

ÉCOLE NORMALE SUPERIEURE

ANNÉE UNIVERSITAIRE : 2013-2014

DIRECTION DE LA FORMATION CONTINUE

UNIVERSITE DE VACANCES

SERVICE DES COURS DE PREPARATION



COURS D'ALGEBRE :
GROUPES-ANNEAUX-CORPS

Dr ABBY-MBOUA Parfait

Maître Assistant à l'Ecole Normale Supérieure

CHAPITRE : GROUPES

I. GENERALITES

1. DEFINITIONS ET EXEMPLES

1.1 Définition

On appelle *groupe*, un ensemble G non vide, muni d'une loi de composition interne, \bullet , telle que :

- La loi est associative : $\forall (x, y, z) \in G \times G \times G, x \bullet (y \bullet z) = (x \bullet y) \bullet z$
- Elle admet un élément neutre dans G : $\exists e \in G / \forall x \in G, x \bullet e = e \bullet x = x$
- Tout élément de G admet un symétrique : $\forall x \in G, \exists x' \in G / x \bullet x' = x' \bullet x = e$

1.2 Remarques

- Si la loi est commutative, le groupe est dit *commutatif* ou *abélien*.
- Si le nombre d'éléments du groupe est fini, ce nombre est appelé *ordre* du groupe.
- $\forall (x, y) \in G \times G$, on a $(x \bullet y)^{-1} = y^{-1} \bullet x^{-1}$.
- $\forall (a, b, x) \in G \times G \times G$, on a $a \bullet x = b \bullet x \Rightarrow a = b$

2. EXEMPLES

2.1 Les ensembles \mathbb{Z} , \mathbb{Q} , \mathbb{R} et \mathbb{C} sont des groupes additifs commutatifs.

2.2 \mathbb{Q}^* , \mathbb{R}^* , \mathbb{C}^* et $\{\{1, -1\}, \times\}$ sont des groupes multiplicatifs commutatifs.

II. SOUS GROUPES

1. CARACTERISATIONS

1.1 Définition

On dit qu'une partie non vide H d'un groupe G , est un *sous-groupe* de G , si elle vérifie la condition suivante : $\forall (x, y) \in H \times H, xy^{-1} \in H$

1.2 Théorème

Soit G un groupe d'élément neutre e et H une partie non vide de G . Les propriétés suivantes sont équivalentes :

- H est un sous groupe de G .
- $e \in H$ et $(\forall (x, y) \in H \times H, xy \in H$ et $x^{-1} \in H)$

1.3 Remarques

- Le sous groupe H muni de la loi induite définie sur G est un groupe.
- Tout groupe G d'élément neutre e , admet au moins deux sous groupes qui sont $\{e\}$ et G .

1.4 Définition

Soit groupe G d'élément neutre e . On appelle *sous groupe propre* de G , tout groupe H distinct de $\{e\}$ et G .

1.5 Remarques

- Pour démontrer qu'un ensemble muni d'une loi de composition est un groupe, il est souvent recommandé de montrer que cet ensemble est un sous-groupe d'un groupe connu.
- Tous les sous groupes propres de \mathbb{Z} sont de la forme $n\mathbb{Z}$ où n est un entier naturel supérieur à 2.
- Les groupes \mathbb{Z} , \mathbb{Q} et \mathbb{R} sont des sous groupes de \mathbb{C} .

2. SOUS GROUPE ENGENDRE PAR UNE PARTIE NON VIDE

1.1 Théorème

Si G un groupe et $(H)_{i \in I}$ une famille de sous groupes de G , alors $H = \bigcap_{i \in I} H_i$ est un sous groupe de G .

1.2 Remarque

La réunion de deux sous groupes d'un groupe est un sous groupe que lorsque l'un d'eux est inclus dans l'autre.

1.3 Théorème

Soit G un groupe et A une partie non vide de G . L'intersection de tous les sous-groupes de G contenant A , est un sous groupe de G . On appelle le sous groupe de G engendré par A . On le note $[A]$ ou $\text{gr}(A)$.

1.4 Définitions

- On dit qu'un sous ensemble A d'un groupe G est une *partie génératrice* de G , si $[A] = G$.
- Si $A = \{x\}$ où $x \in G$, le sous de G engendré par x est $H = \{\dots, x^{-2}, x^{-1}, e, x, x^2, \dots\}$
- Le sous groupe engendré x par est abélien.
- On dit qu'un groupe G est *cyclique* lorsqu'il peut être engendré par un seul élément de G . On dit alors que cet élément est un *générateur* de G .
- On dit qu'un groupe G est *monogène* lorsqu'il est fini et cyclique.

1.5 Définition

Soit G un groupe multiplicatif d'élément neutre e et a un élément de G . On appelle *ordre* de a , le plus petit entier naturel non nul n tel que $a^n = e$.

1.6 Théorème

Si le cardinal d'un groupe G existe, alors

- a) l'ordre de tout élément de G est un diviseur de ce cardinal.
- b) l'ordre de tout sous groupe de G est un diviseur de ce cardinal.

1.7 Remarque

Le cardinal d'un groupe G peut ne pas exister, mais des éléments de G peuvent être d'ordre fini.

III. MORPHISMES DE GROUPES

1. DEFINITIONS ET EXEMPLES

1.1 Définition

Soient $(G, *)$ et (G', \bullet) deux groupes. On appelle *morphisme* ou *homomorphisme* de G dans G' , toute application $f : G \rightarrow G'$ telle que :

$$\forall (x, y) \in G \times G, f(x * y) = f(x) \bullet f(y)$$

1.2 Remarques

- Si de plus f est surjectif, on dit que f est un *épimorphisme* de G dans G' .
- Si f est bijectif, on dit que f est un *isomorphisme* de G dans G' .
- Si f est un isomorphisme, on dit que les groupes G et G' sont *isomorphes*.
- Si $G = G'$, on dit que f est un endomorphisme de G ; un endomorphisme bijectif est un automorphisme.

2. EXEMPLES

2.1 L'application $x \mapsto e^x$, de \mathbb{R} dans \mathbb{R}_+^* , est un morphisme de groupes.

2.2 Soit G un groupe et a un élément de G , alors

- a) L'application $n \mapsto a^n$, de \mathbb{Z} dans G , est un morphisme de groupes.
- b) L'application φ de G dans G définie par $\varphi(x) = x^{-1}$ est un *automorphisme* de G .
- c) L'application f_a de G dans G définie par $f_a(x) = axa^{-1}$ est appelée un *automorphisme intérieurs* de G .

2.3 Définitions

- a) Soit G un groupe et a un élément de G , alors les automorphismes de G de la forme f_a s'appellent les *automorphismes intérieurs* de G .
- b) Soit G un groupe, H un sous groupe de G et a un élément de G , alors l'image de H par tout automorphisme de G s'appelle le *conjugué* de H .

3. PROPRIETES DES MORPHISMES DE GROUPES

3.1 Théorème

Soient G, G' et G'' trois groupes, f un morphisme de G dans G' et g un morphisme de G' dans G'' , alors

- $g \circ f$ est un morphisme de G dans G'' .
- Si f est un isomorphisme de G sur G' , alors l'application f^{-1} est un isomorphisme de G' sur G .
- Si f est un isomorphisme de G sur G' et g est un isomorphisme de G' sur G'' , alors l'application $g \circ f$ est un isomorphisme de G sur G'' .

3.2 Théorème

Soit f un morphisme d'un groupe G dans un groupe G' .

- Si e est l'élément neutre de G et e' est l'élément neutre de G' , alors $f(e) = e'$.
- Si $\forall x \in G$, on a $f(x^{-1}) = (f(x))^{-1}$.

4. IMAGE ET NOYAU D'UN MORPHISME DE GROUPES

4.1 Théorème

Soit f un morphisme d'un groupe G dans un groupe G' .

- L'image par f de tout sous-groupe de G est un sous-groupe de G' .
- L'image réciproque par f de tout sous-groupe de G' est un sous-groupe de G .

4.2 Théorème

Soit f un morphisme d'un groupe G dans un groupe G' , d'élément neutre e' .

- L'image par f du groupe G est un sous-groupe de G' , noté $\text{Im } f$.
- L'image réciproque par f de $\{e'\}$ est un sous-groupe de G , noté $\text{ker } f$.

4.3 Théorème

Soit f un morphisme d'un groupe G dans un groupe G' .

- Pour que f soit injectif, il faut et il suffit que $\text{ker } f = \{e\}$.
- Pour que f soit surjectif, il faut et il suffit que $\text{Im } f = G'$.

IV. GROUPES QUOTIENTS

1. CLASSES MODULO (SUIVANT) UN SOUS GROUPE

1.1 Théorème

Soit G un groupe et H un sous groupe de G . Alors :

- La relation xRy si et seulement si $xy^{-1} \in H$ est une relation d'équivalence sur G .
- La classe de x suivant H est Hx .

1.2 Remarque

On peut définir également la relation d'équivalence xRy si et seulement si $y^{-1}x \in H$.

1.3 Définitions

- L'ensemble Hx s'appelle une *classe à droite modulo H* .
- L'ensemble xH s'appelle une *classe à gauche modulo H* .
- L'ensemble des classes à droite modulo H se note G/H .
- Le nombre de classes modulo à droite H s'appelle l'*indice* de H dans G ou l'*index* de H dans G . il est noté $[H:G]$.

1.4 Théorème (Théorème de Lagrange)

Soit G un groupe fini et H un sous groupe de G . Alors $|G| = [G:H] \times |H|$. On déduit que l'ordre de H divise l'ordre de G .

1.5 Théorème

Soit G un groupe fini d'ordre premier. Alors les seuls sous groupes de G sont $\{e\}$ et G .

2. GROUPES QUOTIENTS

2.1 Définition

On dit qu'un sous groupe H d'un groupe G est *distingué*, ou *normal* ou *invariant* dans G si :

$$\forall x \in G \text{ on a } Hx = xH.$$

On écrit : $H \triangleleft G$

2.2 Remarques

- Dans un groupe commutatif, tout sous groupe est distingué.
- Si H un sous groupe d'un groupe G est invariant par tout automorphisme intérieur de G , alors il est distingué dans G .
- Tout sous groupe de Z est distingué.

2.3 Remarques

Si H un sous groupe distingué d'un groupe G ,

- alors G/H est un groupe.
- alors l'application $s : G \rightarrow G/H$ est morphisme surjectif, appelée *surjection canonique* de G .

2.4 Théorème

Si H est un sous groupe distingué d'un groupe G , alors tout sous groupe K de G contenant H est un sous groupe distingué de G .

2.5 Théorème

Si H est un sous groupe distingué d'un groupe G , alors tout sous groupe de G/H est de la forme K/H tel que K est un sous groupe de G contenant H .

2.6 Théorème

Si f un morphisme du groupe G dans le groupe G' , alors $N = \text{Ker } f$ est un sous groupe distingué de G .

3. DECOMPOSITION D'UN MORPHISME

3.1 Théorème

Un morphisme f d'un groupe G dans un groupe G' peut se décomposer en :

- $s : G \rightarrow G/\text{ker } f$
- $\bar{f} : G/\text{ker } f \rightarrow \text{Im } f$
- $i : \text{Im } f \rightarrow G'$

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ s \downarrow & & \uparrow i \\ G/\text{ker } f & \xrightarrow{\bar{f}} & \text{Im } f \end{array}$$

3.2 Théorème

Si f d'un groupe G dans un groupe G' alors $G/\text{ker } f$ et $\text{Im } f$ sont isomorphes.

3.3 Propriété universelle du noyau d'un morphisme

Soit H un sous groupe d'un groupe G . Si H est distingué d'un groupe G , alors il existe un groupe K et un morphisme f_K de G dans K , tel que $\text{ker } f_K = H$.

V. GROUPES SYMETRIQUES

Dans cette partie, n désigne un entier naturel non nul et IN_n , l'ensemble des n premiers entiers naturels non nuls.

1. GENERALITES

1.1 Définitions

- Soit E un ensemble non vide. On appelle *groupe des permutations* de E ou *groupe symétrique* de E , l'ensemble des bijections de E dans E . Cet ensemble est noté $S(E)$.
- Lorsque $E = IN_n$, le groupe $S(E)$ se note S_n et s'appelle le *groupe symétrique d'ordre n* .
- Le groupe S_n a $n!$ éléments.
- On dit qu'un s élément de S_n est d'ordre r si $s^r = e$, où e désigne l'application identique de E dans E .
- On appelle *permutation circulaire*, l'élément s de S_n tel que $s(1) = 2; s(2) = 3; \dots; s(n-1) = n$ et $s(n) = 1$.

1.2 Définition

On dit qu'un élément s de S_n est un *cycle* si $s \neq e$.

1.3 Théorème

Si s est un cycle, alors l'ordre de s est le nombre d'éléments de s .

1.4 Théorème

$\forall n \geq 2$, tout élément s de S_n peut s'écrire comme composée de cycles à supports disjoints.

1.5 Théorème

Si tout s élément de S_n est écrit comme composée de cycles à supports disjoints, alors son ordre est égal au ppcm des ordres des cycles intervenant dans cette composée.

1.6 Théorème

Le groupe S_n n'est pas commutatif si $n \geq 3$.

2. TRANSPOSITIONS

2.1 Théorème

On dit qu'un s élément de S_n est une *transposition*, s'il existe deux entiers distincts i et j , de IN_n tels que :
 $s(i) = j; s(j) = i$ et $s(k) = k$ pour $\forall k \in IN_n - \{i, j\}$.

2.2 Théorème

$\forall n \geq 2$, tout élément de S_n peut s'écrire comme composé de transpositions.

3. SIGNATURE D'UNE PERMUTATION

3.1 Définition

Soit σ un élément de S_n . On dit qu'un couple (i, j) d'éléments IN_n est une *inversion* pour σ ou est une σ -inversion, si $i < j$ et $\sigma(i) > \sigma(j)$.

3.2 Définition

Soit I_σ le nombre total de σ -inversions.

L'application $\sigma \mapsto \varepsilon(\sigma) = (-1)^{I_\sigma}$ de S_n dans le groupe multiplicatif $\{-1, 1\}$ s'appelle la *signature* de la permutation σ .

- Si $\varepsilon(\sigma) = +1$, on dit que la permutation σ est paire.
- Si $\varepsilon(\sigma) = -1$, on dit que la permutation σ est impaire.

CHAPITRE : ANNEAUX

I. GENERALITES

1. DEFINITIONS ET EXEMPLES

1.1 Définition

On appelle *anneau*, un ensemble A non vide, muni de deux lois de composition interne, l'addition et la multiplication, telles que :

- L'addition est une loi de groupe abélien et admet un élément neutre, appelé élément nul, noté 0
- La multiplication est associative et admet un élément neutre, appelé élément unité, noté 1
- La multiplication est distributive par rapport à l'addition.

1.2 Remarques

- Si A est anneau quelconque, alors il a au moins deux éléments
- Si la loi multiplicative est commutative, l'anneau est dit commutatif.
- Si A est anneau quelconque, on dit que deux éléments a et b de A *commutent* ou sont *permutables* si $ab = ba$.

2. EXEMPLES

- Les ensembles \mathbb{Z} , \mathbb{Q} , \mathbb{R} et \mathbb{C} sont des anneaux commutatifs.
- Soit n un entier naturel non nul, alors $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif.

II. SOUS-ANNEAUX ; IDEAUX

1. SOUS ANNEAUX

1.1 Définition

On dit qu'une partie non vide B d'un anneau A , est un *sous-anneau* de A , si elle vérifie la condition suivante :

- B est un sous groupe du groupe additif A
- Si a et b sont deux éléments de B , alors ab est un élément de B
- L'élément unité 1 est un élément de B .

1.2 Théorème

Soient A un anneau et B une partie non vide de A . Les propriétés suivantes sont équivalentes :

- B est un sous anneau de A .
- $1 \in B$ et $\forall (a; b) \in B \times B$, on a $a - b \in B$ et $ab \in B$

1.3 Exemples

- \mathbb{R} est un sous anneau de \mathbb{C} .
- Soit A un anneau ; A est un sous anneau de A , mais $\{0\}$ n'est pas un sous anneau de A si $A \neq \{0\}$.
- Pour démontrer qu'un ensemble est anneau, il est souvent recommandé de montrer que cet ensemble est un sous-anneau d'un anneau connu.

1.4 Théorème

L'intersection d'une famille d'anneaux de A est un sous anneau de A .

1.5 Théorème

Le plus petit sous anneau contenant une partie non vide H de A est anneau, appelé le *sous anneau engendré par H* .

1.6 Définitions

Soit A un anneau non nul

- On dit qu'un élément a non nul de A est un diviseur de zéro, s'il existe un élément b non nul de A tel que $ab = 0$.
- On dit que l'anneau A est *intègre* ou un anneau *d'intégrité* s'il est commutatif et s'il ne possède pas de diviseurs de zéro.

