SESSION DE 1989

# MATHÉMATIQUES GÉNÉRALES

DURÉE : 6 heures

*Calculatrice électronique de poche — y compris calculatrice programmable et alphanumérique — à fonctionnement autonome, non imprimante, autorisée conformément à la circulaire n° 86-228 du 28 juillet 1986.*

*La clarté et la précision de la rédaction seront prises en compte dans l'appréciation de la copie.*

$\mathbb{N}$ désigne l'ensemble des entiers naturels, $\mathbb{Z}$ l'anneau des entiers relatifs et $\mathbb{C}$ le corps des nombres complexes. Si $p$ est un nombre premier, $\mathbb{F}_p$ désigne le corps $\mathbb{Z}/p\mathbb{Z}$.

Soit S un sous-anneau de $\mathbb{C}$. On note $M_n(S)$ l'anneau des matrices carrées d'ordre $n$ à coefficients dans S et $GL(n, S)$ le groupe des éléments inversibles de $M_n(S)$. Si M est un élément de $M_n(S)$, $M^*$ (resp. ${}^tM$) désigne la matrice adjointe (resp. la matrice transposée) de M.

On dit qu'une matrice hermitienne (resp. une matrice symétrique réelle) A est définie positive si la forme hermitienne (resp. la forme bilinéaire symétrique) associée à A est définie positive.

On dit que S est un anneau principal, si tout idéal de S peut être engendré par un seul élément, euclidien s'il existe une application N de $S - \{0\}$ dans $\mathbb{N}$ telle que si $a$ et $b$ sont deux éléments non nuls de S, il existe $q$ et $r$ appartenant à S vérifiant $a = bq + r$ et $r = 0$ ou $N(r) < N(b)$.

La partie III est largement indépendante des parties I et II.

## I. PRÉLIMINAIRES

A. Dans cette partie, $p$ désigne un nombre premier impair.

A.1.*a*. Montrer que, si $u$, $v$, $w$ sont trois éléments non nuls de $\mathbb{F}_p$ l'équation : $ux^2 + vy^2 = w$

a une solution dans $\mathbb{F}_p$. (On pourra considérer le cardinal de l'ensemble des éléments de la forme $ux^2$ (respectivement de la forme $w - vy^2$)).

A.1.*b*. Soit $n > 1$ un entier tel que $p$ ne divise pas $4n - 1$. Montrer qu'il existe des entiers relatifs $a$, $b$ et un entier $m \geqslant 1$ tels que :

$$a^2 + ab + nb^2 + 1 = mp.$$

A.2. On suppose $p$ de la forme $8k + 1$ ou $8k + 3$, et soit K une extension de $\mathbb{F}_p$, corps de rupture du polynôme $t^4 + 1$. Soit $b$ une racine dans K de ce polynôme ; on pose : $x = b - b^{-1}$.

A.2.*a*. Montrer les relations suivantes : $x^2 = -2$ *et* $x^p = x$.

En déduire que $x$ appartient à $\mathbb{F}_p$.

A.2.*b*. Montrer qu'il existe des entiers $a$ et $m$ tels que : $2a^2 + 1 = (2m - 1)p$

et prouver que la matrice : $\begin{pmatrix} p & a & 0 \\ a & m & 1 \\ 0 & 1 & 2 \end{pmatrix}$ est une matrice symétrique définie positive et de déterminant égal à 1.

Déterminer tous les couples $(a, m)$ lorsque $p = 17$.

B. Soit $D \geqslant 1$ un entier qui n'est pas divisible par le carré d'un nombre premier. On pose :

$$\omega_D = \begin{cases} i\sqrt{D} & \text{si} \quad D \equiv 1 \text{ ou } 2 \pmod 4 \\ \dfrac{1 + i\sqrt{D}}{2} & \text{si} \quad D \equiv 3 \pmod 4 \end{cases}$$

$\mathbb{Z}[\omega_D]$ désigne le sous-anneau de $\mathbb{C}$, ensemble des éléments de la forme $\alpha + \beta\omega_D$, $\alpha$ et $\beta$ éléments de $\mathbb{Z}$.

