

SESSION 2011

---

AGRÉGATION  
CONCOURS EXTERNE

Section : MATHÉMATIQUES

COMPOSITION DE MATHÉMATIQUES GÉNÉRALES

Durée : 6 heures

---

*Calculatrice électronique de poche - y compris calculatrice programmable, alphanumérique ou à écran graphique – à fonctionnement autonome, non imprimante, autorisée conformément à la circulaire n° 99-186 du 16 novembre 1999.*

*L'usage de tout ouvrage de référence, de tout dictionnaire et de tout autre matériel électronique est rigoureusement interdit.*

*Dans le cas où un(e) candidat(e) repère ce qui lui semble être une erreur d'énoncé, il (elle) le signale très lisiblement sur sa copie, propose la correction et poursuit l'épreuve en conséquence.*

*De même, si cela vous conduit à formuler une ou plusieurs hypothèses, il vous est demandé de la (ou les) mentionner explicitement.*

**NB :** *Hormis l'en-tête détachable, la copie que vous rendrez ne devra, conformément au principe d'anonymat, comporter aucun signe distinctif, tel que nom, signature, origine, etc. Si le travail qui vous est demandé comporte notamment la rédaction d'un projet ou d'une note, vous devrez impérativement vous abstenir de signer ou de l'identifier.*

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

## Notations et définitions

Selon l'usage, les corps sont supposés commutatifs. Dans tout le problème,  $n$  est un élément de  $\mathbb{N}^*$ ,  $K$  un corps.

Si  $A$  est un sous-anneau d'un corps, si  $p$  et  $q$  sont deux éléments de  $\mathbb{N}^*$ , on note  $\mathcal{M}_{p,q}(A)$  l'ensemble des matrices à  $p$  lignes et  $q$  colonnes à coefficients dans  $A$ . On abrège  $\mathcal{M}_{p,p}(A)$  en  $\mathcal{M}_p(A)$ ; la matrice identité de  $\mathcal{M}_p(A)$  est notée  $I_p$ . Le groupe des inversibles de l'anneau  $\mathcal{M}_p(A)$  est noté  $\text{GL}_p(A)$ . Pour  $m$  dans  $\mathbb{N}$ , on note  $U_m(A)$  l'ensemble des polynômes unitaires de degré  $m$  de  $A[X]$ .

Deux matrices  $M$  et  $N$  de  $\mathcal{M}_n(A)$  sont dites *semblables sur  $A$*  si et seulement s'il existe  $P$  dans  $\text{GL}_n(A)$  telle que :

$$N = PMP^{-1}.$$

La relation de similitude sur  $\mathcal{M}_n(A)$  est une relation d'équivalence. Les classes de cette relation sont appelées *classes de similitude sur  $A$* ; pour  $A = \mathbb{Z}$ , on les appellera également *classes de similitude entière*.

Pour  $M$  dans  $\mathcal{M}_n(K)$ , soit  $\chi_M$  le polynôme caractéristique (unitaire) de  $M$  :

$$\chi_M(X) = \det(XI_n - M).$$

Pour  $P$  dans  $U_n(K)$ , soit  $\mathcal{E}_K(P)$  l'ensemble des matrices  $M$  de  $\mathcal{M}_n(K)$  telles que  $\chi_M = P$ . Puisque deux matrices semblables de  $\mathcal{M}_n(K)$  ont même polynôme caractéristique,  $\mathcal{E}_K(P)$  est une réunion de classes de similitude sur  $K$ .

Il est clair que si  $M$  est dans  $\mathcal{M}_n(\mathbb{Z})$ ,  $\chi_M$  est dans  $U_n(\mathbb{Z})$ . Si  $P$  est dans  $U_n(\mathbb{Z})$ , on note  $\mathcal{E}_{\mathbb{Z}}(P)$  l'ensemble des matrices  $M$  de  $\mathcal{M}_n(\mathbb{Z})$  telles que  $\chi_M = P$ ; cet ensemble est une réunion de classes de similitude entière. On note  $\mathcal{D}_{\mathbb{Z}}(P)$  l'ensemble des matrices de  $\mathcal{E}_{\mathbb{Z}}(P)$  diagonalisables sur  $\mathbb{C}$ .

