Université du Littoral Côte d'Opale — Année universitaire 2019–2020
Master MEEF — 1ère année

# DS 4 - Préparation à l'écrit d'Algèbre

Durée : 5 h
le 09/01/2020
Documents non autorisés
Calculatrices personnelles autorisées

*Ce devoir est constitué de deux extraits de sujet proposés aux concours de recrutement de professeurs. Ils sont évidement totalement indépendant. Les étudiants traiterons ces extraits sur des copies séparées (pouvant être de même couleur).*

# Extrait 1

On note $\mathbb{N}$ l'ensemble des entiers naturels, $\mathbb{N}_0$ l'ensemble des entiers naturels non nuls et $\mathbb{Z}$ l'ensemble des entiers relatifs. Soient $p$ et $q$ deux entiers relatifs tels que $p \leqslant q$, on note $[\![p, q]\!]$ l'ensemble des entiers relatifs $k$ tels que $p \leqslant k \leqslant q$.

Ce problème a pour objet l'étude de deux méthodes de chiffrement. A chaque lettre de l'alphabet est associé un unique entier compris entre 0 et 25 de la façon suivante : à la lettre A est associé 0, à la lettre B est associé 1, ..., à la lettre Z est associé 25. Cet entier est appelé **rang de la lettre**.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *A* | *B* | *C* | *D* | *E* | *F* | *G* | *H* | *I* | *J* | *K* | *L* | *M* | *N* | *O* | *P* | *Q* | *R* | *S* | *T* | *U* | *V* | *W* | *X* | *Y* | *Z* |

## Partie A - Un chiffrement monographique

L'objectif de cette partie est de démontrer les théorèmes de Bézout, puis de Gauss, et de mettre en œuvre ces théorèmes dans le chiffrement proposé.

**I.** Soient $a$ et $b$ des entiers relatifs non nuls.

**1.** Montrer que s'il existe des entiers relatifs $u$ et $v$ tels que $au + bv = 1$, alors $a$ et $b$ sont premiers entre eux.

**2.** On veut à présent prouver que la réciproque de cette propriété est vraie. On suppose que $a$ et $b$ sont premiers entre eux et on considère l'ensemble $\mathcal{E}$ des entiers relatifs de la forme $au + bv$ où $u$ et $v$ sont des entiers relatifs.

**a.** Montrer que l'ensemble $\mathcal{E} \cap \mathbb{N}_0$ admet un plus petit élément, que l'on notera $n_0$.

**b.** Démontrer que le reste de la division euclidienne de $a$ (respectivement $b$) par $n_0$ vaut 0.

**c.** Conclure.

**3.** Enoncer le théorème ainsi démontré.

**II.** A l'aide du théorème précédent, démontrer que, pour tous les entiers relatifs non nuls $a, b$ et $c$, si $a$ divise $bc$ et si $a$ et $b$ sont premiers entre eux, alors $a$ divise $c$.

**III. Chiffrement lettre à lettre.**

**1. Un exemple.** Dans cette question, on décide de coder chaque lettre d'un mot par un nombre $y$ défini comme suit : *si $x$ est le rang de la lettre à coder, $y$ est le reste de la division euclidienne de* $58x$ *par* 369*.*

**2.** Coder le mot G A U S S.

**3.** Proposer une activité de classe sur le tableur permettant, à partir du codage des 26 lettres de l'alphabet de décoder le mot de 6 lettres qui se cache derrière la suite de nombres :

$$290 \quad 232 \quad 248 \quad 327 \quad 0 \quad 364$$

(Dans cette question, le décodage effectif n'est pas demandé; il le sera plus tard.)

**4. Principe général du chiffrement lettre à lettre.** On se donne un couple d'entiers naturels $(n, e)$ vérifiant les conditions suivantes :

- L'entier $n$ est supérieur ou égal à 26.
- Les entiers $n$ et $e$ sont premiers entre eux.

Chaque lettre est alors codée de la façon suivante : *si $x$ est le rang de la lettre à coder, $y$ est le reste de la division euclidienne de $ex$ par $n$.*

**a.** Démontrer qu'il existe un entier naturel $f$ tel que $fe \equiv 1 \pmod{n}$.

**b.** Démontrer que la connaissance de $f$ permet de retrouver $x$ à partir de $y$. On dit que $f$ est une *clé de décodage* associée à la clé de codage $(n, e)$.

**5. Un procédé de construction d'un clé de codage et d'une clé de décodage associée :**

- On choisit quatre entiers naturels $a, b, c$ et $d$ supérieurs ou égaux à 3.
- On pose : $M = ab - 1$, $e = cM + a$, $f = dM + b$ et $n = \dfrac{ef - 1}{M}$.

