I.3.5. AFFECTATIONS DES AGREGES 1975

Sur les 125 candidats et 87 candidates français admis :

53+ 19... feront une année supplémentaire dans une E.N.S. ;

6+ 11... ont été maintenus ou détachés dans l'enseignement supérieur ;

8+ 2... ont obtenu des chaires préparatoires aux Grandes Ecoles ;

26+ 18... ont obtenu des chaires de TC, TE ou TS dans les lycées ;

1+ 1... ont été nommés dans des Ecoles normales d'instituteurs ;

17+ 19... ont été nommés sur des chaires ordinaires de lycées ou de c.e.s. ;

13+ 3... sont partis en coopération ou au service national ;

1+ 14... suivront un stage de formation professionnelle.

II - ÉPREUVES ÉCRITES

II.1 TEXTE DE L'EPREUVE DE MATHEMATIQUES GENERALES

DURÉE : 6 heures

La partie I est indépendante des deux suivantes

I

n étant un élément de $\mathbf{N}^*$ (entier naturel non nul), on note $(\pi_1, \pi_2, \ldots, \pi_n)$ la base canonique de l'espace vectoriel $\mathbf{Q}^n$. La matrice d'une forme quadratique $\bar{q}$ relative à cette base est appelée matrice canonique de $\bar{q}$; $\bar{q}$ est dite positive si $\bar{q}(x) \geqslant 0$ pour tout x.

$\mathrm{M}_n(\mathbf{Q})$ (resp. $\mathrm{M}_n(\mathbf{Z})$) est l'algèbre des matrices carrées d'ordre n à coefficients dans $\mathbf{Q}$ (resp. $\mathbf{Z}$). $\mathrm{GL}_n(\mathbf{Q})$ (resp. $\mathrm{GL}_n(\mathbf{Z})$) est le groupe multiplicatif des matrices inversibles de $\mathrm{M}_n(\mathbf{Q})$ (resp. inversibles de $\mathrm{M}_n(\mathbf{Z})$). I est la matrice unité de $\mathrm{M}_n(\mathbf{Q})$. ${}^t\mathrm{M}$ (resp. det M) est la transposée (resp. le déterminant) de la matrice M. Dans cette première partie, n ne prend que les valeurs 2 et 3.

1° Soit $\bar{q}$ une forme quadratique de $\mathbf{Q}^2$, de matrice canonique $\mathrm{M} = \begin{bmatrix} u & v \\ v & w \end{bmatrix} \in \mathrm{GL}_2(\mathbf{Z})$. On pose $\delta = \det \mathrm{M}$. Montrer que, si $\bar{q}$ est non dégénérée, positive, alors $\delta = 1$.

2° On suppose toujours $\mathrm{M} \in \mathrm{GL}_2(\mathbf{Z})$ et, pour cette question et la suivante : $\delta = 1$. Montrer que l'une des deux formes $\bar{q}$ ou $-\bar{q}$ est non dégénérée, positive.

3° *a.* Admettant ici que $\bar{q}$ est non dégénérée, positive, démontrer, pour $u \neq 1$, l'existence d'une matrice $\mathrm{P} = \begin{bmatrix} -s & 1 \\ 1 & 0 \end{bmatrix} \in \mathrm{GL}_2(\mathbf{Z})$ telle que, si $\mathrm{M}' = {}^t\mathrm{PMP} = \begin{bmatrix} u' & v' \\ v' & w' \end{bmatrix}$, alors $0 < u' \leqslant \frac{u}{2}$.

b. En déduire l'existence de $\mathrm{N} \in \mathrm{GL}_2(\mathbf{Z})$ telle que $\mathrm{M} = {}^t\mathrm{NN}$. Énoncer une propriété relative à la décomposition de $\bar{q}$ en somme de deux carrés.

4° Jusqu'à la fin de cette première partie, $\bar{q}$ désigne une forme quadratique de $\mathbf{Q}^3$, non dégénérée, positive, dont la matrice canonique

$$M = \begin{bmatrix} m & p & q \\ p & m' & r \\ q & r & m'' \end{bmatrix}$$

est un élément de $GL_3(\mathbf{Z})$.

Que peut-on dire des signes de m, m', m'' et det M?

Montrer que, si M n'est pas égale à I, l'une des six inégalités suivantes est vérifiée :

$$|p| > \frac{m}{2}, |p| > \frac{m'}{2}, |q| > \frac{m}{2}, |q| > \frac{m''}{2}, |r| > \frac{m'}{2}, |r| > \frac{m''}{2}.$$

(on pourra séparer le cas $m = m' = m''$, puis le cas $m \geqslant m' \geqslant m''$, $m > m''$).