Si  $P$  est le polynôme  $X^n - a_{n-1}X^{n-1} - \dots - a_1X - a_0$  de  $K[X]$ , on note  $C(P)$  la matrice compagnon de  $P$ , c'est-à-dire :

$$\begin{pmatrix} 0 & \cdots & \cdots & 0 & a_0 \\ 1 & 0 & & \vdots & a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & a_{n-2} \\ 0 & \cdots & 0 & 1 & a_{n-1} \end{pmatrix} \quad \text{si } n \geq 2 \quad \text{et : } (a_0) \quad \text{si } n = 1.$$

## Objectifs du problème, dépendance des parties

Le thème du problème est l'étude de la relation de similitude entière. La partie **I** rassemble quelques résultats relatifs à la similitude sur un corps et aux polynômes. La partie **II** débute l'étude de la similitude entière. La partie **III** établit le résultat principal du texte : si  $P$  est dans  $U_n(\mathbb{Z})$ , l'ensemble  $\mathcal{D}_{\mathbb{Z}}(P)$  est réunion finie de classes de similitude entière.

Les sous-parties **I.A**, **I.B** et **I.C** sont largement indépendantes. Les sous-parties **II.A** et **II.B** sont indépendantes de la partie **I**. Les sous-parties **III.A**, **III.B**, **III.C** sont largement indépendantes des parties **I** et **II**.

## I. Préliminaires

### A. Matrices à coefficients dans $K$

1. (a) Pour quels  $(a, b, c)$  de  $K^3$  la matrice  $M = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$  est-elle diagonalisable sur  $K$  ?
- (b) Trouver deux matrices de  $\mathcal{M}_2(K)$  non semblables sur  $K$  et ayant même polynôme caractéristique.
- (c) Soient  $M$  et  $M'$  deux éléments de  $\mathcal{M}_n(K)$  diagonalisables sur  $K$  et telles que  $\chi_M = \chi_{M'}$ . Montrer que  $M$  et  $M'$  sont semblables sur  $K$ .
2. Soit  $P$  dans  $U_n(K)$ .
  - (a) Montrer que :  $\chi_{C(P)} = P$ .
  - (b) Si  $\lambda$  est dans  $K$ , montrer que le rang de  $C(P) - \lambda I_n$  est supérieur ou égal à  $n - 1$ .
  - (c) Montrer l'équivalence entre les trois assertions suivantes :
    - (i) le polynôme  $P$  est scindé sur  $K$  à racines simples,
    - (ii) toutes les matrices de  $\mathcal{E}_K(P)$  sont diagonalisables sur  $K$ ,
    - (iii)  $C(P)$  est diagonalisable sur  $K$ .
3. Soient  $r$  et  $s$  dans  $\mathbb{N}^*$ ,  $A$  dans  $\mathcal{M}_r(K)$ ,  $A'$  dans  $\mathcal{M}_s(K)$ ,  $M = \left( \begin{array}{c|c} A & 0 \\ \hline 0 & A' \end{array} \right)$ .  
Montrer que  $M$  est diagonalisable sur  $K$  si et seulement si  $A$  et  $A'$  sont diagonalisables sur  $K$ .
4. Montrer que pour tout  $P$  de  $U_n(K)$  l'ensemble  $\mathcal{E}_K(P)$  est une réunion finie de classes de similitude sur  $K$ . On pourra admettre et utiliser le résultat suivant.  
"Si  $M$  est dans  $\mathcal{M}_n(K)$ , il existe  $r$  dans  $\mathbb{N}^*$  et  $r$  polynômes unitaires non constants  $P_1, \dots, P_r$  de  $K[X]$  tels que  $M$  soit semblable sur  $K$  à une matrice diagonale par blocs dont les blocs diagonaux sont  $C(P_1), \dots, C(P_r)$ ."

### B. Polynômes

1. Soient  $P$  dans  $K[X]$ ,  $a$  dans  $K$  une racine de  $P$ . Montrer que  $a$  est racine simple de  $P$  si et seulement si  $P'(a) \neq 0$ .
2. Soit  $P$  un élément irréductible de  $\mathbb{Q}[X]$ . Montrer que les racines de  $P$  dans  $\mathbb{C}$  sont simples.
3. Soient  $P$  et  $Q$  dans  $\mathbb{Q}[X]$ , unitaires, tels que  $P$  appartienne à  $\mathbb{Z}[X]$  et que  $Q$  divise  $P$  dans  $\mathbb{Q}[X]$ . Montrer que  $Q$  appartient à  $\mathbb{Z}[X]$ . On pourra admettre et utiliser le lemme de Gauss suivant.  
"Si  $U$  est dans  $\mathbb{Z}[X] \setminus \{0\}$ , soit  $c(U)$  le p.g.c.d des coefficients de  $U$ . Alors, pour tout couple  $(U, V)$  d'éléments de  $\mathbb{Z}[X] \setminus \{0\}$  :  $c(UV) = c(U)c(V)$ ."

