**Département de Mathématiques et Informatique** **Année 1999-2000**

D.E.U.G. M.A.S.S. ou I.U.P. (en gros D.E.U.G. A 1 et 2) Algèbre

**Quelques idées d'exos**

---

**Exercice 1 : Le thérème de Cauchy**

Il s'agit de prouver le théorème de Cauchy dont voici l'énoncé : *un groupe fini $G$ d'ordre $pq$, avec $p$ premier, contient un élément d'ordre $p$.*

Pour cela, on introduit $X$ le sous-ensemble de $G^p$ constitué des $p$-uplets suivants :

$$X = \{(g_1, \ldots, g_p) \in G^p,\ g_1 \cdots g_p = 1\}$$

**1.** On commence par dénombrer $X$.

a. Pourquoi $X$ est-il non vide ?

b. Montrer que l'application $X \to G^{p-1}$ qui au $p$-uplet $(g_1, \ldots, g_p) \in X$ associe le $(p-1)$-uplet $(g_1, \ldots, g_{p-1})$ est une bijection.

c. En déduire le cardinal de $X$ (rappel : le cardinal de $E^r$ avec $E$ fini de cardinal $n$, est égal à $n^r$).

**2.** Vérifier l'équivalence entre les deux propriétés suivantes : (i) : $G$ possède un élément d'ordre $p$ et (ii) : $X$ contient un élément dont toutes les coordonnées sont égales et distinctes de 1.

**3.** On introduit $c$ le $p$-cycle $(1, \ldots, p)$ et pour $(g_1, \ldots, g_p) \in G^p$, on pose :

$$c.(g_1, \ldots, g_p) = (g_{c(1)}, \ldots, g_{c(p)}) = (g_p, g_2, g_3, \ldots, g_{p-1}, g_1)$$

Sur le même principe, pour $0 \leqslant i \leqslant p-1$, on définit $c^i.(g_1, \ldots, g_p)$.

a. Si $\eth \in X$, vérifier que $c.\eth \in X$. Montrer que l'on a la même propriété en remplaçant $c$ par une de ses puissances.

**4.** Soient $Y$ et $Z$ les deux sous-ensembles de $X$ définis par :

$$Y = \{(g_1, \ldots, g_p) \in X,\ g_1 = \cdots = g_p\} \qquad Z = \{(g_1, \ldots, g_p) \in X,\ (\exists\, i \neq j,\ g_i \neq g_j)\}$$

Bien s ˚ r, $X$ est la réunion disjointe de $Y$ et $Z$.

a. En permutant les coordonnées, montrer qu'un quelconque élément $(g_1, \ldots, g_p) \in Z$ permet d'en construire $(p-1)$ autres.

b. À l'aide de la question précédente, prouver que le cardinal de $Z$ est divisible par $p$.

c. En déduire le cardinal de $Y$ est lui aussi divisible par $p$.

d. Conclure.

**Exercice 2 : Pas bête ce général chinois**

Pour dénombrer un de ses bataillons, un général chinois a l'idée suivante : tout d'abord, il sait que ce bataillons compte moins de 1000 soldats. Ensuite il exige de ses troupes de se mettre par paquets de sept et remarque que seuls deux soldats n'ont pas trouvé place dans aucun groupe. Il prend note de ce nombre deux. Il réitère le même expérience en exigeant que les soldats se rangent par paquets de onze puis treize. Dans le premier cas il note que seulement trois soldats n'ont pas trouvé place dans aucun groupe et dans le second seul un hurluberlu n'a pas trouvé à s'insérer nul part. Ces informations lui suffisent pour dénombrer son bataillon.

**1.** Quel est donc le secret de cet ingénieux général chinois ?

**Indication :** les premiers 7, 11 et 13 n'ont évidemment pas été choisis au hasard. De même l'ordre des exercices de cette feuille ne relève pas d'un tirage aléatoire...