1.7 Définitions

- On dit qu'un élément a non nul de A est *inversible*, s'il possède un symétrique pour la multiplication (c'est-à-dire qu'il existe un élément b non nul de A tel que $ab = 1$).
- On dit qu'un élément a non nul de A est un élément *nilpotent*, s'il existe un entier naturel non nul n tel que $a^n = 0$.
- On dit qu'un élément a de A est un élément *idempotent*, si $a^2 = a$.

2. IDEAUX

2.1 Définition

On dit qu'une partie I d'un anneau A , est un idéal à gauche de A , si elle vérifie les conditions suivantes :

- I est un sous groupe du groupe additif A
- $\forall a \in A$ et $\forall x \in I, ax \in I$

2.2 Remarques

- On dit que I est un idéal *bilatère* (ou simplement un idéal) si I est à la fois idéal à gauche et à droite de A .
- Dans tout anneau A , les sous groupes triviaux A et $\{0\}$ sont des idéaux. Tout idéal autre que ces deux idéaux est appelé idéal propre de A .
- Dans un anneau commutatif, tous les idéaux sont bilatères.

2.3 Définition

Soit I un idéal de l'anneau A . On dit que I est un idéal *maximal* si I vérifie les conditions suivantes :

- I est différent de A
- Pour tout idéal J différent de I , si I est inclus dans J alors J est égal à A .

2.4 Définition

Soit A un anneau. On dit qu'un idéal I de A est un idéal *principal*, s'il est engendré par un élément de l'anneau A (c'est-à-dire que s'il existe un élément a appartenant à A tel que $I = aA = Aa$).

2.5 Définition

On dit qu'un anneau A est *principal*, s'il est commutatif, intègre et si tout idéal de A est principal.

2.6 Remarque

Les idéaux de \mathbb{Z} sont les ensembles de la forme $n\mathbb{Z}$, où n est élément de \mathbb{N} .

\mathbb{Z} est donc un anneau principal.

2.7 Définition

Soit A un anneau. On dit qu'un idéal P de l'anneau A est *premier*, si P vérifie les conditions suivantes :

- P est différent de A
- $(\forall (x; y) \in A \times A, xy \in P, y \notin P) \Rightarrow x \in P$.

2.8 Définition

Soit A un anneau. On dit qu'un idéal P de l'anneau A est *premier*, si P vérifie les conditions suivantes :

- Q est différent A
- $(\forall (x; y) \in A \times A, xy \in Q, y \notin Q) \Rightarrow (\exists n \in \mathbb{N}^*, x^n \in Q)$.

2.9 Théorème

Soit I un idéal d'un anneau A , alors les idéaux premiers de A/I sont les idéaux de la forme P/I tel que P est un idéal premier de A contenant I .

2.10 Théorème

Soit I un idéal d'un anneau commutatif A .

- L'anneau A/I est intègre si et seulement si l'idéal I est premier.
- L'anneau A/I est un corps si et seulement si l'idéal I est maximal.

III. MORPHISMES D'ANNEAUX

1. DEFINITIONS

1.1 Définition

Soient A et A' deux anneaux dont les éléments nuls respectifs 0 et $0'$ et d'éléments neutres respectifs 1 et $1'$.

On appelle morphisme ou homomorphisme de A dans A' , toute application $f : A \rightarrow A'$ telle que les conditions suivantes sont vérifiées:

- $f(1) = 1'$
- $\forall (a; b) \in A \times A, f(a + b) = f(a) + f(b)$
- $\forall (a; b) \in A \times A, f(ab) = f(a)f(b)$

1.2 Remarques

- Le noyau de f est le noyau du morphisme du groupe $(A, +)$ dans le groupe $(A', +)$.
- Si de plus f est bijectif, on dit que f est un isomorphisme de A .
- Si f est un isomorphisme, on dit que les anneaux A et A' sont isomorphes.
- Si $A = A'$, on dit que f est un endomorphisme de A ; un endomorphisme bijectif est un automorphisme.

1.3 Théorème (décomposition d'un morphisme d'anneaux)

Un morphisme f d'un anneau A dans un groupe A' peut se décomposer en :

- $s : A \rightarrow A / \ker f$
- $\bar{f} : A / \ker f \rightarrow \text{Im } f$
- $i : \text{Im } f \rightarrow A'$

$$\begin{array}{ccc}
 A & \xrightarrow{f} & A' \\
 s \downarrow & & \uparrow i \\
 A / \ker f & \xrightarrow{\bar{f}} & \text{Im } f
 \end{array}$$

1.4 Théorème

Soient A, A' et A'' sont trois anneaux, f un morphisme de A dans A' et g un morphisme de A' dans A'' , alors

- $g \circ f$ est un morphisme de A dans A'' .
- Si f est un isomorphisme de A sur A' , l'application f^{-1} est un isomorphisme de A' sur A .

1.5 Théorème

Soit f un morphisme d'un anneau A dans un anneau A' .

- Si 0 est l'élément nul de A et $0'$ est l'élément nul de A' , alors $f(0) = 0'$.
- $\forall a \in A, f(-a) = -f(a)$
- Si a est un élément inversible de A , on a $f(a^{-1}) = (f(a))^{-1}$.
- Si B est sous anneau de A , alors $f(B)$ est un sous anneau de A' .

e) Si B' est sous anneau de A' , alors $f^{-1}(B')$ est un sous anneau de A .

f) Si I' est un idéal A' , alors $f^{-1}(I')$ est un idéal de A .

g) f est injective si et seulement si $\ker f = \{0\}$

2. CARACTERISTIQUE D'UN ANNEAU

2.1 Définition

On appelle *caractéristique* de l'anneau non nul A , l'entier naturel p tel que $p\mathbb{Z}$ soit le noyau du morphisme $f: \mathbb{Z} \rightarrow A$ défini par $f(n) = n.1$.

2.2 Théorème

Si le morphisme f est injectif, on dit que l'anneau A est de caractéristique nulle, donc A est un ensemble infini.

2.3 Remarques

a) Les anneaux \mathbb{Z} , \mathbb{Q} , \mathbb{R} et \mathbb{C} sont de caractéristique nulle.

b) La caractéristique de tout anneau $\mathbb{Z}/n\mathbb{Z}$ est n pour tout entier naturel n supérieur ou égal à 2.

2.4 Théorème

Si le morphisme f n'est pas injectif, on dit que l'anneau A est de caractéristique p .

2.5 Théorème

A un anneau intègre si et seulement si sa caractéristique p est nulle ou est un nombre premier.

IV. DIVISIBILITE DANS UN ANNEAU

Dans cette partie, on considère A un anneau commutatif intègre (A est un anneau principal) et on note par (a) l'idéal engendré par un élément a de A .

1. GENERALITES

1.1 Définition

Soient a et b deux éléments de l'anneau A .

On dit que a *divise* b (a est un diviseur de b) ou que b est divisible par a (ou b est un multiple de a), s'il existe q dans A tel que $b = aq$.

1.2 Théorème

$(b) \subset (a)$ si et seulement si a divise b

1.3 Définition

Soient a et b deux éléments de l'anneau A

On dit que a et b sont *associés*, s'il existe un élément inversible u de A tel que $b = au$.

1.4 Théorème

$(b) = (a)$ si et seulement si a et b sont associés.

1.5 Définition

On dit qu'un élément non nul de A est *premier* ou *irréductible* ou *extrémal* s'il n'est pas inversible et si ses seuls diviseurs sont les éléments inversibles de A et les éléments qui lui sont associés.

2. PLUS GRAND COMMUN DIVISEUR

2.1 Définition

Soient $a_1; a_2; \dots; a_n$ des éléments non nul de A .

On appelle plus grand commun diviseur de $a_1; a_2; \dots; a_n$, noté $PGCD(a_1; a_2; \dots; a_n)$, tout élément d de

A tel que $dA = a_1A + a_2A + \dots + a_nA$

2.2 Définitions

a) On dit que les éléments non nuls $a_1; a_2; \dots; a_n$ de A sont premiers entre eux dans leur ensemble si

$$PGCD(a_1; a_2; \dots; a_n) = 1$$

- b) On dit que les a_i sont premiers entre eux deux à deux si pour tous les i, j tels que $i \neq j$, on a $PGCD(a_i, a_j) = 1$

2.3 Théorème de Bézout

Soient $a_1; a_2; \dots; a_n$ des éléments non nul de A . Les propriétés suivantes sont équivalentes :

- a) $a_1; a_2; \dots; a_n$ sont premiers entre eux dans leur ensemble.
b) Il existe des éléments $u_1; u_2; \dots; u_n$ de A tels que $a_1 u_1 + a_2 u_2 + \dots + a_n u_n = 1$.

2.4 Corollaire

Soient $a; b$ et c trois éléments non nuls de A .

Si a est premier avec b et si a est premier avec c , alors a est premier avec bc .

2.5 Théorème

Soient a et b deux éléments non nuls de A .

Si on appelle d le $PGCD(a, b)$, alors il existe deux éléments a' et b' premiers entre eux tels que $a = da'$ et $b = db'$.

2.6 Théorème de Gauss

Soient a et b deux éléments non nuls de A et soit d un diviseur du produit ab . Si d est premier avec a , alors d divise b .

3. PLUS PETIT COMMUN MULTIPLE

3.1 Définition

Soient $a_1; a_2; \dots; a_n$ des éléments non nul de A .

On appelle plus petit commun multiple de $a_1; a_2; \dots; a_n$, noté $PPCM(a_1; a_2; \dots; a_n)$, tout élément m de A tel que $(a_1) \cap (a_2) \cap \dots \cap (a_n) = (m)$

3.2 Théorème

Soient a et b deux éléments non nuls de A , tels que $PGCD(a; b) = d$ et $PPCM(a; b) = m$.

Alors il existe un élément inversible λ tel que $ab = \lambda dm$.

3.3 Corollaire

Soient a et b deux entiers relatifs non nuls tels que $PGCD(a; b) = d$ et $PPCM(a; b) = m$.

Alors $|a||b| = md$.

3.4 Corollaire

Soient a et b deux entiers naturels non nuls tels que $PGCD(a; b) = d$ et $PPCM(a; b) = m$.

Alors $ab = dm$.

3.5 Théorème

Soit un entier naturel $n \geq 2$.

Alors il existe une suite croissante de nombres premiers $p_1; p_2; \dots; p_n$ et suite $\alpha_1; \alpha_2; \dots; \alpha_n$ de nombres entiers naturels, tels que $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$

CHAPITRE : CORPS

I. GENERALITES

1. DEFINITIONS ET REMARQUES

1.1 Définitions

- a) On appelle corps tout anneau K non nul dans lequel tout élément non nul est inversible.
- b) On dit qu'un corps est commutatif si la multiplication est commutative.

1.2 Remarque

Toutes les notions définies pour les anneaux (intégrité, morphisme, idéal et caractéristique) s'appliquent également aux corps qui sont des anneaux particuliers.

1.3 Exemple

Les anneaux \mathbb{Q} , \mathbb{R} et \mathbb{C} sont des corps commutatifs de caractéristique nulle.

2. PROPRIETES FONDAMENTALES

2.1 Théorèmes

- a) Dans un corps K , tout élément non nul est régulier pour la multiplication.
- b) Tout corps K est intègre

2.2 Théorème

Soient K et K' deux corps commutatifs et f un morphisme de corps de K dans K' . Alors f est une application injective.

2.3 Théorème

L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.

2.4 Théorème

Soit a un élément non nul de \mathbb{Z} . Dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, l'élément est inversible si et seulement si a et n sont premiers entre eux.

Fiche de travaux dirigés

Exercice 1

Soit a un entier naturel non nul.

On pose $G_a = \left\{ \frac{z}{a} / z \in \mathbb{Z} \right\}$

1. Montrer G_a que est groupe commutatif.
2. Donner une condition nécessaire et suffisante sur a pour que G_a soit inclus dans \mathbb{Z} .

Exercice 2

Soit G un groupe

1. Montrer que si G d'ordre quatre, alors il existe au moins un élément distinct de l'élément neutre et qui soit son inverse.
2. Montrer que si $(ab)^2 = a^2b^2$, pour tous a et b dans G , alors G est commutatif.

Exercice 3

1. Déterminer les sous groupes de $\mathbb{Z}/24\mathbb{Z}$:
2. Déterminer les éléments inversibles de $\mathbb{Z}/24\mathbb{Z}$.

Exercice 4

Résoudre les équations suivantes dans $\mathbb{Z}/13\mathbb{Z}$ 1) $3x = \bar{2}$ et 2) $7x^2 - 5x - \bar{2} = \bar{0}$	Résoudre les équations suivantes dans $\mathbb{Z}/12\mathbb{Z}$ 1) $3x = \bar{0}$ et 2) $x^2 - 7x + \bar{10} = \bar{0}$
--	--

Exercice 5

Dans (G, \cdot) un groupe abélien multiplicatif d'élément neutre e , on considère deux éléments distincts a et b d'ordres finis. Démontrer que si $[a] \cap [b] = \{e\}$ alors l'ordre de l'élément ab est égal au PPCM des ordres des éléments a et b .

Exercice 6

On pose $G = \{z \in \mathbb{C} / |z| = 1\}$

Soit $f : \mathbb{R} \rightarrow G$ définie par $f(x) = e^{2ix}$

1. Montrer que G est un groupe.
2. Montrer que f est un épimorphisme.
3. En déduire que G est isomorphe \mathbb{R}/\mathbb{Z}

Exercice 7

1. Démontrer qu'une matrice est inversible si et seulement si 0 n'est pas une valeur propre.
2. Démontrer que les valeurs propres d'une matrice hermitienne sont des nombres réels.

Exercice 8

Dans le plan euclidien \mathcal{P} , on considère deux points distincts A et B .

Soit I l'ensemble des isométries de \mathcal{P} . Pour tout point M de \mathcal{P} et pour tout i de I , on pose $i(M) = M'$.

Soient $I_1 = \{i \in I / \overline{MA} \cdot \overline{MB} = \overline{M'A} \cdot \overline{M'B}\}$ et $I_2 = \{i \in I / \overline{MA} \cdot \overline{AB} = \overline{M'A} \cdot \overline{AB}\}$

Démontrer que $I_1 \cap I_2$ est isomorphe $\mathbb{Z}/2\mathbb{Z}$.

Exercice 9

Soit $s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 1 & 5 & 8 & 3 & 7 \end{pmatrix}$

1. Déterminer s^{-2} .
2. Calculer l'ordre de s et écrire le plus simplement possible s^{2014} .

Exercice 10

Soit A un anneau, tel que $\forall x \in A, x^2 = x$.

1. Montrer que A est de caractéristique 2. (On pourra calculer $(x + x)^2$ pour tout $x \in A$.)
2. Montrer que A est un anneau commutatif (On pourra calculer $(x + y)^2$ pour tout $(x, y) \in A^2$.)

Exercice 11

On désigne par $E = \mathbb{R}_3[X]$ l'espace vectoriel des polynômes réels de degré strictement inférieur à quatre et rapporté à la base canonique $B = (e_1; e_2; e_3; e_4) = (X^3; X^2; X; 1)$.

Soit l'application u de E dans E , définie par : $\forall P \in E, u(P)X = P'(X+1) + P'(X-1) - P'(X)$

1. Soit $Q(X) = X^3 + X^2 + X + 1$. Déterminer $u(Q)(X)$.
2.
 - a. Montrer que u est un endomorphisme de E .
 - b. Déterminer la matrice A de u par rapport à B .
 - c. En déduire que u n'est pas un automorphisme de E .
3. On donne $v_1 = 2X^3 - 3X^2 + 1; v_2 = -2X^3 + 3X^2; v_3 = X^3 - 2X^2 + X$ et $v_4 = X^3 - X^2$.
 - a. Montrer que $B' = (v_1; v_2; v_3; v_4)$
 - b. Déterminer la matrice de passage de la base duale B^* à la base duale B'^* .

Exercice 12

1. Diviser $A = X + 1$ par $B = X^2 - X + 1$ suivant les puissances croissantes de à l'ordre 2.
2. Décomposer l'inverse de $C = (X^2 - 1)(X^2 + 1)^2$ en éléments simples sur \mathbb{R} .

Exercice 13

1. Déterminer les vecteurs propres de la matrice d'ordre deux suivante $A = \begin{pmatrix} 1 & 4 \\ 2 & -1 \end{pmatrix}$

2. Soient (u_n) et (v_n) deux suites numériques telles que $u_0 = v_0 = 1$ et

$$\forall n \in \mathbb{N}^*, \begin{cases} u_n = u_{n-1} + 4v_{n-1} \\ v_n = 2u_{n-1} - v_{n-1} \end{cases}$$

- a. Ecrire le système sous forme matricielle.
- b. On pose $X_n = (u_n; v_n)$. Exprimer X_n en fonction de X_{n-1} , puis X_n en fonction de n .
- c. En déduire u_n et v_n en fonction de n .