4. Soit  $P$  dans  $U_n(\mathbb{Z})$ . Montrer que  $\mathcal{D}_{\mathbb{Z}}(P)$  n'est pas vide.

### C. Similitude sur $K$ de matrices blocs

Pour  $U$  et  $V$  dans  $\mathcal{M}_n(K)$ , on note  $\Phi_{U,V}$  l'endomorphisme de  $\mathcal{M}_n(K)$  défini par :

$$\forall X \in \mathcal{M}_n(K), \quad \Phi_{U,V}(X) = UX - XV.$$

1. Soient  $U$  dans  $\mathcal{M}_n(K)$ ,  $Q$  dans  $\text{GL}_n(K)$  et  $V = QUQ^{-1}$ . Déterminer un automorphisme du  $K$ -espace  $\mathcal{M}_n(K)$  envoyant le noyau de  $\Phi_{U,V}$  sur celui de  $\Phi_{U,U}$ .

Dans la suite,  $m$  est un entier tel que  $0 < m < n$ ,  $A$  un élément de  $\mathcal{M}_m(K)$ ,  $A'$  un élément de  $\mathcal{M}_{n-m}(K)$ ,  $B$  un élément de  $\mathcal{M}_{m,n-m}(K)$ . On note :

$$M = \left( \begin{array}{c|c} A & B \\ \hline 0 & A' \end{array} \right), \quad N = \left( \begin{array}{c|c} A & 0 \\ \hline 0 & A' \end{array} \right).$$

2. Soient  $Y$  dans  $\mathcal{M}_{m,n-m}(K)$  et  $P = \left( \begin{array}{c|c} I_m & Y \\ \hline 0 & I_{n-m} \end{array} \right)$ .

Vérifier que  $P$  appartient à  $\text{GL}_n(K)$ ; déterminer  $P^{-1}$  et  $P^{-1}NP$ . En déduire que s'il existe  $Y$  dans  $\mathcal{M}_{m,n-m}(K)$  telle que  $B = AY - YA'$ , alors  $M$  et  $N$  sont semblables.

3. Le but de cette question est de démontrer que si  $M$  et  $N$  sont semblables sur  $K$ , alors il existe  $B$  dans  $\mathcal{M}_{m,n-m}(K)$  telle que  $B = AY - YA'$ .

Si  $X$  est dans  $\mathcal{M}_n(K)$ , on pose :

$$X = \left( \begin{array}{c|c} X_{1,1} & X_{1,2} \\ \hline X_{2,1} & X_{2,2} \end{array} \right)$$

avec  $X_{1,1} \in \mathcal{M}_m(K)$ ,  $X_{1,2} \in \mathcal{M}_{m,n-m}(K)$ ,  $X_{2,1} \in \mathcal{M}_{n-m,m}(K)$  et  $X_{2,2} \in \mathcal{M}_{n-m}(K)$ . On note alors :

$$\tau(X) = (X_{2,1}, X_{2,2}).$$

Il est clair que  $\tau$  est une application linéaire de  $\mathcal{M}_n(K)$  dans  $\mathcal{M}_{n-m,n}(K)$ .

(a) Montrer les relations :

$$\begin{cases} \text{Ker } \tau \cap \text{Ker } \Phi_{N,N} = \text{Ker } \tau \cap \text{Ker } \Phi_{M,N} \\ \tau(\text{Ker } \Phi_{M,N}) \subset \tau(\text{Ker } \Phi_{N,N}) \end{cases}$$

(b) On suppose  $M$  et  $N$  semblables sur  $K$ . Montrer :

$$\tau(\text{Ker } \Phi_{M,N}) = \tau(\text{Ker } \Phi_{N,N}).$$

(c) On suppose  $M$  et  $N$  semblables sur  $K$ . Montrer qu'il existe  $Y$  dans  $\mathcal{M}_{m,n-m}(K)$  tel que :  $B = AY - YA'$ .

4. Montrer l'équivalence entre les deux assertions suivantes :
- (i)  $M$  est diagonalisable sur  $K$ ,
  - (ii)  $A$  et  $A'$  sont diagonalisables sur  $K$  et  $B$  est de la forme  $AY - YA'$  avec  $Y$  dans  $\mathcal{M}_{m,n-m}(K)$ .