5° *a.* Déterminer une matrice triangulaire $P \in GL_3(\mathbf{Z})$ telle que $M_1 = {}^tPMP$ soit de même type que M, avec :

$$m_1 = m, \quad m'_1 \leqslant m' - 1, \quad m''_1 = m''.$$

b. En déduire l'existence de $N \in GL_3(\mathbf{Z})$ telle que $M = {}^tNN$.

Énoncer une propriété relative à la décomposition de q en somme de trois carrés.

c. Application numérique : $M = \begin{bmatrix} 5 & 0 & 3 \\ 0 & 1 & 1 \\ 3 & 1 & 3 \end{bmatrix}$ (on se limitera à exhiber une matrice N).

6° Donner un exemple de matrice $M \in GL_3(\mathbf{Z})$, telle que ${}^tM = M$, que det $M = 1$ et qu'il n'existe aucune matrice $N \in GL_3(\mathbf{Z})$ vérifiant $M = {}^tNN$ (un exemple à coefficients dans $\mathbf{N}^*$ serait apprécié).

7° Retrouver les résultats de la question 3° à partir de ceux du 5°. Comparer les deux méthodes.

II

V est un espace vectoriel de dimension n sur $\mathbf{Q}$; H, H' ..., sont, par convention, des sous-groupes additifs de V (confondus, selon l'usage, avec les ensembles sous-jacents). $\mathcal{H}_0 = \mathrm{Hom}(H, \mathbf{Z})$ est l'ensemble des morphismes de groupe de H vers $\mathbf{Z}$. $\hat{H}$ est le sous-espace vectoriel de V engendré par H. La somme $H + H'$ est le sous-groupe de V engendré par $H \cup H'$. Pour $\lambda \in \mathbf{Q}$, λH est l'image de H par l'homothétie de rapport λ.

Une $\mathbf{Z}$-base de H est une famille libre de vecteurs de V telle qu'un vecteur de V appartient à H si, et seulement s'il est combinaison linéaire à coefficients entiers relatifs des vecteurs de la famille. Un réseau est un sous-groupe de V admettant au moins une $\mathbf{Z}$-base de cardinal n. L, L' ..., sont, par convention, des réseaux de V. Un sous-réseau est un réseau d'un sous-espace vectoriel de V.

1° Démontrer que $\hat{L} = V$.

2° $\mathcal{B} = (e_i)_{1 \leqslant i \leqslant p}$ étant une famille finie de vecteurs de V, on note B la matrice des coordonnées des vecteurs e_i, $(1 \leqslant i \leqslant p)$, dans une base (ω_j), $(1 \leqslant j \leqslant n)$, de V considérée comme fixe dans tout le problème : B est appelée matrice canonique de $\mathcal{B}$. Montrer que, B et B' étant les matrices canoniques d'une $\mathbf{Z}$-base $\mathcal{B}$ de L et d'une famille finie $\mathcal{B}'$ de vecteurs de L, $\mathcal{B}'$ est une $\mathbf{Z}$-base de L si, et seulement s'il existe $P \in GL_n(\mathbf{Z})$ telle que $B' = BP$. Montrer que le rationnel vol $L = |\det B|$ est indépendant du choix d'une $\mathbf{Z}$-base de L.

3° L' étant un réseau de V, montrer qu'il existe $d \in \mathbf{N}^*$ tel que $dL' \subset L$ et que $d^n \left(\frac{\text{vol } L'}{\text{vol } L} \right)$ est entier.

4° H étant un sous-groupe de L non réduit à $\{0\}$, montrer que H est un sous-réseau de V (on pourra, par exemple, considérer une $\mathbf{Z}$-base (e_i) de L, rechercher un élément a de $\mathbf{N}^*$, une application coordonnée ψ, un vecteur b tel que $\psi(b) = a$ et utiliser l'endomorphisme θ de H défini par :

$$\theta(x) = x - \frac{\psi(x)}{a} b . \Big)$$

5° Montrer que l'intersection et la somme de deux réseaux de V sont des réseaux.

6° X et Y étant les matrices canoniques de deux vecteurs x et y de V, on note $(x \mid y) = {}^tXY$ (produit de x et de y), et $\| x \|^2 = {}^tXX$ (carré de x). Une partie A de V est dite bornée s'il existe un rationnel $\mathcal{A}$ tel que $\| x \|^2 \leqslant \mathcal{A}$ pour tout $x \in A$. Montrer que tout sous-groupe H de V dont l'intersection avec toute partie bornée de V est finie est un sous-réseau de V (on pourra considérer une famille libre maximale $(h_1, \ldots, h_r)$ de vecteurs de H, la partie Ω de V formée des vecteurs $\sum_{i=1}^{r} \mu_i h_i$, $\mu_i \in \mathbf{Q} \cap [0, 1]$, et associer au vecteur $\sum_{i=1}^{r} \lambda_i h_i$, $\lambda_i \in \mathbf{Q}$, le vecteur

$\sum_{i=1}^{r} (\lambda_i - [\lambda_i]) h_i$, où le symbole [ ] représente la partie entière).