Exercice 14

Résoudre le système différentiel défini par

$$\begin{cases} \frac{dx}{dt} = 2x - y \\ \frac{dy}{dt} = -x + 2y \end{cases}$$

Exercice 15

Soient G un groupe et H un sous groupe distingué de G tel que $[G : H] = p$, avec p premier.

1. Montrer que si K est un sous groupe de G non inclus dans H , alors $G = KH$.
2. En déduire que si K est fini, alors $|K| = p|K \cap H|$.

Epreuve de préparation d'Algèbre

Problème

Dans tout le problème G désigne un groupe multiplicatif d'élément neutre e .

Partie 1.

On suppose que tout élément x de G vérifie $x^2 = e$.

1. Montrer que G est commutatif.
2. Montrer que pour tout sous groupe propre H de G et pour élément a de $G - H$, $H \cup aH$ est un sous groupe de G .
3. Montrer que si G est d'ordre fini, alors il existe un nombre entier nature k , tel que $|G| = 2^k$.

Partie 2

On suppose que G est fini d'ordre pair.

1. Montrer que G contient un élément d'ordre 2.
2. Montrer que si $|G| = 2p$, avec p premier, alors G contient un élément d'ordre p .

Partie 3

On suppose que H et K sont deux sous groupes de G .

1. a) Montrer que $H \cup K$ est un sous groupe de G si et seulement si $H \subset K$ ou $K \subset H$.
b) en déduire qu'aucun groupe n'est la réunion de deux sous groupes propres.
2. Montrer que $G - H$ est fini si et seulement si G est fini ou $G = H$.
3. Montrer que si H est un sous groupe propre de G , alors $gr(G - H) = G$.
4. Soit A une partie finie non vide de G . Montrer que A est un sous groupe de G si et seulement si A est stable pour la loi de G .
5. Montrer que si G est fini, alors toute partie non vide stable de G est un sous groupe de G .

Exercice 1

Soit \perp une loi de composition interne sur \mathbb{R} , définie par : $\forall (x, y) \in \mathbb{R} \times \mathbb{R}, x \perp y = x + y - xy$

1. Déterminer $3 \perp \frac{3}{2}$; $-2 \perp 5$ et $0 \perp \sqrt{7}$.
2. Montrer que $(\mathbb{R} - \{1\}, \perp)$ est un groupe abélien.
3. $\forall n \in \mathbb{N}^*$, on pose $\underbrace{x \perp x \perp \dots \perp x}_{n \text{ fois}} = x^n$. Montrer que $x^n = 1 - (1 - x)^n$.

Exercice 2

Dans cet exercice α désigne un nombre réel, E un espace vectoriel réel de dimension 3 et $B = (e_1; e_2; e_3)$ sa base canonique. Soit f un élément de $L(E)$ tel que

$$\begin{cases} f(e_1) = (3 - \alpha)e_1 - \alpha e_2 + 5e_3 \\ f(e_2) = (-5 + \alpha)e_1 + (\alpha - 2)e_2 - 5e_3 \\ f(e_3) = \alpha e_1 + \alpha e_2 - 2e_3 \end{cases} \quad (\text{On désigne par } A_\alpha \text{ la matrice de } f).$$

1. a. Montrer que le polynôme caractéristique P_α de A_α est indépendant de α et en déduire son polynôme q_A .
b. Montrer que f est un automorphisme de E et déterminer A_α^{-1} (la matrice de f^{-1}) en fonction de α .
2. Pour quelle(s) valeur(s) la matrice A_α est-elle diagonalisable ?
3. Dans toute la suite, on suppose que $\alpha = 0$.
Déterminer A_0^n pour $n \in \mathbb{N}$ et en déduire e^{tA_0} pour $t \in \mathbb{R}$.

Correction de l'épreuve
de préparation d'Algèbre

Problème

Partie 1.

1. Montrons que G est commutatif.

* Soient x, y deux éléments de G . Montrons que $xy = yx$.

$$\begin{aligned}(xy)^2 = e &\Leftrightarrow (xy)(xy) = e \Leftrightarrow xyxy = e \\ &\Leftrightarrow x^2 yxy = x \quad \text{car } x^2 = e \\ &\Leftrightarrow yxy = x \\ &\Leftrightarrow y^2 xy = yx \\ &\Leftrightarrow xy = yx\end{aligned}$$

Ce qui prouve que G est commutatif.

Autre méthode.

* $\forall x \in G, x^2 = e \Leftrightarrow \forall x \in G, x = x^{-1}$.

Ainsi $\forall (x, y) \in G \times G, (xy)^{-1} = y^{-1}x^{-1} = yx$

Ce qui prouve que G est commutatif.

2. H sous groupe propre de G , on a si $a \in G - H$, alors $H \cap aH = \emptyset$

Posons $H_1 = H \cup aH$. On a $H \subset H_1$ donc $H_1 \neq \emptyset$.

Pour tout $x \in H_1$, on a $x \in H$ ou $x \in aH$.

Si $x \in H$, alors $x^{-1} \in H \subset H_1$

Si $x \in aH$, alors il existe $h \in H$ tel que $x = ah$.

Donc $x^{-1} = h^{-1}a^{-1} = ha = ah \in aH \subset H_1$.

Ainsi $\forall x \in H_1, x^{-1} \in H_1$.

Soient x et y dans H_1 . Si $x, y \in H$ alors $xy \in H \subset H_1$.

Si $x, y \in aH$, alors il existe $h_1, h_2 \in H$ tels que $x = ah_1$ et $y = ah_2$.

Alors $xy = ah_1ah_2 = h_1h_2 \in H \subset H_1$ car $a^2 = e$ et $h_1a = ah_1$.

Si $x \in H$ et $y \in aH$, alors y s'écrit $ah = y, h \in H$. Par la suite

$xy = xah = axh \in aH \subset H_1$.

Ainsi $\forall x, y \in H_1, xy \in H_1$, donc H_1 est un sous groupe de G . ①

3. Si G est d'ordre fini, montrons que $\exists k \in \mathbb{N} / |G| = 2^k$.

* Faisons une démonstration par récurrence sur $|G| = n$.

Pour $n=1$, le résultat est vrai.

Supposons que le résultat est vrai pour tout groupe d'ordre $< n$ avec

Soit G un groupe d'ordre n et soit $x \in G, x \neq e$.

Posons $H = \langle x \rangle$ (sous groupe engendré par x)

On a $|H| = 2$. Et le groupe G/H vérifie la condition $\forall \bar{y} \in G/H, \bar{y}^2 = \bar{e}$

D'après l'hypothèse de récurrence, puisque $|G/H| = \frac{|G|}{|H|} = \frac{|G|}{2} < n$

$|G/H| = 2^t, t \in \mathbb{N}$. Alors $|G| = 2^{t+1}$.

Donc $\forall n \in \mathbb{N} / |G| = n \Rightarrow \exists k \in \mathbb{N} / |G| = 2^k$.

* Autre méthode.

Si $|G| = 1$, le résultat est vrai.

Supposons que $|G| > 1$. Soit $x \in G, x \neq e$ et soit $H_1 = \langle x \rangle$

Nous avons $|H_1| = 2 = 2^1$. Ou bien $G = H_1$ ou bien $G \not\subseteq H_1$.

Si $G \not\subseteq H_1$; soit $a_1 \in G \setminus H_1$. D'après Partie 1, 2, on a $H_2 = H_1 \cup a_1 H_1$

est un sous groupe de G . Nous avons $|H_2| = 2^2$.

Si $G \not\subseteq H_2$, prenons $a_2 \in G \setminus H_2$ et posons $H_3 = H_2 \cup a_2 H_2$.

H_3 est un sous groupe de G et $|H_3| = 2^3, \dots$

Comme G est fini, au bout d'un nombre fini d'opérations, on aura

$G = H_n$ et $|H_n| = |G| = 2^n$.

Exercice 2

1. Montrons que G contient un élément d'ordre 2.

Soit $H = \{x \in G \mid x \neq x^{-1}\}$. Pour tout $x \in H$, $x^{-1} \in H$.

Il en résulte que $|H|$ est pair; $|G-H| = |G| - |H|$ est pair et $e \in G-H$. Donc $|G-H| \geq 2$.

Ainsi il existe $a \in G-H$, $a \neq e$. Alors $a = a^{-1}$, c'est à dire $a^2 = e$ et $a \neq e$.

En fait, il y a un nombre impair d'éléments $y \in G$ tel que $y \neq e$ et $y^2 = e$.

Donc G contient des éléments d'ordre 2.

2. Montrons que $|G| = 2p$ (p premier) $\Rightarrow G$ contient un élément d'ordre p .

$$|G| = 2p \quad , p \text{ premier}$$

D'après la question précédente, on peut supposer que $p > 2$.

On sait que tout élément de G est d'ordre 1, 2, p ou $2p$.

Le seul élément d'ordre 1 est l'élément neutre e .

Si tous les éléments de G (autres que e) étaient d'ordre 2, alors $|G|$ serait une puissance de 2 d'après la partie 1.

Comme p est premier et $p > 2$, alors il existe donc un élément de G d'ordre p . En effet, comme $|G|$ n'est pas une puissance de 2, il existe des éléments de G d'ordre p ou bien d'ordre $2p$.

Si $a \in G$ et $o(a) = 2p$ alors a^2 est d'ordre p .

Dans tous les cas, il existe un élément de G d'ordre p .

Partie 3.

1) a) Montrons que HVK est un sous groupe $G \Leftrightarrow H \subset K$ ou $K \subset H$.

Si $H \subset K$ ou $K \subset H$ alors $HVK = K$ ou $HVK = H$ et donc

HVK est un sous groupe de G .

Supposons que HVK est un sous groupe de G et supposons que $K \not\subset H$ et $H \not\subset K$.

Alors, il existe $x \in H \setminus K$ et $y \in K \setminus H$. On a $xy \in HVK$, donc $xy \in H$ ou $xy \in K$.

Mais $xy \in H$ et $x \in H$ implique $y \in H$ ce qui est impossible.

De même $xy \in K$ et $y \in K$ implique $x \in K$ ce qui est impossible.

Ainsi HVK sous groupe de G implique $H \subset K$ ou $K \subset H$.

b). Si H et K sont deux sous groupes propres de G tel que $G = HVK$ alors d'après ce qui précède $G = H$ ou $G = K$.

Ainsi G ne peut être la réunion de deux sous groupes propres de G .

2) Si G est fini ou $G = H$ alors $G - H$ est fini.

Inversement supposons que $G - H$ fini; Alors $[G:H]$ est fini.

Supposons $G \neq H$.

Posons $[G:H] = n$. On a $n \geq 2$. Soit $\{e, x_2, \dots, x_n\}$ un ensemble de représentants des classes à gauche modulo H dans G .

Nous avons $G = H \cup x_2 H \cup \dots \cup x_n H$, et $G - H = x_2 H \cup \dots \cup x_n H$.

Comme $G - H$ est fini, H est fini et donc G est fini.

3) $H \not\subset G$. Pour tout $x \in G - H$ et tout $y \in H$, $xy \notin H$, donc

$xy \in G - H \subset \text{gr}(G - H)$.

Ainsi $y \in \text{gr}(G - H)$. Il en résulte que $H \subset \text{gr}(G - H)$

et donc $G = \text{gr}(G - H)$.

4) Si A est un sous groupe de G , alors A est stable par la loi de G .

Supposons que A est stable par la loi de G . Montrons que $\forall x \in A$, on a $\{x^n/n \in \mathbb{N}^*\} \subset A$ donc $\{x^n/n \in \mathbb{N}\}$ est fini.
Il existe donc $m, n \in \mathbb{N}^*$, $m \neq n$ tels que $x^m = x^n$.

Supposons $m > n$. On obtient donc $x^{m-n} = e$. Ainsi tout élément de A est d'ordre fini. Soit alors $a \in A$ et soit $p = o(a)$.

On a donc $a^{-1} = a^{p-1} \in A$. Ainsi A est un sous groupe de G .

5) Toute partie de G est finie.

Toute partie non vide ^{stable} de G est un sous groupe de G d'après 4).

Le résultat de 5) n'est pas vrai si G est infini.

Par exemple en prenant $G = (\mathbb{Z}, +)$. \mathbb{N} est une partie non vide de $(\mathbb{Z}, +)$, mais $(\mathbb{N}, +)$ n'est pas un sous groupe de $(\mathbb{Z}, +)$.

Exercice 1.

$$1. \quad 3 \perp \frac{3}{2} = 3 + \frac{3}{2} - 3 \times \frac{3}{2} = \frac{9}{2} - \frac{9}{2} = 0$$

$$-2 \perp 5 = -2 + 5 - (-2) \times 5 = 3 + 10 = 13$$

$$0 \perp \sqrt{7} = 0 + \sqrt{7} - 0 \times \sqrt{7} = \sqrt{7}.$$

2. Montrons que $(\mathbb{R} - \{1\}, \perp)$ est un groupe abélien.

Pour tous $x, y \in \mathbb{R} - \{1\}$

$$\begin{aligned} \text{On a } x \perp y &= x + y - xy \\ &= 1 - (1-x)(1-y) \end{aligned}$$

Cette égalité montre que si $x \neq 1$ et $y \neq 1$, on a alors $x \perp y \neq 1$.

La loi est donc interne dans $\mathbb{R} - \{1\}$.

• Montrons que la loi \perp est associative.

$$\forall x, y, z \in \mathbb{R} \setminus \{1\}$$

$$\begin{aligned}(x \perp y) \perp z &= (x+y-xy) \perp z \\ &= x+y-xy+z - (x+y-xy)z \\ &= x+y-xy+z -xz -yz +xyz\end{aligned}$$

De même

$$\begin{aligned}x \perp (y \perp z) &= x \perp (y+z-yz) \\ &= x+y+z-yz - x(y+z-yz) \\ &= x+y+z-yz -xy -xz +xyz\end{aligned}$$

$$\text{D'où } (x \perp y) \perp z = x \perp (y \perp z)$$

Par la suite la loi \perp est associative.

• Montrons que 0 est l'élément neutre
 $\forall x \in \mathbb{R} \setminus \{1\}$

$$0 \perp x = 0+x-0 \cdot x = x$$

$$x \perp 0 = x+0-x \cdot 0 = x$$

Donc 0 est l'élément neutre.

• Montrons que tout élément de $\mathbb{R} \setminus \{1\}$ est inversible (symétrisable).

$\forall x \in \mathbb{R} \setminus \{1\}$, cherchons $x' \in \mathbb{R} \setminus \{1\}$ tel que $x \perp x' = 0$.

$$x \perp x' = 0 \Leftrightarrow 1 - (1-x)(1-x') = 0$$

$$\Leftrightarrow (1-x)(1-x') = 1$$

$$\Leftrightarrow 1-x' = \frac{1}{1-x} \quad \text{car } x \neq 1.$$

$$\Leftrightarrow x' = \frac{x}{x-1}$$

Donc $\forall x \in \mathbb{R} \setminus \{1\}$, x est symétrisable et son symétrique est $\frac{x}{x-1}$.

l'opérateur $(\mathbb{R} \times \mathbb{R}, -)$ est un groupe —
 Puisque dans \mathbb{R} , $+$ et \times sont commutatifs, alors $-$ est commutatif
 dans $\mathbb{R} \times \mathbb{R}$.

ou bien $\forall x, y \in \mathbb{R} \times \mathbb{R}$.

$$x \perp y = x + y - xy = y + x - yx = y \perp x.$$

3) Pour $n \geq 2$

On a $n=2$, $x \perp x = 1 - (1-x)^2$ vrai

supposons que pour $k \geq 2$ donc on a $x^k = 1 - (1-x)^k$

$$\begin{aligned} \text{On a donc } x^{k+1} &= x^k \perp x = 1 - (1-x) [1 - (1-x)^k] \\ &= 1 - (1-x) (1-x)^k \\ &= 1 - (1-x)^{k+1} \end{aligned}$$

D'où $\forall n \in \mathbb{N} \setminus \{1\}$ $x^n = 1 - (1-x)^n$.

• Pour $n=1$, on a $x = 1 - 1 + x = 1 - (1-x)^1$

Donc $\forall n \in \mathbb{N}^*$ $x^n = 1 - (1-x)^n$.