## II. Similitude entière

### A. Généralités, premier exemple

1. Soit  $A$  un sous-anneau d'un corps. Montrer que  $\text{GL}_n(A)$  est l'ensemble des matrices de  $\mathcal{M}_n(A)$  dont le déterminant est un élément inversible de  $A$ . Expliciter ce résultat pour  $A = \mathbb{Z}$ .
2. Soient  $p$  un nombre premier,  $\mathbb{F}_p$  le corps fini  $\mathbb{Z}/p\mathbb{Z}$ . Si  $M$  est une matrice de  $\mathcal{M}_n(\mathbb{Z})$ , on note  $\overline{M}$  la matrice de  $\mathcal{M}_n(\mathbb{F}_p)$  obtenue en réduisant  $M$  modulo  $p$ . Montrer que si  $M$  et  $N$  sont deux matrices de  $\mathcal{M}_n(\mathbb{Z})$  semblables sur  $\mathbb{Z}$ , les matrices  $\overline{M}$  et  $\overline{N}$  sont semblables sur  $\mathbb{F}_p$ .
3. Pour  $a$  dans  $\mathbb{Z}$ , soient :

$$S_a = \begin{pmatrix} 1 & a \\ 0 & -1 \end{pmatrix}, \quad T_a = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}.$$

- (a) Montrer que  $S_0$  et  $S_1$  sont semblables sur  $\mathbb{Q}$  mais ne sont pas semblables sur  $\mathbb{Z}$ .

Soit  $M$  dans  $\mathcal{M}_2(\mathbb{Z})$  telle que  $\chi_M = X^2 - 1$ .

- (b) Montrer qu'il existe  $x_1$  et  $x_2$  dans  $\mathbb{Z}$  premiers entre eux tels que le vecteur colonne  $x = {}^t(x_1, x_2)$  vérifie  $Mx = x$ .
- (c) Montrer que  $M$  est semblable sur  $\mathbb{Z}$  à une matrice  $S_a$  avec  $a$  dans  $\mathbb{Z}$ .
- (d) Pour  $a$  et  $x$  dans  $\mathbb{Z}$ , déterminer  $T_x S_a T_x^{-1}$ ; conclure que  $M$  est semblable sur  $\mathbb{Z}$  à l'une des deux matrices  $S_0, S_1$ .

### B. Les ensembles $\mathcal{E}_{\mathbb{Z}}(X^2 - \delta)$

Dans cette partie, on fixe un élément  $\delta$  de  $\mathbb{Z}^*$  qui n'est pas le carré d'un entier et on considère  $P = X^2 - \delta$ .

1. (a) Vérifier que  $\mathcal{E}_{\mathbb{Z}}(P)$  est l'ensemble des matrices de la forme :

$$\begin{pmatrix} a & c \\ b & -a \end{pmatrix}$$

où  $a, b, c$  sont dans  $\mathbb{Z}$  et vérifient :  $a^2 + bc = \delta$ . Si  $a$  et  $b$  sont deux entiers relatifs tels que  $b$  divise  $\delta - a^2$ , vérifier que l'ensemble  $\mathcal{E}_{\mathbb{Z}}(P)$  contient une unique matrice de la forme :

$$\begin{pmatrix} a & c \\ b & -a \end{pmatrix}.$$

Cette matrice sera notée  $M_{(a,b)}$  dans la suite.

- (b) Soient  $a, b$  dans  $\mathbb{Z}$  tels que  $b$  divise  $\delta - a^2$ ,  $\lambda$  dans  $\mathbb{Z}$ . Montrer que les matrices  $M_{(a,b)}$ ,  $M_{(a,-b)}$ ,  $M_{(a+\lambda b,b)}$ ,  $M_{(-a,(\delta-a^2)/b)}$  sont semblables sur  $\mathbb{Z}$ .
2. Soit  $M$  dans  $\mathcal{E}_{\mathbb{Z}}(P)$ . Puisque  $M_{(a,-b)}$  et  $M_{(a,b)}$  sont semblables sur  $\mathbb{Z}$ , l'ensemble  $\mathcal{B}$  des  $b$  de  $\mathbb{N}^*$  tels qu'il existe une matrice  $M_{(a,b)}$  semblable sur  $\mathbb{Z}$  à  $M$  n'est pas vide; on note  $\beta(M)$  le plus petit élément de  $\mathcal{B}$ .
- (a) Montrer qu'il existe un entier  $a$  tel que  $|a| \leq \frac{\beta(M)}{2}$  et tel que  $M$  soit semblable sur  $\mathbb{Z}$  à  $M_{(a,\beta(M))}$ .
- (b) Comparer  $|\delta - a^2|$  et  $\beta(M)^2$ . En déduire que  $\beta(M)$  est majoré par  $\sqrt{\delta}$  si  $\delta > 0$ , par  $\sqrt{4|\delta|/3}$  si  $\delta < 0$ .
- (c) Montrer que  $\mathcal{E}_{\mathbb{Z}}(P)$  est réunion d'un nombre fini de classes de similitude entière.

