écrit

MATHÉMATIQUES GÉNÉRALES

Sujet (durée : 6 heures)

La rigueur des démonstrations, le soin apporté à leur rédaction, seront des éléments importants d'appréciation.

Les questions marquées d'une étoile ★ peuvent être considérées comme « questions subsidiaires » et laissées de côté dans un premier temps.

Les notations et certains résultats de la partie I *sont utilisés dans les parties* II.B *et* III.B. *Les parties* II *et* III *sont indépendantes l'une de l'autre.*

Dans tout le problème, on désigne par ω un entier strictement positif *pair*, et par Ω un ensemble de cardinal ω.

Pour tout ensemble fini E, on note $|E|$ son cardinal.

Pour tout entier n, on désigne par $\bar{n}$ son image modulo $2\mathbb{Z}$.

On note $\mathbb{Z}[X, Y]$ l'ensemble des polynômes à deux indéterminées à coefficients dans $\mathbb{Z}$.

PARTIE I

I.A. Généralités

I.A.1. Vérifier que l'ensemble des parties de Ω, muni de l'opération « différence symétrique » définie par

$$(x, y) \longmapsto x + y = \{ t \in \Omega \ ; \ (t \in x \cup y) \quad \text{et} \quad (t \notin x \cap y) \}$$

est un groupe abélien.

I.A.2. Démontrer que l'ensemble des parties de Ω peut être muni d'une structure d'espace vectoriel sur le corps à deux éléments $\mathbb{Z}/2\mathbb{Z} = \{ \bar{0}, \bar{1} \}$ dont la loi de groupe additif est celle définie en I.A.1. Grâce à quelle propriété particulière de cette loi de groupe cela est-il possible?

On désigne par $\mathfrak{P}(\Omega)$ l'espace vectoriel sur $\mathbb{Z}/2\mathbb{Z}$ ainsi défini.

I.A.3. Quelle est la dimension de $\mathfrak{P}(\Omega)$? Fournir une base de cet espace.

I.A.4. Vérifier que l'application α de $\mathfrak{P}(\Omega) \times \mathfrak{P}(\Omega)$ dans $\mathbb{Z}/2\mathbb{Z}$ définie par

$$\alpha(x, y) = \overline{|x \cap y|}$$

est une forme bilinéaire symétrique non dégénérée sur $\mathfrak{P}(\Omega)$.

Dans tout ce qui suit, on suppose $\mathfrak{P}(\Omega)$ muni de cette forme bilinéaire α appelée forme bilinéaire naturelle sur $\mathfrak{P}(\Omega)$.

I.A.5. On désigne par $\mathfrak{D}(\Omega)$ le sous-espace vectoriel de dimension 1 de $\mathfrak{P}(\Omega)$ engendré par Ω. On désigne par $\mathfrak{H}(\Omega)$ l'orthogonal de $\mathfrak{D}(\Omega)$. Décrire cet orthogonal, et retrouver ainsi la formule

$$\binom{\omega}{0} + \binom{\omega}{2} + \cdots + \binom{\omega}{2k} + \cdots + \binom{\omega}{\omega} = 2^{\omega-1}.$$

Quel est le noyau de la restriction de la forme bilinéaire naturelle à $\mathfrak{H}(\Omega)$?

I.B. Codes et polynômes des poids

Les sous-espaces vectoriels de $\mathfrak{P}(\Omega)$ sont appelés les codes de $\mathfrak{P}(\Omega)$. Si $\mathfrak{C}$ est un code de $\mathfrak{P}(\Omega)$, on désigne par $\mathfrak{C}^\circ$ son orthogonal. Pour toute permutation s de Ω, on désigne par $\bar{s}$ l'application linéaire de $\mathfrak{P}(\Omega)$ dans $\mathfrak{P}(\Omega)$ définie par

$$x \longmapsto \bar{s}(x) = \{ s(t) ; \quad (t \in x) \}.$$

On dit que deux codes $\mathfrak{C}$ et $\mathfrak{C}'$ de $\mathfrak{P}(\Omega)$ sont isomorphes s'il existe une permutation s de Ω telle que $\bar{s}(\mathfrak{C}) = \mathfrak{C}'$.