Exercice

$$A_\alpha = \begin{pmatrix} 3-\alpha & -5-2 & \alpha \\ -\alpha & \alpha+2 & \alpha \\ 5 & -5 & -2 \end{pmatrix} \text{ et } I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \left[\begin{array}{l} \text{matrice unitaire} \\ \text{d'ordre 3} \end{array} \right]$$

$$\begin{aligned} 1. \text{o. } P_\alpha(x) &= \det(A_\alpha - xI) \\ &= \begin{vmatrix} 3-\alpha-x & -5-2 & \alpha \\ -\alpha & \alpha+2-x & \alpha \\ 5 & -5 & -2-x \end{vmatrix} = \begin{vmatrix} 3-\alpha-x & -2-x & 3-x \\ -\alpha & -2-x & 0 \\ 5 & 0 & 3-x \end{vmatrix} \end{aligned}$$

$$P_{\alpha}(x) = (3-x)(-2-x) \begin{vmatrix} 3-\alpha-x & 1 & 1 \\ -\alpha & 1 & 0 \\ 5 & 0 & 1 \end{vmatrix}$$

$$= (3-x)(-2-x) \begin{vmatrix} -2-\alpha-x & 1 & 1 \\ -\alpha & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix}$$

D'où $P_{\alpha}(x) = -(x-3)(x+2)^2$, indépendant de la valeur α .

$$q_A(x) = (x-3)(x+2).$$

b) $\text{Det}(A_{\alpha}) = P_{\alpha}(0) = 12 \neq 0$ donc $f \in GL(E)$.

$$A_{\alpha}^{-1} = \frac{1}{12} \begin{pmatrix} 3\alpha+4 & -3\alpha-10 & -3\alpha \\ 3\alpha & -3\alpha-5 & -3\alpha \\ 10 & -10 & -6 \end{pmatrix}$$

2) D'après 1)a) A_{α} admet deux valeurs propres : -2 et 3 .

Soit E_{-2} le sous-espace propre associé à la valeur propre -2 .

Si A_{α} est diagonalisable, alors on doit avoir $\dim E_1 = 2$.

Déterminons donc E_{-2} et la dimension de E_{-2} .

$$E_{-2} = \ker(f + 2I_E)$$

$$\text{On a } A_{\alpha} + 2I = \begin{pmatrix} 5-\alpha & -5+\alpha & \alpha \\ -\alpha & \alpha & \alpha \\ 5 & -5 & 0 \end{pmatrix}$$

$$\vec{u} \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \ker(f + \alpha I_E) \Leftrightarrow (A_{\alpha} + 2I) \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\Leftrightarrow \begin{cases} (5-\alpha)x + (-5+\alpha)y + \alpha z = 0 \\ -\alpha x + \alpha y + \alpha z = 0 \\ 5x - 5y = 0 \end{cases} \Leftrightarrow \begin{cases} x = y \\ \alpha z = 0 \end{cases}$$

est un plan vectoriel si et seulement si $\alpha = 0$.
 Dans ce cas $\dim(E_\alpha) = 2$ donc A_α est diagonalisable.

3) $\alpha = 0$. A_0 est diagonalisable.
 Déterminons les sous espaces propres associés respectivement à 3 et -2.

D'après la question précédente $E_{-2} = \langle e_1 + e_2, e_3 \rangle$

Soit E_3 le sous espace propre associé à 3.

$E_3 = \ker(f - 3I_E)$ avec $\dim E_3 = 1$.

On a $A_0 - 3I = \begin{pmatrix} 0 & -5 & 0 \\ 0 & -5 & 0 \\ 5 & -5 & -5 \end{pmatrix}$ on remarque $f(e_1 + e_3) = 0$

donc $E_3 = \langle e_1 + e_3 \rangle$.

Posons $u = e_1 + e_2$; $v = e_3$ et $w = e_1 + e_3$.

et $B' = (u; v; w)$. (B' est une base de E).

La matrice P de passage de B à B' est $P = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$

On a $f(u) = -2u$; $f(v) = -2v$ et $f(w) = 3w$

P est inversible et on a $D = P^{-1}A_0P$, avec $D = \begin{pmatrix} -2 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$

On a $A_0 = PD P^{-1}$

ces calculs nous donnent $P^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 1 & 1 \\ 1 & -1 & 0 \end{pmatrix}$

en \mathbb{N}^* $A_0^n = PD^n P^{-1}$ avec $D^n = \begin{pmatrix} (-2)^n & 0 & 0 \\ 0 & (-2)^n & 0 \\ 0 & 0 & 3^n \end{pmatrix}$

$A_0^n = \begin{pmatrix} 3^n & (-2)^n - 3^n & 0 \\ 0 & (-2)^n & 0 \\ (-2)^{n+1} + 3 & (-9)^n - 3^n & (-2)^n \end{pmatrix}$

Puisque A_0 est inversible alors la relation A_0^n est aussi vraie dans \mathbb{Z}^* .

$$\forall n \in \mathbb{N} \quad A_0^n = \frac{1}{5} [3^n - (-2)^n] A_0 + \frac{1}{5} [2(3^n) + 3(-2)^n] I.$$

$$e^{tA_0} = I + \sum_{n=1}^{+\infty} \frac{t^n A_0^n}{n!} = I + \sum_{n=1}^{+\infty} \frac{t^n}{n!} \left[\frac{3^n}{5} (A_0 + 2I) + \frac{(-2)^n}{5} (3I - A_0) \right]$$

$$= I + \frac{1}{5} \sum_{n=1}^{+\infty} \frac{(3t)^n}{n!} (A_0 + 2I) + \frac{1}{5} \sum_{n=1}^{+\infty} \frac{(-2t)^n}{n!} (3I - A_0)$$

$$= \frac{1}{5} \sum_{n=0}^{+\infty} \frac{(3t)^n}{n!} (A_0 + 2I) + \frac{1}{5} \sum_{n=0}^{+\infty} \frac{(-2t)^n}{n!} (3I - A_0)$$

$$e^{tA_0} = \frac{1}{5} e^{3t} (A_0 + 2I) + \frac{1}{5} e^{-2t} (3I - A_0)$$

Cette épreuve comporte quatre (4) exercices indépendants.

EXERCICE 1

K est un corps commutatif et E est un K espace vectoriel.
 Soit f un élément non nul de $L(E)$.
 On désigne respectivement par $\tilde{0}$ et e , l'endomorphisme nul et l'application identique de E .
 On suppose dans cet exercice que $f^2 = \tilde{0}$.

- 1) 1) Montrer que $\text{Im } f \subset \text{Ker } f$.
 2) On considère g élément de $L(E)$ tel que $g = e - f$.
 a) Montrer que g est un automorphisme de E . 1 b) Déterminer g^{-1} . 1,5
 3) On suppose maintenant que $K = \mathbb{R}$ et $E = \mathbb{R}^3$.
 a) Montrer que $\dim(\text{Im } f) \leq \dim(\text{Ker } f)$. 0,5 b) En déduire alors que $\dim(\text{Im } f) < 2$. (1,5)
 c) Montrer qu'il existe une forme linéaire h sur \mathbb{R}^3 et un vecteur \vec{u} de \mathbb{R}^3 tels que :

$$\forall \vec{x} \in \mathbb{R}^3, f(\vec{x}) = h(\vec{x}) \cdot \vec{u}. \quad 1,5$$

EXERCICE 2

Soit G un groupe d'élément neutre e .

- 1) Montrer que si G est d'ordre 4 alors il existe dans G un élément différent de l'élément e qui est son propre inverse.
 2) Montrer que G est abélien si et seulement si l'application $\psi : G \rightarrow G$
 $g \mapsto g^{-1}$ est un automorphisme de G .

EXERCICE 3

Dire si les affirmations suivantes sont vraies ou fausses en justifiant votre réponse.

- 1) Puisque $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ alors $\mathbb{R}^2 \times \mathbb{R} = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$. F
 2) Tout groupe G d'ordre fini est abélien. F
 3) Toute matrice diagonalisable est inversible. F
 4) Le seul groupe isomorphe à un groupe d'ordre 4 est $\mathbb{Z}/4\mathbb{Z}$. F
 5) Si une matrice a seulement deux valeurs propres distinctes alors elle est symétrique. F
 6) Si un nombre entier naturel divise le produit de deux nombres entiers naturels alors il divise chacun des deux nombres. F
 7) $(\{-1,1\}, +)$ et $(\{-1,1\}, \times)$ sont des groupes. F
 8) Tout polynôme de degré 3 à coefficients réels a au moins une racine réelle. V
 9) Toute matrice triangulaire est diagonalisable. F

EXERCICE 4

Dans l'espace vectoriel réel $E = \mathbb{R}^3$, muni de la base canonique $B = (e_1, e_2, e_3)$, on considère l'endomorphisme f vérifiant :

$$f(e_1) = 3e_1 - 4e_2 + 4e_3; f(e_2) = e_1 - e_2 + 8e_3 \text{ et } f(e_3) = 2e_3.$$

On pose A la matrice de f dans la base B .

- 1) a) Déterminer A . 1 b) f est-il élément de $GL(E)$? 1
 2) a) Déterminer les valeurs propres de A . 1 b) A est elle diagonalisable? 1

- 3) Déterminer une matrice semblable à A de la forme : $\begin{bmatrix} a & 0 & 0 \\ 0 & b & c \\ 0 & 0 & b \end{bmatrix}$ 1,5

1/1

Corrigé et barème

Exercice 1

1) Montrons que $\text{Im}f \subset \text{Ker}f$.

$$\forall x \in E, f^2(x) = 0 \Rightarrow f(f(x)) = 0 \Rightarrow \begin{cases} f(x) \in \text{Ker}f \\ f(x) \in \text{Im}f \end{cases} \Rightarrow \text{Im}f \subset \text{Ker}f$$

2) a) $g = e - f \Rightarrow f = e - g \Rightarrow f^2 = e - 2g + g^2$

or $f^2 = 0$, donc on a $e = g(g - 2e)$

donc g est un automorphisme de E .

b) Puisque $g(g - 2e) = e$, alors $g^{-1} = g - 2e$.

3) a) D'après la question 1), on a $\text{Im}f \subset \text{Ker}f$.

$$\text{Im}f \subset \text{Ker}f \Rightarrow \dim(\text{Im}f) \leq \dim(\text{Ker}f)$$

b) On sait que $\dim E = \dim(\text{Im}f) + \dim(\text{Ker}f)$

or $\dim E = 3$, donc $2 \dim(\text{Im}f) \leq 3$

Par la suite $\dim f \leq \frac{3}{2}$, ce qui prouve que $\dim(\text{Im}f) < 2$.

c) Puisque $\dim(\text{Im}f) < 2$ alors $\text{rg}f = \dim f = 0$ ou $\text{rg}f = 1$.

1^{er} cas si $\text{rg}f = 0$ alors $f = 0$ c-à-d $\forall x \in E, f(x) = \vec{0}$ absurde.

2^{es} cas si $\text{rg}f = 1$ alors $\exists u \in \mathbb{R}^3 \setminus \{\vec{0}\}$ engendrant $\text{Im}f$

c'est à dire $\exists \vec{u} \neq \vec{0} / \text{Im}f = \langle \vec{u} \rangle$.

Ainsi $\forall x \in \mathbb{R}^3 \exists ! h(x) \in \mathbb{R} / f(x) = h(x) \cdot \vec{u}$.

Exercice 2

1) $|G| = 4 = 2^2$ donc $\exists g \in G \setminus \{e\}$ tel que $g^2 = 0$

donc $g = g^{-1}$.

2) $\varphi \in \text{Aut}(G) \iff \forall (a, b) \in G \times G, \varphi(a)\varphi(b) = a^{-1}b^{-1} = \varphi(ba)$

$\iff \forall (a, b) \in G \times G, \varphi(ab) = \varphi(ba)$

$\iff \forall (a, b) \in G \times G, ab = ba$.

Exercice 3

- 1) Faux car $(a, 1, c) \neq ((a, b), c)$
 $\in \mathbb{R}^3$ $\in \mathbb{R}^2 \times \mathbb{R}$.
- 2) Faux S_6 est un groupe fini et non abélien.
- 3) Faux, car $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ est diagonalisable, mais elle n'est pas inversible.
- 4) Faux, car $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est isomorphe à un groupe d'ordre 4.
- 5) Faux, car la matrice $\begin{pmatrix} 1 & 4 \\ 1 & 1 \end{pmatrix}$ a deux valeurs propres distinctes et elle n'est pas symétrique.
- 6) Faux $\mathbb{O}/\mathbb{Z} \times 3$, mais $\mathbb{O} \times 4$ et $\mathbb{O} \times 3$.
- 7) Faux $(-1; 1; +)$ n'est pas un groupe.
- 8) Vrai, évident
- 9) Faux, évident.

Exercice 4.

1) a) $A = \begin{pmatrix} 3 & 1 & 0 \\ -4 & -1 & 0 \\ 4 & 8 & 2 \end{pmatrix}$

1) $\ker(f) = \{1; -2\}$ donc $f \in GL(\mathbb{C})$.

2) $E_1 = \ker(f - \text{Id}_E) = \{ (x, y, z) \in \mathbb{R}^3 \mid 2x + y = -4x - 2y = 4x + 8y - 3z = 0 \}$
 $= \{ y = -2x \text{ et } z = -4x \} = \{ x(1; -2; -4) \mid x \in \mathbb{R} \}$.

~~dim~~ $\dim E_1 = 1$. d. $E_1 = \langle (1; -2; -4) \rangle$

$E_{-2} = \ker(f - 2\text{Id}_E) = \{ (x, y, z) \mid 5x + y = -4x + y = 4x + 8y = 0 \}$
 $= \{ (x, y, z) \in \mathbb{R}^3 \mid x = y = 0 \} = \{ z(0; 0; 1) \mid z \in \mathbb{R} \}$.

$\dim E_{-2} = 1$ donc A n'est pas diagonalisable.

3) $a=2$

on prend $E_1 = (1, 0, 0)$ $E_2 = (1, -2, -4)$

$E_3 = \{ (x, y, z) \in \mathbb{R}^3 \mid (f - \text{Id}_E)E_3 \subset E_2 \}$ comme $E_1 \in \ker f$ / $\begin{cases} 2x + y = c \\ -4x + 2y = 2x \\ -8x - 4y = -6x \end{cases}$
 $\Leftrightarrow \begin{cases} x = y \\ y = y \\ z = 0 \end{cases}$

ou $\begin{pmatrix} -2 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$

I. ALGÈBRE (2h)

I On considère trois ensembles non vides E, F, G , et des applications $f : E \rightarrow F$; $g : F \rightarrow G$ et $h : G \rightarrow E$.

- 1- Montrer que si $h \circ g \circ f$ et $g \circ f \circ h$ sont injectives et $f \circ h \circ g$ surjective alors f, g et h sont bijectives.
- 2- Que peut-on conclure dans le cas où $h \circ g \circ f$ et $g \circ f \circ h$ sont surjectives et $f \circ h \circ g$ injective ?

II A) Soit (G, \cdot) un groupe d'élément neutre e .

Pour tout $a \in G$, $gr(a)$ est le sous-groupe de (G, \cdot) engendré par a .

1- Soient a et b dans G vérifiant $a \cdot b = b \cdot a$ et $gr(a) \cap gr(b) = \{e\}$.

i) Montrer que $a \cdot b$ est d'ordre fini dans (G, \cdot) si et seulement si a et b sont d'ordre fini dans (G, \cdot) .

ii) On suppose que $a \cdot b$ est d'ordre fini dans (G, \cdot) . Montrer que l'ordre de $a \cdot b$ dans (G, \cdot) est le p.p.c.m des ordres de a et de b dans (G, \cdot) .

2- a) Soient a et b dans G tels que $a \cdot b = b \cdot a$.

Si a est d'ordre m dans (G, \cdot) et b d'ordre n dans (G, \cdot) avec $m \wedge n = 1 = \text{pgcd}(m, n)$, montrer que $a \cdot b$ est d'ordre mn dans (G, \cdot) .

b) Soit $a \in G$ d'ordre $r = st$ dans (G, \cdot) . Montrer que a^s est d'ordre t dans (G, \cdot) .

3- On suppose que (G, \cdot) est abélien.

Soient a et b dans G , d'ordre respectif s et t dans (G, \cdot) avec $s \wedge t = 1$

Montrer que ab est d'ordre st dans (G, \cdot) .

4- On suppose que (G, \cdot) est un groupe cyclique d'ordre n engendré par a .

i) Montrer que, pour $k \in \mathbb{Z}$, $gr(a^k) = G$ si et seulement si $k \wedge n = 1$

ii) Quel est le nombre de générateurs de (G, \cdot) ?

B) i) Montrer que tout groupe (G, \cdot) d'ordre 20449 est abélien.

ii) Déterminer tous les types de groupes d'ordre 20449.

III Tous les anneaux sont supposés avoir un élément unité noté 1.

1- A est un anneau non nul. Donner la définition de la caractéristique de A .