B.1. Soit $p$ un nombre premier qui ne divise pas D. Montrer qu'il existe des entiers relatifs $a$, $b$, $m$ tels que la matrice : $\begin{pmatrix} p & a + b\omega_D \\ a + b\omega_D & m \end{pmatrix}$

soit une matrice hermitienne définie positive et de déterminant égal à 1.

Tournez la page S.V.P.

B.2. Dans le plan euclidien rapporté à un repère orthonormé, on désigne par A, B, C les images respectives des nombres 0, 1, $\omega_D$ et par T le triangle, enveloppe convexe des points A, B, C. Le rayon du cercle circonscrit à T est noté R.

B.2.*a*. Montrer que pour tout point M de T, on a : $\inf(\mathrm{MA}, \mathrm{MB}, \mathrm{MC}) \leqslant \mathrm{R}.$

B.2.*b*. On pose :

$$k = \sup_{z \in \mathbf{C}} \left( \inf_{u \in \mathbf{Z}[\omega_D]} |z - u|^2 \right).$$

Prouver l'égalité :

$$k = \sup_{M \in T} \left( \inf(\mathrm{MA}^2, \mathrm{MB}^2, \mathrm{MC}^2) \right).$$

B.2.*c*. En déduire que l'on a :

$$k = \frac{D+1}{4} \quad \text{si } D \equiv 1 \text{ ou } 2 \pmod 4 \qquad k = \frac{(D+1)^2}{16\,D} \quad \text{si } D \equiv 3 \pmod 4.$$

B.2.*d*. Soient $\alpha$, $\beta$ deux éléments de $\mathbf{Z}[\omega_D]$, $\beta$ étant supposé non nul. Montrer qu'il existe $\gamma$, élément de $\mathbf{Z}[\omega_D]$, tel que :

$$|\alpha - \gamma\beta|^2 \leqslant k\,|\beta|^2.$$

En déduire que $\mathbf{Z}[\omega_D]$ est un anneau euclidien lorsque D est égal à l'une des valeurs suivantes : 1, 2, 3, 7, 11.

*Application* : déterminer $\gamma$ lorsque $D = 2, \alpha = 5 + 3\omega_2, \beta = -1 + 3\omega_2$.

## II. MATRICES HERMITIENNES DE LA FORME B* B

Dans cette partie, S désigne l'anneau $\mathbf{Z}$ ou l'un des anneaux $\mathbf{Z}[\omega_D]$ pour $D = 1, 2, 3, 7$, ou 11. Si $S = \mathbf{Z}$, on pose : $k = 1/4$, et si $S = \mathbf{Z}[\omega_D]$, $k$ est la constante définie en I.B.2.*b*.

Deux matrices hermitiennes A et B de $M_n(S)$ sont dites **congruentes** s'il existe $U \in GL(n, S)$ telle que : $A = UBU^*$. Les classes d'équivalence pour cette relation sont appelées classes de congruence.

À un élément $x = (x_1, \dots, x_n)$ de $S^n$ est associée une matrice à une ligne dont les coefficients sont les composantes de $x$ ; on notera également $x$ cette matrice. ${}^t x$ désignera la matrice transposée, et $x^*$ la matrice ${}^t\bar{x}$.

1. Montrer que si A et B sont deux matrices hermitiennes congruentes, alors : $\det A = \det B$.

2.*a*. Soit A une matrice hermitienne définie positive appartenant à $M_n(S)$. Montrer qu'il existe un entier $m(A) > 0$ et un élément $z$ appartenant à $S^n$ dont les composantes sont premières entre elles tels que l'on ait :

$$m(A) = \inf_{x \in S^n \setminus \{0\}} x A x^* = z A z^*$$

2.*b*. A-t-on toujours $m(A) = m(B)$ lorsque A et B sont congruentes ?

2.*c*. Déterminer $m(A)$ lorsque $S = \mathbf{Z}$ et $A = \begin{pmatrix} 2 & 7 \\ 7 & 25 \end{pmatrix}.$

### A Le cas $n = 2$,

Soit A une matrice hermitienne définie positive de $M_2(S)$ et soit $z$ un élément de $S^2$ tel que : $m(A) = z A z^*$.

A1.*a*. Montrer que ${}^t z$ est vecteur colonne d'une matrice inversible $U_0$ de $GL(2, S)$ et en déduire l'existence d'une matrice hermitienne $B = (b_{ij})$, $1 \leqslant i, j \leqslant 2$, où $b_{11} = m(A)$, telle que A et B soient congruentes.