I.B.1. Un code $\mathfrak{C}$ de $\mathfrak{P}(\Omega)$ est dit auto-orthogonal si $\mathfrak{C} = \mathfrak{C}^\circ$. Quelle est la dimension d'un code auto-orthogonal ? Démontrer que si $\mathfrak{C}$ est auto-orthogonal on a $\mathfrak{D}(\Omega) \subset \mathfrak{C} \subset \mathfrak{H}(\Omega)$.

Soit $\mathfrak{C}$ un code de $\mathfrak{P}(\Omega)$. On appelle polynôme des poids de $\mathfrak{C}$ et on note $P_{\mathfrak{C}}(X, Y)$ l'élément de $\mathbb{Z}[X, Y]$ défini par

$$P_{\mathfrak{C}}(X, Y) = \sum_{x \in \mathfrak{C}} X^{|x|} Y^{\omega - |x|}.$$

I.B.2. On pose $\omega = 2m$ et $\Omega = \{ t_1, t_2, \ldots, t_m, u_1, u_2, \ldots, u_m \}$. Construire un code auto-orthogonal dont le polynôme des poids est

$$P_\omega(X, Y) = (X^2 + Y^2)^m.$$

Soit $\Gamma(\Omega)$ l'ensemble des codes auto-orthogonaux de $\mathfrak{P}(\Omega)$ dont le polynôme des poids est $P_\omega(X, Y)$. Démontrer que deux éléments quelconques de $\Gamma(\Omega)$ sont isomorphes.

★ I.B.3. Pour $\omega = 2m$ multiple de 4

et $\Omega = \{t_1, t_2, \ldots, t_m, u_1, u_2, \ldots, u_m\}$,

vérifier que le code $\mathcal{B}_\omega$ engendré par $\{t_1, \ldots, t_m\}, \{u_1, \ldots, u_m\}, \{t_h, t_j, u_h, u_j\}$

pour $h \neq j$ et $1 \leqslant h \leqslant m$, $1 \leqslant j \leqslant m$,

est un code auto-orthogonal dont le polynôme des poids est

$$Q_\omega(X,Y) = \frac{1}{2}\left((X^2+Y^2)^m + (X^2-Y^2)^m + (2XY)^m\right).$$

On dit qu'un code auto-orthogonal est pair si les cardinaux de tous ses éléments sont multiples de 4. Vérifier que si ω est multiple de 8, le code $\mathcal{B}_\omega$ défini ci-dessus est pair.

Pour $\omega = 16$, mettre en évidence un code $\mathcal{B}'_{16}$, non isomorphe à $\mathcal{B}_{16}$, dont le polynôme des poids est égal à $Q_{16}(X, Y)$.

I.B.4. Soit $\mathcal{C}$ un code de $\mathfrak{P}(\Omega)$. On se propose de démontrer la « formule de Mac-Williams » :

$$2^{\dim(\mathcal{C})} P_{\mathcal{C}^0}(X,Y) = P_{\mathcal{C}}(Y-X, X+Y).$$

I.B.4. *a*. Soit $f : \mathfrak{P}(\Omega) \to M$ une application à valeurs dans un groupe abélien M dont la loi est notée additivement. On pose $(-1)^{\bar{0}} = 1$ et $(-1)^{\bar{1}} = -1$, et on note alors $\hat{f} : \mathfrak{P}(\Omega) \to M$ la fonction définie par

$$\hat{f}(x) = \sum_{y \in \mathfrak{P}(\Omega)} (-1)^{\alpha(x,y)} f(y).$$

Démontrer que pour tout code $\mathcal{C}$ de $\mathfrak{P}(\Omega)$, on a

$$\sum_{x \in \mathcal{C}} \hat{f}(x) = 2^{\dim(\mathcal{C})} \sum_{y \in \mathcal{C}^0} f(y).$$

I.B.4. *b*. En prenant pour M le groupe additif de $\mathbb{Z}[X, Y]$, et en choisissant judicieusement la fonction f, démontrer la formule de Mac-Williams.

PARTIE II

II.A. Invariants d'un groupe fini

Soit V un espace vectoriel complexe de dimension finie $n \geqslant 1$. Si g est un endomorphisme de V, on note $\mathrm{Tr}(g)$ sa trace. On note I l'endomorphisme-identité de V.