2- A est un anneau intègre. Montrer que la caractéristique de A est soit zéro, soit un nombre premier.

3- A est un anneau intègre fini. Montrer que A est un corps. Quelle est sa caractéristique ?

4- A est un corps (non nécessairement commutatif)

i) Montrer que le centre de A , $\mathcal{C}(A) = \{x \in A \mid \forall y \in A, xy = yx\}$ est un sous-corps commutatif de A .

ii) Rappeler la définition du sous-corps premier de A .

5- i) Rappeler la définition d'un corps premier.

ii) Montrer qu'un corps premier est commutatif.

iii) Déterminer tous les corps premiers (à un isomorphisme près).

iv) Démontrer que le sous-corps premier d'un corps A est un corps premier.

6- Démontrer que le cardinal d'un corps fini est une puissance d'un nombre premier.

II. ANALYSE (2h)

Exercice 1

Soit $(E, \|\cdot\|)$ un espace de Banach et $B : E \times E \rightarrow E$ une application bilinéaire et continue.

On rappelle qu'alors $\exists C_0 > 0, \forall x, y \in E : \|B(x, y)\| \leq C_0 \|x\| \|y\|$.

Soit $a \in E$ tel que $\|a\| < \frac{1}{4C_0}$.

On se propose de démontrer que l'équation $x = a + B(x, x)$ (*) possède une solution $x \in E$.

1. Montrer que $B(x, x) - B(y, y) = \frac{1}{2} [B(x - y, x + y) + B(x + y, x - y)]$.

En déduire que l'application $\Phi : x \mapsto a + B(x, x)$ est lipschitzienne dans toute boule $\{x \in E : \|x\| \leq r\}$ et préciser une constante de Lipschitz pour Φ .

2. Résoudre l'inéquation

$$C_0 r^2 - r + \|a\| \leq 0.$$

Trouver ensuite $0 < r_1 < r_2$ tels que pour tout élément r de l'intervalle $[r_1, r_2]$ on ait :

$$\|x\| \leq r \implies \|a + B(x, x)\| \leq r.$$

3. Trouver un $r > 0$ tel que Φ soit une contraction dans la boule $\{x \in E : \|x\| \leq r\}$.

4. En déduire que l'équation (*) possède une solution $x \in E$. Cette solution est-elle unique?

Exercice 2

Soit $(E, \|\cdot\|)$ un espace vectoriel normé et f une fonction de E dans E qui vérifie

$$\forall t \in \mathbb{R}, \forall x \in E, f(tx) = t^2 f(x).$$

1. Montrer que si f est différentiable en 0 alors sa différentielle en 0 est identiquement nulle c'est-à-dire $Df(0) = 0$.

2. On suppose que f est bornée sur la sphère unité $S = \{x \in E : \|x\| = 1\}$.
Montrer que f est différentiable en 0.

Exercice 3

On considère l'espace mesuré $(\mathbb{R}, \mathcal{B}(\mathbb{R}), \lambda)$, où $\mathcal{B}(\mathbb{R})$ et λ désignent la tribu borélienne et la mesure de Lebesgue respectivement.

Soit $\mathcal{P}(\mathbb{R})$ l'ensemble des parties de \mathbb{R} . Pour $A \in \mathcal{P}(\mathbb{R})$ et $a \in \mathbb{R}$ on note : $A + a = \{x + a : x \in A\}$.

Soit $a \in \mathbb{R}$ fixé.

1. Montrer que

$$\mathcal{T}_a = \{A \in \mathcal{P}(\mathbb{R}) : A + a \in \mathcal{B}(\mathbb{R})\}$$

est une tribu sur \mathbb{R} .

2. Montrer que $\mathcal{B}(\mathbb{R}) \subset \mathcal{T}_a$ puis que $\mathcal{B}(\mathbb{R}) = \mathcal{T}_a$.

3. Pour $A \in \mathcal{B}(\mathbb{R})$ on pose $\mu(A) = \lambda(A + a)$.

Montrer que μ est une mesure sur $(\mathbb{R}, \mathcal{B}(\mathbb{R}))$.

4. En déduire que pour tout $A \in \mathcal{B}(\mathbb{R})$, on a $\lambda(A + a) = \lambda(A)$ (invariance de la mesure de Lebesgue par translation).

$f: E \rightarrow F, g: F \rightarrow G, h: G \rightarrow E$

- 1- $hogof$ et $gofoh$ injectives implique f et h injectives.
 $fohog$ surjective implique f surjective.
 Ainsi $hogof$ et $gofoh$ injectives et $fohog$ surjective implique f bijective et h injective.
 $gofoh$ injective et $fohog$ surjective implique foh injective et surjective, donc foh est bijective. Comme foh et f sont bijectives alors $h = f^{-1} \circ f \circ h$ est bijective.
 $hogof$ injective implique gof injective. Comme f est bijective, $g = gof \circ f^{-1}$ est injective.
 $fohog$ surjective et f bijective implique $hog = f^{-1} \circ fo hog$ surjective. Comme h est bijective, on a $h^{-1} \circ hog = g$ surjective. Ainsi g est bijective.
 On obtient ainsi que f, g et h sont bijectives.
- 2- $hogof$ et $gofoh$ surjectives implique h et g surjectives.
 $fohog$ injective implique g injective.
 Ainsi $hogof$ et $gofoh$ surjectives et $fohog$ injective implique g bijective et h surjective.
 $hogof$ surjective et $fohog$ injective implique hog surjective et injective, donc bijective.
 Comme hog et g sont bijectives, $h = hog \circ g^{-1}$ est bijective.
 $gofoh$ surjective implique gof surjective. Comme g est bijective, on a $f = g^{-1} \circ gof$ surjective.
 $fohog$ injective et hog bijective implique $f = fo hog \circ (hog)^{-1}$ injective. Ainsi f est bijective.

Il en résulte que $hogof$ et $gofoh$ surjectives et $fohog$ injective implique f, g et h bijectives.
 (G, \cdot) est un groupe d'éléments neutre e .

- 1- i) ab d'ordre fini dans (G, \cdot) signifie qu'il existe $n \in \mathbb{N}^*$ tel que $(ab)^n = e = a^n \cdot b^n$.
 Il existe $n \in \mathbb{N}^*$ tel que $a^n \cdot b^n = e$ équivaut à: il existe $n \in \mathbb{N}^*$ tel que $a^n = b^n \in \text{gr}(a) \cap \text{gr}(b)$.
 $\text{gr}(b) = \{e\}$. Il existe $n \in \mathbb{N}^*$ tel que $a^n = b^n = e$ équivaut à: il existe $n \in \mathbb{N}^*$ tel que $a^n = b^n = e$. Ainsi a, b d'ordre fini dans (G, \cdot) équivaut à a et b d'ordre fini dans (G, \cdot) .
- ii) D'après i) a, b d'ordre fini dans (G, \cdot) équivaut à: a et b d'ordre fini dans (G, \cdot) .
 Posons $m = o(a \cdot b), n = o(a), p = o(b)$.
 Nous avons: $(a \cdot b)^m = a^m \cdot b^m = e$ donc $a^m = b^m = e$ (cf i). Ainsi $n | m$ et $p | m$.
 Par suite $nvp = p \cdot p \cdot e \cdot m(n, p)$ divise m .
 Posons $l = nvp$. Nous avons $(a \cdot b)^l = a^l \cdot b^l = e \cdot e = e$ donc $m | l = nvp$. Il en résulte que $m = o(ab) = l = nvp = o(a) \vee o(b)$.
- 2- a) $o(a) = m, o(b) = n$ et $mn = 1$, alors $\text{gr}(a) \cap \text{gr}(b) = \{e\}$ car $\text{gr}(a) \cap \text{gr}(b)$ est un sous-groupe de $\text{gr}(a)$ et de $\text{gr}(b)$. $|\text{gr}(a) \cap \text{gr}(b)|$ divise donc m et n . Ainsi $|\text{gr}(a) \cap \text{gr}(b)| = 1$.
 D'après 1. a, b est d'ordre fini dans (G, \cdot) et $o(a \cdot b) = mn = m \cdot n$.
- b) $a^r = e = a^{st} = (a^s)^t$ donc $o(a^s) | t$. Soit $n = o(a^s)$. Nous avons $(a^s)^n = a^{sn} = e$ donc $n = o(a) | sn$ i.e. $st | sn$. Par suite $t | n$. Ainsi $n = t$.

3 - $(\mathbb{Z}, +)$ est abélien
 a et b étant dans \mathbb{Z} , nous avons $ab = ba$
 D'après 3-a) $e(a-b) = ab$

4 - (G, \cdot) est un groupe cyclique d'ordre n engendré par a.
 a) $G = \langle a \rangle$. $k \in \mathbb{Z}$, $\langle a^k \rangle = G$ si et seulement si $a \in \langle a^k \rangle$
 $a \in \langle a^k \rangle$ équivaut à: il existe $u \in \mathbb{Z}$ tel que $a = (a^k)^u = a^{ku}$
 Il existe $u \in \mathbb{Z}$ tel que $a = a^{ku}$ équivaut à: il existe $u \in \mathbb{Z}$ tel que $a^{ku-1} = e$
 Il existe $u \in \mathbb{Z}$ tel que $a^{ku-1} = e$ équivaut à: il existe $u \in \mathbb{Z}$ tel que $n | ku-1$
 Ce qui s'écrit: il existe u et v dans \mathbb{Z} tels que $ku-1 = nv$ i.e. il existe u et v dans \mathbb{Z} tels que $ku - nv = 1$. D'après Bezout, ceci équivaut à $kn = 1$
 ii) $G = \langle a \rangle = \{e, a, \dots, a^{n-1}\}$. D'après i), pour $k \in \{1, \dots, n-1\}$, $\langle a^k \rangle = G$ qui vaut à $kn = 1$. Le nombre de générateurs de (G, \cdot) est alors $\varphi(n)$ où φ est l'indicateur d'Euler.

5) i) Soit (G, \cdot) un groupe d'ordre $20449 = 11^2 \times 13^2$
 D'après Sylow, (G, \cdot) a un 11-sous-groupe H d'ordre 11^2 et un 13-sous-groupe K d'ordre 13^2 . Le nombre ν_{11} de 11-sous-groupes de Sylow de (G, \cdot) vérifie les relations:
 $\nu_{11} \equiv 1 \pmod{11}$ et $\nu_{11} | 13^2$. Il en résulte que $\nu_{11} = 1$
 De même, $\nu_{13} \equiv 1 \pmod{13}$ et $\nu_{13} | 11^2$. Donc $\nu_{13} = 1$
 Ainsi $H \triangleleft G$ et $K \triangleleft G$. (G, \cdot) est produit direct des sous-groupes H et K.
 H et K sont abéliens donc (G, \cdot) est abélien.

b) Les types de groupes d'ordre 11^2 sont $(\mathbb{Z}/11\mathbb{Z}, +)$ et $(\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}, +)$ group produit.
 De même les types de groupes d'ordre 13^2 sont $(\mathbb{Z}/13\mathbb{Z}, +)$ et $(\mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}, +)$ groupe produit.
 On obtient donc quatre types de groupes d'ordre 20449:
 $(\mathbb{Z}/20449\mathbb{Z}, +)$; $(\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}, +)$; $(\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}, +)$ et $(\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}, +)$.

III 1 - A est un anneau non nul, d'élément unité 1.
 La caractéristique de A est l'ordre de 1 dans $(A, +)$. Si cet ordre est infini on dit que A est de caractéristique zéro (0).
 2 - A est un anneau intègre. Supposons que A est de caractéristique $p \in \mathbb{N}^*$ et que $p = m \cdot n$ avec $1 < m < p$, $1 < n < p$. Alors $p \cdot 1 = (m \cdot n) \cdot 1 = (m \cdot 1) \cdot (n \cdot 1) = 0$. Comme A est intègre, on a $m \cdot 1 = 0$ ou $n \cdot 1 = 0$, ce qui est

3 - A est un anneau intègre fini. Soit $a \in A - \{0\}$.

Les applications $\gamma_a: A \rightarrow A$ et $\delta_a: A \rightarrow A$ sont injectives
 $x \mapsto ax$ et $x \mapsto xa$

Comme A est fini, ce sont des permutations de A .
 Il existe donc b et c dans A tels que $a \cdot b = 1 = c \cdot a$. Alors $c \cdot a \cdot b = c = b$. Ainsi
 a est inversible dans A . Tout élément non nul de A étant inversible dans A ,

A est un corps (commutatif) (Tout corps fini étant commutatif).
 La caractéristique de A est un nombre premier d'après 2-

4 - A est un corps (non nécessairement commutatif)

i) $\mathcal{C}(A) = \{x \in A \mid \forall y \in A, xy = yx\}$

$\mathcal{C}(A) \neq \emptyset$ car 0 et 1 sont dans $\mathcal{C}(A)$.

Pour a, b dans $\mathcal{C}(A)$, $a-b \in \mathcal{C}(A)$ car pour tout $y \in A$, $(a-b) \cdot y = ay - by = ya - yb = y(a-b)$. On a aussi $(a \cdot b) \cdot y = a \cdot (by) = a \cdot (y \cdot b) = (a \cdot y) \cdot b = (y \cdot a) \cdot b = y \cdot (a \cdot b)$ donc $a \cdot b \in \mathcal{C}(A)$. De plus pour $a \in \mathcal{C}(A) - \{0\}$ et pour tout $y \in A$ on a $a \cdot y = y \cdot a$ donc $a^{-1} \cdot a \cdot y = a^{-1} \cdot y \cdot a = y$ et $a^{-1} \cdot y \cdot a \cdot a^{-1} = y \cdot a^{-1} = a^{-1} \cdot y$. Ainsi $a^{-1} \in \mathcal{C}(A)$. $\mathcal{C}(A)$ est un sous-corps commutatif de A .

ii) Le sous-corps premier de A est l'intersection de tous les sous-corps de A .

5 - i) Un corps premier est un corps qui n'a pas de sous-corps propre.

ii) A est un corps premier. D'après 4 - i) $\mathcal{C}(A)$ est un sous-corps commutatif de A . Comme A est un corps premier, $A = \mathcal{C}(A)$.

iii) A est un corps premier. Si A est de caractéristique zéro alors A contient un sous-anneau isomorphe à \mathbb{Z} , donc contient un sous-corps isomorphe à \mathbb{Q} . Comme A est un corps premier, A est isomorphe à \mathbb{Q} .

Si A est de caractéristique $p \in \mathbb{N}^+$ alors p est un nombre premier et A contient un sous-anneau isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Étant un corps, A contient un sous-corps isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Comme A est premier, A est isomorphe au corps $\mathbb{Z}/p\mathbb{Z}$.

Les corps premiers sont donc à un isomorphisme près, \mathbb{Q} et les corps $\mathbb{Z}/p\mathbb{Z}$ où $p \in \mathbb{N}$, p premier.

iv) A est un corps, A_0 le sous-corps premier de A . Tout sous-corps de A_0 est un sous-corps de A , donc contient A_0 . Par suite tout sous-corps de A_0 est égal à A_0 . A_0 est un corps premier.

6 - A est un corps fini. La caractéristique de A est un nombre premier p . A contient un sous-corps \mathbb{F}_p isomorphe à $\mathbb{Z}/p\mathbb{Z}$. A est un \mathbb{F}_p -espace vectoriel de dimension finie n . A est tant que \mathbb{F}_p espace vectoriel est isomorphe à \mathbb{F}_p^n . Ainsi $|A| = |\mathbb{F}_p^n| = p^n$.

**CONCOURS PROFESSIONNEL D'ACCES AU CYCLE DE FORMATION DE
PROFESSEUR CAP/CM - OPTION : MATHÉMATIQUES, AU TITRE DE L'ANNEE 2005**
SESSION DU SAMEDI 14 MAI 2005

EPREUVE : ALGÈBRE

Devoir de Maison N°2

DURÉE : 4 H 00
COEFFICIENT : 2

I-1- Soit (G, \cdot) un groupe fini

- Rappeler la définition de l'ordre du groupe (G, \cdot) (0,5)
- Soit $a \in G$. Rappeler la définition de l'ordre de a dans (G, \cdot) (1)
et démontrer que l'ordre de a dans (G, \cdot) divise l'ordre de (G, \cdot) (1)

2- On suppose que (G, \cdot) est un groupe fini d'ordre un nombre premier p .

- Déterminer tous les sous-groupes de (G, \cdot) (1)
 - Montrer que (G, \cdot) est un groupe cyclique. (1)
- 3- Donner la valeur de vérité (avec justification) des propositions suivantes :
- Tout groupe abélien est monogène (0,5)
 - Tout groupe monogène est abélien (0,5)
 - Tout groupe fini d'ordre un nombre premier est abélien (0,5)
 - Tout groupe d'ordre 6 est abélien. (0,5)

II - Trouver tous les ensembles de trois nombres complexes $\{x, y, z\}$ tels que

$$\begin{cases} |x| = |y| = |z| = 1 \\ x + y + z = 1 \\ xyz = 1 \end{cases}$$

(1+1+1)

(On pourra déterminer un polynôme $P(x) \in \mathbb{C}[x]$ ayant x, y, z pour zéros et ensuite déterminer x, y, z).