A1.*b*. Montrer qu'il existe $s \in S$ tel que : $|b_{11} s + b_{12}| \leqslant k^{\frac{1}{2}} b_{11}$

et en déduire l'existence d'une matrice C : $C = \begin{pmatrix} a & b \\ \bar{b} & c \end{pmatrix}$

congruente à A, qui vérifie les deux conditions :

i. $a = m(A) = m(C)$.

ii. $k^{-\frac{1}{2}} |b| \leqslant a \leqslant c$.

Tournez la page S.V.P.

A.1.*c.* Montrer que si $A \in M_2(S)$ est une matrice hermitienne définie positive de déterminant égal à $d$, alors on a :

$$m(A) \leqslant (1-k)^{-\frac{1}{2}} d^{\frac{1}{2}}.$$

A.1.*d.* En déduire la finitude de l'ensemble des classes de congruence de matrices hermitiennes d'ordre 2 à coefficients dans S, définies positives, de déterminant donné.

A2.*a.* On suppose que $d$ est égal à 1 et que S est l'un des anneaux suivants :

$$S = \mathbb{Z}, \ S = \mathbb{Z}[\omega_D] \text{ pour } D = 1, 3, 7.$$

Montrer alors que $m(A) = 1$ et qu'il existe $B \in GL(2, S)$ telle que $A = B^* B$.

A2.*b.* En déduire les propriétés suivantes :

i. Tout nombre premier est somme de quatre carrés.

ii. Quel que soit le nombre premier $p$, il existe des entiers relatifs $a, b, c, d$ tels que :

$$p = a^2 + ab + b^2 + c^2 + cd + d^2.$$

iii. Quel que soit le nombre premier $p$, il existe des entiers relatifs $a, b, c, d$ tels que :

$$p = a^2 + ab + 2b^2 + c^2 + cd + 2d^2.$$

## B. Matrices symétriques à coefficients entiers.

B.1.*a.* Soit $f: \mathbb{Z}^n \to \mathbb{Z}$ un homomorphisme surjectif de groupes abéliens, et soit $x \in \mathbb{Z}^n$ tel que $f(x) = 1$. Montrer que $\mathbb{Z}^n$ est la somme directe du sous-groupe engendré par $x$ et du noyau de $f$.

B.1.*b.* Soit $x = (x_1, \dots, x_n)$ un élément de $\mathbb{Z}^n$. Montrer que les conditions suivantes sont équivalentes :

i. $x$ appartient à une base de $\mathbb{Z}^n$.

ii. Il existe $M \in GL(n, \mathbb{Z})$ admettant ${}^t x$ comme vecteur-colonne.

iii. Il existe des entiers relatifs $a_i$, $1 \leqslant i \leqslant n$, tels que : $\displaystyle\sum_{i=1}^{n} a_i x_i = 1$.

iv. Il existe $f: \mathbb{Z}^n \to \mathbb{Z}$ homomorphisme surjectif de groupes abéliens tels que $f(x) = 1$.

B.2. Soit A une matrice symétrique d'ordre $n > 1$ définie positive à coefficients dans $\mathbb{Z}$. Montrer l'existence d'une matrice $B = (b_{ij})$, $1 \leqslant i, j \leqslant n$, congruente à A et telle que : $b_{11} = m(A)$.

B.3. Soit $A = (a_{ij})$, $1 \leqslant i, j \leqslant n$, une matrice symétrique définie positive à coefficients dans $\mathbb{Z}$ telle que $m(A) = a_{11}$. Si $x = (x_1, \dots, x_n)$ est un élément de $\mathbb{Z}^n$, on définit l'élément $y = (y_1, \dots, y_n)$ par les relations suivantes :

$$y_1 = x_1 + \sum_{i=2}^{n} a_{1i}\, a_{11}^{-1} x_i, \qquad y_i = x_i \text{ pour } 2 \leqslant i \leqslant n,$$