On désigne par G un sous-groupe fini du groupe des automorphismes de V.

II.A.1. On note V^G le sous-espace vectoriel de V formé des $v \in V$ tels que $g(v) = v$ pour tout g appartenant à G. Démontrer que

$$\dim(V^G) = \frac{1}{|G|} \sum_{g \in G} \mathrm{Tr}(g).$$

(On pourra utiliser l'endomorphisme $p_G = \frac{1}{|G|} \sum_{g \in G} g$ et démontrer en particulier que $V^G = p_G(V)$.)

On choisit une fois pour toutes une base $(e_1, \ldots, e_n)$ de V. On note A l'algèbre $\mathbb{C}[X_1, \ldots, X_n]$; à tout élément g de G on associe l'application $\sigma_g : A \to A$ définie de la manière suivante

Si, pour $1 \leqslant h \leqslant n$, on a $g(e_h) = \sum_{1 \leqslant j \leqslant n} \gamma_{j,h} e_j$, et si $P(X_1, \ldots, X_n)$ est un polynôme, élément de A, on pose

$$\sigma_g(P)(X_1, \ldots, X_n) = P\Big(\sum_{1 \leqslant j \leqslant n} \gamma_{j,1} X_j, \ldots, \sum_{1 \leqslant j \leqslant n} \gamma_{j,n} X_j\Big).$$

Pour tout entier naturel k, on note A_k l'espace vectoriel complexe des polynômes homogènes de degré k en n variables.

II.A.2. Vérifier que l'application $g \longmapsto \sigma_g$ est un homomorphisme de G dans le groupe des automorphismes de l'algèbre A. Vérifier que pour tout g appartenant à G l'application σ_g induit, pour tout entier naturel k, un automorphisme de l'espace vectoriel A_k

On note A_k^G l'ensemble des $P \in A_k$ tels que $\sigma_g(P) = P$ pour tout g appartenant à G.

II.A.3. On note a_k (resp. $a_k(G)$) la dimension de l'espace vectoriel A_k (resp. A_k^G). Démontrer que les séries entières $\sum_{k=0}^{\infty} a_k z^k$ et $\sum_{k=0}^{\infty} a_k(G) z^k$ ont des rayons de convergence strictement positifs (on pourra vérifier que, pour $|z| < 1$, on a $\frac{1}{(1-z)^n} = \sum_{k=0}^{\infty} a_k z^k$.)

On pose

$$\Phi_G(z) = \sum_{k=0}^{\infty} a_k(G) z^k.$$

II.A.4. Pour tout $g \in G$, on désigne par g_k l'automorphisme de A_k défini par g. Comparer la trace de g_k au coefficient de z^k dans le développement en série entière de $\frac{1}{\det(I - zg)}$. En déduire que pour $|z| < 1$, on a

$$\Phi_G(z) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I - zg)}.$$

II.B. Algèbre associée aux polynômes des poids

On utilise ici les notations, définitions et résultats des parties I.A., I.B., II.A.

On note G le groupe de matrices engendré par

$$\mu = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{et} \quad \rho = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Si $P(X,Y) \in \mathbb{C}[X,Y]$ et si $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, on pose (voir II.A.)

$$\sigma_g(P)(X, Y) = P(aX + cY, bX + dY).$$

II.B.1. Soit $\mathcal{C}$ un code auto-orthogonal de $\mathcal{P}(\Omega)$. Démontrer que $P_{\mathcal{C}}(X, Y)$ est invariant par les transformations σ_g pour $g \in G$.

II.B.2. Démontrer que le groupe monogène H engendré par $\rho\mu$ est distingué dans G. Quel est le cardinal de H ? Étudier le groupe quotient G/H, et en déduire que G est de cardinal 16.

On pose $A = \mathbb{C}[X, Y]$ et on utilise les notations de II.A. pour $n = 2$.

II.B.3. Décomposer $\dfrac{1}{(1 - X^2)(1 - X^8)}$ en éléments simples dans $\mathbb{R}(X)$.