**a.** Vérifier que $(n, e)$ est une clé de codage et que $f$ est une clé de décodage associée.

**b.** Calculer $n, e$ et $f$ lorsque $a = 3$, $b = 4$, $c = 5$ et $d = 6$.

**c.** Un mot de 6 lettres a été codé à l'aide de la clé définie à la question précédente :

$$290 \quad 232 \quad 248 \quad 327 \quad 0 \quad 364$$

Décoder ce mot

**6. Ensemble des clés de décodage associées à une clé de codage donnée.** On revient au cas général où $n$ est un entier naturel supérieur ou égale à 26 et $e$ un entier naturel premier avec $n$ et on se propose de déterminer l'ensemble des couples $(u, v)$ d'entiers relatifs tels que $nu + ev = 1$.
L'algortihme d'Euclide, qui permet de déterminer le PGCD de deux entiers naturels non nuls, assure l'existence d'un entier naturel $N$ strictement supérieur à 1 et de deux suites finies $(r_k)_{k\in[\![0,N+1]\!]}$ et $(q_k)_{k\in[\![1,N]\!]}$ telles que :

- La suite $(r_k)_{k\in[\![0,N+1]\!]}$ est strictement décroissante.
- $r_0 = n$, $r_1 = e$ et $r_{N+1} = 0$.
- $\forall k \in [\![1, N]\!]$, $r_{k-1} = r_k q_k + r_{k+1}$.

**a.** Que vaut $r_N$ ?

**b.** Démontrer qu'il existe deux suites d'entiers relatifs $(u_k)_{k\in[\![0,N]\!]}$ et $(v_k)_{k\in[\![0,N]\!]}$ vérifiant, pour tout $k \in [\![0, N]\!]$,

$$r_k = nu_k + ev_k$$

**c.** En déduire une clé de décodage associée à la clé de codage $(n, e)$.

**d.** On met en œuvre cette méthode à l'aide d'un tableur à partir de la clé de codage $(369, 58)$ :

| | A | B | C | D |
|---|---|---|---|---|
| 1 | r | q | u | v |
| 2 | 369 | | 1 | 0 |
| 3 | 58 | 6 | 0 | 1 |
| 4 | 21 | 2 | 1 | -6 |
| 5 | 16 | 1 | -2 | 13 |

Quelle formule a-t-on saisie dans le cellule C4 pour que, tirée en bas à droite, elle permette de déterminer les valeurs des termes des deux suites $(u_k)$ et $(v_k)$?

**e.** Déterminer un couple $(u, v)$ d'entiers relatifs tels que $369u + 58v = 1$ et une clé de décodage associée à la clé de codage $(369, 58)$.

**f.** Déterminer l'ensemble des couples $(u, v)$ d'entiers relatifs tels que $369u + 58v = 1$ et l'ensemble des clés de décodage associées à la clé de codage $(369, 58)$.

## Partie B - Chiffrement de Hill

L'objectif de cette partie est de retrouver quelques résultats sur les matrices carrées d'ordre 2 à coefficients réels, puis de les appliqur aux chiffrements de Hill.
La matrice nulle de $M_2(\mathbb{R})$ est notée $O_2$ et la matrice unité est notée $I_2$. Pour tout entier naturel $n$ non nul, si $P$ et $Q$ sont deux matrices carrées de $M_2(\mathbb{Z})$ de coefficients respectifs $p_{i,j}$ et $q_{i,j}$, on dit qu'elles sont congrues modulo $n$ et on note $P \equiv Q \pmod n$ lorsque

$$\forall (i, j) \in [\![1, 2]\!],\ p_{i,j} \equiv q_{i,j} \pmod n.$$

De même, on dit que les vecteurs colonnes à coefficients dans $\mathbb{Z}$

$$X = \begin{bmatrix} x \\ y \end{bmatrix} \quad \text{et} \quad X' = \begin{bmatrix} x' \\ y' \end{bmatrix}$$

sont congrus modulo $n$ et on note $X \equiv X' \pmod n$ lorsque $x \equiv x' \pmod n$ et $y \equiv y' \pmod n$. Dans toute cette partie, la matrice $A$ est définie par

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad \text{où } a, b, c \text{ et } d \text{ désignent quatre réels.}$$

**I. Questions de cours.**

**1.** Donner la définition d'une matrice inversible et démontrer l'unicité de son inverse.

**2.** Etablir que $A^2 - (a+d)A + (ad-bc)I_2 = O_2$.

**3.** Démontrer que la matrice $A$ est inversible si et seulement si $ad - bc \neq 0$.

**II.** Dans cette question on suppose que $a$, $b$, $c$ et $d$ sont des entiers relatifs.

**1.** Donner un exemple de matrice inversible à coefficients dans $\mathbb{Z}$, mais dont l'inverse n'a pas tous ses coefficients dans $\mathbb{Z}$.

