la calculatrice est autorisé pour cette épreuve et qu'il est préférable d'en avoir une. Ceux qui ont tenté de traiter cette question sans calculatrice ont eu peu de réussite, fournissant des dessins fantaisistes et ne vérifiant pas la symétrie par rapport à la première bissectrice pourtant établie peu de temps auparavant. Rappelons qu'outre la rigueur et la précision, on attend d'un futur enseignant cohérence et honnêteté. Que penser d'un candidat qui affirme que l'équation $cosz = 0$ n'a pas de solution complexe après avoir mis en évidence une infinité d'entre elles ou d'un autre qui affirme à la question **II.2** que $e_4 = 5$ bien que son étude ne mette en évidence que 4 permutations alternantes ?

Dans l'ensemble les copies sont bien présentées et assez claires mais la rédaction souffre souvent de ses deux maux habituels : étendue à l'infini dans les questions les plus simples, elle se condense et s'obscurcit dès que des justifications non-triviales sont requises. Quelques candidats multiplient les précautions inutiles, et détruisent leurs raisonnements exacts par des clauses absurdes ; parfois le choix est laissé au correcteur entre plusieurs réponses incompatibles. Enfin certaines rares copies sont rendues difficilement compréhensibles par une graphie convulsive ou une orthographe naufragée.

Bien entendu, quelques compositions plus que satisfaisantes échappent aux travers dénoncés. De nombreux candidats ont prouvé qu'ils avaient préparé avec soin et sérieux cette épreuve et nous invitons les futurs candidats à voir dans les remarques çi-dessus un encouragement et une aide pour préparer le concours de l'année prochaine.

Remarques sur les questions

I.A : en général bien traitée, même si beaucoup affirment sans démonstration que la courbe est une ellipse (**I-A-3**). La moitié des candidats ne sait pas reconnaître une ellipse par son équation cartésienne non réduite.

I.B :

- I.5.a. L'étude globale d'une fonction a donné lieu à des généralisations étranges de son étude locale.

- I.5.c. Pour beaucoup de candidats, l'existence d'un développement limité à l'ordre k équivaut à la classe C^k ; quant au théorème de dérivation sous le signe intégrale, il est souvent appliqué sans aucune vérification.

- I.5.d. Cette question très discriminante a été la plupart du temps traitée de façon incomplète. (Ici il fallait vérifier plusieurs conditions les unes après les autres.) La définition d'un difféomorphisme a été presque toujours ignorée.

I.C

- I.6. A nouveau la définition d'un difféomorphisme est ignorée. De nombreux candidats identifient (ne voient pas la différence entre ?) h et $(x, y) \mapsto (h(x), h(y))$.

- I.7.a. Les candidats confondent x ou y s'annule avec x et y s'annulent simultanément.

- I.7.b Question peu abordée, et souvent traitée de façon incomplète. En particulier rares sont ceux qui signalent que la racine carrée de g est surjective.

II.

-II.1 c. Question très discriminante correctement traitée par un nombre significatif des candidats. On rencontre souvent des erreurs dans les développements limités.

-II.1.d. Question peu abordée. Les candidats confondent souvent les propriétés $u_n \sim v_n$ et $u_n - v_n \to 0$ et évaluent la série en $z = 1$. Il fallait ici évaluer la série en $z \geqslant \frac{\pi}{2}$ pour pouvoir conclure.

-II.2.a. Assez bien traitée dans l'ensemble.

-II.2.b. Si l'idée est souvent comprise, rares sont ceux qui exhibent une bijection correcte entre les deux ensembles de permutations. On voit fréquemment des compositions dans le mauvais sens.

-II.2.c et d. Très peu traitées.

III.

-III.1.2. Bien traitées.

-III.3. Beaucoup de candidats abordent cette question, mais peu la traitent complètement.

-III.5. Trop d'erreurs dans ce dénombrement élémentaire.

La suite de la partie **III** a été peu abordée. Elle a été abordée par des candidats de bon niveau mais ceux ci ont souvent éprouvé de grandes difficultés à formaliser rigoureusement leurs intuitions.

IV.

-IV.1. Cette question a été traitée avec succès par les candidats qui l'ont abordée.

-IV.2. Des confusions entre inf et min. Certains candidats pensent qu'ils suffit d'affirmer que l'intégrale n'est jamais nulle pour conclure.

-IV.3. Bien

La suite de la partie **IV** a été peu abordée, mais parfois traitée brillamment par les excellents candidats.

Chapitre 5

Épreuves orales d'algèbre et d'analyse et Mathématiques pour l'informatique

5.1 Organisation des épreuves

Les modalités, mises en place au concours 2001, ont cette année encore donné entière satisfaction et sont reconduites pour la session 2009. Elles sont décrites ci-après de manière détaillée, prenant en compte l'expérience acquise.
Pour les candidats de l'option D, des changements de modalités sur les leçons de mathématiques interviennent en 2009. Ils tireront au hasard un couple de leçons prélevées dans la liste jointe dans ce rapport. Par conséquent ils pourront éventuellement se voir proposer un choix de deux leçons d'algèbre ou 2 leçons d'analyse ou une de chaque .

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. Noter clairement sur le plan écrit les propositions de développement.

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.

5.1.1 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. 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.

5.1.2 Deuxième partie : le développement

Le jury veille à la cohérence du plan et des propositions de développements eu égard au niveau du candidat. Il est souhaitable que le candidat recherche une adéquation entre son niveau intrinsèque et les développements proposés. Un candidat ne sera pas avantagé, s'il présente un développement non maîtrisé ou mal compris. Il faut toutefois veiller à rester au niveau de l'Agrégation ; les développements de niveau d'une classe de Terminale ne peuvent constituer une proposition de développement.

Le jury demande au candidat de présenter deux développements au moins. Ceux-ci doivent être clairement mentionnés sur le plan écrit et non pas vaguement évoqués à l'oral. Le candidat doit préciser ce qu'il va démontrer, et le cas échéant, les résultats de son plan qu'il va admettre. Il dispose de 15mn (maximum) pour mener à bien ce développement.

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.

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. Il est inutile de se précipiter et il est utile de préciser ses notations !

Le développement ressemble parfois à une succession plus ou moins convaincante de résultats intermédiaires ad hoc.

On ne saurait trop conseiller aux candidats d'illustrer leur développement (et éventuellement leur plan) par un ou plusieurs dessins : l'exposé y gagnerait en clarté pour le jury, le candidat pourrait ainsi montrer un souci louable de pédagogie.

Rappelons que le développement doit être en rapport avec le sujet traité, la leçon présentée et le plan écrit.

La récitation d'un développement est lourdement sanctionnée ; le jury veille à ce que les futurs enseignants comprennent ce qu'ils exposent et savent exposer ce qu'ils comprennent. C'est une qualité essentielle d'un futur agrégé.

Tout hors sujet est sévèrement sanctionné. Toute utilisation d'un lemme non démontré et enfermant l'essence de la preuve est sanctionné. Le jury peut exiger la démonstration d'un lemme, soit-disant admis, si celui-ci est essentiellement le cœur du développement.

Dans le cas d'un développement ambitieux, il ne faut pas négliger les cas élémentaires.

Enfin, même si le jury laisse évoluer le candidat durant son développement, en intervenant le moins souvent, il peut en cas de lacunes ou d'erreurs manifestes interrompre le candidat pour demander des explications. Cette intervention ne donne pas droit à extension du temps consacré au développement.

5.1.3 Troisième partie : questions et dialogue

Le jury vérifie systématiquement la maîtrise approfondie du plan présenté. C'est à dire qu'une part importante de la discussion portera sur le plan, ou trouvera sa source dans le plan présenté par le candidat.

Le jury pose aussi des exercices en rapport direct avec la leçon, mais ne s'attend pas à ce que le candidat trouve une solution immédiate. Le but est plutôt de voir évoluer le futur agrégé dans une démarche scientifique rigoureuse et méthodique. Le candidat doit réfléchir, utiliser son plan et rattacher l'exercice à sa leçon. Le fait de ne pas résoudre un exercice ne doit pas être compris comme un échec et le candidat ne doit pas se décourager. Il doit au contraire rester attentif aux suggestions du jury. La qualité du dialogue est aussi un élément d'appréciation.
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 doit se préparer à des questions élémentaires et à des calculs éventuels sur ce point. 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.

5.1.4 Rapport détaillé sur les épreuves orales

Le Jury suggère la lecture des rapports des trois dernières années. Les commentaires sur les leçons y restent d'actualité.

Voici quelques remarques supplémentaires concernant certaines leçons de la session 2008. Les candidats sont invités à étendre ces commentaires aux leçons non commentées.

Les candidats de l'option *D* consulteront la liste *ad hoc* des 40 titres (repérés par un numéro unique) reprenant ceux de l'oral des options A, B, C en algèbre et analyse.

Leçons d'Algèbre

101 - Groupe opérant sur un ensemble. Il faut savoir relier les stabilisateurs de deux éléments d'une même orbite.

103 - Notions de sous-groupe distingué et de groupe quotient. La notion de produit semi-direct n'est plus exigible (programme 2009). Seuls les candidats solides pourront s'y aventurer. La notion de quotient est importante en mathématiques et peut être utilement illustrée dans cette leçon, notamment au travers du sous-groupe dérivé. Des exemples et applications en géométrie élémentaire sont nécessaires.

105 - Groupe des permutations d'un ensemble fini. Les décompositions en cycles, la signature doivent être connues.

106 - Groupe linéaire d'un espace vectoriel de dimension finie E. Les applications topologiques sont acceptables dans la leçon d'algèbre.

108 - Exemples de parties génératrices d'un groupe. Il est important de réfléchir à l'utilisation des générateurs d'un groupe pour établir des propriétés de certains morphismes (automorphismes du groupe diédral par exemple). Le leçon ne se limite pas aux groupes finis (on peut penser à certains groupes libres) ou à la simplicité de $\mathfrak{A}_n, n \geqslant 5$.

109 - Anneaux $\mathbf{Z}/n\mathbf{Z}$. Cette leçon classique demande toutefois une préparation minutieuse. Bien maîtriser le lemme chinois et sa réciproque. Distinguer clairement propriétés de groupes additifs et d'anneaux. Connaître les automorphismes, les idempotents.

110 - Nombres premiers. La répartition des nombres premiers est un résultat historique important. Sa démonstration n'est bien-sûr pas exigible au niveau de l'Agrégation. Il faut savoir si 113 est un nombre premier ! Attention aux choix des développements, ils doivent être pertinents.

111 - Anneaux principaux. On pourra aussi penser à des applications en algèbre linéaire.

112 - Corps finis. Les constructions des corps de petit cardinal doivent avoir été pratiquées. Il convient de montrer comment l'utilisation des corps de rupture permet de prouver l'irréductibilité d'un polynôme.

113 - Groupe des nombres complexes de module 1. Racines de l'unité. Les polynômes cyclotomiques (programme 2009) trouveront naturellement leur place dans cette leçon. Leur irréductibilité doit être maîtrisée.