Démontrer la réciproque.

III

H étant un sous-groupe de V, on note H_0 l'ensemble des $x \in V$ tels que, pour tout $y \in H$, on ait $(x \mid y) \in \mathbf{Z}$. Un réseau L est dit r-modulaire (resp. unimodulaire) si $L_0 = rL$ (resp. $L_0 = L$); il est dit r-modulaire trivial s'il existe une $\mathbf{Z}$-base (e_i) de L orthogonale (c'est-à-dire vérifiant $(e_i \mid e_j) = 0$ pour $i \neq j$) et telle que $\| e_i \|^2 = \frac{1}{r}$ pour tout i ($\frac{1}{r}$ s'appelle alors le carré de la $\mathbf{Z}$-base; cette dernière est dite orthonormale si $r = 1$). $\mathbf{F}_2$ est le corps à deux éléments.

1° *a.* Démontrer que, si L est un réseau de V, $\mathfrak{L}_0 = \mathrm{Hom}\,(L, \mathbf{Z})$ est un réseau d'un certain espace vectoriel W de dimension n sur $\mathbf{Q}$ (on pourra utiliser la famille (e_i^0) de $\mathfrak{L}_0$ définie par $e_i^0(e_j) = \delta_{ij}$).

b. Définir un isomorphisme α du groupe L_0 sur $\mathfrak{L}_0$, indépendant de tout choix de $\mathbf{Z}$-base de L. En déduire que L_0 est un réseau de V, dont on explicitera une $\mathbf{Z}$-base à partir d'une $\mathbf{Z}$-base de L.

2° L et L′ étant deux réseaux de V, démontrer les égalités :

$$L_{00} = L, \quad (L + L')_0 = L_0 \cap L'_0, \quad (L \cap L')_0 = L_0 + L'_0,$$
$$(\mathrm{vol}\ L)(\mathrm{vol}\ L_0) = 1.$$

Calculer vol L dans le cas où L est r-modulaire.

3° On suppose jusqu'à la fin de cette partie que L est un réseau r-modulaire trivial. Montrer que L est r-modulaire, et qu'il existe une « similitude directe » (notion que l'on définira par analogie avec la structure euclidienne de $\mathbf{R}^n$) transformant le réseau fondamental Λ, sous-groupe engendré par la base canonique (ω_i) de V, en L.

4° *a.* On note Aut L l'ensemble des morphismes de groupe s de L dans lui-même tels que $(s(x) \mid s(y)) = (x \mid y)$ pour tout couple (x, y) de L^2. On considère une $\mathbf{Z}$-base (e_i) de L, orthogonale et de carré $\frac{1}{r}$. À tout élément s de Aut L, on associe la matrice S des coordonnées des vecteurs $e'_i = s(e_i)$ dans la $\mathbf{Z}$-base (e_i). Montrer qu'il existe un élément k de S_n (groupe des permutations de $[1, n]$) et une application ε de $[1, n]$ dans $\{-1, +1\}$ tels que l'élément (i, j) de S s'écrive sous la forme $s_{ij} = \varepsilon(j)\,\delta_{i,\,k(j)}$. Calculer le cardinal de Aut L.

b. Étudier l'ensemble U des $s \in$ Aut L auxquels on peut associer une application f de $[1, n]$ dans $\{-1, +1\}$ telle que l'élément (i, j) de S s'écrive $s_{ij} = f(i)\,\delta_{i,\,j}$; un tel s sera noté s_f. Comparer U et le groupe $(\mathbf{F}_2^n, +)$.

c. Étudier l'ensemble T des $s \in$ Aut L tels que, $k \in S_n$ étant défini comme en *a.* l'élément (i, j) de S s'écrive $s_{ij} = \delta_{i,\,k(j)}$; un tel s sera noté s_k.

Comparer T et le groupe $(S_n, \circ)$.

5° *a.* Montrer que tout $s \in$ Aut L se décompose, de manière unique, sous la forme $s = s_f \circ s_k$, $(s_f, s_k) \in U \times T$.

b. Déterminer un morphisme φ de T dans le groupe Aut U des automorphismes de groupe de U tel que $U \times T$, muni de la loi :

$$(s_f, s_k) \square (s_{f'}, s_{k'}) = (s_f \circ \varphi(s_k)(s_{f'}), s_k \circ s_{k'})$$

soit isomorphe à Aut L, muni de la loi $\circ$.

6° Déterminer une loi $*$ sur le produit cartésien $\mathbf{F}_2^n \times S_n$ telle qu'il existe un isomorphisme θ de ce produit sur Aut L. Caractériser, par analogie avec φ, un morphisme F de S_n dans le groupe linéaire de dimension n sur $\mathbf{F}_2$, en calculant la matrice de $F(k)$ relative à la base canonique de $\mathbf{F}_2^n$.