**2.** Enoncer une condition suffisante pour que la matrice $A$ soit inversible et que sont inverse $A^{-1}$ soit à coefficients dans $\mathbb{Z}$.

**3.** Quelle notion mathématique (qui ne figure pas dans les programmes de lycée) permet de prouver que cette condition est nécessaire? Proposer une démonstration du résultat.

**III.** La méthode étudiée ci-après utilise un chiffrement par blocs de 2 lettres pour coder un mot comportant un nombre pair de lettres :

- On choisit quatre entiers naturels non nuls $a$, $b$, $c$ et $d$.
- On note $x$ le rang de la première lettre du bloc et $y$ le rang de la deuxième lettre du bloc.
- On définit les entiers $x'$ et $y'$ de la manière suivante :

$$(S) \qquad \begin{cases} x' &= ax + by \\ y' &= cx + dy \end{cases}$$

- Le rang de la première lettre du bloc codé est le reste modulo 26 de $x'$, le rang de la deuxième lettre du bloc codé est le reste modulo 26 de $y'$.

Un tel chiffrement est dit digraphique.

**1.** Traduire le système $(S)$ par une relation matricielle à l'aide de la matrice $A$ qui est appelée **matrice de codage**.

**2.** On donne : $a = 4$, $b = 3$, $c = 5$ et $d = 4$.

**a.** Coder le mot B E Z O U T.

**b.** En détaillant les étapes, décoder le mot S F X M O J.

**3.** On donne à présent $a = 3$, $b = 2$, $c = 1$ et $d = 3$. On souhaite décoder le mot

A K X O U E V H D L

**a.** Démontrer qu'il existe un unique entier $u$ compris entre 0 et 25 tel que $7u \equiv 1 \pmod{26}$.

**b.** On note $A$ la matrice de codage associée aux entiers $a$, $b$, $c$ et $d$. Déterminer une matrice $B$, à coefficients entiers relatifs, telle que $uBA \equiv I_2 \pmod{26}$.

**c.** Décoder le mot en détaillant la démarche pour le premier bloc de deux lettres.

**4.** A quelle condition sur $a$, $b$, $c$ et $d$ peut-on décoder tout mot comportant un nombre pair de lettres ?

# Extrait 2

On note $\mathbb{N}$ l'ensemble des entiers naturels, $\mathbb{N}_0$ l'ensemble des entiers naturels non nuls et $\mathbb{Z}$ l'ensemble des entiers relatifs. Soient $p$ et $q$ deux entiers relatifs tels que $p \leqslant q$, on note $[\![p, q]\!]$ l'ensemble des entiers relatifs $k$ tels que $p \leqslant k \leqslant q$. On rappelle que, pour tout nombre réel $x$, il existe un unique entier relatif $E(x)$ tel que $E(x) \leqslant x < E(x) + 1$. Cet entier $E(x)$ est appelé *partie entière de $x$.*

## Partie A - Ecriture d'un entier en base deux

Le but de cette partie des de démontrer que tout entier naturel $N$ supérieur ou égal à 2 s'écrit de manière unique

$$N = \sum_{k=0}^{n-1} d_k 2^k \quad \text{avec} \quad n \geqslant 2 \text{ et } \begin{cases} \forall k \in [\![0, n-2]\!],\ d_k \in \{0, 1\}, \\ d_{n-1} = 1. \end{cases}$$

L'égalité précédente se note $N = \overline{d_{n-1} d_{n-2} \dots d_0}$ (écriture de $N$ en base deux); la suite finie $(d_k)_{0 \leqslant k \leqslant n-1}$ s'appelle la suite des chiffres dans l'écriture de $N$ en base deux.
Dans toute cette partie, $N$ désigne un entier naturel supérieur ou égal à 2.

**I.** On suppose que $N = \sum_{k=0}^{n-1} d_k 2^k$ avec $d_k \in \{0, 1\}$ pour $k \in [\![0, n-2]\!]$ et $d_{n-1} = 1$.