115 - Corps des fractions rationnelles. La décomposition en éléments simples sur **R** ou **C** doit être maîtrisée. Les techniques de développements limités sont efficaces et peuvent être exposées.

117 - Algèbre des polynômes à n indéterminées. Polynômes symétriques. Le théorème fondamental sur la structure de l'algèbre des polynômes symétriques est vrai sur **Z**. L'algorithme peut être présenté sur un exemple. Les applications aux quadriques, aux relations racines coefficients ne doivent pas être négligées. Il faut connaître la structure de l'anneau des polynômes symétriques.

120 - 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 ! Il faut présenter une définition cohérente et pratique de la dimension finie. 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, ou le théorème du rang, n'est pas suffisant au niveau de l'Agrégation.

121 - Matrices équivalentes. Matrices semblables. Ce n'est pas une leçon réduite à la réduction des endomorphismes. L'extension des opérations au cas des anneaux principaux est délicate, alors que le cas des anneaux euclidiens suffit largement au niveau de l'Agrégation. On peut s'interroger sur la réciproque de A, B semblables implique A^k, B^k équivalentes pour tout $k \geqslant 0$.

122 - Opérations élémentaires sur les lignes et les colonnes. On pourra utilement dissocier les opérations sur les lignes de celles sur les colonnes. Rappelons que $A = PB$ avec A, B des matrices de $Mat(n, p, \mathbf{K})$ est équivalent au fait que on peut passer de A vers B par manipulation des lignes et est équivalent au fait que A et B ont même noyau ; la notion de matrices échelonnées interviendra utilement dans cette leçon.

123 - Déterminant. Le jury ne peut se contenter d'un Vandermonde ou d'un déterminant circulant ! Le résultant et les applications simples à l'intersection ensembliste de deux courbes algébriques planes (programme 2009) peuvent trouver leur place dans cette leçon. 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.

126 - Endomorphismes diagonalisables. Il faut pouvoir donner des exemples naturels d'endomorphismes diagonalisables et des critères.

127 - Exponentielle de matrices. C'est une leçon difficile et ce n'est pas une leçon d'analyse. Toutefois les applications aux équations différentielles doivent être évoquées. On pourra par exemple faire le lien entre réduction et comportement asymptotique. Les notions d'algèbres de Lie ne sont pas au programme de l'Agrégation, on conseille d'aborder ces sujets qu'à condition d'avoir une certaine solidité.

128 - Endomorphismes nilpotents. Il est possible de mener une leçon de bon niveau, même sans la décomposition de Jordan (qui n'est plus exigible dans le programme 2009), à l'aide des noyaux itérés.

129 - Algèbre des polynômes d'un endomorphisme. Ce n'est pas une leçon sur la réduction. Les polynômes d'un endomorphisme ne sont pas tous nuls ! Les candidats doivent connaître sans hésiter la dimension de l'algèbre $\mathbf{K}[f]$. Les propriétés globales pourront être étudiées (dimension, commutant). Il faut s'interroger sur les idempotents et le lien avec la décomposition en somme de sous-espaces caractéristiques.

130 - Matrices symétriques réelles, matrices hermitiennes. C'est une leçon transversale.

131 - Formes quadratiques. Orthogonalité, isotropie. Il faut savoir reconnaître une forme quadratique lorsqu'on dispose d'un polynôme homogène du second degré en plusieurs variables. La preuve de la loi d'inertie de Silvester doit être connue. Le cône isotrope est un aspect important de cette leçon. L'algorithme de Gauss doit être énoncé et pouvoir être pratiqué sur une forme quadratique de $\mathbf{R}^3$. Le lien avec la signature doit être clairement énoncé. Il est important d'illustrer cette leçon d'exemples naturels.

132 - Formes linéaires et hyperplans. Il est important de replacer la thématique de la dualité dans cette leçon. L'exposé doit être bien organisé et raisonnablement complet. Les liens entre base duale et fonctions de coordonnées doivent être parfaitement connus. 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 sous différents aspects : géométrie, algèbre, topologie etc... Il faut que les développements proposés soient en lien direct, comme toujours, avec la leçon : proposer la trigonalisation simultanée est un peu osé !

133 - Endomorphismes remarquables d'un espace vectoriel euclidien. Il faut savoir caractériser correctement les symétries orthogonales et les projections orthogonales en utilisant l'adjoint. Si on présente en développement la réduction des endomorphismes normaux, il convient d'avoir réfléchi à l'unicité de la forme réduite proposée et d'en déduire la réduction des endomorphismes autoadjoints et orthogonaux.

135 - Isométries. Forme réduite. Applications en dimensions 2 et 3. La classification des isométries en dimension 2 ou 3 est exigible. Théorème de décomposition commutative. En dimension 3 : déplacements (translation, rotations, vissage) ; antidéplacements (symétries planes, symétries glissées, et isométrie négative à point fixe unique).

136 - Coniques. Les propriétés classiques des coniques doivent être présentées. Bien distinguer les notions affines, métriques ou 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. Les applications à la trajectoire des planètes doivent être connues.

139 - Applications des nombres complexes à la géométrie. Cette leçon ne serait rester au niveau de la Terminale. C'est le moment de mettre à plat la notion d'angle !

140 - Systèmes d'équations linéaires. Systèmes échelonnés. Résolution. Les matrices échelonnées (programme 2009) trouveront des applications dans la résolution des systèmes linéaires. Le théorème de Rouché n'est pas d'un grand intérêt dans sa version traditionnellement exposée. Il est important de le replacer dans le contexte des opérations. Les candidats sont invités à réfléchir non seulement à la résolution pratique de systèmes linéaires (à coefficient sur $\mathbf{Q}, \mathbf{R}, \mathbf{F}_p$), mais aussi à l'écriture d'un système d'équations linéaires (par exemple les équations d'un sous-espace).

141 - 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.

145 - Méthodes combinatoires, problèmes de dénombrement. Il faut dans un premier temps dégager clairement les méthodes et les illustrer d'exemples significatifs. L'utilisation de séries génératrices (programme 2009) est un outil puissant pour le calcul de certains cardinaux et simplifie bien souvent les problèmes de convergence. On peut aussi dénombrer les classes de similitude d'endomorphisme nilpotents dans $Mat(n, \mathbf{C})$ ou le nombre de sous-espace stables d'un endomorphisme cyclique ou les sous-groupes d'un groupe abélien, voire le cardinal de l'ensemble des matrices nilpotentes de rang $n-1$ dans $Mat(n, \mathbf{F}_p)$. La partie élémentaire de cette leçon ne doit pas être oubliée. Le jury s'attend à ce que les candidats sachent calculer des cardinaux classiques et certaines probabilités !

149 - Groupes finis de petit cardinal. Après avoir cité rapidement 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 la leçon "Groupes finis". Une bonne référence reste les exercices du chapitre 1 du livre de Perrin.

Oral d'analyse

Les leçons 210, 222, 227, 231, 248 ne seront plus proposées à la session 2009.

Leçons de probabilité : Le Jury considère que ce chapitre à vocation à se développer dans l'enseignement secondaire et post-baccalauréat. Les candidats à un futur poste d'enseignant en mathématiques doivent maîtriser les notions centrales de ces thématiques. Il y a 5 leçons de probabilité.

203 - Utilisation de la notion de compacité. Confusion entre la notion de compacité et l'utilisation de la compacité. Il est important de ne pas concentrer la leçon sur la compacité générale, sans proposer des exemples d'utilisation significatifs. On ne peut pas proposer en développement des théorèmes de caractérisation de la compacité, a contrario le théorème de Stone-Weierstrass, par exemple, trouve largement sa place dans cette leçon.

204 - Connexité. De très bons candidats proposent de démontrer la simplicité du groupe $SO_3(\mathbf{R})$ comme application de la connexité. Ils semblent désemparés lorsque le jury demande d'établir que ni $SO_2(\mathbf{R})$, ni $SO_4(\mathbf{R})$ ne sont simples.

207 - Prolongement de fonctions. Le théorème de Hahn-Banach (en dimension infinie) n'est pas une nécessité absolue pour faire une leçon de niveau acceptable surtout quand on manque de recul sur la thématique.

213 - Espaces de Hilbert. Bases hilbertiennes. Il est important d'avoir réfléchi en termes de base algébrique et de base hilbertienne et de présenter des applications substantielles.

215 - Applications différentiables. Les exemples annoncés par le candidat doivent non seulement illustrer les notions présentées, mais aussi pouvoir être expliqués par le candidat. Par exemple certains donnent une formule pour la différentielle de l'inversion d'une matrice sans pouvoir la retrouver.

217 - Sous variétés de $\mathbf{R}^n$. Exemples. Cette leçon est nouvelle et ne serait être réduite à un cours de géométrie différentielle abstrait. Le jury attend une leçon concrète, montrant une compréhension géométrique locale. Aucune notion globale n'est exigible, ni de notion de variété abstraite. Le candidat doit pouvoir être capable de donner plusieurs représentations locales (paramétriques, équations ...) et illustrer la notion d'espace tangent sur des exemples classiques. Le jury invite les candidats à réfléchir à la pertinence de l'introduction de la notion de sous-variétés. En ce qui concerne les surfaces de $\mathbf{R}^3$, les candidats sont invités à réfléchir aux notions de formes quadratiques fondamentales et à leurs interprétations géométriques.

218 - Applications des formules de Taylor. Il est absurde de vouloir donner une formule de Taylor dans un cadre général, sans être capable d'expliciter la dite formule pour des fonctions numériques d'une variable réelle ou d'utiliser les formules de Taylor pour calculer la tangente à une courbe. On fera attention au fait que les développements doivent faire intervenir les formules de Taylor de manière significative.

220 - Équations différentielles $X' = f(t, X)$. Le jury attire l'attention sur le fait que dans l'équation différentielle $X' = f(t, X)$, X peut désigner une fonction vectorielle. Le lemme de Grönwall semble trouver toute sa place dans cette leçon. L'utilisation du théorème de Cauchy-Lipschitz doit pouvoir être mis en oeuvre sur des exemples concrets.

223 - Convergence des suites numériques. Il est important de préciser les vitesses de convergence des exemples proposés. Le Jury attend d'autres exemples que la traditionnelle suite récurrente $u_{n+1} = \sin(u_n)$.

229 - Fonctions monotones. Fonctions convexes. Les candidats sont invités à réfléchir à l'incidence de ces notions en théorie des probabilités. La dérivabilité presque partout des fonctions monotones est un résultat substantiel et difficile.

232 - Méthodes d'approximation des solutions d'une équation $F(X) = 0$. Le Jury attire l'attention sur le fait que X peut désigner un vecteur.

236 - Illustrer par des exemples quelques méthodes de calcul d'intégrales. Il faut savoir énoncer correctement le théorème de changement de variables en dimension n et l'appliquer. La méthode des résidus ne doit pas être oubliée. Il est important de montrer, sur des exemples, l'interaction entre le calcul d'intégrales multiples et d'intégrales simples.