IV

On définit dans V les isométries (resp. les rotations), et les groupes matriciels correspondants $O_n(\mathbf{Q})$ (resp. $O_n^+(\mathbf{Q})$) par analogie avec les notions similaires des espaces euclidiens réels. Σ_n est l'ensemble des entiers m de la forme $m = \alpha_1^2 + \ldots + \alpha_n^2$, $\alpha_i \in \mathbf{Z}$.

1° Dans toute cette partie, L est un réseau unimodulaire de V. (e_i) étant une $\mathbf{Z}$-base quelconque de L, de matrice canonique B, on considère l'automorphisme λ de V de matrice canonique B, et la forme quadratique $\bar{q}$ définie par $\bar{q}(x) = \| \lambda(x) \|^2$. Que peut-on dire de la matrice canonique M de $\bar{q}$? de l'image $\bar{q}(\Lambda)$ du réseau fondamental Λ par $\bar{q}$?

2° Dans les questions suivantes (jusqu'à IV 5° incluse), on suppose $n = 3$. Montrer que $\bar{q}(\Lambda) = \Sigma_3$.

3° Démontrer que L est unimodulaire trivial. Caractériser, à l'aide des ensembles $O_3^+(\mathbf{Q})$ et $GL_3(\mathbf{Z})$, les matrices canoniques des $\mathbf{Z}$-bases des réseaux unimodulaires de V. Comment obtient-on ces réseaux à partir de Λ?

4° Résoudre l'équation matricielle ${}^tKK = {}^tBB$, où $K \in GL_3(\mathbf{Z})$ et B est définie au IV 1°. Dénombrer les solutions.

5° Si L′ est un réseau de V tel que $L' \subset L'_0$, démontrer l'existence d'un réseau unimodulaire trivial L tel que $L' \subset L \subset L'_0$ (on pourra considérer $(\Lambda + L') \cap L'_0$).

6° Indiquer brièvement ce que deviennent les questions précédentes pour $n = 2$.

V

$\mathbf{F}_p$ est le corps à p éléments (p : entier naturel premier). La notation p.g.c.d. (x, y, z) représente le plus grand commun diviseur, nécessairement positif, des entiers (x, y, z).

1° Démontrer que le triplet $(x, y, z) \in \mathbf{N}^3$ est solution de l'équation

$$x z - y^2 = 1$$

si, et seulement s'il existe $(a, b, c, d) \in \mathbf{Z}^4$ tels que :

$$ad - bc = 1\,, \quad a^2 + b^2 = x\,, \quad 0 \leqslant ac + bd = y\,, \quad c^2 + d^2 = z\,.$$

2° Démontrer que l'équation $x^2 + 1 = 0$ n'a de solutions dans $\mathbf{F}_p$ que si, et seulement si $p \in \Sigma_2$. Montrer qu'alors ou bien $p = 2$, ou bien il existe $q \in \mathbf{N}$ tel que $p = 4q + 1$.

3° S'il existe $q \in \mathbf{N}$ tel que $p = 4q + 1$ soit premier, démontrer (par exemple à l'aide du groupe multiplicatif de $\mathbf{F}_p$) que p divise $[(2q)!]^2 - (p-1)!$ et $[(2q)!]^2 + 1$. En déduire les éléments de Σ_2 qui sont des nombres premiers.

4° Donner une condition nécessaire et suffisante, portant sur la parité des exposants des diviseurs premiers d'un entier m, pour que $m \in \Sigma_2$. En déduire que, si $\bar{q}$ est la forme quadratique définie en IV 1°, pour $n = 2$, et si x et y sont des vecteurs de Λ tels que $\bar{q}(y)$ divise $\bar{q}(x)$, il existe alors $z \in \Lambda$ tel que $\bar{q}(x) = \bar{q}(y)\,\bar{q}(z)$.

La propriété analogue serait-elle vraie pour $n = 3$? (considérer par exemple le nombre 7.)

5° *a.* Soit m un entier; démontrer que l'équation

$$x^2 + y^2 = mz^2$$

n'a de solution $(x, y, z) \in \mathbf{N}^3$ autre que $(0, 0, 0)$ que si, et seulement si $m \in \Sigma_2$. Déterminer alors toutes les solutions $(x, y, z) \in \mathbf{Q}^3$.

b. En déduire que l'équation :

$$\begin{vmatrix} 1 & p & q \\ p & 1 & r \\ q & r & 1 \end{vmatrix} = 1\,, \qquad (p, q, r) \in \mathbf{Z}^3$$

n'admet que la solution $(0, 0, 0)$ (on pourra poser, par exemple, $m = p^2 - 1$).