### C. Diagonalisabilité et réduction modulo $p$

Soient  $p$  un nombre premier,  $\overline{\mathbb{F}_p}$  une clôture algébrique du corps  $\mathbb{F}_p$  défini en II.A.2,  $l$  dans  $\mathbb{N}^*$ . Pour  $P$  dans  $\mathbb{Z}[X]$ , on note  $\overline{P}$  l'élément de  $\overline{\mathbb{F}_p}[X]$  obtenu en réduisant  $P$  modulo  $p$ . Si  $M$  est dans  $\mathcal{M}_l(\mathbb{Z})$ , on note  $\overline{M}$  la matrice de  $\mathcal{M}_l(\overline{\mathbb{F}_p})$  obtenue en réduisant  $M$  modulo  $p$ .

1. Soit  $P$  dans  $\mathbb{Z}[X]$  non constant dont les racines dans  $\mathbb{C}$  sont simples.
- (a) Montrer qu'il existe  $d$  dans  $\mathbb{N}^*$ ,  $S$  et  $T$  dans  $\mathbb{Z}[X]$  tels que :
- $$SP + TP' = d.$$
- (b) Si  $p$  ne divise pas  $d$ , montrer que les racines de  $\overline{P}$  dans  $\overline{\mathbb{F}_p}$  sont simples.
2. Soit  $M$  dans  $\mathcal{M}_l(\mathbb{Z})$  diagonalisable sur  $\mathbb{C}$ .
- (a) Montrer qu'il existe un élément  $P$  de  $\mathbb{Z}[X]$  unitaire, dont les racines complexes sont toutes simples et tel que  $P(M) = 0$ .
- (b) Montrer qu'il existe un entier  $d_M$  tel que si  $p$  ne divise pas  $d_M$  alors  $\overline{M}$  est diagonalisable sur  $\overline{\mathbb{F}_p}$ .

### D. Un résultat de non finitude

Soit  $P$  un élément de  $U_n(\mathbb{Z})$  dont les racines dans  $\mathbb{C}$  ne sont pas toutes simples.

1. Montrer qu'il existe  $l$  dans  $\mathbb{N}^*$ ,  $m$  dans  $\mathbb{N}$ ,  $Q$  dans  $U_l(\mathbb{Z})$ ,  $R$  dans  $U_m(\mathbb{Z})$  tels que :  $P = Q^2 R$ .

Grâce à I.B.4, on dispose de  $A$  dans  $\mathcal{D}_{\mathbb{Z}}(Q)$  et, si  $m > 0$ , de  $B$  dans  $\mathcal{D}_{\mathbb{Z}}(R)$ . Si  $p$  est un nombre premier, soit  $E_p$  la matrice :

$$\left( \begin{array}{c|c|c} A & pI_l & O \\ \hline O & A & O \\ \hline O & O & B \end{array} \right) \text{ si } m > 0, \quad \left( \begin{array}{c|c} A & pI_l \\ \hline O & A \end{array} \right) \text{ si } m = 0.$$

2. Les entiers  $d_A$  et  $d_B$  (si  $m > 0$ ) sont ceux définis en **II.C**. Soient  $p$  et  $q$  deux nombres premiers distincts tels que  $p$  ne divise ni  $d_A$ , ni  $l$ , ni  $d_B$  si  $m > 0$ . Montrer que  $E_p$  et  $E_q$  ne sont pas semblables sur  $\mathbb{Z}$ .
3. Conclure que  $\mathcal{E}_{\mathbb{Z}}(P)$  n'est pas réunion finie de classes de similitude entière.

### III. Un théorème de finitude

Si  $(\Gamma, +)$  est un groupe abélien et  $r$  un élément de  $\mathbb{N}^*$ , on dit que la famille  $(e_i)_{1 \leq i \leq r}$  d'éléments de  $\Gamma$  est une  $\mathbb{Z}$ -base de  $\Gamma$  si et seulement si tout élément de  $\Gamma$  s'écrit de façon unique  $\lambda_1 e_1 + \dots + \lambda_r e_r$  avec  $(\lambda_1, \dots, \lambda_r)$  dans  $\mathbb{Z}^r$ .