Démontrer que pour $|z| < 1$ on a

$$\Phi_G(z) = \frac{1}{(1 - z^2)(1 - z^8)}.$$

II.B.4. Si r est un réel, on note $[r]$ sa partie entière. Démontrer que la dimension de l'espace A_k^G des polynômes homogènes à deux variables de degré k invariants par G est

$$a_k(G) = \left[\frac{k}{8}\right] + 1 \quad \text{si } k \text{ est pair,}$$

$$a_k(G) = 0 \quad \text{si } k \text{ est impair.}$$

II.B.5. Démontrer que l'algèbre A^G des polynômes à deux variables, invariants par G, est l'algèbre

$\mathbb{C}[P_2(X, Y), Q_8(X, Y)] = \{P(P_2(X, Y), Q_8(X, Y)) ; (P(X, Y) \in \mathbb{C}[X, Y])\}$

(les polynômes P_ω et Q_ω sont définis respectivement en I.B.2. et I.B.3.).

II.B.6. On pose $\Delta(X, Y) = X^2Y^2(X^2 - Y^2)^2$. Démontrer que si $\mathcal{C}$ est un code auto-orthogonal de $\mathcal{P}(\Omega)$, le polynôme $P_{\mathcal{C}}(X, Y)$ appartient à l'algèbre

$\mathbb{Z}[P_2(X, Y), \Delta(X, Y)] = \{P(P_2(X, Y), \Delta(X, Y)) ; (P(X, Y) \in \mathbb{Z}[X, Y])\}$.

PARTIE III

Dans tout ce qui suit, on suppose que l'espace vectoriel $\mathbb{Q}^\omega$ est muni du produit scalaire canonique (pour lequel la base canonique de $\mathbb{Q}^\omega$ est orthonormale) noté

$$(v, w) \longmapsto v \cdot w \in \mathbb{Q}.$$

Soit L un sous-groupe du groupe additif de $\mathbb{Q}^\omega$. On dit que L est un réseau de $\mathbb{Q}^\omega$ s'il existe une base $(e_1, e_2, \ldots, e_\omega)$ de $\mathbb{Q}^\omega$ telle que L soit l'ensemble des combinaisons linéaires à coefficients entiers relatifs des vecteurs $e_1, \ldots, e_\omega$. On dit alors que $(e_1, \ldots, e_\omega)$ est une $\mathbb{Z}$ - base de L.

III.A. Généralités sur les réseaux

III.A.1. Soit L un réseau de $\mathbb{Q}^\omega$. On appelle dual de L et on note L^0 l'ensemble des $v \in \mathbb{Q}^\omega$ tels que $v \cdot w \in \mathbb{Z}$ pour tout $w \in L$. Démontrer que le dual d'un réseau est un réseau.

III.A.2. Soit L un réseau de $\mathbb{Q}^\omega$. Vérifier que la valeur absolue du déterminant d'une $\mathbb{Z}$-base de L par rapport à une autre $\mathbb{Z}$-base de L est égale à 1. En déduire que la valeur absolue du déterminant d'une $\mathbb{Z}$-base de L par rapport à une base orthonormale de $\mathbb{Q}^\omega$ ne dépend que de L. Cette valeur est appelée « volume de L » et notée vol(L). Démontrer que $\mathrm{vol}(L)\mathrm{vol}(L^\circ) = 1$.

III.A.3. Soit M un sous-groupe du groupe additif de $\mathbb{Q}^\omega$ qui est engendré par un nombre fini d'éléments de $\mathbb{Q}^\omega$. Démontrer que si M contient un réseau de $\mathbb{Q}^\omega$, alors M est lui-même un réseau de $\mathbb{Q}^\omega$.

(On pourra procéder ainsi :

a. Démontrer qu'il existe un réseau L contenant M.

b. Soit $(e_1, \ldots, e_\omega)$ une $\mathbb{Z}$-base de L. Pour tout $k \in \{1, \ldots, \omega\}$ désignons par L_k le groupe engendré par $e_1, \ldots, e_k$. Démontrer par récurrence sur k que $M \cap L_k$ est engendré par k vecteurs de $\mathbb{Q}^\omega$.)

III.A.4. On suppose ω multiple de 4. Soit $(w_1, w_2, \ldots, w_\omega)$ une base orthogonale de $\mathbb{Q}^\omega$ telle que pour tout $j \in \{1, 2, \ldots, \omega\}$ on a $w_j \cdot w_j = 1/4$.