**Exercice 3 : Calculs de minimum**

Considérons $\mathcal{C}([0,1],\mathbb{R})$, l'espace des fonctions continues de $[0,1]$ vers $\mathbb{R}$, muni du produit scalaire :

$$\langle f, g\rangle = \int_0^1 f(t)g(t)dt$$

**1.** Soit $F$ le sous-espace de $\mathcal{C}([0,1],\mathbb{R})$ constitué des applications affines, c'est-à-dire $F = \{t \mapsto at+b,\ (a,b) \in \mathbb{R}^2\}$ ; il s'agit de déterminer la valeur $\min_{(a,b)\in\mathbb{R}^2} \left\{\int_0^1 (t^2 - at - b)^2 dt\right\}$.

a. Lier le minimum cherché à la distance d'un élément de $\mathcal{C}([0,1],\mathbb{R})$ à $F$.

b. Calculer une base orthonormée de $F$.

c. Calculer $\pi_F(t^2)$ le projeté orthogonal de la fonction $t \mapsto t^2$ sur $F$.

d. Conclure.

**2.** Reprendre les questions précédentes, *la dernière étant hors barême*, afin de déterminer la valeur $\min_{(a,b,c)\in\mathbb{R}^3} \left\{\int_0^1 (t^3 - at^2 - bt - c)^2 dt\right\}$. (penser à ré-investir vos calculs antérieurs).

**Exercice 4 : L'égalité $SL_n(\mathbb{R}) = E_n(\mathbb{R})$**

On désigne par $E_{ij}$ la matrice $n \times n$ dont tous les termes sont nuls sauf le $(ij)$-ème qui vaut 1 et pour $i \neq j$ et $\lambda \in \mathbb{R}$, on introduit la matrice $B_{ij}(\lambda) = \mathrm{I}_n + \lambda E_{ij}$. C'est un grand honneur pour moi de vous présenter $B_{31}(\lambda)$ pour $n = 4$ :

$$B_{31}(\lambda) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \lambda & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Enfin on note $E_n(\mathbb{R})$ le sous-groupe de $GL_n(\mathbb{R})$ engendré par les matrices $B_{ij}(\lambda)$ pour $\lambda \in \mathbb{R}$. Nous allons établir l'égalité $SL_n(\mathbb{R}) = E_n(\mathbb{R})$.

**1.** Que vaut le produit $B_{ij}(\lambda)B_{ij}(\mu)$ pour $\lambda, \mu \in \mathbb{R}$ ? Quel est l'inverse de $B_{ij}(\lambda)$ ?

**2.** Quel est l'effet sur une matrice $M \in M_n(\mathbb{R})$ d'une multiplication par $B_{ij}(\lambda)$ à droite ? Et à gauche ?

**3.** Momentanément, on suppose que $n = 2$.

a. Commencer par dresser un dictionnaire liant les quatres transformations :

$$L_1 \leftarrow L_1 + \lambda L_2 \qquad L_2 \leftarrow L_2 + \lambda L_1 \qquad C_1 \leftarrow C_1 + \lambda C_2 \qquad C_2 \leftarrow C_2 + \lambda C_1$$

et les quatres multiplications par $B_{12}(\lambda)$ à gauche et à droite et par $B_{21}(\lambda)$ à gauche et à droite.

b. Montrer que pour toute matrice $M$ de la forme $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $a$ ou $b$ non nul, il existe $Q \in E_2(\mathbb{R})$ telle que :

$$MQ = \begin{pmatrix} 1 & 0 \\ c' & d' \end{pmatrix}$$

(on pourra distinguer les cas $a = 0$, $b = 0$ et $a, b$ non nuls).

c. En déduire que pour toute matrice $M$ de taille $2 \times 2$ avec une première ligne non nulle, il existe $P, Q \in E_2(\mathbb{R})$ telles que :

$$PMQ = \begin{pmatrix} 1 & 0 \\ 0 & \Delta \end{pmatrix}$$

Au fait que vaut $\Delta$ ?

d. Montrer que pour toute matrice $M \in SL_2(\mathbb{R})$ il existe $P, Q \in E_2(\mathbb{R})$ telles que $PMQ = \mathrm{I}_2$. Pourquoi cela prouve-t-il que $M \in E_2(\mathbb{R})$.

e. À titre d'exemple, pour $a \in \mathbb{R}^*$ écrire la matrice $\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix}$ comme produit de $B_{ij}(\lambda)$.

**4.** Bon, il faut grandir maintenant et passer au cas $n$ quelconque en considérant $M \in SL_n(\mathbb{R})$.

a. Commencer par montrer qu'il existe $P, Q \in E_n(\mathbb{R})$ telles que :

$$PMQ = \begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix}$$

avec $N \in SL_{n-1}(\mathbb{R})$.

b. En déduire que $SL_n(\mathbb{R}) = E_n(\mathbb{R})$.