**1.** Montrer que $2^{n-1} \leqslant N \leqslant 2^n - 1$.

**2.** Montrer que $d_0$ est le reste de la division euclidienne de $N$ par 2.

**3.** Démontrer que la suite $(d_0, \dots, d_{n-1})$ est déterminée de manière unique.

**II.** On définit deux suites d'entiers $(y_k)_{k \in \mathbb{N}}$ et $(d_k)_{k \in \mathbb{N}}$ par $y_0 = N$ et pour tout entier naturel $k$, $y_{k+1}$ et $d_k$ désignent respectivement le quotient et le reste de la division euclidienne de $y_k$ par 2.

**1.** On fixe $k \in \mathbb{N}^*$. Exprimer $N$ en fonction de $k$, $d_0, \dots, d_{k-1}$ et $y_k$.

**2.** Démontrer que la suite $(y_k)_{k \in \mathbb{N}}$ est nulle à partir d'un certain rang et qu'il existe un entier $n \geqslant 1$ tel que $\overline{d_{n-1} d_{n-2} \dots d_0}$ soit l'écriture de $N$ en base deux.

**3.** Ecrire un algorithme qui, pour tout entier naturel $N$ supérieur ou égal à 2 donné, renvoie la suite $(d_0, d_1, \dots, d_{n-1})$ des chiffres de son écriture en base deux.

**4.** Ecrire en base deux le nombre qui s'écrit 391 en base dix.

**III.** On se propose à présent de calculer le nombre $N$ qui s'écrit $\overline{d_{n-1} d_{n-2} \dots d_0}$ en base deux.

**1.** Première méthode : méthode "naïve". On écrit $N = \sum_{k=0}^{n-1} d_k 2^k$. Combien d'opérations (additions et multiplications) doit-on effectuer à priori pour calculer $N$ avec cette méthode?

**2.** Deuxième méthode : méthode de Hörner. On écrit

$$N = ((((d_{n-1} \times 2 + d_{n-2}) \times 2 + d_{n-3}) \times 2 + \dots) \times 2 + d_0.$$

Combien d'opérations (additions et multiplications) doit-on effectuer a priori pour calculer $N$ avec cette méthode?

**3.** Ecrire un algorithme qui, pour toute suite de chiffres $(d_0, \dots, d_{n-1})$ donnée, renvoie la valeur de $N$ calculée à l'aide de cette deuxième méthode.

**4.** Quel est le nombre dont l'écriture en base deux est $\overline{101001000100001}$?

## Partie B - Nombres dyadiques

L'ensemble $D_2 = \left\{ \frac{a}{2^p};\ a \in \mathbb{Z},\ p \in \mathbb{N} \right\}$ est appelé ensemble des nombres dyadiques. On note $D_2^+$ l'ensemble des nombres dyadiques positifs ou nuls.

**I.** Montrer que $\mathbb{Z}$ est strictement inclus dans $D_2$ et que $D_2$ est strictement inclus dans $\mathbb{Q}$.

*Indication:* On pourra montrer que $\frac{1}{3} \notin D_2$.

**II.** Soit $x \in D_2^+ \setminus \mathbb{N}$. On se propose de démontrer qu'il existe un unique entier $n \geqslant 1$ et une unique suite $(a_0, a_1, \ldots, a_n)$ avec $a_0 \in \mathbb{N}$ et $(a_1, \ldots, a_n) \in \{0,1\}^n$ tels que

$$x = \sum_{k=0}^{n} a_k 2^{-k}, \quad \text{avec } a_n \neq 0.$$

Le membre de droite de cette égalité s'appelle le développement dyadique de $x$.

**1.** On suppose qu'une telle suite existe. Montrer que $a_0 = E(x)$ puis montrer que la suite $(a_0, a_1, \ldots, a_n)$ est déterminée de manière unique.

**2.** On souhaite à présent montrer l'existence d'une telle suite. A l'aide de la partie précédente, montrer l'existence d'un entier $a_0$, d'un entier $p \geqslant 1$ et d'une suite de nombres entiers $d_0, \ldots, d_{p-1}$ égaux à 0 ou 1, non tous nuls, tels que

$$x = a_0 + \sum_{k=0}^{p-1} d_k 2^{k-p}.$$

**3.** Conclure

**III.** Donner le développement dyadique de $\frac{35}{4}$.

## Partie C - Développement dyadique illimité

On appelle suite dyadique toute suite $(a_k)_{k\in\mathbb{N}_0}$ où pour tout $k \in \mathbb{N}_0$, $a_k$ est un élément de $\{0,1\}$. De plus :

- une suite dyadique $(a_k)_{k\in\mathbb{N}_0}$ est dite impropre s'il existe un entier $m \in \mathbb{N}_0$ tel que pour tout $k \geqslant m$, $a_k = 1$;
- une suite dyadique $(a_k)_{k\in\mathbb{N}_0}$ est dite propre si elle n'est pas impropre.