On pose : $\quad z = (x_2, \dots, x_n), \quad {}^t y = U\,{}^t x.$

B.3.*a.* Montrer que l'on a : $\quad x A\, {}^t x = a_{11} y_1^2 + a_{11}^{-1} z B\, {}^t z$

où B est une matrice symétrique définie positive appartenant à $M_{n-1}(\mathbb{Z})$ et qui vérifie les deux relations :

$$A = {}^t U \begin{pmatrix} a_{11} & 0 \\ 0 & a_{11}^{-1} B \end{pmatrix} U \qquad \det B = (a_{11})^{n-2} \det A.$$

B.3.*b.* Montrer que l'on a : $\quad m(A) \leqslant \left(\dfrac{4}{3}\right)^{\frac{n-1}{2}} (\det A)^{\frac{1}{n}}$

(on choisira $x$ de telle sorte que l'on ait : $|y_1| \leqslant \dfrac{1}{2}$ ; $z B\, {}^t z = m(B)$).

B.4.*a.* On suppose $n \leqslant 5$ et soit $A \in M_n(\mathbb{Z})$ une matrice symétrique définie positive dont le déterminant est égal à 1. Montrer que $m(A) = 1$ et en déduire qu'il existe $B \in M_n(\mathbb{Z})$ telle que $A = {}^t B\, B$.

B.4.*b.* Montrer que tout nombre premier de la forme $8n + 1$ ou $8n + 3$ est somme de trois carrés.

**Tournez la page S.V.P.**

## III. CLASSES D'IDÉAUX ET ANNEAUX PRINCIPAUX

On rappelle que deux éléments A et B de $M_n(\mathbb{Z})$ sont semblables s'il existe un élément Q de $GL(n, \mathbb{Z})$ tel que $A = QBQ^{-1}$ ; les classes d'équivalence pour cette relation sont appelées classes de similitude.

A. Soit $P(X)$ un polynôme unitaire de degré $n > 1$, à coefficients dans $\mathbb{Z}$ et irréductible sur $\mathbb{Q}[X]$. Si $\theta$ est une racine complexe de $P(X)$, on note $\mathbb{Z}[\theta]$ le sous-anneau de $\mathbb{C}$, ensemble des éléments de la forme :

$$\sum_{i=0}^{n-1} a_i \theta^i \quad \text{où } a_i \in \mathbb{Z} \text{ pour } i = 0, \ldots, n-1 .$$

On dit que deux idéaux I et J de $\mathbb{Z}[\theta]$ appartiennent à la même classe s'il existe deux éléments non nuls $a$ et $b$ de $\mathbb{Z}[\theta]$ tels que $aI = bJ$. A désigne un élément de $M_n(\mathbb{Z})$ tel que $P(A) = 0$.

A.1. Montrer que tout idéal non nul de $\mathbb{Z}[\theta]$ est un groupe abélien libre de rang $n$.

A.2.*a*. Montrer qu'il existe $x = (x_1, \ldots, x_n)$ élément de $\mathbb{Z}[\theta]^n \setminus \{0\}$ tel que : $A\,{}^t x = \theta\,{}^t x$.

A2.*b*. Montrer que $\mathbb{Z}x_1 + \ldots + \mathbb{Z}x_n$ est un idéal de $\mathbb{Z}[\theta]$ dont la classe est indépendante du vecteur propre ${}^t x$ choisi.

On notera $I_A$ la classe de l'idéal $\mathbb{Z}x_1 + \ldots + \mathbb{Z}x_n$.

A.2.*c*. Soit Q un élément de $GL(n, \mathbb{Z})$. Montrer que :

$$I_A = I_{QAQ^{-1}} .$$

A3. Soit $J = \mathbb{Z}y_1 + \ldots + \mathbb{Z}y_n$ un idéal de $\mathbb{Z}[\theta]$, on pose :

$$y = (y_1, \ldots, y_n).$$

Montrer qu'il existe une matrice B à coefficients entiers telle que :

$$B\,{}^t y = \theta\,{}^t y, \quad P(B) = 0.$$

A.4. Montrer qu'il existe une bijection entre l'ensemble des classes de similitude des matrices A, éléments de $M_n(\mathbb{Z})$, telles que $P(A) = 0$ et l'ensemble des classes d'idéaux de $\mathbb{Z}[\theta]$.