**5.** Soit $M \in GL_n(\mathbb{R})$, montrer qu'il existe $P \in E_n(\mathbb{R})$ et une autre $Q \in E_n(\mathbb{R})$ telles que $M = P \times \operatorname{diag}(1, \dots, 1, \Delta) = \operatorname{diag}(1, \dots, 1, \Delta) \times Q$.

**Exercice 5 : Déterminant de Gram et distance d'un point à un sous-espace**

Le déterminant de Gram d'une famille $v_1, \dots, v_n$ de vecteurs d'un espace euclidien $E$ de dimension finie est noté $\operatorname{Gram}(v_1, \dots, v_n)$ et est défini par :

$$\operatorname{Gram}(v_1, \dots, v_n) = \det(\langle v_i, v_j \rangle_{i,j})$$

**1.** Montrer que $\operatorname{Gram}(v_1, \dots, v_n)$ est nul si et seulement si la famille $\{v_1, \dots, v_n\}$ est liée.

**2.** Soit $F$ un sous-espace vectoriel de $E$ et $\{f_1, \dots, f_m\}$ une base (quelconque) de $F$. On décompose tout $v \in E$ sous la forme $v = v' + v''$ avec $v' \in F$ et $v'' \in F^\perp$. Montrer que :

$$\operatorname{Gram}(v, f_1, \dots, f_m) = \|v''\|^2 \operatorname{Gram}(f_1, \dots, f_m)$$

et en déduire que :

$$d(v, F)^2 = \frac{\operatorname{Gram}(v, f_1, \dots, f_m)}{\operatorname{Gram}(f_1, \dots, f_m)}$$

où $d(v, F)$ désigne la distance de $v$ à $F$.

**Exercice 6 : Matrice compagnon et dualité**

Soit $K$ un corps ($K = \mathbb{R}$ ou $\mathbb{C}$ si vous préférez), $E$ un $K$-espace vectoriel de dimension finie $n$ et $u \in \mathcal{L}(E)$ un endomorphisme de $E$. On suppose que $(E, u)$ est un espace **monogène** c'est-à-dire qu'il existe $x \in E$ tel que :

$$E = Kx \oplus Ku(x) \oplus \cdots \oplus Ku^{n-1}(x)$$

Autrement dit, la famille $\mathcal{B} = \{x, u(x), \dots, u^{n-1}(x)\}$ est une $K$-base de $E$.

**1.** Montrer l'existence de coefficents $a_0, \dots, a_{n-1} \in K$ tels que :

$$u^n(x) + a_{n-1}u^{n-1}(x) + \cdots + a_0 x = 0$$

**2.** À l'aide de ces coefficients, dresser la matrice $M$ de $u$ dans la base $\mathcal{B}$.

**3.** En déduire que le polynôme caractéristque de $u$ n'est rien d'autre que :

$$(-1)^n(X^n + a_{n-1}X^{n-1} + \cdots + a_0)$$

(indication : développer $\det(M - X\,\mathrm{Id})$ par rapport à la dernière colonne). En déduire que :

$$u^n + a_{n-1}u^{n-1} + \cdots + a_0 = 0$$

**4.** Considérons $E^*$ l'espace dual de $E$ ainsi que $v = {}^t u$ l'endomorphisme transposé de $u$. On va montrer que $(E^*, v)$ est lui aussi un espace monogène ; notons, pour alléger, $e_i = u^{i-1}(x)$ et considérons $\{e_i^*\}_i$ la base duale de $\{e_i\}_i$. Vérifier que :

$$E^* = Ke_n^* \oplus Kv(e_n^*) \oplus \cdots \oplus Kv^{n-1}(e_n^*)$$

Conclure.

**5.** Dresser la matrice de $v$ dans la base $\{e_n^*, v(e_n^*), \dots, v^{n-1}(e_n^*)\}$. Que remarquez-vous ?
**6.** En déduire que la matrice $M$ est semblable à sa transposée[1].