6° *a.* Déduire des relations :

$$(x, y, z, t) \in \mathbf{N}^{*4}\,, \quad \text{p.g.c.d. } (x, y, z) = 1\,, \quad xz = y^2 + t^2$$

que x et tous les diviseurs premiers qui figurent dans x à une puissance impaire appartiennent à Σ_2.

b. Démontrer qu'il existe alors $B' \in GL_2(\mathbf{Q})$, $P \in M_2(\mathbf{Z})$, $N \in GL_2(\mathbf{Z})$ telles que :

$$M = \begin{bmatrix} x & y \\ y & z \end{bmatrix} = {}^tB'B' = {}^t(NP)NP.$$

7° Démontrer que le quadruplet $(x, y, z, t) \in \mathbf{N}^4$ est solution de l'équation $xz = y^2 + t^2$, $t \neq 0$ si, et seulement s'il existe $(a, b, c, d, \delta) \in \mathbf{Z}^5$ tels que :

$$x = \delta(a^2 + b^2)\,, \quad y = \delta(ac + bd)\,, \quad z = \delta(c^2 + d^2)\,, \quad t = \delta(ad - bc) \neq 0,$$

δ étant le produit des nombres premiers p de la forme $4q + 3$ figurant dans x avec un exposant impair.

8° $M = \begin{bmatrix} x & y \\ y & z \end{bmatrix}$ étant une matrice de $GL_2(\mathbf{Q})$, démontrer qu'il existe $A \in M_2(\mathbf{Z})$ telle que $M = {}^tAA$ si, et seulement si $(x, y, z) \in \mathbf{Z}^3$, $\sqrt{xz - y^2} \in \mathbf{N}^*$, $x \in \Sigma_2$.

Examiner le cas où $M \in M_2(\mathbf{Q})$, $\det M = 0$.

9° ω appartenant à $\mathbf{Z}$, démontrer que le quadruplet $(x, y, z, t) \in \mathbf{Z}^4$ est solution de l'équation

$$xz = y^2 + \omega t^2$$

si, et seulement s'il existe $(\alpha, \beta, \gamma, \delta, g, p, q) \in \mathbf{Z}^7$ tel que :

$\omega = \alpha\gamma - \beta^2$, $x = d(\alpha p^2 + 2\beta pq + \gamma q^2)$, $y = dg(\beta p + \gamma q)$, $z = d g^2 \gamma$, $t = dgp$.

(On pourra par exemple se ramener au cas où p.g.c.d. $(t, y) = 1$, en posant : d = p.g.c.d. (x, y, z, t), $d\Delta$ = p.g.c.d. (t, y), $d\delta$ = p.g.c.d. $(d\Delta, x)$ et en exprimant y en fonction de t et z).

En déduire que le quadruplet $(x, y, z, t) \in \mathbf{Z}^4$ est solution de l'équation

$$xz = y^2 + t^2$$

si, et seulement s'il existe $(a, b, c, d, \delta) \in \mathbf{Z}^5$ tels que

$x = \delta(a^2 + b^2)$, $y = \delta(ac + bd)$, $z = \delta(c^2 + d^2)$, $t = \delta(ad - bc)$.

II.2 RAPPORT SUR L'EPREUVE DE MATHEMATIQUES GENERALES

II.2.1. THEME DU SUJET

L'équation $xz - y^2 = t^2$, $(x, y, z, t) \in \mathbf{Z}^4$, possède plusieurs interprétations intéressantes. Elle correspond d'une part à la recherche des diviseurs des entiers de la forme $(y^2 + t^2)$; elle est donc liée à l'étude de l'ensemble Σ_2 des nombres de ce type. D'autre part, toute égalité matricielle de la forme :

$$M = \begin{bmatrix} x & y \\ y & z \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} a & c \\ b & d \end{bmatrix} = {}^t NN,$$

donne les solutions particulières :

$$x = a^2 + b^2,\ z = c^2 + d^2,\ y = ac + bd,\ t = ad - bc$$

solutions que redonne immédiatement l'identité de Lagrange. Ce qui est assez remarquable, c'est que ces solutions particulières sont, en quelque sorte, les seules. Le problème de mathématiques générales de l'agrégation 1975 demandait, en effet, de démontrer que la solution générale de cette équation était de la forme :

$$x = \delta(a^2 + b^2),\ y = \delta(ac + bd),\ z = \delta(c^2 + d^2),\ t = \delta(ad - bc)$$

avec $(a, b, c, d, \delta) \in \mathbf{Z}^5$ — on peut même choisir δ de telle façon qu'aucun diviseur de δ n'appartienne à Σ_2. Ce résultat peut être interprété de la manière suivante : pour qu'une matrice de $M_2(\mathbf{Q})$ puisse s'écrire sous la forme $M = {}^t AA$,

où $A \in M_2(\mathbf{Z})$, il faut et suffit que $(x, y, z, \sqrt{xz - y^2}) \in \mathbf{Z}^4$, $x \in \Sigma_2 - \{0\}$ ou $(x = y = 0, z \in \Sigma_2)$.