238 - Méthodes de calcul approché d'intégrales. Il faut connaître les majorations d'erreurs de chaque méthode proposée.

245 - Fonctions holomorphes et méromorphes sur un ouvert de C. Les conditions de Cauchy-Riemann doivent être parfaitement connues.

246 - Séries de Fourier. Exemples et applications Les différents types de convergence (L^2, Fejer, Dirichlet etc...) doivent être connus. Il faut avoir les idées claires sur la notion de fonctions de classe $\mathscr{C}^1$ par morceaux (elles ne sont pas forcément continues). Cette leçon ne doit pas se réduire à un cours abstrait sur les coefficients de Fourier.

Chapitre 6

Épreuve orale de modélisation

6.1 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. Le jury apprécie en effet que le candidat reste honnête quant à sa compréhension du texte, plutôt que de se lancer dans une présentation des parties du texte qu'il ne comprend absolument pas. 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 texte sont très appréciées. Lorsqu'une démonstration est ébauchée dans le texte, le candidat peut choisir de la compléter. Il est alors particulièrement apprécié que le candidat précise les point mathématiques nécessaires pour une démonstration rigoureuse. Le candidat peut, tout comme le texte, utiliser des arguments heuristiques s'il les signale comme tels. Cependant le candidat ne doit pas oublier qu'il s'agit d'une épreuve de l'agrégation externe de mathématiques, et qu'un exposé ne comportant aucun argument mathématique précis est vivement déconseillé.

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.

Sur le plan

Il est conseillé aux candidats de présenter un plan *succinct* de leur exposé, précisant les moments où il compte présenter ses simulations informatiques. Ceci permet au jury de guider le candidat dans sa gestion du temps.

Sur la présentation

Nous rappelons ici que l'agrégation est un concours visant à recruter des *enseignants*. Ainsi seront appréciés une bonne gestion du tableau, un exposé clair et pédagogique, et une bonne capacité à effectuer des calculs analytiques clairs, corrects et lisibles.

6.2 Option A : probabilités et statistiques

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 programme

Lors de la discussion avec le candidat, le jury peut interroger celui-ci sur *la totalité du programme*. En particulier, il est fréquent que le jury pose 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. Encore trop de candidats ont du mal à formaliser précisément des notions qui font partie du programme de l'option.

Probabilités

- La loi des grands nombres et le théorème limite central sont des points fondamentaux en probabilités comme en statistiques. Il convient d'en connaître les hypothèses précises, et de ne pas confondre les différents types de convergence.
- Les propriétés fondamentales des chaînes de Markov sont souvent mal connues : classification des états, conditions de convergence vers la loi stationnaire (apériodicité), etc. Les candidats gagneraient à utiliser plus souvent une représentation graphique des chaînes de Markov manipulées.
- Il est souvent très utile d'interpréter la notion d'espérance conditionnelle en terme de projecteur orthogonal.
- 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. Les candidats doivent connaître les problématiques d'estimation (notion de biais et de consistance) et de test d'hypothèses.
- Le jury a observé cette année une amélioration sur la connaissance des principes de construction d'un intervalle de confiance.
- Les candidats sont souvent rebutés par le modèle linéaire gaussien. Celui-ci est pourtant couramment utilisé dans différents modèles.
- Dans le cadre des tests d'adéquation, les candidats ont du mal à motiver le choix du test qu'ils proposent (chi-2, Kolmogorov-Smirnoff, ...).

6.3 Option B : Calcul scientifique

Au cours de la session 2008, le jury a relevé un certain nombre de faiblesses sur des éléments clefs du programme :

– Analyse des équations différentielles ordinaires et calcul différentiel : un trop grand nombre de candidats se révèle totalement incapable de résoudre des équations différentielles simples, du 2ème ordre à coefficients constants (homogènes et inhomogènes) par exemple ou des équations du 1er ordre à variables séparées. Si les candidats connaissent un peu mieux les arguments donnant l'existence-unicité de solutions, en revanche les questions liées au comportement qualitatif, l'analyse de stabilité linéaire, l'utilisation de portrait de phases et les critères garantissant l'existence globale semblent ignorés. Le lemme de Gronwall paraît faire l'objet d'une impasse condamnable et peu de candidats en font un outil permettant

d'obtenir une estimation utile des solutions. La dérivation d'intégrales à paramètres suscite des réponses troublantes.
- Schémas numériques pour les équations différentielles ordinaires : les notions de stabilité, consistance et convergence de schémas numériques restent manifestement assez mal maîtrisées, y compris pour les schémas d'Euler explicite et implicite. Le jury se montre particulièrement sensible aux confusions, malheureusement trop fréquentes, entre l'approximation X_n et l'évaluation $X(t_n)$ de la solution au temps t_n.
- Optimisation : des lacunes ou des confusions importantes ont été observées quant aux théorèmes d'existence et aux méthodes de recherche d'extrema. En particulier les problèmes de minimisation sous contrainte sont trop souvent méconnus. La dérivation de fonctions de plusieurs variables constitue pour certains un obstacle insurmontable.
- Equations aux dérivées partielles : des notions de base sur les équations classiques en dimension 1 — ondes, chaleur, transport, équations elliptiques— doivent être connues. 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. Toutefois, aucune connaissance des notions de solutions faibles, ni des espaces fonctionnels liés à la théorie des distributions n'est attendue des candidats.
- Algèbre linéaire numérique : les candidats doivent connaître des méthodes de résolution de systèmes linéaires et de recherche d'éléments propres et être capables d'évaluer leur complexité.
- Enfin, il est toujours pénible de constater les nombreuses erreurs relatives à l'utilisation de l'alphabet grec qui rend parfois le dialogue avec le jury difficile.

6.4 Option C : Algèbre et Calcul formel

Il convient d'abord de se féliciter du fait que, dans l'ensemble, le traitement de l'épreuve par les candidats progresse, au moins dans la forme. En contrepartie, à plusieurs reprises, on a pu voir des candidats reprendre des développements de leçons d'algèbre ou d'analyse, impliquant des digressions n'ayant souvent qu'un rapport assez lointain avec le texte. Si une telle digression peut être admise dans le cas où elle se raccorde clairement au texte et est synthétique et de courte durée, elle n'en reste pas moins relativement éloignée de l'esprit de l'épreuve.

En contrepartie, les candidats se saisissent toujours aussi peu des "perches" tendues dans les textes : énoncés sans démonstrations, affirmations volontairement non justifiées sont répétées souvent sans même un regard critique. Les résultats obtenus dans les textes ne sont que rarement commentés par les candidats, là où le jury apprécierait une prise de recul, ou un retour au problème initial.

Remarques spécifiques à l'option C.

Suite aux remarques des rapports précédents, on peut noter un retour à la normale sur les connaissances en algèbre linéaire. La notion de résultant est généralement connue, le lien avec la résolution explicite de systèmes d'équations polynomiales est vu avec plus ou moins d'aide du jury. Il reste néanmoins une marge de progression, en particulier sur les aspects plus fins (corps non algébriquement clos, termes de tête de polynômes qui s'annulent).

Le jury déplore année après année que les suites récurrentes linéaires à coefficients constants soient connues d'un nombre de plus en plus restreint des candidats.

Enfin, l'évaluation du nombre d'opérations effectuées dans un calcul ne fait pas encore partie ni de la culture, ni des réflexes des candidats. On peut regretter que la complexité de deux des algorithmes les plus classiques, le pivot de Gauss et l'algorithme d'Euclide, soit toujours autant ignorée par les candidats ; il en est de même de la complexité (naïve) des opérations arithmétiques élémentaires ; on a même pu entendre à plusieurs reprises que la division de A par B se faisait de façon purement soustractive, en temps $O(A/B)$.

Beaucoup de candidats voient la partie "illustration informatique" de l'épreuve comme une partie "programmation". Si programmer une des méthodes suggérées dans le texte est effectivement pertinent, il est généralement possible de fournir des illustrations intéressantes sans se lancer dans de la programmation délicate ; on peut penser à simplement traiter un exemple, mais aussi conduire des calculs fastidieux à l'aide d'un logiciel de calcul formel, tracer une courbe pour discuter le comportement d'une fonction, visualiser la vitesse de convergence ou le comportement asymptotique d'une suite, comparer expérimentalement différentes méthodes...

6.5 Utilisation de l'outil informatique

Le jury observe avec plaisir une utilisation plus pertinente de l'outil informatique, due certainement à une meilleure préparation des candidats.

Il est attendu du candidat un commentaire sur les résultats de sa simulation (résultats numériques ou graphiques), mais aussi du code mis en œuvre. Le jury regrette toutefois l'utilisation parfois abusive de « boites noires » de simulation au sein de leur programme, qui peuvent être source d'incompréhension sur les sorties.

Rappelons que le candidat ne doit pas avoir peur de présenter un programme non abouti. Le jury est sensible à la démarche employée.

D'un point de vue purement pratique, il est dommage de voir des candidats gênés durant l'épreuve de modélisation tout simplement parce qu'ils ne savent pas sauvegarder leur travail sur fichier, certains -rares heureusement- fermant directement l'application en ignorant les messages d'avertissement du logiciel utilisé et perdant ainsi tout ce qu'ils ont fait. Rappelons à ce sujet que le site du jury de l'agrégation décrit dans ses pages les logiciels utilisés et propose des outils pour qu'un candidat puisse se familiariser avec l'environnement proposé (voir http ://agreg.org/Agreg/installation.html).

Chapitre 7

Épreuves orales de l'option informatique

7.1 Remarques sur l'épreuve de leçon de mathématiques

Dans tous les cas, le jury a aussi interrogé le candidat sur la partie du programme non couverte par le sujet : question d'analyse pour les candidats ayant traité un sujet d'algèbre et vice-versa.

Les remarques concernant cette épreuve ne sont pas différentes des remarques concernant les épreuves de leçon des autres options, et le lecteur est invité à se reporter à la section du rapport consacrée à ce point.

Cette épreuve va évoluer à partir de l'année prochaine : le candidat tirera un couple de sujets au sein d'une liste d'une quarantaine de sujets d'algèbre et d'analyse extraite de la liste générale des autres options. **Mais il n'y aura donc plus nécessairement un sujet d'algèbre et un sujet d'analyse !** Il pourra y avoir deux sujets d'algèbre ou deux sujets d'analyse, par exemple : *Loi binomiale* et *Fonctions monotones*. Le nouveau programme précise en effet :

> *Les candidats se verront proposer deux sujets, dans un corpus d'algèbre, de géométrie, d'analyse et de probabilités.*

Il est donc impératif que les candidats ajustent leur préparation à cette nouvelle organisation. La liste des leçons sera disponible dès la rentrée sur le site Web de l'Agrégation.

7.2 Remarques détaillées sur l'épreuve de leçon d'informatique

L'épreuve de leçon d'informatique a été organisée exactement sur le modèle de celles de mathématiques. Un ensemble de 27 titres de leçons a été proposé aux candidats.