**Exercice 7 : Suites récurrentes linéaires**

On note $\mathcal{F}(\mathbb{N}, \mathbb{C})$ le $\mathbb{C}$-espace vectoriel des suites complexes et on s'intéresse au sous-ensemble $E$ de $\mathcal{F}(\mathbb{N}, \mathbb{C})$ constitué des suites $(u_n)_{n\in\mathbb{N}}$ vérifiant la relation :

$$u_{n+2} + au_{n+1} + bu_n = 0 \qquad (1)$$

où $(a, b) \in \mathbb{C} \times \mathbb{C}^*$. On introduit de plus l'application $\varphi$ définie par :

$$\begin{array}{rccc} \varphi : & E & \longrightarrow & \mathbb{C}^2 \\ & (u_n)_{n\in\mathbb{N}} & \longmapsto & (u_0, u_1) \end{array}$$

**1.** Commencer par vérifier :
a. que l'ensemble $E$ est un sous-espace vectoriel de $\mathcal{F}(\mathbb{N}, \mathbb{C})$ ;
b. et que l'application $\varphi$ est linéaire.
**2.** On cherche ici à déterminer la dimension (sur $\mathbb{C}$) de $E$ ; procéder comme suit.
a. Vérifier que $\varphi$ est surjective.
b. Étudier l'injectivité de $\varphi$.
c. En déduire la dimension de $E$ (rappel : deux espaces vectoriels isomorphes ont même dimension).
**3.** Soit $r \in \mathbb{C}^*$ ; à quelle condition (sur $r$) la suite géométrique de raison $r$ — c'est-à-dire la suite $(r^n)_{n\in\mathbb{N}}$ — appartient-elle à $E$.
**4.** On se place ici dans le cas où le polynôme $X^2 + aX + b$ admet deux racines distinctes $r_1$ et $r_2$.
a. Montrer que les suites géométriques $(r_1^n)_{n\in\mathbb{N}}$ et $(r_2^n)_{n\in\mathbb{N}}$ sont linéairement indépendantes.
b. En déduire que pour tout $(u_n)_{n\in\mathbb{N}} \in E$ il existe $(\lambda, \mu) \in \mathbb{C}^2$ unique tel que $u_n = \lambda r_1^n + \mu r_2^n$.
**5.** On se place pour finir dans le cas où le polynôme $X^2 + aX + b$ admet une racine double notée $r$.
a. Montrer que la suite $(nr^n)_{n\in\mathbb{N}}$ appartient alors à $E$.
b. Vérifier que les suites $(r^n)_{n\in\mathbb{N}}$ et $(nr^n)_{n\in\mathbb{N}}$ sont linéairement indépendantes.
c. En déduire la forme des éléments de $E$ dans ce cas.

**Exercice 8 :**

Un phare émet deux signaux lumineux l'un de couleur rouge à raison d'un signal tous les quarts d'heure, l'autre de couleur jaune toutes les 28 minutes. Un observateur remarque un signal rouge à 0h 02 et un jaune à 0h 08. Il se demande s'il est possible de voir les deux signaux en même temps et décide d'attendre jusqu'à ce qu'un tel phénomène se produise.
**1.** Son attente est-elle vaine ?
**2.** Si non, jusqu'à quelle heure devra-t-il patienter afin de voir les deux premiers signaux simultanément ?

**Exercice 9 : Pauvre forme, elle est dégénérée**

Soit $q : \mathbb{R}^3 \to \mathbb{R}$ la forme quadratique définie par $q(x, y, z) = x^2 - z^2 + 2xy + 2yz$ et $\varphi$ sa forme polaire.
**1.** Écrire $q$ sous la forme de somme de carrés.
**2.** En déduire le rang, la signature de $q$, une base orthogonale pour $\varphi$ et enfin $N$ le noyau de $\varphi$ (on rappelle que $N = \{v \in \mathbb{R}^3,\ (\forall w \in \mathbb{R}^3,\ \varphi(v, w) = 0)\}$.
**3.** Soit $F$ le sous-espace de $\mathbb{R}^3$ engendré par le vecteur $(1, 1, 1)$.
a. Déterminer $F^\perp$, c'est-à-dire $\{v \in \mathbb{R}^3,\ (\forall w \in F,\ \varphi(v, w) = 0)\}$.
b. Vérifier que $N \subset F^\perp$

[1] Plus généralement, on peut montrer que toute matrice (à coefficients dans un corps) est semblable à sa transposée.

c. Déterminer ${F^{\perp}}^{\perp}$

d. Vérifier que ${F^{\perp}}^{\perp} = N + F$. Ce genre de phénomène peut-il se produire dans un espace euclidien ?