**I.** On suppose que $a = (a_k)_{k\in\mathbb{N}_0}$ est une suite dyadique.

**1.** Démontrer que la série de terme général $a_k 2^{-k}$ est convergente. On note sa somme

$$s(a) = \sum_{k=1}^{+\infty} a_k 2^{-k}.$$

**2.** Soit $N$ un entier naturel. Que vaut $\displaystyle\sum_{k=N}^{+\infty} 2^{-k}$ ?

**3.** Vérifier que $s(a) \in [0,1]$.

**4.** Montrer que si $a$ est une suite dyadique propre, alors $s(a) \in [0,1[$.

**5.** Montrer que si $a$ est une suite dyadique impropre, alors $s(a)$ est un nombre dyadique.

**6.** Soit $a = (a_k)_{k\in\mathbb{N}^*}$ la suite définie par

$$a_k = \begin{cases} 0 \text{ si } k \text{ est impair,} \\ 1 \text{ si } k \text{ est pair.} \end{cases}$$

Montrer que $s(a) = \dfrac{1}{3}$.

**II.** Soit $x$ un nombre dyadique compris dans l'intervalle $[0, 1[$.

**1.** En utilisant les résultats de la partie B, montrer qu'il existe une suite dyadique propre $a$ telle que

$$x = \sum_{k=1}^{+\infty} a_k 2^{-k}.$$

**2.** Montrer que si $x$ est non nul, alors il existe également une suite dyadique impropre $b$ telle que

$$x = \sum_{k=1}^{+\infty} b_k 2^{-k}.$$

**III.** Dans cette question, on cosidère un nombre réel $x$ appartenant à l'intervalle $[0, 1[$. On lui associe la suite $\alpha(x) = (\alpha_k(x))_{k\in\mathbb{N}_0}$ définie pour tout $k \in \mathbb{N}_0$ par l'égalité

$$\alpha_k(x) = E(2^k x) - 2E(2^{k-1}x).$$

Pour tout $n \in \mathbb{N}_0$, on pose $u_n(x) = \sum_{k=1}^{n} \alpha_k(x)2^{-k}$ et $v_n(x) = u_n(x) + 2^{-n}$.

**1.** Démontrer que la suite $(\alpha_k(x))_{k\in\mathbb{N}_0}$ est dyadique.

**2.** Démontrer que les deux suites $(u_n(x))_{n\in\mathbb{N}_0}$ et $(v_n(x))_{n\in\mathbb{N}_0}$ sont adjacentes et prennent leurs valeurs dans $D_2 \cap [0, 1]$.

**3.** Vérifier que $E(2^n x) = 2^n u_n(x)$ et en déduire que pour tout entier naturel $n \geqslant 1$,

$$u_n(x) \leqslant x < v_n(x).$$

**4.** Quelle est la limite commune des suites $(u_n(x))_{n\in\mathbb{N}_0}$ et $(v_n(x))_{n\in\mathbb{N}_0}$?

**5.** Montrer que $(\alpha_k(x))_{k\in\mathbb{N}_0}$ est une suite dyadique propre et que

$$x = \sum_{k=1}^{+\infty} \alpha_k(x)2^{-k}.$$

**6.** En déduire que pour tout nombre réel $x$ dans l'intervalle $[0, 1[$, il existe une unique suite dyadique propre $(a_k)_{k\in\mathbb{N}_0}$ telle que

$$x = \sum_{k=1}^{+\infty} a_k(x)2^{-k}.$$

On note alors

$$x = \overline{0, a_1 a_2 a_3 ...}$$

Cette nouvelle représentation de $x$ est appelée la *représentation dyadique propre* de $x$. Si la suite $(a_k)_{k\in\mathbb{N}_0}$ est nulle à partir d'un certain rang, on dit que la représentation dyadique de $x$ est finie.

**7.** Si $d = (d_n)_{n\in\mathbb{N}_0}$ est une suite dyadique propre, on note $x = s(d)$ et $d' = (d_{n+1})_{n\in\mathbb{N}_0}$. Justifier que $d_1 = E(2x)$ et $s(d') = 2x - d_1$.
En déduire un algorithme qui prend en entrées un nombre réel $x \in [0, 1[$ et un entier $n \in \mathbb{N}_0$ et qui renvoie la liste des $n$ premiers chiffres du développement dyadique propre de $x$. On admettra l'existence d'une fonction `floor` qui renvoie la partie entière de son argument.