Si  $\Gamma$  admet une  $\mathbb{Z}$ -base finie, on dit que  $\Gamma$  est un groupe abélien libre de type fini ou, en abrégé, un g.a.l.t.f. On sait qu'alors toutes les  $\mathbb{Z}$ -bases de  $\Gamma$  ont même cardinal ; ce cardinal commun est appelé rang de  $\Gamma$ . Par exemple,  $(\mathbb{Z}^r, +)$  est un g.a.l.t.f de rang  $r$  (et tout g.a.l.t.f de rang  $r$  est isomorphe à  $\mathbb{Z}^r$ ).

On pourra admettre et utiliser le résultat suivant.

"Soient  $(\Gamma, +)$  un g.a.l.t.f de rang  $r$ ,  $\Gamma'$  un sous-groupe non nul de  $\Gamma$ . Alors il existe une  $\mathbb{Z}$ -base  $(e_i)_{1 \leq i \leq r}$  de  $\Gamma$ , un entier naturel non nul  $s \leq r$  et des éléments  $d_1, \dots, d_s$  de  $\mathbb{N}^*$  tels que  $(d_i e_i)_{1 \leq i \leq s}$  soit une  $\mathbb{Z}$ -base de  $\Gamma'$ . En particulier,  $\Gamma'$  est un g.a.l.t.f de rang  $\leq r$ ."

#### A. Groupes abéliens libres de type fini

1. Soient  $\Gamma$  un g.a.l.t.f de rang  $n$ ,  $(e_i)_{1 \leq i \leq n}$  une  $\mathbb{Z}$ -base de  $\Gamma$ ,  $(f_j)_{1 \leq j \leq n}$  une famille d'éléments de  $\Gamma$ . Si  $1 \leq j \leq n$ , on écrit :

$$f_j = \sum_{i=1}^n p_{i,j} e_i$$

où la matrice :  $P = (p_{i,j})_{1 \leq i,j \leq n}$  est dans  $\mathcal{M}_n(\mathbb{Z})$ . Montrer que  $(f_j)_{1 \leq j \leq n}$  est une  $\mathbb{Z}$ -base de  $\Gamma$  si et seulement si  $P$  appartient à  $\text{GL}_n(\mathbb{Z})$ .

2. Soient  $\Gamma$  un g.a.l.t.f,  $\Gamma'$  un sous-groupe de  $\Gamma$ . Montrer que le groupe quotient  $\Gamma/\Gamma'$  est fini si et seulement si  $\Gamma$  et  $\Gamma'$  ont même rang.
3. Soient  $R$  un anneau commutatif intègre dont le groupe additif est un g.a.l.t.f,  $I$  un idéal non nul de  $R$ .
  - (a) Montrer que l'anneau quotient  $R/I$  est fini.
  - (b) Montrer que l'ensemble des idéaux de  $R$  contenant  $I$  est fini.
4. Soient  $m$  et  $n$  dans  $\mathbb{N}^*$  avec  $m \leq n$ ,  $V$  un sous-espace de dimension  $m$  de  $\mathbb{Q}^n$ . Montrer qu'il existe une  $\mathbb{Z}$ -base  $(e_i)_{1 \leq i \leq n}$  de  $\mathbb{Z}^n$  telle que  $(e_i)_{1 \leq i \leq m}$  soit une  $\mathbb{Q}$ -base de  $V$ .

Dans les parties **III.B** et **III.C**,  $P$  est un élément de  $U_n(\mathbb{Z})$  irréductible sur  $\mathbb{Q}$ ,  $\alpha$  une racine de  $P$  dans  $\mathbb{C}$ ,  $\mathbb{Q}[\alpha]$  la  $\mathbb{Q}$ -sous-algèbre de  $\mathbb{C}$  engendrée par  $\alpha$ , c'est-à-dire le sous-espace du  $\mathbb{Q}$ -espace vectoriel  $\mathbb{C}$  dont  $(\alpha^i)_{0 \leq i \leq n-1}$  est une base. On rappelle que  $\mathbb{Q}[\alpha]$  est un sous-corps de  $\mathbb{C}$ . Si l'élément  $x$  de  $\mathbb{Q}[\alpha]$  s'écrit  $x_0 + x_1 \alpha + \dots + x_{n-1} \alpha^{n-1}$  où  $(x_0, \dots, x_{n-1})$  est dans  $\mathbb{Q}^n$ , on pose :

$$\mathcal{N}(x) = \max_{0 \leq i \leq n-1} |x_i|.$$

On note  $\mathbb{Z}[\alpha]$  le sous-anneau de  $\mathbb{Q}[\alpha]$  :

$$\mathbb{Z}[\alpha] = \left\{ \sum_{i=0}^{n-1} x_i \alpha^i, (x_0, \dots, x_{n-1}) \in \mathbb{Z}^n \right\}.$$