III - On considère $P(x) = x^3 + x^2 - x + 2$ et $Q(x) = 2x^3 + 7x^2 + 8x + 4$ dans $\mathbb{R}[x]$

- Déterminer l'idéal de $\mathbb{R}[x]$ engendré par $P(x)$ et $Q(x)$. (1,5)
- On note $D(x) = P(x) \wedge Q(x) = \text{pgcd}(P(x), Q(x))$. Soient $P_1(x)$ le quotient de la division euclidienne de $P(x)$ par $D(x)$ et $Q_1(x)$ le quotient de la division euclidienne de $Q(x)$ par $D(x)$. Déterminer $P_1(x)$ et $Q_1(x)$. (On rappelle que $D(x)$ est un polynôme unitaire). (1)

3- Résoudre dans \mathbb{R}^4 le système d'équations linéaires suivant.

$$\begin{cases} 2a & & + c & & = 0 \\ 3a & + 2b & - c & + d & = 0 \\ 2a & + 3b & + c & - d & = 0 \\ & 2b & & + d & = 1 \end{cases}$$

(a, b, c, d sont les inconnues).
(1)

1/2

X

4- a) En utilisant la décomposition en éléments simples dans $\mathbb{R}(X)$ de $F(X) = \frac{1}{P_1(X)Q_1(X)}$, déterminer deux polynômes $U_0(X)$ et $V_0(X)$ dans $\mathbb{R}[X]$.

tels que $U_0(X)P(X) + V_0(X)Q(X) = D(X)$

b) Déterminer tous les couples de polynômes de $\mathbb{R}[X]$, $(U(X), V(X))$ vérifiant la relation $U(X)P(X) + V(X)Q(X) = D(X)$.

IV - Pour $a \in \mathbb{R}$ on pose $A(a) = \begin{pmatrix} a & 1 & 1 \\ 1 & a & 1 \\ 1 & 1 & a \end{pmatrix} \in M_3(\mathbb{R})$

1- Déterminer les valeurs de a pour lesquelles $A(a) \in GL(3, \mathbb{R})$

2- Pour quelles valeurs de a , $A(a)$ est-elle diagonalisable?

3- On prend $a=0$

a) Déterminer les valeurs propres de $A(0)$

b) Déterminer une matrice $P \in GL(3, \mathbb{R})$ telle que $P^{-1}A(0)P$ soit diagonale.

c) Déterminer le polynôme minimal de $A(0)$

d) Pour tout $n \in \mathbb{Z}$, exprimer $A(0)^n$ en fonction de I et $A(0)$ où

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

e) Pour tout $x \in \mathbb{R}$, calculer $e^{xA} = I + \sum_{k \in \mathbb{N}^*} \frac{x^k A^k}{k!}$

V - 1- Pour tout $m \in \mathbb{R}$ on pose $D_m = \begin{vmatrix} m+2 & 2m+3 & 3m+4 \\ 2m+3 & 3m+4 & 4m+5 \\ 3m+5 & 5m+8 & 4m+17 \end{vmatrix}$

Calculer D_m . (On trouvera $D_m = -3(m+1)^2(m+2)$)

2- On considère le système linéaire (S_m) suivant :

$$(S_m) \begin{cases} (m+2)x + (2m+3)y + (3m+4)z = a \\ (2m+3)x + (3m+4)y + (4m+5)z = b \\ (3m+5)x + (5m+8)y + (4m+17)z = c \end{cases}$$

où m, a, b, c sont des paramètres réels.

a) Déterminer le rang r du système linéaire (S_m) suivant les valeurs du paramètre réel m .

b) Dans chacun des cas où $r < 3$, étudier la compatibilité du système linéaire (S_m) et déterminer les solutions quand elles existent.

1- (G, \cdot) un groupe fini

- a) L'ordre du groupe (G, \cdot) est le cardinal de l'ensemble G . $o(G) = |G|$ (95)
- b) $a \in G$ - L'ordre de a dans (G, \cdot) est l'ordre du sous-groupe $\langle a \rangle$ de (G, \cdot) engendré par a . $o(a) = |\langle a \rangle|$
- d'après le théorème de Lagrange, $|\langle a \rangle|$ divise $|G|$ (1)

2- (G, \cdot) groupe fini, $|G| = p$ un nombre premier

- a) D'après le théorème de Lagrange, G et $\{e\}$ sont les seuls sous-groupes de (G, \cdot)
- b) Pour tout $a \in G - \{e\}$, $\langle a \rangle = G$. (G, \cdot) est donc un groupe cyclique. (1)

3- a) Faux, $(\mathbb{Q}, +)$ est un groupe abélien non monogène (et l'ensemble des nombres rationnels). (1)

b) Vrai (Théorème de Cauchy). (1)

c) Vrai. D'après 2- tout groupe fini d'ordre un nombre premier est cyclique i.e. monogène et fini, et tout groupe monogène est abélien. (0,5)

d) Faux (S_3, \cdot) est un groupe non abélien d'ordre 6. (0,5)

II- Nous avons:

$$\begin{cases} x+y+z=1 \\ xy+z=1 \\ |x|=|y|=|z|=1 \end{cases}$$

donc $x^{-1} = \bar{x}, y^{-1} = \bar{y}, z^{-1} = \bar{z}$
 $xy+yz+zx = z^{-1} + y^{-1} + x^{-1} = \bar{z} + \bar{y} + \bar{x} = \overline{x+y+z} = 1$ (1)

x, y, z non

$$x^2(x-2) + x - 1 = (x-1)(x^2+1) = (x-1)(x+1)(x-1)$$

Ainsi $\{x, y, z\} = \{1, -1, -1\}$

III - $P(x) = x^3 + x^2 - x + 2 \in \mathbb{R}[x]$, $Q(x) = 2x^3 + 7x^2 + 8x + 4 \in \mathbb{R}[x]$

1- \mathbb{R} étant un corps commutatif, $\mathbb{R}[x]$ est un anneau principal.

Nous avons $(P(x), Q(x)) = (P(x)) + (Q(x)) = (P(x) \wedge Q(x))$

Nous avons $P(x) \wedge Q(x) = P(x) \wedge (5x^2 + 10x) = P(x) \wedge 5(x^2 + 2x) = P(x) \wedge (x^2 + 2x) = (x^2 + 2x) \wedge (x+2) = x+2$

Ainsi $(P(x) \wedge Q(x)) = (x+2) = (P(x), Q(x))$ (1)

2- Nous avons $P(x) = (x+2)(x^2 - x + 1)$, $P_1(x) = x^2 - x + 1$

$Q(x) = (x+2)(2x^2 + 3x + 2)$, $Q_1(x) = 2x^2 + 3x + 2$

3- Nous avons:

$$\begin{cases} a+b=0 \\ 2a+c=0 \\ d+3a=0 \\ 2b+d = -2a - 3a = 1 = -5a \end{cases}$$

$a = -\frac{1}{5} = -b$
 $c = -2a = \frac{2}{5}$
 $d = -3a = \frac{3}{5}$ (1)

La solution du système est $(a, b, c, d) = (-\frac{1}{5}, \frac{1}{5}, \frac{2}{5}, \frac{3}{5})$

4- a) $F(x) = \frac{1}{P_1(x) Q_1(x)}$

$P_1(x) \wedge Q_1(x) = 1$, $P_1(x)$ et $Q_1(x)$ sont irréductibles dans $\mathbb{R}[x]$, donc

$$F(x) = \frac{ax+b}{x^2-x+1} + \frac{cx+d}{2x^2+3x+2} = \frac{(ax+b)(2x^2+3x+2) + (cx+d)(x^2-x+1)}{P_1(x) Q_1(x)}$$

$$= \frac{(2a+c)x^3 + (3a+2b-c+d)x^2 + (2a+3b+c-d)x + 2b+d}{P_1(x) Q_1(x)}$$

(a, b, c, d) est solution du système

$$\begin{cases} 2a + c = 0 \\ 3a + 2b - c + d = 0 \\ 2a + 3b + c - d = 0 \\ 2b + d = 1 \end{cases}$$

i.e. $(a, b, c, d) = \left(-\frac{1}{5}, \frac{1}{5}, \frac{2}{5}, \frac{3}{5}\right)$

Ainsi $F(x) = \frac{-x+1}{5(x^2-x+1)} + \frac{2x+3}{5(2x^2+3x+2)}$ (1)

Nous obtenons: $\frac{1}{5}(-x+1)Q_1(x) + \frac{1}{5}(2x+3)P_1(x) = 1$

Alors $\frac{1}{5}(-x+1)Q_1(x)(x+2) + \frac{1}{5}(2x+3)P_1(x)(x+2) = x+2$ i.e.

$\frac{1}{5}(-x+1)Q(x) + \frac{1}{5}(2x+3)P(x) = x+2$. On peut prendre

$U_0(x) = \frac{1}{5}(2x+3)$ et $V_0(x) = \frac{1}{5}(-x+1)$. (1)

b) Des relations $U_0(x)P(x) + V_0(x)Q(x) = x+2 = U(x)P(x) + V(x)Q(x)$ nous tirons

$(U(x) - U_0(x))P(x) + (V(x) - V_0(x))Q(x) = 0$ i.e. $(U(x) - U_0(x))P_1(x) + (V(x) - V_0(x))Q_1(x) = 0$

soit $(U(x) - U_0(x))P_1(x) = (V_0(x) - V(x))Q_1(x)$.

Comme $P_1(x) \wedge Q_1(x) = 1$, nous avons $U(x) - U_0(x) = Q_1(x)H(x)$ et $V_0(x) - V(x) = P_1(x)H(x)$

i.e. $U(x) = U_0(x) + Q_1(x)H(x)$ et $V(x) = V_0(x) - P_1(x)H(x)$ où $H(x) \in \mathbb{R}[x]$.

Inversement, pour tout $H(x) \in \mathbb{R}[x]$, les polynômes $U(x) = U_0(x) + H(x)Q_1(x)$ et $V(x) = V_0(x) - P_1(x)H(x)$ vérifient la relation $U(x)P(x) + V(x)Q(x) = x+2$. (1)

Les couples de polynômes recherchés sont alors $(U_0(x) + Q_1(x)H(x), V_0(x) - P_1(x)H(x))$ où $H(x)$ est un polynôme quelconque de $\mathbb{R}[x]$.

IV - $\alpha \in \mathbb{R}$, $A(\alpha) = \begin{pmatrix} \alpha & 1 & 1 \\ 1 & \alpha & 1 \\ 1 & 1 & \alpha \end{pmatrix} \in M_3(\mathbb{R})$.

1 - $\det A(\alpha) = \begin{vmatrix} \alpha & 1 & 1 \\ 1 & \alpha & 1 \\ 1 & 1 & \alpha \end{vmatrix} = \begin{vmatrix} \alpha+2 & 1 & 1 \\ \alpha+2 & \alpha & 1 \\ \alpha+2 & 1 & \alpha \end{vmatrix} = (\alpha+2) \begin{vmatrix} 1 & 1 & 1 \\ 1 & \alpha & 1 \\ 1 & 1 & \alpha \end{vmatrix} = (\alpha+2) \begin{vmatrix} 1 & 1 & 1 \\ 0 & \alpha-1 & 0 \\ 0 & 0 & \alpha-1 \end{vmatrix}$

$= (\alpha+2)(\alpha-1)^2$. $A(\alpha) \in GL(3, \mathbb{R})$ si et seulement si $\alpha \in \mathbb{R} \setminus \{-2, 1\}$ (1)

a) est une matrice symétrique réelle. Elle est diagonalisable pour tout $a \in \mathbb{R}$. (1)

a) $A(a) = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ $P_{A(a)}(x) = \begin{vmatrix} -x & 1 & 1 \\ 1 & -x & 1 \\ 1 & 1 & -x \end{vmatrix} = (2-x)(x+1)^2$

$\text{Sp } A(a) = \{2, -1\}$ (1)

b) $A(a) - 2I = \begin{pmatrix} -2 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & -2 \end{pmatrix}$ $V_{A(a)}(2) = \text{vect}(e_1 + e_2 + e_3)$

$A(a) + I = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ $V_{A(a)}(-1) = \text{vect}(e_1 - e_2, e_1 - e_3)$

$P = \begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 0 \\ 1 & 0 & -1 \end{pmatrix}$ (1); $P^{-1}A(a)P = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} = D$

c) $q_{A(a)}(x) = (x+1)(x-2)$ (1)

d) Pour $n \in \mathbb{N}^*$, nous avons:

$x^n = q_{A(a)}(x) u(x) + a_n x + b_n$

$\begin{cases} (-1)^n = -a_n + b_n \\ 2^n = 2a_n + b_n \end{cases} \Rightarrow 3a_n = 2^n - (-1)^n \Rightarrow a_n = \frac{1}{3}(2^n - (-1)^n)$

$b_n = (-1)^n + a_n = (-1)^n + \frac{1}{3}(2^n - (-1)^n) = \frac{2}{3}(-1)^n + \frac{1}{3}2^n = \frac{1}{3}(2^n + 2(-1)^n)$

Ainsi $A(a)^n = \frac{1}{3}(2^n - (-1)^n)A(a) + \frac{1}{3}(2^n + 2(-1)^n)I$

$A(a)^n = \frac{1}{3}2^n(A(a) + I) + \frac{1}{3}(-1)^n(2I - A(a))$

Cette formule est valable pour $n=0$. ($A(a) \in GL(3, \mathbb{R})$)
Donc pour tout $n \in \mathbb{N}$, $A(a)^n = \frac{1}{3} \left[2^n(A(a) + I) + (-1)^n(2I - A(a)) \right]$ (1)

Nous avons: $(A(a) + I)(A(a) - 2I) = 0 = A(a)^2 - A(a) - 2I = A(a)(A(a) - I) - 2I$

Donc $A(a)^{-1} = \frac{1}{2}(A(a) - I) = \frac{1}{3} \left[2^{-1}(A(a) + I) + (-1)^{-1}(2I - A(a)) \right]$

Pour $n \in \mathbb{N}^*$,
 $\frac{1}{3} \left[2^n(A(a) + I) + (-1)^n(2I - A(a)) \right] \times \frac{1}{3} \left[2^{-n}(A(a) + I) + (-1)^{-n}(2I - A(a)) \right] =$
 $\frac{1}{9} \left[(A(a) + I)^2 + (-2)^n(A(a) + I)(2I - A(a)) + (-2)^{-n}(2I - A(a))(A(a) + I) + (2I - A(a))(2I - A(a)) \right]$

$$= \frac{1}{9} \left[A(\omega)^2 + 2A(\omega) + I + (-2)^n (A(\omega) - A(\omega)^2 + 2I) + (-2)^{-n} (A(\omega) + 2I - A(\omega)^2) + 4I - 4A(\omega) \right]$$

$$= \frac{1}{9} \left[A(\omega)^2 + 2A(\omega) + I + 4I - 4A(\omega) + A(\omega)^2 \right] = \frac{1}{9} \left[A(\omega) + 2I + 2A(\omega) + 5I - 4A(\omega) + A(\omega) + 2I \right]$$

$$= \frac{1}{9} (9I) = I. \text{ Ainsi: } (A(\omega))^{-1} = A(\omega)^{-1} = \frac{1}{3} \left[2^{-n} (A(\omega) + I) + (-1)^{-n} (2I - A(\omega)) \right]$$

Pour tout $n \in \mathbb{Z}$, $A(\omega)^n = \frac{1}{3} \left[2^n (A(\omega) + I) + (-1)^n (2I - A(\omega)) \right]$ (1)

e) $t \in \mathbb{R}$, $e^{tA} = I + \sum_{k \in \mathbb{N}^*} \frac{t^k A^k}{k!}$

$$= \frac{1}{3} (A(\omega) + I) \left(\sum_{k \in \mathbb{N}} \frac{(2t)^k}{k!} \right) + \frac{1}{3} (2I - A(\omega)) \left(\sum_{k \in \mathbb{N}} \frac{(-t)^k}{k!} \right)$$

$$= \frac{1}{3} (A(\omega) + I) e^{2t} + \frac{1}{3} (2I - A(\omega)) e^{-t}$$

$$e^{tA} = \frac{1}{3} e^{2t} (A(\omega) + I) + \frac{1}{3} e^{-t} (2I - A(\omega))$$
 (1.15)

V 1- $m \in \mathbb{R}$.

$$D_m = \begin{vmatrix} m+2 & 2m+3 & 3m+4 \\ 2m+3 & 3m+4 & 4m+5 \\ 3m+5 & 5m+8 & 6m+17 \end{vmatrix} = \begin{vmatrix} m+2 & 2m+3 & 3m+4 \\ m+1 & m+1 & m+1 \\ m+2 & 2(m+2) & 6(m+2) \end{vmatrix} =$$

$$(m+1)(m+2) \begin{vmatrix} m+2 & 2m+3 & 3m+4 \\ 1 & 1 & 1 \\ 1 & 2 & 6 \end{vmatrix} = (m+1)(m+2) \begin{vmatrix} m+2 & m+1 & m+1 \\ 1 & 0 & 0 \\ 1 & 1 & 4 \end{vmatrix}$$

$$= - (m+1)(m+2) \begin{vmatrix} m+1 & m+1 \\ 1 & 4 \end{vmatrix} = - (m+1)^2 (m+2) \begin{vmatrix} 1 & 1 \\ 1 & 4 \end{vmatrix} = -3(m+1)^2 (m+2)$$

$$D_m = -3(m+1)^2 (m+2)$$
 (1.5)

2- a) Le déterminant de la matrice du système (S_m) est $D_m = -3(m+1)^2 (m+2)$

(0.5) - Pour $m \in \mathbb{R} - \{-1, -2\}$, (S_m) est un système de Cramer. Le rang du système est 3.