Le candidat tire un couplage de deux titres 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.

Cette épreuve va évoluer à partir de l'année prochaine : on trouvera la nouvelle liste de leçons dans le rapport 2008 qui sera disponible dès la rentrée sur le site Web de l'Agrégation. Essentiellement, les leçons de *programmation* (langages typés, sémantique, typage, compilation) ont été retirées de la liste ainsi que certaines leçons élémentaires d'*algorithmique*. Par contre, la liste de leçons a été raffinée en ce qui concerne la *logique*, en particulier les preuves de programme. Nous espérons que ces modifications contribueront à faciliter la tâche des préparateurs.

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 est particulièrement net dans la bonne focalisation des présentations. Beaucoup de candidats cernent bien le sujet de leurs leçons et proposent des développements intéressants mais le niveau est assez hétérogène, ce qui conduit à une grande dispersion des notes.

7.2.1 Organisation de la leçon

De même, l'organisation de la leçon est le plus souvent pertinente. On remarque cependant quelques candidats qui se présentent devant le jury avec des plans d'une seule page, peut-être par ignorance des modalités de l'épreuve.

Il est recommandé aux candidats de bien situer le domaine de la leçon avant de se lancer dans les raffinements techniques. C'est particulièrement important à cause de la largeur thématique du programme.

Une tentation bien compréhensible pour les candidats est de *mathématiser* les sujets de leçons en oubliant l'aspect informatique. Ainsi, sur le sujet *Langages algébriques*, il était tentant de faire une leçon contrée sur un aspect théorique unique comme le Lemme d'itération d'Ogden, en oubliant complètement les aspects plus concrets de ce domaine et ses multiples applications, par exemple à l'analyse syntaxique et aux compilateurs.

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.

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*. Ce point avait déjà été souligné dans le rapport de l'an passé et les titres des leçons ont été affinés en conséquence. Les titres des leçons concernant des modèles formels de l'informatique sont maintenant libellés en mentionnant explicitement *exemples et applications*.

Les candidats de niveau moyen ont souvent montré des connaissances assez solides pour les résultats théoriques, mais par contre un manque de réflexion manifeste en ce qui concerne leurs applications et exemples concrets de mise en oeuvre.

Les deux questions-clés de cette épreuve sont toujours les mêmes.
- À quoi cet outil mathématique sert-il dans le cadre informatique considéré ? Pouvez-vous décrire quelques exemples pertinents de son application concrète ?
- La complexité ou le coût de son utilisation sont-ils bien compensés par la qualité supplémentaire d'information qu'il permet d'obtenir ?

Ces questions sont très souvent posées par le jury, sous une forme ou une autre. Le jury invite les candidats à se préparer tout particulièrement 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.

7.2.2 Développement d'un point du plan

Lors de la présentation de son plan, le candidat propose au moins deux développements au jury. Parmi ceux-ci, le jury en choisit un.

Il n'est donc pas nécessaire de préparer des développements de très haut niveau. Au contraire, les candidats doivent s'entraîner à exposer des points simples du programme de manière pédagogique et stimulante. C'est particulièrement le cas s'il existe des livres usuels consacrés au thème de la leçon : les plans sont alors excellents... mais les développements souvent bien décevants !

Un point important dans la présentation du développement est de bien situer le problème considéré, de définir les notations utilisées et de préciser l'objectif visé, comme on le ferait pour un cours à des élèves. Attention à ne pas présenter la solution avant d'avoir bien expliqué le problème !

7.2.3 Interaction avec le jury

Environ la moitié de l'épreuve est consacrée à l'interaction avec le jury. En informatique, cette interaction ne prend pas la forme d'exercice d'application. Il s'agit plutôt d'explorer de manière plus approfondie les notions qui ont été présentées, les domaines connexes, et surtout les exemples d'application de ces notions.

L'interaction est conduite sous la forme d'un *dialogue* avec le candidat. Le jury respecte le niveau choisi par le candidat : les questions s'ajustent à ce niveau.

Ce long temps d'interaction doit être considéré comme une *chance* pour le candidat de montrer ses connaissances ! À lui de guider le jury dans la direction adéquate. Il est indispensable que les candidats s'entraînent à ce type d'exercice avec leurs préparateurs.

7.3 Remarques générales sur l'épreuve de modélisation analyse de systèmes informatiques

Le jury a apprécié le travail accompli pour la préparation de cette épreuve.

7.3.1 Présentation du texte

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 décrite par le texte. Il n'est pas attendu que le candidat présente l'ensemble du texte, mais par contre il est attendu qu'il reste fidèle à l'esprit du texte et des développements proposés.

Le candidat dispose de 40 minutes pour décrire le problème, développer sa modélisation et présenter l'exercice d'informatique. Le jury n'est pas sensé connaître le texte à l'avance (même s'il en a une copie devant lui). C'est au candidat d'introduire le sujet du texte et de motiver la présentation qui va suivre. Cette motivation sera le plus souvent l'évocation de situations concrètes dans lesquelles on a besoin d'outils informatiques spécifiques. Ces situations peuvent être proposées par le texte lui-même, mais elle peuvent aussi être tirées de l'expérience personnelle du candidat. Toute contribution personnelle à ce niveau sera très appréciée !

Beaucoup de candidats omettent cette phase indispensable d'introduction et de motivation. Une manière simple de commencer est de présenter le plan de l'exposé. Ainsi, le jury pourra mieux se repérer par la suite, et éventuellement aider le candidat à mieux organiser son temps.

7.3.2 Exercice de programmation.

Au cours de l'exposé, le candidat présente son exercice de programmation. Pour cette partie de l'épreuve nous donnons quelques recommandations à la fin de ce rapport.

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. Si l'exercice n'a pas été présenté au bout d'une trentaine de minutes, le jury lui rappellera de le faire.

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.

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. Dans tous les cas, que le programme *tourne* ou pas, le jury évalue la qualité générale du code réalisé. Cette évaluation interactive permet à un candidat réactif de repérer une erreur, voire de la corriger, de recompiler et de relancer l'exécution.

7.3.3 Pédagogie

Le déroulement de l'épreuve de modélisation est très variable du fait des textes eux-mêmes. Les points d'attention du jury sont la présentation du plan, l'organisation du tableau, la lisibilité des écritures, la cohérence des notations, l'introduction et la motivation des définitions.

Dans cette épreuve, le candidat 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.

7.3.4 Interaction avec le jury

Les règles générales sont les mêmes que pour l'épreuve de leçon d'informatique ci-dessus. Essentiellement, c'est le candidat qui détermine le niveau et la forme de l'interrogation, et il est important qu'il se saisisse de ce rôle.

Il est attendu du candidat qu'il prenne le temps de réfléchir aux questions ou aux suggestions qui lui sont proposées. Il est normal qu'un candidat réponde au jury qu'il ne voit pas comment répondre à une question et le jury fera bien sûr tout son possible pour lui permettre de reprendre pied dans le dialogue. Si en plus le candidat est capable de préciser *pourquoi* il ne voit pas ce qui est attendu de lui, cela simplifiera la tâche du jury.

Il est bien sûr attendu du candidat qu'il connaisse les notions utilisées dans le texte, mais aussi qu'il sache les utiliser ! En particulier, le jury ne fait pas de cloisonnement strict entre informatique et mathématiques. La réponse à des questions concernant les programmes, par exemple l'estimation du temps de calcul, peut nécessiter l'utilisation d'outils mathématiques du programme, par exemple des résultats simples de combinatoire ou d'analyse. Le jury demandera alors souvent de justifier tel ou tel choix de conception.

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 !

7.4 Exercice de programmation informatique

Voici quelques recommandations plus précises concernant l'exercice de programmation. Elles sont motivées par les présentations des candidats de cette année. Nous espérons qu'elles seront utiles pour les candidats des années à venir.

D'une manière générale, le candidat doit proposer un code lisible et mettre en valeur ses connaissances en programmation. À titre de repère, la partie centrale du code devrait tenir sur un écran.

Les candidats sont invités à présenter le schéma algorithmique et les structures de données utilisés avant de lancer leur programme. Par contre, il est inutile de descendre dans les détails les plus triviaux du code, que le jury peut lire lui-même sur les écrans de contrôle. Le jury pourra demander au candidat d'évaluer la complexité de son implémentation ou de discuter de choix alternatifs de conception.

Le candidat choisit son langage. Cette année, nous avons vu peu de programmes en Java. Les candidats se partagent équitablement entre Caml et C (en fait, ils utilisent dans le langage C les extensions C++ admises par le compilateur `gcc`). Ce choix peut orienter les questions, car l'implémentation d'un problème peut être 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 de cette fonction et la complexité des opérations concernées.

L'exercice est soigneusement spécifié dans les textes proposés. Il doit être conduit dans l'un des langages proposés (C, Caml ou Java) : un candidat qui n'utilise pas les langages proposés reçoit la note 0 à l'exercice de programmation.

De même, le candidat doit respecter la spécification qui est donnée dans l'énoncé. Il peut, s'il le souhaite, présenter ensuite un deuxième programme implémentant une autre spécification. Il devra alors expliquer pourquoi il le fait. Le fait que l'exercice proposé dans l'énoncé soit trivial ou inintéressant n'est évidemment pas une explication suffisante ! 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 que ses capacités en programmation.

Dans le cas d'une programmation en C, il sera systématiquement demandé au candidat de recompiler son programme avec le niveau maximal d'avertissement :

```
gcc -Wall prog.c -o prog
```

Un programme qui produit des avertissements sera pénalisé et le candidat devra le corriger pendant l'interrogation. La même chose sera vérifiée en Caml ou Java.

Certains candidats ont passé beaucoup de temps à programmer des entrées *interactives* au clavier. Ce n'est pas nécessaire et souvent inutilement complexe, notamment en C (appel par référence dans la fonction `scanf`, etc.). Il est recommandé de coder le jeu de données dans une procédure d'initialisation qui pourra être facilement modifiée à la demande du jury.

Il est demandé aux candidats d'exécuter leurs programmes sur différents jeux de données, et il est souhaitable qu'ils aient anticipé ce point. La manière dont ces jeux de données sont choisis devra être justifiée par la démonstration de divers aspects du comportement du programme. Les candidats sont souvent interrogés sur leurs critères de choix.

Il est très souvent demandé aux candidats d'exécuter leurs programmes sur les cas limites de leurs spécifications, sauf si ces cas ont été explicitement exclus dans la présentation préalable : liste vide pour les algorithmes de tri, nombres négatifs pour des algorithmes de factorisation, etc.

La lisibilité et l'élégance de l'expression sont particulièrement appréciées par le jury. Il est essentiellement attendu que le style de programmation des programmes soit *cohérent* : utilisation de structures d'itération (bornées `for` ou non-bornées `while`), initialisation des variables, découpage plus ou moins fin en fonctions auxiliaires, etc. Les critères d'arrêt des boucles doivent être parfaitement maîtrisés. Toutes les quantités présentes dans les programmes doivent être définies par des constantes symboliques.