Soit Λ_ω l'ensemble des vecteurs $v = \sum_{1 \leqslant j \leqslant \omega} \lambda_j w_j$ tels que

(*a*) les λ_j sont entiers et tous de même parité,

(*b*) $\sum_{1 \leqslant j \leqslant \omega} \lambda_j$ est multiple de 4.

Démontrer que Λ_ω est un réseau de $\mathbb{Q}^\omega$, et que $\Lambda_\omega^\circ = \Lambda_\omega$.

III.A.5. Soit L un réseau de $\mathbb{Q}^\omega$. Démontrer qu'il existe des entiers $d \geqslant 1$ tels que pour tout v dans L on ait $d(v.v) \in \mathbb{N}$. On note d_L le plus petit de ces entiers. Pour tout entier naturel k, on note $c_k(L)$ le nombre de vecteurs de L de carré scalaire (k/d_L). Démontrer que la série $\sum_{k=0}^{\infty} c_k(L)\, e^{\pi i k z}$ est convergente lorsque z appartient au demi-plan supérieur ouvert du plan de Cauchy (on rappelle que si $\zeta = a + ib$ est un nombre complexe, a et b étant réels, on pose $e^\zeta = e^a(\cos b + i \sin b)$).

On pose

$$\theta_L(z) = \sum_{k=0}^{\infty} c_k(L)\, e^{\pi i k z / d_L}.$$

On a ainsi

$$\theta_L(z) = \sum_{v \in L} e^{\pi i (v.v) z}.$$

III.B. Codes et réseaux

III.B.1. Démontrer qu'il existe une base orthogonale $(v_1, v_2, \ldots, v_\omega)$ de $\mathbb{Q}^\omega$ telle que pour tout $j \in \{1, 2, \ldots, \omega\}$ on ait $v_j \cdot v_j = 1/2$.

On choisit une telle base, et on désigne dorénavant par R le réseau qu'elle engendre.

III.B.2. Vérifier que les $\mathbb{Z}$-bases orthogonales de R ont toutes même ensemble image par la surjection canonique de R sur R / 2R.

On note Ω l'ensemble image d'une $\mathbb{Z}$-base orthogonale de R dans R / 2R.

III.B.3. On désigne par $\bar{v}$ l'image de $v \in$ R dans R / 2R. Le groupe R / 2R est muni d'une structure naturelle d'espace vectoriel sur le corps à deux éléments $\mathbb{Z}/2\mathbb{Z}$. On munit cet espace de la forme bilinéaire symétrique β définie par $\beta(\bar{v}, \bar{w}) = \overline{2v \cdot w}$. Vérifier que l'espace vectoriel R / 2R muni de la forme bilinéaire β est canoniquement isomorphe à $\mathcal{P}(\Omega)$ muni de la forme bilinéaire naturelle α.

On identifie dorénavant R / 2R et $\mathcal{P}(\Omega)$.

III.B.4. Soit $\mathcal{C}$ un code de $\mathcal{P}(\Omega)$. On désigne par $L(\mathcal{C})$ l'image réciproque de $\mathcal{C}$ par la surjection canonique de R sur R / 2R = $\mathcal{P}(\Omega)$. Vérifier que $L(\mathcal{C})$ est un réseau de $\mathbb{Q}^\omega$. Démontrer que $L(\mathcal{C})^\circ = L(\mathcal{C}^\circ)$,
et que $\mathrm{vol}(L(\mathcal{C})) = 2^{(\omega/2) - \dim(\mathcal{C})}$.

On dit que deux réseaux L et L′ de $\mathbb{Q}^\omega$ sont isomorphes s'il existe une isométrie τ de $\mathbb{Q}^\omega$ telle que $\tau(L) = L'$. Si deux codes $\mathcal{C}$ et $\mathcal{C}'$ sont isomorphes, les réseaux $L(\mathcal{C})$ et $L(\mathcal{C}')$ sont isomorphes.

III.B.5. Soit $\mathcal{A}$ un élément de l'ensemble $\Gamma(\Omega)$ [voir I.B.2.]. Démontrer que $L(\mathcal{A})$ est isomorphe à $\mathbb{Z}^\omega$.