(0.5) - Pour $m = -1$ la matrice du système est $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 2 & 3 & 7 \end{pmatrix}$; $\text{rg}(S_m) = \text{rg} A = 2$

(0.5) - Pour $m = -2$ la matrice du système est $A = \begin{pmatrix} 0 & -1 & -2 \\ -1 & -2 & -3 \\ -1 & -2 & -3 \end{pmatrix}$, $\text{rg}(S_m) = \text{rg} A = 2$

Pour $m = -1$ nous avons :

$$(S_{-1}) \begin{cases} x+y+z = a \\ x+y+z = b \\ 2x+3y+7z = c \end{cases} \quad A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 2 & 3 & 7 \end{pmatrix}$$

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & a \\ 1 & 1 & 1 & b \\ 2 & 3 & 7 & c \end{array} \right) \rightarrow \left(\begin{array}{ccc|c} 1 & 1 & 1 & a \\ 0 & 0 & 0 & b-a \\ 0 & 1 & 5 & c-2a \end{array} \right) \rightarrow \left(\begin{array}{ccc|c} 1 & 1 & 1 & a \\ 0 & 1 & 5 & c-2a \\ 0 & 0 & 0 & b-a \end{array} \right)$$

Le système (S_{-1}) est compatible si et seulement si $b = a$. (0,75)

Dans ces conditions nous obtenons $y = c - 2a - 5z$

$$x = a - c + 2a + 5z - z = 3a - c + 4z$$

$$S = \left\{ (3a - c + 4z, c - 2a - 5z, z) \mid z \in \mathbb{R} \right\} = \left\{ (3a - c, c - 2a, 0) + z(4, -5, 1) \mid z \in \mathbb{R} \right\}$$

C'est la droite affine de \mathbb{R}^3 passant par $(3a - c, c - 2a, 0)$ de direction vect $((4, -5, 1))$

ii) Pour $m = -2$ nous avons :

$$\begin{cases} -y - 2z = a \\ -x - 2y - 3z = c \end{cases}$$

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & -b \\ 1 & 2 & 3 & -c \\ 0 & 1 & 2 & -a \end{array} \right) \rightarrow \left(\begin{array}{ccc|c} 1 & 2 & 3 & -b \\ 0 & 0 & 0 & b-c \\ 0 & 1 & 2 & -a \end{array} \right) \rightarrow \left(\begin{array}{ccc|c} 1 & 2 & 3 & -b \\ 0 & 1 & 2 & -a \\ 0 & 0 & 0 & b-c \end{array} \right)$$

Le système (S_{-2}) est compatible si et seulement si $b = c$. (0,75)

Dans ces conditions, nous obtenons $y = -a - 2z$; $x = -b - 2y - 3z =$

$$-b + 2a + 4z - 3z = 2a - b + z$$

$$S = \left\{ (2a - b + z, -a - 2z, z) \mid z \in \mathbb{R} \right\} = \left\{ (2a - b, -a, 0) + z(1, -2, 1) \mid z \in \mathbb{R} \right\}$$

C'est la droite affine de \mathbb{R}^3 passant par $(2a - b, -a, 0)$ de direction vect $((1, -2, 1))$.

.....

ECOLE NORMALE SUPERIEURE D'ABIDJAN (E.N.S.) *****		Service des Examens et Concours (S.E.C.)	
Concours d'entrée à l'ENS pour la préparation du CAP/PL		Discipline : Mathématiques	
Epreuve : Algèbre		Durée : 4 Heures	Session : 2014

Cette épreuve comporte cinq (05) exercices indépendants. Le candidat doit traiter les questions posées, dans l'ordre chronologique présenté. Toute réponse sera proposée avec le maximum de rigueur.

Exercice 1

Soit (G, \bullet) un groupe multiplicatif d'élément neutre e , tel que pour tout (x, y) de G^2 , on a $(x \bullet y)^2 = x^2 \bullet y^2$. Soient a et b deux éléments distincts de G , d'ordres respectifs m et n .

1. Montrer (G, \bullet) est commutatif.
2. Démontrer que ab est d'ordre fini.
3. On suppose que $[a] \cap [b] = \{e\}$. Démontrer que l'ordre de l'élément ab est le PPCM $(m; n)$.

Exercice 2

Soit E est un \mathbb{R} -espace vectoriel dimension finie n ($n \in \mathbb{N}^*$). f et g sont deux éléments de $\mathcal{L}_K(E)$.

1. Montrer que $f \circ g$ est bijectif si et seulement si $g \circ f$ est bijectif.
2. Montrer que 0 est une valeur propre de $f \circ g$ si et seulement si 0 est une valeur propre de $g \circ f$.
3. Soit λ une valeur propre non nulle de $f \circ g$ et soit \vec{u} un vecteur propre de $f \circ g$ associé à λ .
 - a) Montrer que $g(\vec{u}) \neq \vec{0}$ et que $g(\vec{u})$ est un vecteur propre de $g \circ f$.
 - b) Quelle est la valeur propre de $g \circ f$ associée à $g(\vec{u})$?
4. Dédurre de ce qui précède que pour tout couple (f, g) de $\mathcal{L}_K(E) \times \mathcal{L}_K(E)$, $f \circ g$ et $g \circ f$ ont les mêmes valeurs propres.

Exercice 3

\mathbb{C} désigne l'ensemble des nombres complexes. Soient a et b deux éléments \mathbb{C} et $f_{a,b}$ l'application définie par.

$$f_{a,b}: \mathbb{C} \rightarrow \mathbb{C}$$

$$z \mapsto az + b\bar{z}$$

1.
 - a) Montrer que $f_{a,b}$ est un endomorphisme de $(\mathbb{C}, +)$.
 - b) Montrer que pour tout couple (m_1, m_2) de \mathbb{R}^2 et pour tout couple (z_1, z_2) de \mathbb{C}^2 ,

$$f_{a,b}(m_1 z_1 + m_2 z_2) = m_1 f_{a,b}(z_1) + m_2 f_{a,b}(z_2)$$
2.
 - a) Pour quelles valeurs des nombres complexes a et b , $f_{a,b}$ est-elle l'application nulle ?
 - b) Déterminer deux nombres complexes α et β , pour que $f_{a,b} \circ f_{a,b} = f_{\alpha, \beta}$
3. Traduire par un système Σ de deux relations entre les nombres complexes a, b, \bar{a} et \bar{b} , la condition pour que $f_{a,b}$ soit involutive.
4. On suppose que $ab \neq 0$. Pour tout couple (z, z') de \mathbb{C}^2 , on pose $f_{a,b}(z) = z'$
 - a) Trouver une condition entre les nombres complexes a, b, \bar{a} et \bar{b} pour que $f_{a,b}$ soit bijective.
 - b) Exprimer alors $f_{a,b}^{-1}$.

Exercice 4

Dans tout cet exercice, n désigne un entier naturel non nul. On considère la fonction définie par

$$\varphi: \mathbb{N}^* \rightarrow \mathbb{N}^*$$

$n \mapsto m$ où m désigne le nombre des entiers naturels plus petits que n et premiers avec n .

1.

a) Calculer $\varphi(1)$

b) Montrer que pour tout n de $\mathbb{N}^* - \{1\}$, $\varphi(n)$ est le nombre des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

c) En déduire $\varphi(p)$ pour p premier.

2. Soit p nombre premier et k un entier naturel non nul, montrer que $\varphi(p^k) = p^k (1 - \frac{1}{p})$

3. Soient p et q deux entiers naturels plus grands que 1, tels que $p \wedge q = 1$.

a) Montrer que $\varphi(pq) = \varphi(p)\varphi(q)$

b) Généraliser par récurrence, l'égalité au cas de n entiers naturels plus grands que 1 et deux à deux premiers entre eux.

4. En déduire que pour tout n de $\mathbb{N}^* - \{1\}$, si $n = \prod_{i=1}^m p_i^{\alpha_i}$, où les p_i sont nombres premiers, deux à deux distincts et les α_i sont des nombres entiers naturels, éléments de $\mathbb{N}^* - \{1\}$, alors on a

$$\varphi(n) = n \prod_{i=1}^m (1 - \frac{1}{p_i})$$

Exercice 5

Dans tout cet exercice, A est un anneau commutatif, unitaire d'élément neutre unité 1, et intègre.

(A peut être \mathbb{Z} , \mathbb{Q} ou \mathbb{R}).

On désigne par α un élément de A qui n'est le carré d'aucun élément de A .

On considère dans $A \times A$, l'addition et la multiplication, définies respectivement par $\forall (a, b) \in A^2$ et

$$\forall (c, d) \in A^2$$

$$(a, b) + (c, d) = (a + c, b + d)$$

$$(a, b) \cdot (c, d) = (ac + abd, ad + bc)$$

1.

a) Montrer que $(A \times A, +, \cdot)$ est un anneau commutatif.

b) Cet anneau est-il unitaire ?

c) Montrer que cet anneau contient un sous-anneau A' isomorphe à l'anneau A .

2.

a) Calculer le carré de $\omega = (0, 1)$.

b) Quels sont les couples (a, b) dont le carré est $(\alpha, 0)$?

Cet anneau $(A \times A, +, \cdot)$ sera noté $A[\sqrt{\alpha}]$.

c) Montrer que si l'on identifie les éléments homologues de $A[\sqrt{\alpha}]$ et de A' , tout élément $z = (a, b)$ de $A[\sqrt{\alpha}]$ s'écrit $z = a + \omega b$.

3. Pour tout élément $z = (a, b)$ de $A[\sqrt{\alpha}]$, on note $\bar{z} = a - \omega b$ et $\varphi(z) = z\bar{z}$.

a) Montrer que l'application $\phi: z \mapsto \bar{z}$ de $A[\sqrt{\alpha}]$ dans $A[\sqrt{\alpha}]$ est un automorphisme de $A[\sqrt{\alpha}]$.

b) Montrer que pour tout élément z de $A[\sqrt{\alpha}]$, $\varphi(z) \in A'$.

c) Montrer que $\forall (z_1, z_2) \in A[\sqrt{\alpha}] \times A[\sqrt{\alpha}]$, $\varphi(z_1 z_2) = \varphi(z_1)\varphi(z_2)$.

d) Montrer que l'élément z de $A[\sqrt{\alpha}]$ admet un inverse dans $A[\sqrt{\alpha}]$ si et seulement si $\varphi(z)$ admet un inverse dans A' .

e) En déduire que si A est un corps, alors $A[\sqrt{\alpha}]$ est un corps.

Exercice 1.

1. $\forall (x, y) \in G, (x \cdot y)^2 = (x \cdot y) \cdot (x \cdot y)$, or $(x \cdot y)^2 = x^2 \cdot y^2$

Donc, on a $x \cdot y \cdot x \cdot y = x \cdot x \cdot y \cdot y \Rightarrow y \cdot x = x \cdot y$
ce qui prouve que (G, \cdot) est commutatif.

2. $(a \cdot b)^{mn} = a^{mn} \cdot b^{mn}$ car (G, \cdot) est commutatif.
 $= e^n \cdot e^m$ car $a^m = e$ et $b^n = e$.
 $= e$

Donc $a \cdot b$ est d'ordre fini et son ordre divise mn .

3. Soit λ l'ordre de $a \cdot b$.

$(a \cdot b)^\lambda = e \Rightarrow a^\lambda \cdot b^\lambda = e$ car (G, \cdot) est commutatif.
 $\Rightarrow a^\lambda = (b^\lambda)^{-1}$
 $\Rightarrow \begin{cases} a^\lambda \in [a] \cap [b] \\ b^\lambda \in [a] \cap [b] \end{cases} \Rightarrow \begin{cases} a^\lambda = e \\ b^\lambda = e \end{cases}$

Donc $\lambda = \text{PPCM}(m, n)$.

Exercice 2

1. $g \circ f$ est bijective $\Rightarrow g \circ f$ est injective $\Rightarrow f$ est injective $\Rightarrow f$ est bijective car $\dim E < +\infty$
 $g \circ f$ est bijective $\Rightarrow g \circ f$ est surjective $\Rightarrow g$ est surjective $\Rightarrow g$ est bijective car $\dim E < +\infty$
Par conséquent, $f \circ g$ est bijective.

2. Evident, d'après la question 1.

3. a) $f \circ g(\vec{u}) = \lambda \vec{u} \Rightarrow f(g(\vec{u})) = \lambda \vec{u} \Rightarrow g(\vec{u}) \neq \vec{0}$ car $\lambda \vec{u} \neq \vec{0}$.

$g \circ f(g(\vec{u})) = g(f \circ g(\vec{u})) = g(\lambda \vec{u}) = \lambda g(\vec{u})$, donc $g(\vec{u})$ est un vecteur propre de $g \circ f$.

b) λ est la valeur propre de $g \circ f$ associée à $g(\vec{u})$.

4) Soit λ une valeur propre de $f \circ g$.

• si $\lambda = 0$ alors $f \circ g$ n'est pas bijective.

$f \circ g$ n'est pas bijective $\Rightarrow 0$ est une valeur propre de $g \circ f$, d'après 2.

• $\lambda \neq 0 \Rightarrow \lambda$ est une valeur propre de $g \circ f$.

Donc, $\forall \lambda \in \mathbb{R}$, $g \circ f$ et $f \circ g$ ont les mêmes valeurs propres.

Exercice 3.

1.

a) $\forall (z_1, z_2) \in \mathbb{C} \times \mathbb{C}, f_{a,b}(z_1 + z_2) = a(z_1 + z_2) + b(\overline{z_1 + z_2})$

ce qui prouve que $f_{a,b}$ est un élément de $d(\mathbb{C}) = f_{a,b}(z_1) + f_{a,b}(z_2)$

b) $\forall (m_1, m_2) \in \mathbb{R}^2, \forall (z_1, z_2) \in \mathbb{C}^2$

$f_{a,b}(m_1 z_1 + m_2 z_2) = f_{a,b}(m_1 z_1) + f_{a,b}(m_2 z_2)$
 $= m_1 f_{a,b}(z_1) + m_2 f_{a,b}(z_2)$ car $m_1 = \overline{m_1}$ et $m_2 = \overline{m_2}$

2

a) $f_{a,b}$ est l'application nulle ssi $\forall z \in \mathbb{C}, f_{a,b}(z) = 0$.

Donc on a $f_{a,b}(1) = 0$ et $f_{a,b}(i) = 0$

$\begin{cases} f_{a,b}(1) = 0 \\ f_{a,b}(i) = 0 \end{cases} \Rightarrow \begin{cases} a+b=0 \\ a i - b i = 0 \end{cases} \Rightarrow \begin{cases} a+b=0 \\ a-b=0 \end{cases} \Rightarrow a=b=0$

b) $\forall z \in \mathbb{C}, f_{a,b} \circ f_{a,b}(z) = f_{a,b}(a z + b \overline{z})$
 $= a(a z + b \overline{z}) + b(\overline{a z + b \overline{z}})$
 $= (a^2 + |b|^2) z + b(a + \overline{a}) \overline{z}$

Donc $\begin{cases} \alpha = a^2 + |b|^2 \\ \beta = b(a + \overline{a}) \end{cases}$

3) $f_{a,b}$ est involutive ssi $\forall z \in \mathbb{C}, f_{a,b} \circ f_{a,b}(z) = z$.