● On peut obtenir ces résultats de manière très rapide, purement arithmétique, à l'occasion de l'étude de l'équation plus générale $xz - y^2 = \omega t^2$; la toute dernière question du problème, indépendante de ce qui précède, permettait de résoudre cette équation par la méthode de L.E. Dickson, dans son *«Introduction to the theory of numbers»*. Aussi bien le problème cité ci-dessus n'avait pas essentiellement pour but d'aboutir à une résolution assez banale, mais plutôt d'inviter les candidats à quelques excursions dans les domaines connexes des matrices à coefficients entiers — ici, symétriques et d'ordres 2 ou 3 —, des réseaux — c'est-à-dire des groupes abéliens libres de type fini — et des équations diophantiennes du second degré. Notons que l'on pouvait traiter intégralement ce problème en ne sortant pas de $\mathbf{Q}$ et $\mathbf{Z}$; on sait qu'il est assez rare que des résultats d'arithmétique ne fassent peu ou prou, appel à $\mathbf{R}$, voire à $\mathbf{C}$ ou à la clôture algébrique de $\mathbf{Q}$, mais les résultats rassemblés par l'énoncé étaient à la vérité assez triviaux. Seul le fait de les réunir par le fil conducteur de l'équation $xz - y^2 = t^2$ leur donnait un certain intérêt.

● Le point le moins simple de l'étude de Σ_2 est certainement le fait qu'il est équivalent, pour un nombre premier p, d'appartenir à Σ_2 ou de déterminer un corps fini à p éléments où le polynôme X^2+1 est réductible. Ce point résulte ici très simplement du théorème selon lequel toute matrice de $M_2(\mathbf{Z})$ de déterminant 1 est (à une multiplication par — 1 près) de la forme ${}^t NN$, $N \in GL_2(\mathbf{Z})$; un algorithme de recherche de N est même proposé par le texte. Que les conditions précédentes soient équivalentes à $(p = 2$ ou $p = 4q + 1)$ résulte du théorème de Wilson $((p - 1)! \equiv -1\ [p])$ et de la congruence : $(2q)!^2 \equiv (4q)!\ [4q + 1]$. Parmi les propriétés de Σ_2, certaines sont très connues ; ainsi le fait qu'un nombre appartienne à Σ_2 si et seulement si tous ses diviseurs premiers de la forme $(4q + 3)$ y figurent avec un exposant pair, et le fait que le produit de deux éléments de Σ_2 est encore une somme de deux carrés. Une réciproque partielle, due à Lagrange, est moins connue : si le quotient de deux éléments de Σ_2 est entier, il est lui-même somme de deux carrés. Le théorème analogue est faux pour Σ_3

$\left(7 = \dfrac{1^2 + 2^2 + 3^2}{0^2 + 1^2 + 1^2} \notin \Sigma_3\right)$, mais évidemment exact pour Σ_4, car $\Sigma_4 = \mathbf{N}$.

● Une partie importante du problème concernait les réseaux, sous-groupes de

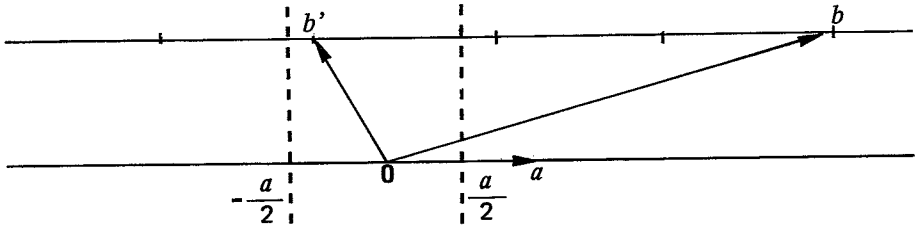
$\mathbf{Q}^n$ engendrés par une base de $\mathbf{Q}^n$. L étant un tel réseau on note L_0 l'ensemble des $x \in \mathbf{Q}^n$ tels que