★III.B.6. On suppose ω multiple de 4. Démontrer que le réseau Λ_ω défini en III.A.4. contient un réseau isomorphe à 2R. Démontrer que Λ_ω est isomorphe à $L(\mathcal{B}_\omega)$, et que si ω est multiple de 8 les carrés scalaires des vecteurs de Λ_ω sont tous pairs.

III.B.7. Pour z parcourant le demi-plan supérieur ouvert du plan de Cauchy, on pose

$$\varphi_2(z) = 2 \sum_{k=0}^{\infty} e^{2\pi i \left(k + \frac{1}{2}\right)^2 z} \quad \text{et} \quad \varphi_3(z) = 1 + 2 \sum_{k=1}^{\infty} e^{2\pi i k^2 z}.$$

Soit $\mathcal{C}$ un code de $\mathcal{P}(\Omega)$. Démontrer que

$$\theta_{L(\mathcal{C})}(z) = P_{\mathcal{C}}(\varphi_2(z), \varphi_3(z)).$$

RAPPORT SUR L'EPREUVE DE MATHEMATIQUES GENERALES

Certains résultats fondamentaux de la «nouvelle» théorie des «codes linéaires correcteurs d'erreurs» ont servi de support à ce problème, dont l'ambition était simplement de faire travailler les candidats sur des parties variées du programme d'algèbre : combinatoire et algèbre linéaire élémentaire en caractéristique 2 dans la première partie ; polynômes, groupes finis et algèbre linéaire pour la démonstration, dans un cas concret, d'un résultat de la «vieille» théorie des invariants dans la seconde partie ; résultats élémentaires sur les réseaux et étude de quelques exemples non triviaux dans la troisième partie.

Un «code linéaire» est tout simplement un sous-espace vectoriel de $(\mathbf{F}_q)^n$ «repéré» dans la base canonique de $(\mathbf{F}_q)^n$; les questions sur les codes linéaires concernent essentiellement ce repérage, et en particulier le nombre de coordonnées non nulles d'un vecteur du code. C'est pourquoi on associe, à tout code $\mathscr{C}$ de $(\mathbf{F}_q)^n$, le polynôme $P_{\mathscr{C}}(X, Y) = \sum_{0 < k < n} a_k X^k Y^{n-k}$, où a_k désigne le nombre de vecteurs de $\mathscr{C}$ qui ont k coordonnées non nulles sur la base canonique de $(\mathbf{F}_q)^n$.

La formule de Mac-Williams, reliant le polynôme $P_{\mathscr{C}^\circ}(X, Y)$ au polynôme $P_{\mathscr{C}}(X, Y)$ (cf. I. B. 4) permet d'utiliser la théorie des invariants pour trouver des conditions nécessaires non triviales afin qu'un polynôme homogène de $\mathbf{Z}[X, Y]$ puisse être le polynôme associé à un code auto-orthogonal (cf. II. B. 6).

Il est intéressant de noter les analogies entre cette partie de la théorie des codes et certains aspects de la théorie des réseaux. En partant de la construction exposée en III.B., on peut par exemple interpréter le polynôme des poids comme la «traduction» de la fonction thêta, et la formule de Mac-Williams comme la «traduction» de la formule de Poisson.

Il ne peut évidemment être question, dans le cadre d'un tel rapport, de donner une copie «modèle». Essayons simplement de donner quelques conseils aux candidats futurs. Un coup d'œil sur les statistiques des notes indique que 20 % des concurrents ont une note $n < \frac{5}{60}$, et 40 % une note $< \frac{10}{60}$. Ces résultats sont frappants, surtout si l'on remarque que le problème de 1978 était plus facile que les précédents.