Chapitre 8

Annexe 1 : Leçons d’oral (options A, B et C)

Leçons d'algèbre et géométrie

❁ ❁ ❁

Les leçons 126, 130 et 140 n'ont pas été posées en 2008 mais pourront l'être en 2009.

101 Groupe opérant sur un ensemble. Exemples et applications.

---

103 Exemples et applications des notions de sous-groupe 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 $\mathrm{O}(2,\mathbf{R})$ et de $\mathrm{SO}(3,\mathbf{R})$. Applications.

---

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

---

109 Anneaux $\mathbf{Z}/n\mathbf{Z}$. Applications.

---

110 Nombres premiers. Applications.

---

111 Anneaux principaux. Applications.

---

112 Corps finis. Applications.

---

113 Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications.

---

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.

---

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. Exemples et applications.

---

123 Déterminant. Exemples et applications.

---

124 Polynômes d'endomorphisme en dimension finie. 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 Algèbre des polynômes d'un endomorphisme en dimension finie. Applications.

---

130 Matrices symétriques réelles, matrices hermitiennes.

---

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. Forme réduite. 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 projective complexe. Applications.

---

139 Applications des nombres complexes à la géométrie.

---

140 Systèmes d'équations linéaires. Systèmes échelonnés. Résolution. Exemples et applications.

---

141 Utilisation des groupes en géométrie.

---

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

---

145 Méthodes combinatoires, problèmes de dénombrement.

---

148 Formes quadratiques réelles. Exemples et applications.

---

149 Groupes finis de petit cardinal.

Leçons d'analyse et probabilités

Les leçons 210, 222, 227, 231 et 248 ne seront pas posées en 2009.

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.

---

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

---

213 Espaces de HILBERT. 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 $\mathbf{R}^n$. Exemples et applications.

---

216 Étude métrique des courbes. Exemples.

---

217 Sous variétés de $\mathbf{R}^n$. Exemples.

---

225 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 de 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 développements asymptotiques.

---

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.

---

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

---

235 Suites et séries de fonctions intégrables. Exemples et applications.

---

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

---

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 Utilisation en probabilités de la transformation de FOURIER ou de LAPLACE et du produit de convolution.

---

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

---

245 Fonctions holomorphes et méromorphes sur un ouvert de **C**. Exemples et applications.

---

246 Séries de FOURIER. Exemples et applications.

---

247 Exemples de problèmes d'interversion de limites.

---

248 Approximation des fonctions numériques par des fonctions polynomiales. Exemples.

---

249 Suites de variables de BERNOULLI indépendantes.

---

250 Loi des grands nombres. Théorème de la limite centrale. Applications.

---

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

---

252 Loi binomiale. Loi de POISSON. Applications.

Chapitre 9

Annexe 2 : Leçons de mathématiques pour l'informatique et leçons d'informatique

Leçons de mathématiques pour l'informatique

❁ ❁ ❁

Les leçons 122, 210, 222 et 231 ne seront pas posées en 2009.

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.

---

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

---

109 Anneaux $\mathbf{Z}/n\mathbf{Z}$. Applications.

---

110 Nombres premiers. Applications.

---

112 Corps finis. Applications.

---

116 Polynômes irréductibles à une indéterminée. Corps de rupture. 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 Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme. Applications.

---

128 Endomorphismes nilpotents.

---

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).

---

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

---

139 Applications des nombres complexes à la géométrie.

---

140 Systèmes d'équations linéaires. Systèmes échelonnés. Résolution. Exemples et applications.

---

141 Utilisation des groupes en géométrie.

---

145 Méthodes combinatoires, problèmes de dénombrement.

---

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 $\mathbf{R}^n$. Exemples et applications.

---

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.

---

224 Comportement asymptotique de 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.

---

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.

---

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.

---

246 Séries de FOURIER. Exemples et applications.

---

252 Loi binomiale. Loi de POISSON. Applications.

Leçons d'informatique

❁ ❁ ❁

Cette liste prend en compte les nouveaux programmes 2009.

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 Problèmes NP-complets : exemples

---

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. Exemples et applications.

---

912 Fonctions récursives primitives et non primitives. Exemples.

---

913 Machines de Turing. Applications.

---

914 Décidabilité et indécidabilité. Exemples.

---

915 Classes de complexité : exemples.

---

916 Formules du calcul propositionnel : représentation, formes normales, satisfiabilité.

---

917 Logique du premier ordre : syntaxe et sémantique.

---

918 Systèmes formels de preuve en logique du premier ordre : exemples.

---

919 Unification : algorithmes et applications.

---

920 Réécriture et formes normales.

---

921 Algorithmes de recherche et structures de données associées.

---

922 Ensembles récursifs, récursivement énumérables. Exemples.

---

923 Analyses lexicale et syntaxique : applications.

---

924 Théories en logique du premier ordre. Exemples.

---

925 Graphes : représentations et algorithmes.

---

926 Analyse des algorithmes : complexité. Exemples.

---

927 Exemples de preuves d'algorithmes : correction, terminaison.

Chapitre 10

Annexe 3 : Le programme 2009

Le programme des épreuves de l'agrégation n'est pas rédigé comme un plan de cours. Il décrit un ensemble de connaissances que le candidat doit maîtriser. Il comporte des répétitions lorsque des notions interviennent naturellement à plusieurs endroits.

D'une façon générale, les candidats doivent connaître des applications qui illustrent les notions générales. Le programme en propose ainsi un certain nombre. Il ne s'agit que de simples suggestions d'applications possibles, qui peuvent être complétées ou remplacées par d'autres.

10.1 Programme du tronc commun

Dans les paragraphes I à V qui suivent, tous les corps sont supposés commutatifs.

10.1.1 Algèbre linéaire

Espaces vectoriels

Espaces vectoriels, applications linéaires. Produit d'espaces vectoriels. Sous-espaces, image et noyau d'une application linéaire. Espaces quotients. Somme de sous-espaces, somme directe, supplémentaires. Familles libres, génératrices ; bases. Algèbre des endomorphismes d'un espace vectoriel E, groupe linéaire $GL(E)$.

Sous-espaces stables d'un endomorphisme. Valeurs propres, vecteurs propres, sous-espaces propres.

Espaces vectoriels de dimension finie

1. Espaces vectoriels de dimension finie (exemple $\mathbf{K}^n$). Existence de bases, de supplémentaires d'un sous-espace. Rang d'une application linéaire, rang d'un système de vecteurs. Espace dual. Rang d'un système d'équations linéaires. Transposée d'une application linéaire. Base duale. Bidualité. Orthogonalité.
2. Applications multilinéaires. Déterminant d'un système de vecteurs, d'un endomorphisme. Groupe spécial linéaire $SL(E)$. Orientation d'un $\mathbf{R}$-espace vectoriel.
3. Matrices à coefficients dans un corps. Opérations matricielles. Rang d'une matrice. Représentations matricielles d'une application linéaire. Changement de base.

   Opérations élémentaires sur les lignes et les colonnes d'une matrice. Méthode du pivot de GAUSS. Notion de matrices échelonnées. Application à la résolution de systèmes d'équations linéaires, au calcul de déterminants, à l'inversion des matrices carrées, à la détermination du rang d'une matrice, à la détermination d'équations définissant un sous-espace vectoriel.

   Extension élémentaire de ces notions aux matrices à coefficients dans un anneau commutatif.

4. Sous-espaces stables d'un endomorphisme, lemme des noyaux. Polynôme caractéristique, polynômes annulateurs d'un endomorphisme, polynôme minimal. Théorème de CAYLEY-HAMILTON. Diagonalisation, trigonalisation, applications. Sous-espaces caractéristiques, décomposition de DUNFORD. Exponentielle des matrices réelles ou complexes.

10.1.2 Groupes et géométrie

Les différentes notions de théorie des groupes introduites dans les paragraphes suivants seront illustrées et appliquées dans des situations géométriques.

1. Groupes, morphismes de groupes. Produit direct de groupes. Sous-groupes. Sous-groupe engendré par une partie. Ordre d'un élément. Sous-groupes distingués (ou normaux), groupes quotients. Opération d'un groupe sur un ensemble. Stabilisateur d'un point, orbites, espace quotient. Formule des classes. Classes de conjugaison. Application à la détermination des groupes d'isométries d'un polyèdre régulier en dimension 3.
2. Groupes cycliques. Groupes abéliens de type fini. Groupe des racines complexes n-ièmes de l'unité, racines primitives.
3. Groupe des permutations d'un ensemble fini. Décomposition d'une permutation en produit de transpositions, en produit de cycles à supports disjoints. Signature. Groupe alterné. Application : déterminants.
4. Définition des groupes classiques d'automorphismes d'un espace vectoriel de dimension finie : groupe général linéaire, groupe spécial linéaire ; groupe orthogonal, groupe spécial orthogonal ; groupe unitaire, groupe spécial unitaire.

10.1.3 Anneaux, corps, polynômes et fractions rationnelles

1. Anneaux (unitaires), morphisme d'anneaux, sous-anneaux. L'anneau $\mathbf{Z}$ des entiers relatifs. Produit d'anneaux. Idéaux d'un anneau, anneaux quotients. Idéaux premiers, idéaux maximaux d'un anneau commutatif. Notion de module sur un anneau commutatif, d'algèbre (associative ou non) sur un anneau commutatif.
2. Algèbre des polynômes à une ou plusieurs indéterminées sur un anneau commutatif. Polynômes homogènes. Polynômes symétriques.

   Décomposition en polynômes homogènes. Tout polynôme symétrique s'exprime en fonction des polynômes symétriques élémentaires.
3. Séries formelles à une indéterminée à coefficients dans un corps. Addition, multiplication, composition, éléments inversibles.
4. Corps, sous-corps. Caractéristique. Extension de corps. Corps des fractions d'un anneau intègre. Le corps $\mathbf{Q}$ des nombres rationnels. Le corps $\mathbf{R}$ des nombres réels. Le corps $\mathbf{C}$ des nombres complexes. Théorème de D'ALEMBERT-GAUSS.
5. Divisibilité dans les anneaux commutatifs intègres. Éléments irréductibles, éléments inversibles, éléments premiers entre eux. Anneaux factoriels. Plus grand diviseur commun, plus petit multiple commun.

   Factorialité de $A[X]$ quand A est un anneau factoriel. Anneaux principaux. Théorème de BÉZOUT. Anneaux euclidiens. Algorithme d'EUCLIDE. Cas de l'anneau $\mathbf{Z}$ et de l'algèbre $K[X]$. Polynômes irréductibles. Exemples : polynômes cyclotomiques dans $\mathbf{Q}[X]$, critère d'EISENSTEIN.
6. Congruences dans $\mathbf{Z}$. Nombres premiers. Étude de l'anneau $\mathbf{Z}/n\mathbf{Z}$ et de ses éléments inversibles. Théorème chinois et applications : multiplication, pivot de GAUSS, systèmes linéaires...