$$\forall\, y \in \mathrm{L}\ ,\ (x \mid y) \in \mathbf{Z}.$$

Un réseau modulaire, c'est-à-dire tel que $\mathrm{L}_0 = \mathrm{L}$, peut être construit à partir de $\Lambda = \mathbf{Z}^n$ par une similitude directe quelconque. Pour $n \leqslant 3$, la réciproque est exacte. C'est ce résultat qui est utilisé dans la résolution de l'équation $xz - y^2 = t^2$, équation plus délicate que $xz - y^2 = 1$. Le rapport entre matrices et réseaux est clair ; notons que si B est la matrice de l'une des $\mathbf{Z}$–bases du réseau L, ${}^t\mathrm{B}^{-1}$ est celle de L_0, ce qui explique le lien entre matrices orthogonales et réseaux unimodulaires. Pour cette étude, il est nécessaire de connaître quelques propriétés des réseaux, concernant les sous-réseaux, (dont le théorème équivalant au résultat bien connu selon lequel tout sous-groupe de $\mathbf{Z}^n$ est du type $\mathbf{Z}^p$, corollaire du théorème classique sur les modules libres de type fini sur un anneau principal), les intersections et les sommes de deux réseaux, ainsi que les formules de «dualité» :

$$\mathrm{L}_{00} = \mathrm{L},\ (\mathrm{L} + \mathrm{L}')_0 = \mathrm{L}_0 \cap \mathrm{L}'_0\ ,\ (\mathrm{L} \cap \mathrm{L}')_0 = \mathrm{L}_0 + \mathrm{L}'_0.$$

● Il serait intéressant de savoir si, pour $n = 4$ par exemple, les réseaux unimodulaires sont tous semblables à Λ. Ceci serait exact si l'on pouvait démontrer que, pour toute forme quadratique q non dégénérée, positive, de discriminant 1 et de matrice $\mathrm{M} \in \mathrm{GL}_4(\mathbf{Z})$, il existe $\mathrm{N} \in \mathrm{GL}_4(\mathbf{Z})$ telle que $\mathrm{M} = {}^t\mathrm{NN}$. Pour $n = 2$ ou 3, le résultat analogue a été obtenu par des manipulations explicites sur les coefficients de M, manipulations d'origine géométrique ; il s'agit toujours de diminuer la valeur d'un produit scalaire $|(a \mid b)|$ en remplaçant le vecteur b par $b' = b - ka$, où $k \in \mathbf{Z}$; le schéma géométrique suivant montre comment obtenir k :



Une manipulation directe sur une matrice de $\mathrm{M}_4(\mathbf{Z})$ semble a priori pénible (ne serait-ce que parce que la formule donnant le déterminant comporte alors 17 termes !). Il faudrait utiliser des méthodes plus abstraites et plus puissantes qui s'écartent du caractère volontairement élémentaire du problème de 1975. Ceci pourrait déboucher sur l'étude bien connue de Σ_4.

II.2.2. OBSERVATIONS DES CORRECTEURS

● La correction du problème a été décevante. Seule une copie a prouvé chez son auteur une maîtrise complète de résultats dont l'analyse ci-dessus montre le caractère élémentaire ; le candidat n'a évidemment pu, faute de temps, résoudre toutes les questions posées, mais, en s'appuyant sur les réponses explicitement données dans l'intitulé de ces mêmes questions et en s'attaquant aux points forts du problème, il a montré au jury qu'il s'était attaché à comprendre l'agencement des différentes parties et qu'il avait dominé les difficultés essentielles.

● La très grande majorité des candidats (au moins 90 %) n'a obtenu quelques points à cette épreuve qu'en «grapillant» ça et là. Sous peine de produire un énoncé difficile, le jury ne peut — contrairement à ce qui était la règle au siècle dernier — que graduer ses questions, donc proposer une multitude de petits exercices fort simples (et par suite peu «rémunérés») qui conduisent aux véritables difficultés. Un usage regrettable veut que les candidats esquivent les questions fondamentales pour se jeter sur tout ce qui leur paraît accessible. Les points obtenus de cette façon sont peu significatifs de la qualité mathématique de l'agrégatif 1975 ; tout au plus correspondent-ils à une mesure de l'aptitude à discerner, parmi 34 mini-problèmes, les points dont l'intérêt est le plus faible ! A privilégier ainsi les platitudes simplement posées là comme jalons menant vers les points importants, la quasi-unanimité des candidats en vient à s'empêcher délibérément d'apercevoir la forêt en choisissant de l'aborder par ses arbres plus épais.

Peut-être une épreuve réduite à deux ou trois pages d'énoncé et cinq ou six questions, donc plus proche de la simulation d'un réel problème mathématique, serait-elle mieux adaptée au but du concours. Certes de très nombreuses copies obtiendraient la note zéro ; mais il faut bien avouer que cela fournirait l'exacte signification des actuels 2/60, 4/60,..., 10/60 ; des totaux aussi bas demandent beaucoup de temps aux correcteurs, mais ils ne servent guère les candidats quant au résultat final, même si des échafaudages de points ainsi obtenus permettent à certains d'atteindre de justesse le droit de prouver à l'oral une faiblesse qu'on ne leur pardonne pas.

