Année Académique 2018/2019

TYPE	TRAVAUX DIRIGES
CYCLE	Licence
FILIERE ET NIVEAU	GL III
EPREUVE	**Théorie des groupes et applications**

Exercice 1 :

On donne la matrice A= $\begin{bmatrix} -10 & -6 \\ 18 & 11 \end{bmatrix}$ et on désigne par T la transformation linéaire de la matrice A relativement à une base orthonormée $\{e_1, e_2\}$ de l'espace $V_2(R)$

i) Montrer que T est régulier. Déterminer le polynôme caractéristique de T et calculer ses racines.

ii) Déterminer une base de $V_2(R)$ former des vecteurs propres X_1 et X_2 de T.

iii) Donner la matrice D de T relativement a la base $\{X_1, X_2\}$

iv) Donner la matrice H de passage de la base $\{e_1, e_2\}$ a la base $\{X_1, X_2\}$ ainsi que sa matrice inverse H^{-1}

v) Etant donné un trinôme du second dégré $P_2(x) = ax^2 + bx + c$ et une matrice M on pose $P_2(M) = aM^2 + bM\ cI_2$.

Montrer que A est racine de son polynôme caractéristique et déduire que quel que soit l'entier n, la matrice A^n est de la forme $A^n = \alpha_n A + \beta_n I_2$ ou I_2 est la matrice unité et α_n et β_n sont des scalaires.

vi) Calculer α_n et β_n Pour n= 1,2,3,4.

vii) Montrer que quel que soit l'entier n positif, on a : $A^n = HD^nH^{-1}$

viii) Déduire que $D^n = \begin{bmatrix} (-1)^n & 0 \\ 0 & 2^n \end{bmatrix}$ et en déduire les éléments de la matrice A^n.

Exercice 2:

1- Donner la definition d'une matrice nilpotente

Soit N une matrice nilpotente. Montrer que :

a) Det(I + N) = 1

b) Si A est matrice qui commute avec N alors det(A + N) = det A

Soit A la matrice A= $\begin{pmatrix} 8 & -1 & -5 \\ -2 & 3 & 1 \\ 4 & -1 & -1 \end{pmatrix}$

2- Montrer qu-il existe une matrice P telle que $P^{-1}AP$ soit triangulaire.

3- Soit Q=$\begin{pmatrix} 1 & 1 & 1/3 \\ 1 & -1 & 1/3 \\ 1 & 1 & 0 \end{pmatrix}$. Calculer $T_1 = Q^{-1}AQ$. Montrer que $T_1=D_1 + N_1$ ou D_1 est diagonale, N_1 nilpotente et $D_1N_1=N_1D_1$

4- Déduire T_1^n et A_n pour tout $n \in N$

Exercice 3 :

Soit la matrice A =$\begin{pmatrix} 1 & -1 & 0 \\ 1 & 0 & -1 \\ -1 & 0 & 2 \end{pmatrix}$

1-Factoriser le polynôme caractéristique de A

2-determiner les sous-espaces propres et caractéristiques de A

3-Demontrer qu'il existe une base de $\mathbb{R}^3$ dans laquelle la matrice de f est :

B=$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$

4-Resoudre le système $\frac{dx}{dt} = Ax$

5-Donner la décomposition de Dunford de B et calculer B^n pour $n \in \mathbb{N}$.

Exercice 4 :

Soit la matrice A=$\begin{pmatrix} 3 & 2 & 4 \\ -1 & 3 & -1 \\ -2 & -1 & -3 \end{pmatrix}$

1- Factoriser le polynôme caractéristique de A.

2- Déterminer les sous espaces propres et caractéristique de A.

3- Démontrer qu'il existe une base de $\mathbb{R}^3$ dans laquelle B=$\begin{bmatrix} -1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{bmatrix}$

4- Donner la décomposition de Dunford de B

5- Calculer e^B.

Exercice 5

Soit A = $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix}$

1- Quel est nature de la matrice A ?

- déterminer ses valeurs propres. Quel est la base des vecteurs propres de A.

2- On a exp(B)=A.

a) Montrer que si A=exp(B) alors AB=BA.

b) Déduire que la base (e_1, e_2, e_3) est une base de vecteur propre B.

c) Déterminer toutes les matrices B є $M_{3\times3}(\mathbb{R})$ / e^B=k

Exercice 6 :

Soit l'application f : $\mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}$ par :

$F(x, y) = X_1Y_1 - 2X_2Y_2 - 2X_3Y_3 + 2X_3Y_2 - X_1Y_3 + 2X_2Y_3 + X_1Y_2 + X_2Y_1 - X_3Y_1$

1- Déterminer la matrice associée à f.

2- Déterminer a forme quadratique associée à f.

3- Soit le système (S) : X'(t)= AX(t) ou A=$\begin{bmatrix} 1 & -3 & 4 \\ 4 & -7 & 8 \\ 6 & -7 & 7 \end{bmatrix}$

- Déterminer les solutions de ce système différentiel.

Exercice 7 :

On appelle E un procédé de chiffrement à clef publique et D le procédé de déchiffrement associé.

On suppose qu'il existe un procédé de signature associé à E que l 'on notera S. On notera VS le procédé de vérification de signature associé.

On suppose que toutes les personnes intervenant dans cet exercice ont chacune un couple (clef privé e, clef publique) correspondant aux procédés cités ci-dessus. Par souci de simplification, on suppos era que le même couple peut servir indifféremment aux opérations de chiffrement ou de signature.

Question 1 : Alice veut envoyer un message chiffré à Bob, avec quelle clef doit-elle le chiffrer ? A l'arrivée, quelle clef, Bob doit-il utiliser pour déchiffrer le message ?

Question 2: Alice veut envoyer un message signé à Bob, avec quelle clef doit-elle le signer ? A l'arrivée, quelle clef, Bob doit-il utiliser pour vérifier la signature du message ?

Question 3: Alice veut envoyer un message chiffré et signé à Bob, avec quelle clef doit-elle le chiffrer ?

Le signer ?

A l'arrivée, quelle clef, Bob doit-il utiliser pour déchiffrer le message ? Pour vérifier la signature ?

Question 4: Alice veut envoyer un message chiffré et signé à Bob, Gérard, Jackie, Ahmed, ... (25 destinataires) avec quelle clef doit-elle le chiffrer ? Le signer ?

<u>Exercice 8 :</u>

Voici un exemple de l'utilisation de RSA, avec des petits nombres :

X souhaiterait envoyer le message suivant à **Y** : « Kisses from Iraq ». Malheureusement, **W** les espionne, et pourrait intercepter ce message. Nos deux compères vont donc crypter leurs échanges avec la méthode RSA. **Ils ont** choisi **p = 37** et **q = 43**.

- Déterminer les clés privés et publics

X va utiliser ces clés pour crypter son message, mais il doit avant tout convertir son texte en une suite de nombres. Comme **X** veut envoyer le message sous forme d'un fichier informatique.

- Expliquer le processus que vas suivre le message envoyé entre son émission et ça réception
- En vous servant des clés trouvées plus haut et en vous appuyant le procédés décrit chiffrer :

  « Kisses from Iraq »