D. S. Agrégation Externe, le 15 novembre 2013

Pour tout nombre premier p, on note $\mathbb{F}_p$ le corps $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ des classes résiduelles modulo p.

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

On dit qu'une matrice hermitienne (resp. 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,b sont deux éléments non nuls de S, il existe q,r appartenant à S vérifiant $a=bq+r$ et $r=0$ ou $N(r)<N(b)$.

– I – Préliminaires

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

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 (resp. de la forme $w-vy^2$)).

   (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 $m\geq 1$ tels que :
$$a^2+ab+nb^2+1=mp.$$

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

   (a) Montrer les relations suivantes : $x^2=-2$ et $x^p=x$. En déduire que x appartient à $\mathbb{F}_p$.

   (b) Montrer qu'il existe des entiers a,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 $D\geq 1$ un entier qui n'est pas divisible par le carré d'un nombre premier. On pose :
$$\omega_D=\begin{cases} i\sqrt{D} \text{ si } D\equiv 1 \text{ ou } 2 \pmod 4\\ \dfrac{1+i\sqrt{D}}{2} \text{ si } D\equiv 3 \pmod 4\end{cases}$$

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

1. Montrer que pour tout $\lambda\in\mathbb{Z}[\omega_D]$, $|\lambda|^2$ est un entier.
2. Montrer que λ est inversible dans $\mathbb{Z}[\omega_D]$ si, et seulement si, $|\lambda|=1$.
3. Soit p un nombre premier impair qui ne divise pas D. Montrer qu'il existe des entiers relatifs a,b,m tels que la matrice :
$$\begin{pmatrix} p & a+b\omega_D\\ a+b\overline{\omega_D} & m\end{pmatrix}$$
   soit une matrice hermitienne définie positive et de déterminant égal à 1.
4. 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.

   (a) Montrer que pour tout point M de T, on a :
$$\inf(MA,MB,MC)\leq R.$$

(b) On pose :

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

Prouver l'égalité :

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

(c) En déduire que l'on a :

$$\begin{cases} k = \dfrac{D+1}{4} \text{ si } D \equiv 1 \text{ ou } 2 \pmod 4 \\ k = \dfrac{(D+1)^2}{16D} \text{ si } D \equiv 3 \pmod 4 . \end{cases}$$

(d) Soient α, β deux éléments de $\mathbb{Z}[\omega_D]$, β étant supposé non nul. Montrer qu'il existe γ, élément de $\mathbb{Z}[\omega_D]$, tel que :

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

En déduire que $\mathbb{Z}[\omega_D]$ est un anneau euclidien lorsque D est égal à l'une des valeurs suivantes : $1, 2, 3, 7, 11$. Application : déterminer γ 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 $\mathbb{Z}$ ou l'un des anneaux $\mathbb{Z}[\omega_D]$ pour $D = 1, 2, 3, 7$ ou 11. Si $S = \mathbb{Z}$, on pose $k = \dfrac{1}{4}$, et si $S = \mathbb{Z}[\omega_D]$, k est la constante définie en **I.B.4.b.**

Deux matrices hermitiennes A, B de $\mathcal{M}_n(S)$ 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 $x = (x_1, \cdots, x_n)$ de S^n est associé 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 $\overline{{}^t x}$.

1. Montrer que si A, B sont deux matrices congruentes, alors $\det(A) = \det(B)$.

2.

(a) Soit A une matrice hermitienne définie positive appartenant à $\mathcal{M}_n(S)$. 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 :

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

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

(c) Déterminer $m(A)$ lorsque $S = \mathbb{Z}$ et :

$$A = \begin{pmatrix} 2 & 7 \\ 7 & 25 \end{pmatrix}.$$

A. Le cas $n = 2$

Soit A une matrice hermitienne définie positive appartenant à $\mathcal{M}_2(S)$ et soit z un élément de S^2 tel que $m(A) = zAz^*$.

1.

(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 $B = (b_{ij})$, $1 \leq i, j \leq 2$, où $b_{11} = m(A)$, telle que A et B soient congruentes.