● Une analyse complète du problème de 1975 est impossible. Signalons cependant les erreurs les plus souvent rencontrées dans les parties abordées par un nombre non négligeable de candidats :

1re partie : Confusion entre «forme définie» et «forme non dégénérée» ; confusion entre les propositions :

$$\forall (x, y) \in \mathbf{Q}^2 \quad \overline{q}(x,y) \geqslant 0 \ ; \ \forall (x, y) \in \mathbf{R}^2 \quad \overline{q}(x, y) \geqslant 0.$$

[Ou bien il fallait ici étudier directement la notion non classique de forme rationnelle, ou bien il fallait évoquer une propriété équivalente à la densité de $\mathbf{Q}^2$ dans $\mathbf{R}^2$] ; oubli de la condition $u' > 0$ ($u' \geqslant 0$ étant triviale) ; oubli du cas particulier $u = 1$; affirmation tranquille du fait que les restrictions de la forme $\overline{q}$ du 4° aux sous-espaces de dimension 2 engendrés par (π_1, π_2), (π_2, π_3) et (π_3, π_1) satisfont aux conditions du 1° ; abus (involontaire ?) consistant à écrire $(m > 0)$ à la fin d'un raisonnement prouvant simplement $(m \geqslant 0)$; impossibilité, parfois bien déguisée, de passer de la conclusion du 5° a) au résultat du 5° b).

2e partie : Extension non motivée aux modules de résultats sur les vectoriels, essentiellement l'invariance du cardinal d'une $\mathbf{Z}$–base ; confusion entre $\mathrm{GL}_n(\mathbf{Z})$ et ensemble des matrices de $\mathrm{M}_n(\mathbf{Z})$ admettant un inverse... dans $\mathrm{GL}_n(\mathbf{Q})$; substitution d'un énoncé vague et généralement faux aux constructions effectivement demandées par l'énoncé du 4° ; démonstrations optimistes du 5° par confusion entre réseau et sous-réseau ; oubli de la vérification du caractère borné de Ω au 6°.

3e partie : Définition floue de $\mathbf{W}$ au 1° ; bluff dans la preuve de l'égalité $(\mathrm{L} \cap \mathrm{L}')_0 = \mathrm{L}_0 + \mathrm{L}'_0$, difficile à démontrer directement (mais conséquence triviale de l'égalité duale).

5e partie : Oubli des conditions $ad - bc > 0$, $ac + bd \geqslant 0$ dans l'utilisation des résultats du I 3° b.

II.2.3. LES NOTES (sur 60)

• *Candidats :* (1 587 copies)

0	7,13 %	25 à 28	2,97 %
1 à 4	41,41 %	29 à 32	1,14 %
5 à 8	19,57 %	33 à 36	0,88 %
9 à 12	9,47 %	37 à 40	0,38 %
13 à 16	7,32 %	41 à 44	0,32 %
17 à 20	5,62 %	45 à 48	0,25 %
21 à 24	2,90 %	49 à 60	0,63 %

• *Candidates :* (870 copies)

0	66	26 à 30	43
1 à 5	259	31 à 35	31
6 à 10	135	36 à 40	15
11 à 15	119	41 à 50	16
16 à 20	103	51 à 60	4
21 à 25	79		

II.3 TEXTE DE L'EPREUVE D'ANALYSE

ANALYSE

DURÉE : 6 heures

Préambule

Les propriétés suivantes de la fonction Γ *pourront être utilisées sans démonstration; elles n'interviennent pas dans la première partie du problème.*

Soit s un nombre complexe; on note $\mathrm{Re}(s)$ sa partie réelle, $\mathrm{Im}(s)$ sa partie imaginaire. Pour $\mathrm{Re}(s) > 0$, on pose :

$$\Gamma(s) = \int_0^{+\infty} e^{-t}\, t^{s-1}\, dt\,.$$

La fonction Γ est holomorphe dans le demi-plan $\mathrm{Re}(s) > 0$. Elle se prolonge en une fonction méromorphe dans $\mathbf{C}$ dont les pôles sont les entiers négatifs ou nuls. Ces pôles sont simples, et le résidu de Γ au point $s = -p$, $(p \in \mathbf{N})$, est $\dfrac{(-1)^p}{p\,!}$.

Si s n'est pas un pôle, on a : $\Gamma(s+1) = s\,\Gamma(s)$, et : $\Gamma(s) \neq 0$.

Soient σ_1, σ_2 des nombres réels tels que $\sigma_1 \leqslant \sigma_2$, et m un entier positif; on a : $\lim_{|t| \to +\infty} |\, t^m\, \Gamma(\sigma + it)\,| = 0$, uniformément pour σ élément de $[\sigma_1, \sigma_2]$.

Enfin, si c et x sont des nombres réels strictement positifs, on a :

$$e^{-x} = \frac{1}{2i\pi} \int_{\mathrm{Re}(s) = c} x^{-s}\, \Gamma(s)\, ds\ ,$$