7. Racines d'un polynôme, multiplicité. Polynôme dérivé. Éléments algébriques et transcendants. Extensions algébriques. Corps algébriquement clos. Corps de rupture et corps de décomposition. Corps finis.
8. Relations entre les coefficients et les racines d'un polynôme scindé. Sommes de NEWTON. Résultant. Discriminant. Application à l'intersection ensembliste de deux courbes algébriques planes.
9. Corps des fractions rationnelles à une indéterminée sur un corps. Décomposition en éléments simples. Cas réel et complexe. Dérivée logarithmique d'un polynôme et applications.

10.1.4 Formes bilinéaires et quadratiques sur un espace vectoriel

1. Formes bilinéaires. Formes bilinéaires alternées. Formes bilinéaires symétriques, formes quadratiques, forme polaire d'une forme quadratique (en caractéristique différente de 2). Éléments orthogonaux, interprétation géométrique. Formes non dégénérées. Adjoint d'un endomorphisme. Représentation matricielle, changement de base. Rang d'une forme bilinéaire.
2. Orthogonalité. Sous-espaces isotropes. Décomposition d'une forme quadratique en somme de carrés. Théorème d'inertie de SYLVESTER. Classification dans le cas de **R** ou **C**. Procédés d'orthogonalisation.
3. Espaces vectoriels euclidiens, espaces vectoriels hermitiens. Isomorphisme d'un espace vectoriel euclidien avec son dual. Supplémentaire orthogonal. Inégalité de CAUCHY-SCHWARZ. Norme. Bases orthonormales.
4. Groupe orthogonal, groupe spécial orthogonal. Exemple de générateurs du groupe orthogonal : décomposition d'un automorphisme orthogonal en produit de réflexions. Endomorphismes symétriques, endomorphismes normaux. Diagonalisation d'un endomorphisme symétrique. Réduction simultanée de deux formes quadratiques réelles, l'une étant définie positive. Décomposition polaire dans $GL(n,\mathbf{R})$. Espaces vectoriels euclidiens de dimension 2 ou 3 : groupe des rotations ; produit mixte ; produit vectoriel.
5. Angles en dimension 2 : angles de vecteurs, angles de droites. Théorème de l'angle inscrit. Cocyclicité.
6. Groupe unitaire, groupe spécial unitaire. Diagonalisation des endomorphismes normaux. Décomposition polaire dans $GL(n,\mathbf{C})$.

10.1.5 Géométries affine, projective et euclidienne

Tous les espaces considérés dans ce chapitre sont de dimension finie.

1. Espace affine et espace vectoriel associé. Application affine et application linéaire associée. Sous-espaces affines, barycentres. Repères affines, équations d'un sous-espace affine. Groupe affine, notion de propriété affine. Groupe des homothéties-translations, affinités. Parties convexes, enveloppe convexe d'une partie d'un espace affine réel, points extrémaux.
   Projection sur un convexe fermé.
2. Droite projective réelle ou complexe : groupe des homographies, birapport.
3. Groupe des isométries d'un espace affine euclidien. Déplacements et antidéplacements. Décomposition commutative en une translation et une isométrie à point fixe (forme dite réduite). Exemple de générateurs du groupe des isométries : décomposition en produit de réflexions.
4. Espace affine euclidien de dimension 2.
   Classification des isométries.
   Similitudes directes et indirectes.
   Groupe des isométries laissant stable une partie du plan. Polygones réguliers.
   Relations métriques dans le triangle.
   Utilisation des nombres complexes en géométrie plane.

5. Espace affine euclidien de dimension 3.
   Rotations. Vissages. Groupe des isométries laissant stable une partie de l'espace.
6. Coniques et quadriques. Application des formes quadratiques à l'étude des coniques propres du plan affine euclidien et des quadriques de l'espace affine euclidien de dimension 3.
   Classification des coniques.
   Intersection de quadriques et résultant.
   Propriétés géométriques (affines et métriques) des coniques. Définition par foyer et directrice, définition bifocale.

10.1.6 Analyse à une variable réelle

1. Nombres réels
   Le corps **R** des nombres réels. Topologie de **R**. Sous-groupes additifs de **R**. Droite numérique achevée. Suites de nombres réels : convergence, valeur d'adhérence. Limites inférieure et supérieure. Suites de Cauchy. Complétude de **R**. Théorème de BOLZANO-WEIERSTRASS. Parties compactes de **R**. Parties connexes de **R**.
   Convergence des séries à termes réels. Séries géométriques, séries de RIEMANN. Séries à termes positifs. Sommation des relations de comparaison. Comparaison d'une série et d'une intégrale. Estimations des restes. Convergence absolue. Produits de séries. Séries alternées.
2. Fonctions définies sur une partie de **R** et à valeurs réelles
   (a) Continuité Limite, continuité à droite, à gauche, continuité.
   Opérations algébriques sur les fonctions continues. Théorème des valeurs intermédiaires, image d'un segment. Étude de la continuité des fonctions monotones. Continuité d'une fonction réciproque.
   (b) Dérivabilité
   Dérivée en un point, dérivée à droite, à gauche. Fonctions dérivables. Opérations algébriques sur les fonctions dérivables. Dérivée d'une fonction composée. Dérivabilité d'une fonction réciproque.
   Théorèmes de ROLLE et des accroissements finis. Application au sens de variation d'une fonction.
   Dérivées d'ordre supérieur. Applications de classe $\mathscr{C}^k$, de classe $\mathscr{C}^k$ par morceaux. Formule de LEIBNITZ. Formule de TAYLOR avec reste intégral, formule de TAYLOR-LAGRANGE, formule de TAYLOR-YOUNG.
   Calcul de développements limités et de développements asymptotiques.
3. Intégrale sur un segment des fonctions continues par morceaux et calcul de primitives
   Propriétés de l'intégrale : linéarité, relation de CHASLES, positivité. Sommes de RIEMANN. Primitives d'une fonction continue. Changement de variable. Intégration par parties. Méthodes usuelles de calcul d'intégrales.
4. Intégrales généralisées. Intégrales absolument convergentes. Intégration des relations de comparaison. Intégrales semi-convergentes.
5. Suites et séries de fonctions
   Convergence simple, convergence uniforme. Continuité et dérivabilité de la limite. Cas des séries de fonctions : convergence normale.
   Théorèmes d'approximation de WEIERSTRASS polynomial et de WEIERSTRASS trigonométrique.
6. Fonctions usuelles
   Fonctions polynômes, fonctions rationnelles. Logarithmes. Exponentielles. Fonctions puissances. Fonctions circulaires et hyperboliques. Fonctions circulaires et hyperboliques réciproques.

7. Convexité

   Fonctions convexes d'une variable réelle. Continuité et dérivabilité des fonctions convexes. Caractérisations de la convexité.

8. Suites définies par une relation $u_{n+1} = f(u_n)$. Étude graphique. Points fixes attractifs. Points fixes répulsifs.

9. Polynôme d'interpolation de LAGRANGE.

10. Méthodes d'approximation

    Approximation quadratique : polynômes orthogonaux.

11. Méthodes de résolution approchée des équations $f(x) = 0$: dichotomie, méthode de PICARD, méthode de NEWTON. Estimation de l'erreur pour la méthode de NEWTON.

12. Intégration numérique : méthode des trapèzes, de SIMPSON ; estimation de l'erreur.

10.1.7 Analyse à une variable complexe

1. Séries entières

   Rayon de convergence. Propriétés de la somme d'une série entière sur son disque de convergence : continuité, dérivabilité par rapport à la variable complexe, primitives.

   Fonctions analytiques sur un ouvert. Principe des zéros isolés. Opérations algébriques sur les fonctions analytiques. Composition.

   Exponentielle complexe ; propriétés. Extension des fonctions circulaires au domaine complexe.

   Développement en série entière des fonctions usuelles.

2. Fonctions d'une variable complexe

   Fonctions holomorphes. Conditions de CAUCHY-RIEMANN. Intégrale d'une fonction continue le long d'un chemin $\mathscr{C}^1$ par morceaux. Primitives d'une fonction holomorphe sur un ouvert étoilé. Déterminations du logarithme.

   Indice d'un chemin fermé $\mathscr{C}^1$ par morceaux par rapport à un point.

   Formules de CAUCHY. Analyticité d'une fonction holomorphe. Principe du prolongement analytique. Principe du maximum.

   Singularités isolées. Séries de LAURENT. Fonctions méromorphes. Théorème des résidus.

   Suites et séries de fonctions holomorphes.

10.1.8 Calcul différentiel

1. Topologie de $\mathbf{R}^n$

   Parties ouvertes, fermées. Voisinages. Parties compactes. Théorème de BOLZANO-WEIERSTRASS.

   Parties connexes. Normes usuelles. Limites. Applications continues. Complétude de $\mathbf{R}^n$.

2. Fonctions différentiables

   Applications différentiables sur un ouvert de $\mathbf{R}^n$. Différentielle (application linéaire tangente). Dérivée selon un vecteur.

   Dérivées partielles. Opérations algébriques sur les applications différentiables. Composition d'applications différentiables. Théorème des accroissements finis. Applications de classe $\mathscr{C}^1$.

   Matrice jacobienne. Applications de classe $\mathscr{C}^k$. Dérivées partielles d'ordre k. Interversion de l'ordre des dérivations. Formule de TAYLOR avec reste intégral, formule de TAYLOR-YOUNG.

   Étude locale des applications à valeurs dans $\mathbf{R}$. Développements limités. Recherche des extremums locaux.

   Difféomorphismes. Théorème d'inversion locale. Théorème des fonctions implicites.

3. Équations différentielles

   Équations différentielles sur un ouvert de $\mathbf{R}^n$, de la forme $X' = f(t, X)$. Théorème de CAUCHY-LIPSCHITZ. Solutions maximales. Problème de l'existence globale. Dépendance par rapport aux conditions initiales.

   Portrait de phase, comportement qualitatif.

   Systèmes différentiels linéaires.

   Méthode de variation de la constante. Cas des coefficients constants. Équations différentielles linéaires d'ordre supérieur à un.

10.1.9 Calcul intégral et probabilités

1. Définition des espaces mesurables, tribu produit, cas particulier des tribus boréliennes. Définition d'une mesure, cas particuliers de la mesure de comptage, de la mesure de LEBESGUE (construction admise) et des mesures de probabilité. Définition d'une fonction mesurable ; opérations élémentaires sur les fonctions mesurables.
2. Intégration

   Intégrale des fonctions mesurables positives, théorème de convergence monotone. Lemme de Fatou. Fonctions intégrables, théorème de convergence dominée. Continuité, dérivabilité, holomorphie d'une intégrale dépendant d'un paramètre. Espaces L^p, où $1 \leqslant p \leqslant \infty$: inégalités de MINKOWSKI, HÖLDER et JENSEN. Théorème de FUBINI.