(b) Montrer qu'il existe $s \in S$ tel que :

$$|b_{11}s + b_{12}| \leq k^{\frac{1}{2}} b_{11}$$

et en déduire l'existence d'une matrice

$$C = \begin{pmatrix} a & b \\ \overline{b} & c \end{pmatrix}$$

congruente à A, qui vérifie les deux conditions :

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

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

(c) Montrer que si $A \in \mathcal{M}_2(S)$ est une matrice hermitienne définie positive de déterminant égal à d, alors on a :

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

(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.

2.

(a) On suppose que $d = 1$ 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 $A = B^* B$.

(b) En déduire les propriétés suivantes :

i. Tout nombre premier est somme de quatre carrés (théorème de Lagrange).

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

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) Soit $x = (x_1, \cdots, x_n)$ 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, $1 \leq i \leq n$, tels que $\sum_{i=1}^{n} a_i x_i = 1$.

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

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

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

$$\begin{cases} y_1 = x_1 + \sum_{i=2}^{n} a_{1i} a_{11}^{-1} x_i, \\ y_i = x_i \text{ pour } 2 \leq i \leq n. \end{cases}$$

On pose :

$$z = (x_2, \cdots, x_n),\ {}^t y = U\, {}^t x.$$

(a) Montrer que l'on a :

$$x A\, {}^t x = a_{11} y_1^2 + a_{11}^{-1} z B\, {}^t z,$$

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

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

(b) Montrer que l'on a :

$$m(A) \leq \left(\frac{4}{3}\right)^{\frac{n-1}{2}} (\det(A))^{\frac{1}{n}}.$$

On choisira x de telle sorte que l'on ait :

$$|y_1| \leq \frac{1}{2},\ z B\, {}^t z = m(B).$$

4.

(a) On suppose $n \leq 5$ et soit $A \in \mathcal{M}_n(\mathbb{Z})$ une matrice symétrique définie positive dont le déterminant est égal à 1. Montrer que $m(A) = 1$ et en déduire qu'il existe $B \in \mathcal{M}_n(\mathbb{Z})$ telle que $A = {}^tBB$.

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

– III – Classes d'idéaux et anneaux principaux

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

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

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

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 $\mathcal{M}_n(\mathbb{Z})$ tel que $P(A) = 0$.

1. Montrer que tout idéal non nul de $\mathbb{Z}[\theta]$ est un groupe abélien libre de rang n.
2.
   (a) Montrer qu'il existe $x = (x_1, \cdots, x_n)$ élément de $\mathbb{Z}[\theta]^n \setminus \{0\}$ tel $A\,{}^tx = \theta\,{}^tx$.
   (b) Montrer que $\mathbb{Z}x_1 + \cdots + \mathbb{Z}x_n$ est un idéal de $\mathbb{Z}[\theta]$ dont la classe est indépendante du vecteur propre ${}^tx$ choisi.
   On notera I_A la classe de l'idéal $\mathbb{Z}x_1 + \cdots + \mathbb{Z}x_n$.
   (c) Soit Q un élément de $GL(n, \mathbb{Z})$. Montrer que $I_A = I_{QAQ^{-1}}$.
3. Soit $J = \mathbb{Z}y_1 + \cdots + \mathbb{Z}y_n$ un idéal non nul de $\mathbb{Z}[\theta]$. On pose $y = (y_1, \cdots, y_n)$. Montrer qu'il existe une matrice B à coefficients entiers telle que $B\,{}^ty = \theta\,{}^ty$, $P(B) = 0$.
4. Montrer qu'il existe une bijection entre l'ensemble des classes de similitude des matrices A, éléments de $\mathcal{M}_n(\mathbb{Z})$ telles que $P(A) = 0$, et l'ensemble des classes d'idéaux non nuls de $\mathbb{Z}[\theta]$.
5. Montrer que les conditions suivantes sont équivalentes :
   (a) $\mathbb{Z}[\theta]$ est un anneau principal.
   (b) Il existe une seule classe de similitude dans $\mathcal{M}_n(\mathbb{Z})$ de matrices A d'ordre n à coefficients entiers telles que $P(A) = 0$.