On vérifie que  $\mathbb{Q}[\alpha]$  est le corps des fractions de  $\mathbb{Z}[\alpha]$ ; la justification n'est pas demandée. Si  $P$  est une partie non vide de  $\mathbb{Q}[\alpha]$  et  $a$  un élément de  $\mathbb{Q}[\alpha]$ , on note  $aP$  l'ensemble :

$$\{ax, x \in P\}.$$

On note  $\mathcal{I}$  l'ensemble des idéaux non nuls de  $\mathbb{Z}[\alpha]$ .

## B. Classes d'idéaux

1. Montrer qu'il existe  $C > 0$  tel que :

$$\forall (x, y) \in \mathbb{Q}[\alpha]^2, \quad \mathcal{N}(xy) \leq C \mathcal{N}(x) \mathcal{N}(y).$$

2. Si  $y$  est dans  $\mathbb{Q}[\alpha]$  et  $M$  dans  $\mathbb{N}^*$ , montrer qu'il existe  $m$  dans  $\{1, \dots, M^n\}$  et  $a$  dans  $\mathbb{Z}[\alpha]$  tels que :

$$\mathcal{N}(my - a) \leq \frac{1}{M}.$$

*Indication.* Posant  $y = y_0 + y_1\alpha + \dots + y_{n-1}\alpha^{n-1}$  avec  $(y_0, \dots, y_{n-1})$  dans  $\mathbb{Q}^n$ , on pourra considérer, pour  $0 \leq j \leq M^n$  :

$$u_j = \sum_{i=0}^{n-1} (jy_i - [jy_i]) \alpha^i,$$

où  $[x]$  désigne, pour  $x$  dans  $\mathbb{R}$ , la partie entière de  $x$ .

3. On définit la relation  $\sim$  sur  $\mathcal{I}$  en convenant que  $I_1 \sim I_2$  si et seulement s'il existe  $a$  et  $b$  dans  $\mathbb{Z}[\alpha] \setminus \{0\}$  tels que  $aI_1 = bI_2$ , c'est-à-dire s'il existe  $x$  dans  $\mathbb{Q}[\alpha] \setminus \{0\}$  telle que  $I_2 = xI_1$ . Il est clair que  $\sim$  est une relation d'équivalence sur  $\mathcal{I}$ . On se propose de montrer que le nombre de classes de cette relation est fini.

On fixe  $I$  dans  $\mathcal{I}$ ,  $z$  dans  $I \setminus \{0\}$  tel que  $\mathcal{N}(z)$  soit minimal (ce qui est possible car l'image d'un élément non nul de  $\mathbb{Z}[\alpha]$  par  $\mathcal{N}$  appartient à  $\mathbb{N}^*$ ).

Soient également  $M$  un entier strictement supérieur à  $C$  et  $\ell$  le ppcm des éléments de  $\mathbb{N}^*$  inférieurs ou égaux à  $M^n$ .

- (a) Soit  $x$  dans  $I$ . En appliquant la question 2 à  $y = \frac{x}{z}$  montrer que :

$$\ell I \subset z\mathbb{Z}[\alpha].$$

- (b) Vérifier que  $J = \frac{\ell}{z}I$  est un idéal de  $\mathbb{Z}[\alpha]$  contenant  $\ell\mathbb{Z}[\alpha]$  et conclure.