   Changement de variables dans une intégrale multiple. Calculs d'aires de domaines plans et de volumes.

   Convolution. Régularisation et approximation par convolution.
3. Analyse de FOURIER

   Séries de FOURIER des fonctions localement intégrables périodiques d'une variable réelle. Lemme de RIEMANN-LEBESGUE. Produit de convolution de fonctions périodiques. Théorèmes de DIRICHLET et de FEJER. Théorie L^2 : convergence en moyenne quadratique, formule de PARSEVAL.

   Transformée de FOURIER d'une fonction intégrable sur $\mathbf{R}$. Lemme de RIEMANN-LEBESGUE.

   Formule d'inversion. Transformée d'un produit de convolution. Théorie L^2 : formule de PLANCHEREL.
4. Probabilités.

   Définition d'un espace de probabilité. Variables aléatoires, lois de probabilité d'une variable aléatoire, fonction de répartition. Indépendance d'une famille d'événements, de tribus ou de variables aléatoires.

   Espérance et variance d'une variable aléatoire à valeurs réelles.

   Exemples de lois : loi de BERNOULLI, loi binomiale, loi de POISSON, loi uniforme, loi normale, loi exponentielle.

   Fonction caractéristique et transformée de LAPLACE, applications à la somme de variables aléatoires indépendantes, lien avec la convolution.

   Probabilités conditionnelles : définition, théorème de BAYES.

   Convergence de suites de variables aléatoires : en probabilité, dans L^p , presque partout, en loi.

   Inégalité de MARKOV, inégalité de BIENAIMÉ-TCHEBYSCHEV. Loi faible des grands nombres. Théorème de la limite centrale.

10.1.10 Analyse fonctionnelle

1. Topologie et espaces métriques

   Topologie d'un espace métrique. Topologie induite.

   Suites. Valeurs d'adhérence. Limites. Applications continues. Homéomorphismes.

Produit fini d'espaces métriques.

Compacité. Connexité. Composantes connexes. Connexité par arcs.

Propriétés métriques : applications lipschitziennes, applications uniformément continues.

Espaces métriques complets. Théorème du point fixe pour les applications contractantes.

2. Espaces vectoriels normés sur **R** ou **C**.

   Topologie d'un espace vectoriel normé. Normes équivalentes. Cas des espaces de dimension finie. Espaces de BANACH. Séries absolument convergentes dans un espace de Banach.

   Applications linéaires continues, norme.

   Norme de la convergence uniforme. Espace des fonctions continues bornées sur un espace métrique, à valeurs dans un espace BANACH.

   Étude de la compacité de parties d'un espace vectoriel normé : théorème de RIESZ ; théorème d'ASCOLI.

   Complétude des espaces L^p, où $1 \leqslant p \leqslant \infty$.

3. Espaces de HILBERT

   Projection sur un convexe fermé. Projection orthogonale sur un sous-espace vectoriel fermé.

   Dual d'un espace de HILBERT.

   Cas des espaces L^2.

   Bases hilbertiennes (dans le cas séparable). Exemples de bases : fonctions trigonométriques, polynômes orthogonaux.

10.1.11 Géométrie différentielle

Sous-variétés de $\mathbf{R}^n$. Définitions équivalentes : graphe local, paramétrisation locale, équation locale. Espace tangent. Notions métriques : longueur d'un arc, paramétrisation normale, courbure d'un arc en dimensions 2 et 3. Gradient.

Tracé de courbes usuelles.

Surfaces dans $\mathbf{R}^3$: position par rapport au plan tangent.

Définition de la divergence d'un champ de vecteurs.

Extremums locaux d'une fonction définie sur une sous-variété (extremums liés).

10.2 ÉPREUVES ÉCRITES

Les épreuves écrites comportent deux épreuves :

A. Composition de mathématiques générales

Le programme de cette épreuve est constitué par les titres I à XI ci-dessus.

B. Composition d'analyse et probabilités

Le programme de cette épreuve est constitué par les titres I à XI ci-dessus.

10.3 ÉPREUVES ORALES

Les candidats ont le choix entre quatre options :
Option A : probabilité et statistiques
Option B : calcul scientifique
Option C : algèbre et calcul formel
Option D : informatique

10.3.1 Épreuves orales des options A, B, C

1re Épreuve : Épreuve d'Algèbre et Géométrie

2e Épreuve : Épreuve d'Analyse et Probabilités

Le programme de ces deux épreuves, communes aux options A, B et C, est constitué des titres I à XI ci-dessus.

3e Épreuve : Épreuve de Modélisation

L'épreuve porte sur un programme commun aux options A, B et C et sur un programme spécifique à l'option choisie.

L'épreuve consiste en un exposé de modélisation mathématique construit en partant d'un texte proposé par le jury. Le programme définit un cadre de théories mathématiques et de techniques d'application adaptées pour l'épreuve. Ce programme comporte une partie commune aux options A, B et C et, pour chacune de ces options, une partie spécifique.

10.3.2 Modélisation : programme de la partie commune aux options A, B, C

Le corpus des logiciels disponibles est constitué de Maple, Mathematica, MuPAD, Matlab, Scilab, Octave, R, Maxima, Axiome, Giac/Xcas, Pari/GP, Gap.

À l'aide d'un ou plusieurs de ces logiciels, les candidats devront montrer leur capacité à :

- mettre en œuvre avec précision et rigueur les concepts et outils mathématiques au programme,
- distinguer les représentations exactes ou approchées des objets mathématiques
- estimer le coût et les limitations d'algorithmes simples : complexité, précision
- analyser la pertinence des modèles.

Le programme de cette partie comprend les méthodes numériques, probabilistes, statistiques et symboliques citées dans les programmes des épreuves écrites et celles citées dans les paragraphes suivants.

1. Calcul numérique et symbolique
   Utilisation des logiciels au programme : simulation, intégration, différentiation, calcul de sommes et d'intégrales, résolution d'équations algébriques et différentielles.
2. Probabilités discrètes : tirages uniformes ; échantillons.
3. Validation et précision des résultats
   Méthodes numériques : notion de conditionnement des systèmes linéaires.
   Précision du schéma numérique d'EULER explicite à pas constant.
   Moyenne et variance empiriques.
   Méthode de Monte Carlo : vitesse de convergence ; applications au calcul d'intégrales multiples (exemple : calculs de volumes).
4. Moindres carrés linéaires (sans contrainte).

10.3.3 Programme spécifique de l'option A

1. Utilisation de lois usuelles (voir section 9. 4 , loi géométrique) pour modéliser certains phénomènes aléatoires. Exemples : temps d'attente ou durée de vie, erreurs de mesure, sondages ...
2. Convergence presque sûre. Lemme de BOREL-CANTELLI. Loi forte des grands nombres.

3. Chaînes de MARKOV homogènes à espace d'états fini. Classification des états. Convergence vers une loi stationnaire (théorème ergodique et théorème de la limite centrale admis).

   Chaînes de MARKOV homogènes à espace d'états dénombrable, transience, récurrence positive ou nulle, exemple de la marche aléatoire simple.

   Espérance conditionnelle, définition des martingales, temps d'arrêt. Exemples d'utilisation, des théorèmes de convergence presque sûre et L^2, des martingales à temps discret.

4. Vecteurs gaussiens : définition, simulation en dimension 2, théorème de COCHRAN. Théorème de la limite centrale dans $\mathbf{R}^n$, Utilisation du lemme de SLUTSKY. Définition et calcul d'intervalles de confiance.

   Lois Gamma. Définition de l'estimation du maximum de vraisemblance.

5. Tests sur un paramètre. Tests du χ^2. Fonction de répartition empirique et tests de KOLMOGOROV-SMIRNOV (population de taille finie et comportement asymptotique). Exemples d'utilisation.

   Modèle linéaire gaussien : calculs par moindres carrés, régression simple ou multiple, exemples d'utilisation.

   Simulation de variables aléatoires.

   Fonctions génératrices. Processus de vie et de mort.

10.3.4 Programme spécifique de l'option B.

1. Résolution de systèmes d'équations linéaires ; définition du conditionnement. Factorisation LU.

   Méthode du gradient pour les systèmes linéaires symétriques définis positifs.

   Recherche des valeurs propres : méthode de la puissance.

   Résolution de systèmes d'équations non linéaires. Méthode de NEWTON : définition, vitesse de convergence, estimation de l'erreur.

2. Intégration numérique : méthode des trapèzes, de SIMPSON ; estimation de l'erreur.

3. Équations différentielles ordinaires. Espaces de phase. Étude qualitative. Stabilité des points critiques.

   Aspects numériques du problème de CAUCHY. Méthodes d'EULER explicite et implicite : consistance, stabilité, convergence, ordre. Utilisation de la méthode de RUNGE-KUTTA 4.

4. Notions élémentaires sur les équations aux dérivées partielles classiques en dimension un.

   Équation de transport (advection) linéaire : méthode des caractéristiques.

   Équations des ondes et de la chaleur : résolution par transformée de FOURIER et séparation des variables. Aspects qualitatifs élémentaires.

   Équations elliptiques.

   Exemples de discrétisation de problèmes aux limites en dimension un par la méthode des différences finies : notions de consistance, stabilité, convergence, ordre.

5. Optimisation et approximation

   Interpolation de LAGRANGE.

   Extremums des fonctions réelles de n variables réelles : multiplicateurs de LAGRANGE. Mise en œuvre de l'algorithme de gradient à pas constant.

   Méthode des moindres carrés et applications.

10.3.5 Programme spécifique de l'option C.

1. Représentation et manipulation des entiers longs, flottants multiprécision, nombres complexes, polynômes, éléments de $\mathbf{Z}/n\mathbf{Z}$ et des corps finis. Addition, multiplication, division, extraction de racine carrée.

2. Algorithmes algébriques élémentaires.
   Exponentiation ($n \mapsto a^n$, pour $n \in \mathbf{N}$), algorithme d'EUCLIDE étendu.
   Test de primalité de FERMAT.
3. Matrices à coefficients dans un corps.
   Méthode du pivot de GAUSS, décomposition LU. Calcul du rang, du déterminant.
   Exemples de codes correcteurs linéaires : codes de répétition, codes de HAMMING binaires.
4. Matrices à coefficients entiers.
   Opérations élémentaires sur les lignes et les colonnes. Application aux systèmes linéaires sur **Z** et aux groupes abéliens de type fini.
5. Polynômes à une indéterminée.
   Évaluation (schéma de HORNER), interpolation (LAGRANGE, différences finies).
   Localisation des racines dans **R** ou **C** : majoration en fonction des coefficients.
6. Polynômes à plusieurs indéterminées.
   Résultants, élimination ; intersection ensembliste de courbes et de surfaces algébriques usuelles.
7. Estimation de la complexité des algorithmes précités dans le cas le pire. Aucune formalisation d'un modèle de calcul n'est exigée.