A.5. Montrer que les conditions suivantes sont équivalentes ;

i. $\mathbb{Z}[\theta]$ est un anneau principal.

ii. Il existe une seule classe de similitude dans $M_n(\mathbb{Z})$ de matrices A d'ordre $n$ à coefficients entiers telles que $P(A) = 0$.

B. $D \geq 1$ désigne un entier qui n'est pas divisible par le carré d'un nombre premier ; $\mathbb{Z}[\omega_D]$ est l'anneau introduit en I.B.

B.1. On suppose $D \equiv 1$ ou $2 \pmod 4$ :

$$A(\alpha, \beta, \gamma) = \begin{pmatrix} -\alpha & \beta \\ \gamma & \alpha \end{pmatrix}$$

désigne une matrice à coefficients dans $\mathbb{Z}$ dont le polynôme caractéristique est :

$$P(X) = X^2 + D.$$

En considérant les valeurs $\alpha = 0$ et $\alpha = 1$, montrer que $\mathbb{Z}[\omega_D]$ est principal si et seulement si $D = 1$ ou 2.

**Tournez la page S.V.P.**

B.2. On suppose $D \equiv 3 \pmod 4$ et l'on pose :

$$K = \frac{D+1}{4}.$$

Soit A un élément de $M_2(\mathbb{Z})$ dont le polynôme caractéristique est :

$$P(X) = X^2 - X + K.$$

B.2.*a*. Soit :

$$B = \begin{pmatrix} -a & -b \\ c & a+1 \end{pmatrix}$$

une matrice semblable à A telle que $|a|$ soit minimum.

En calculant $PAP^{-1}$ lorsque P est l'une des matrices suivantes :

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

montrer que l'on peut supposer que les coefficients de B vérifient :

$$a \geqslant 0,\ c \geqslant 2a + 1,\ b \geqslant 2a + 1,\ 3(a^2 + a) + 1 \leqslant K.$$

B.2.*b*. Soient $\alpha, \beta, \gamma$ trois entiers tels que :

$$0 \leqslant \alpha < K - 1, \qquad 1 < \beta \leqslant \gamma, \qquad \beta\gamma = K + \alpha^2 + \alpha.$$

Montrer que, quel que soit l'élément $(x, y)$ de $\mathbb{Z}^2 \backslash \{0\}$, on a :

$$\beta x^2 + \gamma y^2 + (2\alpha + 1)\, xy > y^2.$$

En déduire que les matrices :

$$A = \begin{pmatrix} 0 & -K \\ 1 & 1 \end{pmatrix} \qquad M = \begin{pmatrix} -\alpha & -\gamma \\ \beta & \alpha + 1 \end{pmatrix}$$

ne sont pas semblables.

B.2.*c*. On suppose que $\mathbb{Z}[\omega_D]$ est un anneau principal. Montrer que $K = 1$ ou que $K + a^2 + a$ est un nombre premier pour tout entier $a$ tel que : $0 \leqslant a < K - 1$.

B.2.*d*. On suppose que $K = 1$ ou que $K + a^2 + a$ est premier quel que soit $a \geqslant 0$ vérifiant $3(a^2 + a) + 1 \leqslant K$. Prouver que $\mathbb{Z}[\omega_D]$ est un anneau principal.

B.2.*e*. On suppose $D \leqslant 200$. Prouver que $\mathbb{Z}[\omega_D]$ est principal si et seulement si $D = 3, 7, 11, 19, 43, 67, 163$.

B.2.*f*. On suppose $D \leqslant 10^6$. Écrire un programme permettant de vérifier que les valeurs trouvées sont les seules pour lesquelles l'anneau $\mathbb{Z}[\omega_D]$ est principal.

C. S désigne l'un des anneaux $\mathbb{Z}[\omega_D]$ pour $D = 19, 43, 67, 163$ et on suppose S euclidien pour une application N de $S - \{0\}$ dans $\mathbb{N}$. Soit $a$ un élément non inversible de $S - \{0\}$ tel que $N(a)$ soit minimum.

C.1. Montrer que $S/aS$ est isomorphe à l'un des corps $\mathbb{F}_2$ ou $\mathbb{F}_3$.

C.2. En déduire que pour $D = 19, 43, 67, 163$, $\mathbb{Z}[\omega_D]$ est un anneau principal non euclidien.

- FIN -