Il faut donc faire comprendre que le grappillage de points, véritable miroir aux alouettes, se révèle toujours peu payant. Des questions très simples ne figuraient dans l'énoncé qu'à titre d'indications conduisant aux véritables problèmes (par exemple I.A.1 à I.A.3, II.A.1 et II.B.1). La résolution correcte de ces exercices faciles, même remplissant une ou deux copies, ne donnait guère de points. Il va de soi, au contraire, que les démonstrations demandées en I.B.4., II.A.4 ou III.A.3., qui pouvaient être conduites après une étude rapide des questions faciles qui les entouraient, étaient beaucoup plus rentables. Il semble donc raisonnable de conseiller aux agrégatifs, après une lecture soignée de l'ensemble du sujet pendant une dizaine de minutes (ce qui éclaire souvent le sens des premières questions), de préparer brièvement la résolution des parties qui leur paraissent accessibles et de consacrer, par exemple, la deuxième et la troisième heure de l'épreuve à essayer de résoudre quelques questions visiblement plus intéressantes. La seconde partie des six heures commençant par une rédaction aussi précise que possible des résultats déjà acquis, pourra se terminer par de nouvelles tentatives sur des points difficiles. Une organisation rationnelle du temps, faisant alterner les périodes de recherche tendue et les «repos» relatifs (mises au point), permet de mieux utiliser un capital en réalité assez court : tous ceux qui s'acharnent de manière désordonnée, qui écrivent au fil de la plume sans méthode, le savent bien qui se retrouvent épuisés, plus par leur débauche d'énergie incontrôlée que par les difficultés réelles du problème...

Ajoutons deux remarques complémentaires. Si les résultats démontrés dans d'autres parties non triviales montrent une capacité technique honorable, il est parfaitement permis à un candidat de se contenter d'énoncer, dans les questions de routine, ceux des résultats qui lui paraissent évidents — par exemple du niveau d'une terminale — et de prouver uniquement les points qui exigent un peu plus qu'une vérification mécanique.(Par exemple, dans le I.A.1., seule l'associativité faisait réellement problème si l'on attaquait la question «à la main» ; autre exemple : l'isomorphisme de la fin du I.B.2 ne pouvait être simplement qualifié d'«évident» ; mais une remarque simple sur le cardinal de l'ensemble des paires et l'affirmation du caractère disjoint de celles-ci suffisait, dans une copie convenable par ailleurs, pour obtenir le maximum pour ce point). Le jury est toujours sensible à une concision de bon aloi qui prouve que l'on sait aller à l'essentiel.

Enfin il reste à attirer vigoureusement l'attention des candidats sur une notion morale : l'honnêteté intellectuelle. Certains comptent visiblement sur la lassitude des correcteurs pour bluffer de manière inadmissible, écrivant à peu près n'importe quel calcul qui se termine de manière abrupte par ... le bon résultat. Il est certain qu'un petit nombre d'entre eux peuvent, par chance, tromper ainsi le jury et voler quelques points. Il faut quand même savoir que la probabilité en est faible ; la double correction élimine la plus grande partie des coups de bluff qui auraient échappé au premier examinateur ; il faut également savoir que le poker est un art difficile, car de multiples indices (symétrie, homogénéité entre autres) permettent souvent de repérer le caractère frauduleux d'un «calcul» sans en avoir nécessairement testé chaque ligne. Enfin, la copie d'un candidat convaincu de malhonnêteté en un endroit sera évidemment lue par ailleurs avec une rigueur maximum et des points seront refusés systématiquement si le texte risque de présenter des obscurités ou des négligences. Le jeu n'en vaut donc pas la chandelle. Espérons donc voir régresser de telles pratiques.

Pour conclure, c'est avec quelque pessimisme que le jury se croit obligé de signaler, encore une fois, toujours en vain semble-t-il, que l'Agrégation est aussi un concours pédagogique ; redisons donc très vite que le respect des marges, l'encadrement des résultats, la séparation des étapes d'un raisonnement, des différentes questions d'une partie, sont toujours souhaitables, à défaut de nécessaires... *A fortiori,* faut-il encore réclamer une écriture lisible, des ratures franches plutôt que des mots surchargés, une orthographe correcte dans les mots usuels ? S'il est vrai que tout ceci peut paraître du détail et n'est pas officiellement comptabilisé dans la note, les candidats doivent savoir qu'il en résulte une impression d'ensemble qui, dans les cas de doute où il faut trancher un dilemne, peut servir un candidat qui, au moins, sait faire preuve ainsi d'un esprit clair et méthodique. L'utilité de cette qualité pour un mathématicien n'est évidemment pas à démontrer.

Répartition des notes

Notes	Nombre de candidats
0	42
1 – 4	359
5 – 8	309
9 – 12	364
13 – 16	316
17 – 20	256
21 – 24	178
25 – 28	103
29 – 32	40
33 – 36	46
37 – 40	22
41 – 48	15
49 – 60	7