10.4 Épreuves de l'option D : informatique

1re Épreuve : Mathématiques

Le programme de cette épreuve est constitué des titres I à XI ci-dessus. Les candidats se verront proposer deux sujets, dans un corpus d'algèbre, de géométrie, d'analyse et de probabilités.

2e Épreuve : Informatique Fondamentale

Le programme de cette épreuve est constitué des titres 1 à 4 ci-après.

3e Épreuve : Analyse de système informatique

Le programme de cette épreuve est constitué des titres 1 à 4 ci-après.

Deux textes décrivant une classe de systèmes informatiques sont proposés au candidat qui doit choisir l'un des deux. La compréhension de ces textes et leur exploitation dans cette épreuve requièrent les connaissances en informatique correspondant aux matières enseignées en L1-L2 de Maths-Info ou dans l'option informatique des classes préparatoires auxquelles s'ajoutent celles du programme.

L'objectif de l'épreuve est d'évaluer la capacité des candidats à mettre en place un processus d'analyse d'un système informatique dans un contexte applicatif. Ce processus s'appuie sur les notions au programme.

Les langages informatiques C, Caml et Java seront disponibles pour cette épreuve et sa préparation. Le rapport du Jury précisera la nature de l'environnement logiciel.

Programme spécifique de l'option D.

L'ensemble du programme correspond à 250h de formation (cours et/ou TD et/ou TP) de niveau Licence et première année de Master, à partir des acquis des deux premières années de Licence ou de l'option informatique des classes préparatoires. L'objectif de cette option est de s'assurer que les candidats maîtrisent les fondements essentiels et structurants de la science informatique.

Le programme n'est pas rédigé comme un plan de cours, il décrit les notions que les candidats doivent maîtriser.

Le programme n'impose aucun langage de programmation particulier. Les candidats doivent maîtriser au moins un langage et son environnement de programmation parmi CAML, Java ou C.

10.4.1 Algorithmique fondamentale

Cette partie insiste sur les notions de preuve et de complexité des algorithmes. Elle est relativement indépendante de tout langage de programmation, mais le candidat doit être capable de mettre en oeuvre sur machine les structures de données et les algorithmes étudiés.

1. Structures de données. Types abstraits : définition des tableaux, listes, piles, files, arbres, graphes (orientés et non orientés), ensembles, dictionnaires, file de priorité. Interface abstraite et implantation (implémentation) concrète.
2. Schémas algorithmiques classiques : approche gloutonne, diviser pour régner, programmation dynamique. Exemples : algorithme de DIJKSTRA, tri-fusion, plus longue sous-séquence commune.
3. Complexité. Analyse des algorithmes : relations de comparaison O, Θ et Ω. Analyse dans le pire cas. Exemple d'analyse en moyenne : recherche d'un élément dans un tableau.
4. Preuve d'algorithmes : correction, terminaison. Méthodes de base : assertions, pré-post conditions, invariants et variants de boucles, logique de HOARE, induction structurelle.
5. Algorithmes de tri et de recherche. Méthodes de tri par comparaison (tri-fusion, tri-tas, tri rapide), arbre de décision et borne inférieure du tri par comparaisons. Méthodes de recherche séquentielle et dichotomique. Arbres binaires de recherche. Arbres équilibrés : définition, relation entre la taille et la hauteur, maintien de l'équilibre.
6. Algorithmes de graphes. Parcours de graphes : algorithmes de parcours en largeur, en profondeur, algorithme de DIJKSTRA. Arbres couvrants : algorithmes de PRIM et de KRUSKAL. Fermeture transitive.

10.4.2 Automates et langages

1. Automates finis. Langages reconnaissables. Lemme d'itération. Existence de langages non reconnaissables. Automates complets. Automates déterministes. Algorithme de déterminisation. Propriétés de clôture des langages reconnaissables.
2. Expressions rationnelles. Langages rationnels. Théorème de KLEENE.
3. Automate minimal. Résiduel d'un langage par un mot. Algorithme de minimisation.
4. Utilisation des automates finis : recherche de motifs, analyse lexicale.
5. Langages algébriques. Lemme d'OGDEN. Existence de langages non algébriques. Grammaires algébriques. Propriétés de clôture des langages algébriques.
6. Automates à pile. Langages reconnaissables par automates à pile.
7. Utilisation des automates à pile : analyse syntaxique. Grammaires LL(1).

10.4.3 Calculabilité, décidabilité et complexité

1. Définition des fonctions primitives récursives ; schémas primitifs (minimisation bornée). Définition des fonctions récursives ; fonction d'ACKERMAN.
2. Définitions des machines de TURING. Équivalence entre classes de machines (exemples : nombre de rubans, alphabet). Équivalence avec les fonctions récursives.
3. Universalité. décidabilité, Indécidabilité. Théorème de l'arrêt. Théorème de RICE. Réduction de TURING. Définitions et caractérisations des ensembles récursifs, récursivement énumérables.
4. Complexité en temps et en espace : classe P. Machines de TURING non déterministes : classe NP. Acceptation par certificat. Réduction polynomiale. NP-complétude. Théorème de COOK.

10.4.4 Logique et démonstration

1. Calcul propositionnel : syntaxe et sémantique. Tables de vérité, tautologies, formes normales, forme clausale. Théorème de complétude du calcul propositionnel.
2. Logique du premier ordre : aspects syntaxiques. Langages, termes, formules. Variables libres et variables liées, substitutions, capture de variables.
3. Réécriture : filtrage syntaxique du premier ordre, définition de l'unification syntaxique. Confluence, confluence locale, formes normales, paires critiques, lemme de NEWMAN, algorithme de complétion de KNUTH-BENDIX.
4. Logique du premier ordre : systèmes formels de preuve. Calcul des séquents, déduction naturelle. Algorithme d'unification des termes. Preuves par résolution.
5. Logique du premier ordre : aspects sémantiques. Interprétation d'une formule dans un modèle. Validité, satisfiabilité. Théories cohérentes, théories complètes. Théories décidables, indécidables. Exemples de théories : égalité, arithmétique de Peano. Théorème de complétude du calcul des prédicats du premier ordre.

Chapitre 11

Annexe 4 : La bibliothèque de l'agrégation

ABELSON 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
ARNOLD A. **GUESSARIAN I.**	Mathématiques pour l'informatique	EDISCIENCES
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
BAJARD J.C.	Exercices d'Algorithmique	ITP
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
DANTZER J.F.	Mathématiques pour l'agrégation interne	VUIBERT
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
DRAPPER N. **SCHMITH H.**	Applied regression analysis	WILEY
DUBUC S.	Géométrie plane	PUF
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.	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
GATHEN (von zur) J. **GERHARD .J**	Modern computer algebra	Cambridge University press
GANTMACHER F.R.	Théorie des matrices – Tome 1 – Tome 2	Dunod
GAREY M. **JOHNSON D.**	Computers and intractability	Freeman
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
GRAHAM R. **KNUTH D.** **PATASHNIK O.**	Concrete mathematics	ADISON-WESLEY
GRAMAIN A.	Géométrie élémentaire	HERMANN
GRAMAIN A.	Intégration	HERMANN
GRIMMET G. **WELSH D.**	Probability (an introduction)	OXFORD
GUJARATI D. N.	Basic Econometrics	WILEY
GUSFIELD D.	Algorithms on strings, trees and sequences	CAMBRIDGE UNIVERSITY PRESS
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
HOCHART **SCIUTO**	Algèbre Analyse Géométrie (MPSI/PCSI)	VUIBERT
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

KERBRAT Y. **BRAEMER J-M.**	Géométrie des courbes et des surfaces	HERMANN
KERNIGHAN B. **RITCHIE D.**	Le langage C	DUNOD
KNUTH D.E.	The art of computer programming – Volume 1 : Fundamental algorithms – Volume 2 : Seminumerical algorithms – Volume 3 : Sorting and Searching	ADDISON-WESLEY
KOBLITZ N.	A course in number theory and cryptography quantite1	
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
KRIVINE J.L.	Théorie des ensembles	CASSINI
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
LE BRIS G.	Maple Sugar : une initiation progressive à Maple	CASSINI
LEBOEUF C. **GUEGAND J.** **ROQUE J.L.** **LANDRY P.**	Exercices corrigés de probabilités	ELLIPSES
LEBORGNE D.	Calcul différentiel et géométrie	PUF
LEBOSSÉ C. **HÉMERY C.**	Géométrie. Classe de Mathématiques	JACQUES GABAY
LEHMANN D. **SACRÉ C.**	Géométrie et topologie des surfaces	PUF
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 – Using Matlab Graphics	

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
MENEZES A.J. **van OORSCHOT P.C.** **VANSTONA S.A.**	Handbook of applied cryptography	CRC PRESS
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
OŔOURKE J.	Computational géométrie in C (second édition)	CAMBRIDGE
OPREA J.	Differential geometry	PRENTICE HALL

OUVRARD J.Y.	– Probabilités 2 (maîtrise, agrégation)	CASSINI
PAPADIMITRIOU C.H.	Computational complexity	PEARSON EDUCATION
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
PETROVŠEK **WILF** **ZEILBERGER**	A=B	A.K. PETERS
PEVZNER P.	Computational molecular biology- an algorithmic approach	MIT PRESS
PÓLYA G. **SZEGÖ G.**	Problems and Theorems in Analysis – Volume I – Volume II	SPRINGER VERLAG
POMMELLET A.	Agrégation de Mathématiques. Cours d'Analyse	ELLIPSES
PREPARATA F.P. **SHAMOS M.I.**	Computational géométrie - an introduction	SPRINGER

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
RAMIS J.P. **WARUSFEL A.**	Mathématiques - Tout en un pour la licence	DUNOD
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
RIESZ F. **NAGY SZ. B.**	Leçons d'analyse fonctionnelle	GAUTHIER-VILLARS
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
ROUVIÈRE F.	Petit guide de calcul différentiel à l'usage de la licence et de l'agrégation	CASSINI
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
SAKAROVITCH J.	Eléments de théorie des automates	VUIBERT
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
SCHNEIER B.	Applied cryptography	WILEY

SCHWARTZ L.	Analyse – I Topologie générale et analyse fonctionnelle – II Calcul différentiel et équations différentielles	HERMANN
SCHWARTZ L.	Cours d'Analyse – Tome 1 – Tome 2	HERMANN
SCHWARTZ L.	Méthodes Mathématiques pour les sciences physiques	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
STEWART I.	Galois theory	CHAPMAN AND HALL
STROUSTRUP B	Le langage C++	PEARSON EDUCATION

SZPIRGLAS A.	Exercices d'algèbre	CASSINI
TAUVEL P.	Cours de Géométrie	DUNOD
TAUVEL P.	Cours d'algè bre	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
VAUTHIER J. PRAT J-J.	Cours d'Analyse Mathématique de l'Agrégation	MASSON
VAZIRANI V.V.	Algorithmes d'approximation	SPRINGER
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
WATERMAN M.S.	Introduction to computational biology	CHAPMAN AND HALL / CRC
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
WILF H.	Algorithms and complexity	A.K. PETERS
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