### C. Classes de similitude et classes d'idéaux

- Soient  $M$  dans  $\mathcal{E}_{\mathbb{Z}}(P)$ ,  $X_M$  l'ensemble des éléments  $x = (x_1, \dots, x_n)$  non nuls de  $\mathbb{Z}[\alpha]^n$  tels que le vecteur colonne  ${}^t x$  soit vecteur propre de  $M$  associé à  $\alpha$ .
  - Montrer que  $X_M$  n'est pas vide, que si  $x$  et  $y$  sont dans  $X_M$  il existe  $a$  et  $b$  dans  $\mathbb{Z}[\alpha] \setminus \{0\}$  tels que  $ax = by$ .
  - Si  $x = (x_1, \dots, x_n)$  est dans  $X_M$ , soit  $(x)$  le sous-groupe de  $(\mathbb{Z}[\alpha], +)$  engendré par  $x_1, \dots, x_n$ . Montrer que  $(x)$  est un idéal de  $\mathbb{Z}[\alpha]$ , que  $(x_1, \dots, x_n)$  en est une  $\mathbb{Z}$ -base, que si  $y$  est dans  $X_M$ , alors  $(x) \sim (y)$ .  
On notera  $j$  l'application de  $\mathcal{E}_{\mathbb{Z}}(P)$  dans l'ensemble quotient  $\mathcal{I}/\sim$  qui à  $M$  associe la classe de  $(x)$  pour  $\sim$ .
- Montrer que l'application  $j$  est surjective.
  - Soient  $M$  et  $M'$  dans  $\mathcal{E}_{\mathbb{Z}}(P)$ . Montrer que  $M$  et  $M'$  sont semblables sur  $\mathbb{Z}$  si et seulement si  $j(M) = j(M')$ .

De **III.B** et **III.C** il découle que si l'élément  $P$  de  $U_n(\mathbb{Z})$  est irréductible sur  $\mathbb{Q}$ , alors  $\mathcal{E}_{\mathbb{Z}}(P)$  est réunion finie de classes de similitude entière.

### D. Finitude de l'ensemble $\mathcal{D}_{\mathbb{Z}}(P)$

On se propose d'établir que pour tout polynôme unitaire non constant  $P$  de  $\mathbb{Z}[X]$ , l'ensemble  $\mathcal{D}_{\mathbb{Z}}(P)$  est réunion finie de classes de similitude entière. On raisonne par récurrence sur le degré de  $P$ . Le cas où ce degré est 1 étant évident, on suppose  $n \geq 2$  et le résultat prouvé pour tout  $P$  de degré majoré par  $n - 1$ .

On fixe désormais  $P$  dans  $U_n(\mathbb{Z})$ . Si  $P$  est irréductible sur  $\mathbb{Q}$ , on a vu à la fin de **III.C** que  $\mathcal{E}_{\mathbb{Z}}(P)$  est réunion finie de classes de similitude entière. On suppose donc  $P$  réductible sur  $\mathbb{Q}$ , et on se donne un diviseur irréductible  $Q$  de  $P$  dans  $\mathbb{Q}[X]$  unitaire non constant, dont on note  $m$  le degré. D'après la question **I.B.3**,  $Q$  et  $P/Q$  sont respectivement dans  $U_m(\mathbb{Z})$  et  $U_{n-m}(\mathbb{Z})$ . On dispose donc (récurrence) de  $r$  et  $s$  dans  $\mathbb{N}^*$ , de  $r$  éléments  $A_1, \dots, A_r$  de  $\mathcal{D}_{\mathbb{Z}}(Q)$  (resp. de  $s$  éléments  $A'_1, \dots, A'_s$  de  $\mathcal{D}_{\mathbb{Z}}(P/Q)$ ) tels que tout élément de  $\mathcal{D}_{\mathbb{Z}}(Q)$  (resp.  $\mathcal{D}_{\mathbb{Z}}(P/Q)$ ) soit semblable sur  $\mathbb{Z}$  à un et un seul  $A_i$  (resp.  $A'_j$ ).

Soit  $M$  dans  $\mathcal{D}_{\mathbb{Z}}(P)$ .

- Montrer que  $M$  est semblable sur  $\mathbb{Z}$  à une matrice de la forme :

$$\left( \begin{array}{c|c} A_i & B \\ \hline O & A'_j \end{array} \right)$$

avec  $1 \leq i \leq r, 1 \leq j \leq s, B \in \mathcal{M}_{m, n-m}(\mathbb{Z})$ .

- Montrer que :

$$\Gamma = \mathcal{M}_{m, n-m}(\mathbb{Z}) \cap \{A_i X - X A'_j ; X \in \mathcal{M}_{m, n-m}(\mathbb{Q})\}$$

$$\text{et } : \Gamma' = \{A_i X - X A'_j ; X \in \mathcal{M}_{m, n-m}(\mathbb{Z})\}$$

sont deux g.a.l.t.f de même rang.

- Conclure que  $\mathcal{D}_{\mathbb{Z}}(P)$  est réunion finie de classes de similitude entière.