$\Rightarrow \begin{cases} a^2 + |b|^2 = 1 \\ b(a + \overline{a}) = 0 \end{cases} \Rightarrow \begin{cases} a^2 = 1 \\ b = 0 \end{cases}$ ou $\begin{cases} a^2 + |b|^2 = 1 \\ a + \overline{a} = 0 \end{cases}$

4)

a) $\forall (z, z') \in \mathbb{C}^2, f_{a,b}(z) = z' \Rightarrow a z + b \overline{z} = z' \Rightarrow \overline{b} z + \overline{a} \overline{z} = \overline{z}'$

$\Rightarrow \begin{cases} a z + b \overline{z} = z' \\ \overline{b} z + \overline{a} \overline{z} = \overline{z}' \end{cases} \Rightarrow z(a \overline{a} - b \overline{b}) = \overline{a} z' - b \overline{z}'$

$f_{a,b}$ est bijective ssi $a \overline{a} - b \overline{b} \neq 0$.

b) Dans le cas où $f_{a,b}$ est bijective, on a

$f_{a,b}^{-1} : \mathbb{C} \rightarrow \mathbb{C}$
 $z \mapsto \frac{\overline{a}}{|a|^2 - |b|^2} z - \frac{b}{|a|^2 - |b|^2} \overline{z}$ $f_{a,b}^{-1} = \frac{\overline{a}}{|a|^2 - |b|^2}; -\frac{b}{|a|^2 - |b|^2}$

a) $1 \leq 1$ et 1 est premier avec 1 (seul diviseur commun 1).
 $\varphi(1) = 1$.

b) Soit $\alpha \in \mathbb{Z}/n\mathbb{Z}$ et α l'élément de la classe α tel que $1 \leq \alpha \leq n$
 α inversible $\Leftrightarrow \exists \beta \in \mathbb{Z}/n\mathbb{Z} \quad \alpha\beta = \bar{1}$
 $\Leftrightarrow \exists b \in \mathbb{Z} \quad ab \equiv 1 [n]$
 $\Leftrightarrow \exists b \in \mathbb{Z}, \exists \lambda \in \mathbb{Z} \quad ab + \lambda n = 1$
 $\Leftrightarrow a$ et n sont premiers entre eux (d'après le théorème de Bézout)

Le nombre des entiers a tels que $1 \leq a \leq n$ et premiers avec n , c'est à dire $\varphi(n)$ est donc égal au nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.
 En particulier, si n est premier (notons le p), alors $\mathbb{Z}/p\mathbb{Z}$ est un corps et a donc $p-1$ éléments inversibles, donc $\varphi(p) = p-1$, pour p premier.

Remarque

Pour calculer $\varphi(p^k)$, on peut aussi utiliser la définition de φ , car $1, 2, \dots, p-1$ sont premiers avec p , donc $\varphi(p) = p-1$.

2. des multiples m de p tels que $1 \leq m \leq p^k$ sont $p, 2p, \dots, p^k$
 Soit: $1 \cdot p, 2 \cdot p, \dots, p^{k-1} \cdot p$; il y en a donc p^{k-1} .
 • D'autre part, il y a p^k nombres tels que $1 \leq m \leq p^k$.
 • Donc $\varphi(p^k) = p^k - p^{k-1}$
 $= p^{k-1} \left[1 - \frac{1}{p} \right]$

3. a) Soient p et q , deux nombres entiers naturels plus grands que 1, premiers entre eux, on sait que les anneaux $\mathbb{Z}/pq\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ sont isomorphes.
 Donc, ils ont le même nombre d'éléments inversibles.

Or le nombre d'éléments inversibles est:
 • $\varphi(pq)$ pour $\mathbb{Z}/pq\mathbb{Z}$ d'après 1, b.
 • $\varphi(p) \times \varphi(q)$ pour $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$,
 Car un élément $(\alpha, \beta) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ est inversible ssi α est inversible dans $\mathbb{Z}/p\mathbb{Z}$ et β est inversible dans $\mathbb{Z}/q\mathbb{Z}$, et il y a $\varphi(p)$ éléments inversibles dans $\mathbb{Z}/p\mathbb{Z}$, et $\varphi(q)$ éléments

b) Soient p_1, p_2, \dots, p_m , m entiers naturels plus grands que 1, deux à deux premiers entre eux, démontrons par récurrence que

$$\varphi(p_1 \cdot p_m) = \varphi(p_1) \cdots \varphi(p_m)$$

• l'égalité est vraie pour $m=1$ $\varphi(p_1) = \varphi(p_1)$.

• Si elle est vraie pour m , elle est vraie pour $m+1$:

Soient $p_1, p_2, \dots, p_m, p_{m+1}$ $m+1$ entiers naturels plus grands que 1, deux à deux premiers entre eux.

p_{m+1} est premier avec p_1, p_2, \dots, p_m , donc il est premier avec leur produit $p_1 p_2 \cdots p_m$.

Donc d'après ce qu'on a montré au début de cette question,

$$\begin{aligned}\varphi(p_1 \cdots p_m p_{m+1}) &= \varphi(p_1 \cdots p_m) \varphi(p_{m+1}) \\ &= \varphi(p_1) \cdots \varphi(p_m) \cdot \varphi(p_{m+1}), \text{ car } \varphi(p_1 \cdots p_m) = \varphi(p_1) \cdots \varphi(p_m).\end{aligned}$$

Par conséquent, l'égalité est vraie au cas de n entiers naturels plus grands que 1 et deux à deux premiers entre eux.

4-
Soit $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$

• Si $m=1$ $n = p_1^{\alpha_1}$ et $\varphi(n) = n \left(1 - \frac{1}{p_1}\right)$

• Si $m \geq 2$; les $p_i^{\alpha_i}$ sont deux à deux premiers entre eux (car les p_i le sont, car des nombres premiers distincts sont premiers entre eux);

D'après la question 3,

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \varphi(p_2^{\alpha_2}) \cdots \varphi(p_m^{\alpha_m})$$

$$= p_1^{\alpha_1} \left(1 - \frac{1}{p_1}\right) \cdot p_2^{\alpha_2} \left(1 - \frac{1}{p_2}\right) \cdots p_m^{\alpha_m} \left(1 - \frac{1}{p_m}\right) \text{ d'après la question 2}$$

$$= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_m}\right)$$

$$= n \prod \left(1 - \frac{1}{p_i}\right).$$

a) L'addition $(a, b) + (c, d) = (a+c, b+d)$ sur A^2 de la structure de groupe produit, car A est un groupe.

A étant abélien, A^2 est lui-même un groupe abélien.

On montre aisément que la multiplication

$(a, b) \cdot (c, d) = (ac + abd, ad + bc)$ est commutative, elle est associative et elle est distributive par rapport à l'addition, donc $(A^2, +, \cdot)$ est un anneau commutatif.

b) Cet anneau est unitaire, car l'élément $(1, 0)$ de A^2 est l'élément neutre de A^2 pour la multiplication.

c) Considérons le sous-ensemble A' de A^2 défini par

$$A' = \{(a, 0), a \in A\}.$$

• $A' \neq \emptyset$, car $(0, 0) \in A'$

• $\forall (a, 0) \in A'$ et $\forall (c, 0) \in A'$, $(a, 0) - (c, 0) = (a-c, 0) \in A'$
donc A' est un sous-groupe de A^2 .

• $\forall (a, 0) \in A'$ et $\forall (c, 0) \in A'$, $(a, 0) \cdot (c, 0) = (ac, 0) \in A'$
donc A' est stable pour la multiplication.

Donc A' est un sous-anneau de A^2 .

• Soit f l'application de A vers A' définie par $f(a) = (a, 0)$.

Cette application est de façon évidente bijective.

$$\forall a \in A \text{ et } \forall c \in A$$

$$f(a+c) = (a+c, 0) = (a, 0) + (c, 0) = f(a) + f(c)$$

$$f(ac) = (ac, 0) = (a, 0) \cdot (c, 0) = f(a) \cdot f(c)$$

f est donc un isomorphisme d'anneaux de A sur A' .

A^2 contient donc un sous-anneau isomorphe à A .

2.

$$a) \omega^2 = (0, 1) \cdot (0, 1) \\ = (\alpha, 0).$$

b) soit $(a, b) \in A^2$

$$(a, b)^2 = (\alpha, 0) \Leftrightarrow (a^2 + \alpha b^2, 2ab) = (\alpha, 0)$$

$$\Leftrightarrow \begin{cases} a^2 + \alpha b^2 = \alpha \\ 2ab = 0 \end{cases} \Leftrightarrow \begin{cases} b = 0 \\ a^2 = \alpha \end{cases} \text{ ou } \begin{cases} a = 0 \\ b^2 = 1 \end{cases}$$

Car A est un anneau intègre.

α n'est pas par hypothèse, le carré d'aucun élément de A ,
donc les seules solutions dans A^2 de $(a, b)^2 = (\alpha, 0)$

sont $\omega = (0, 1)$ et $(0, -1)$

$$\text{Car } b^2 - 1 = (b-1)(b+1) \text{ et } (b-1)(b+1) = 0 \Leftrightarrow b=1 \text{ ou } b=-1$$

c)

si l'on convient d'identifier des anneaux isomorphes A et A' ,
On notera à la fois l'élément a de A et l'élément $(a, 0)$ de A' .

$$\text{Alors } z = (a, b) = (a, 0) + (0, b) = (a, 0) + (0, 1)(b, 0) \quad /$$

$$\text{donc on écrira } z = a + \omega b.$$

3. a) L'application ϕ est involutive (car $\overline{\overline{z}} = z$) donc bijective.Soient $z_1 = a + \omega b$ et $z_2 = c + \omega d$ deux éléments de $A[\sqrt{\alpha}]$

$$\phi(z_1 + z_2) = a + c - \omega(b + d)$$

$$= (a - \omega b) + (c - \omega d)$$

$$= \phi(z_1) + \phi(z_2)$$

$$\phi(z_1 z_2) = ac + \alpha bd - \omega(ad + bc)$$

$$= (a - \omega b)(c - \omega d)$$

$$= \phi(z_1) \phi(z_2) \quad \text{car } \omega^2 = \alpha.$$

Donc ϕ est un automorphisme involutif de l'anneau $A[\sqrt{\alpha}]$ On peut aussi montrer que ϕ est un isomorphisme de $A[\sqrt{\alpha}]$ sur $A[\sqrt{\alpha}]$.

b) soit $z = a + wb$ un élément de $A[\sqrt{\alpha}]$, calculons $\varphi(z)$ (4)

$$\varphi(z) = z \bar{z} = (a + wb)(a - wb) = a^2 - w^2 b^2 = a^2 - \alpha b^2 \text{ car } w^2 = \alpha$$

donc $\varphi(z) \in A'$.

c) Soient z_1 et z_2 deux éléments de $A[\sqrt{\alpha}]$

Alors grâce à l'automorphisme ϕ et à la commutativité dans $A[\sqrt{\alpha}]$

$$\varphi(z_1 z_2) = z_1 z_2 \overline{z_1 z_2} = z_1 z_2 \bar{z}_1 \bar{z}_2 = \varphi(z_1) \varphi(z_2)$$

$$\text{Donc } \varphi(z_1 z_2) = \varphi(z_1) \varphi(z_2) \quad \forall (z_1, z_2) \in A[\sqrt{\alpha}] \times A[\sqrt{\alpha}]$$

d) Montrons que l'élément z de $A[\sqrt{\alpha}]$ admet un inverse si $\varphi(z)$ est inversible dans A' .

$$z \text{ inversible dans } A[\sqrt{\alpha}] \Rightarrow \exists z' \in A[\sqrt{\alpha}] \quad z z' = 1.$$

$$\Rightarrow \varphi(z z') = \varphi(1)$$

$$\Rightarrow \varphi(z) \varphi(z') = 1$$

$$\Rightarrow \varphi(z) \text{ inversible dans } A'$$

Réciproquement, si $\varphi(z)$ est inversible dans A' , l'élément $\frac{\bar{z}}{\varphi(z)}$ a un

sens dans $A[\sqrt{\alpha}]$, car $\frac{1}{\varphi(z)} \in A' \subset A[\sqrt{\alpha}]$

$$\text{et } z \times \frac{\bar{z}}{\varphi(z)} = \frac{z \bar{z}}{\varphi(z)} = 1 \quad ; \quad z \text{ est inversible dans } A[\sqrt{\alpha}].$$

e) Si A est un corps, l'isomorphisme d'anneaux f fait de A' un corps et tout élément non nul de A' est alors inversible.

De ce qui précède, on déduit que tout élément non nul de $A[\sqrt{\alpha}]$ est inversible, donc si A est un corps alors $A[\sqrt{\alpha}]$ est aussi un corps.

La qualité de la rédaction, la clarté et la précision des raisonnements entreront pour une part importante dans l'appréciation des copies.

Exercice I

1-Déterminer pour quelles valeurs du couple $(\alpha, \beta) \in \mathbb{R}^2$ les intégrales suivantes sont convergentes. *les 2 les deux sup (4)*

a) $\int_0^\infty \frac{dx}{x^\alpha(1+x^\beta)}$ (2 pts) b) $\int_0^\infty \frac{(1+t)^\alpha - t^\alpha}{t^\beta} dt$ (2 pts)

2-On dessinera dans le plan l'ensemble des couples (α, β) lesquels il y a convergence.

Exercice II

On adoptera la définition suivante :

Une suite de fonctions f_n converge uniformément sur A vers une fonction f si, pour tout $\epsilon > 0$, il existe $n_0 \in \mathbb{N}^*$ tel que $\forall n \in \mathbb{N}$ $n > n_0$ implique $|f_n(x) - f(x)| < \epsilon$ pour tout $x \in A$.

1-Prouver qu'une suite de fonctions $\{f_n\}$ définies sur $B \subset A$ vers $f : B \rightarrow \mathbb{R}$ est uniformément convergente sur $B \subset A$ vers $f : B \rightarrow \mathbb{R}$ et seulement si la suite réelle d_n , *est cette Necess (2 pt) est suff (2 pt)*

$$d_n = \sup\{|f_n - f(x)|, x \in B\}, n \in \mathbb{N}^*$$

converge vers 0.

2- Soient f_n et g_n deux suites convergeant uniformément vers f et g respectivement. Montrer que $f_n + g_n$ converge uniformément vers $f + g$. *(2 pts)*

3- Considerons les suites $f_n(x) = x(1 - \frac{1}{n})$ et $g_n(x) = \frac{1}{x}$. Etudier la convergence uniforme de $f_n g_n$. Que peut-on conclure? *(1 pt)*

Exercice III

Soit l'application de \mathbb{R}^2 dans \mathbb{R} définie par

$$f(0,0) = 0 \text{ et } f(x,y) = xy \sin\left(\frac{1}{x^2+y^2}\right) \text{ si } (x,y) \neq (0,0)$$

1- Montrer que f est différentiable en tout point de \mathbb{R}^2 . Calculer $df(0;0)$. *(5 pts)*

2- Les dérivées partielles de f sont elles continues au point $(0,0)$? *(2 pts)*

EXERCICE I

1 Déterminer pour quelles valeurs du couple $(\alpha, \beta) \in \mathbb{R}^2$ les intégrales suivantes sont convergentes

a) $I(\alpha, \beta) = \int_0^{+\infty} \frac{dx}{x^\alpha (1+x^\beta)}$

$\forall (\alpha, \beta) \in \mathbb{R}^2$, $I(\alpha, \beta)$ est intégrable sur tout compact $[a, b] \subset]0, +\infty[$.

• Au voisinage de 0

Soit $f(x) = \frac{1}{x^\alpha (1+x^\beta)} \sim \frac{1}{x^\alpha} \quad \forall \beta > 0$

donc $I(\alpha, \beta)$ est $\begin{cases} \text{cv} & \text{si } \alpha < 1 \\ \text{div} & \text{si } \alpha \geq 1 \end{cases}$

si $\beta = 0 \Rightarrow f(x) = \frac{1}{2x^\alpha}$ d'où $I(\alpha, \beta)$ est $\begin{cases} \text{cv} & \text{si } \alpha < 1 \\ \text{div} & \text{si } \alpha \geq 1 \end{cases}$

si $\beta < 0 \Rightarrow f(x) = \frac{1}{x^\alpha (1 + \frac{1}{x^{-\beta}})} = \frac{1}{x^{\alpha+\beta} (x+1)} \sim \frac{1}{x^{\alpha+\beta}}$

donc $I(\alpha, \beta)$ est $\begin{cases} \text{cv} & \text{si } \alpha + \beta < 1 \\ \text{div} & \text{si } \alpha + \beta \geq 1 \end{cases}$

• Au voisinage de $+\infty$

si $\beta > 0 \quad f(x) = \frac{1}{x^{\alpha+\beta} (1+x^{-\beta})} \sim \frac{1}{x^{\alpha+\beta}}$

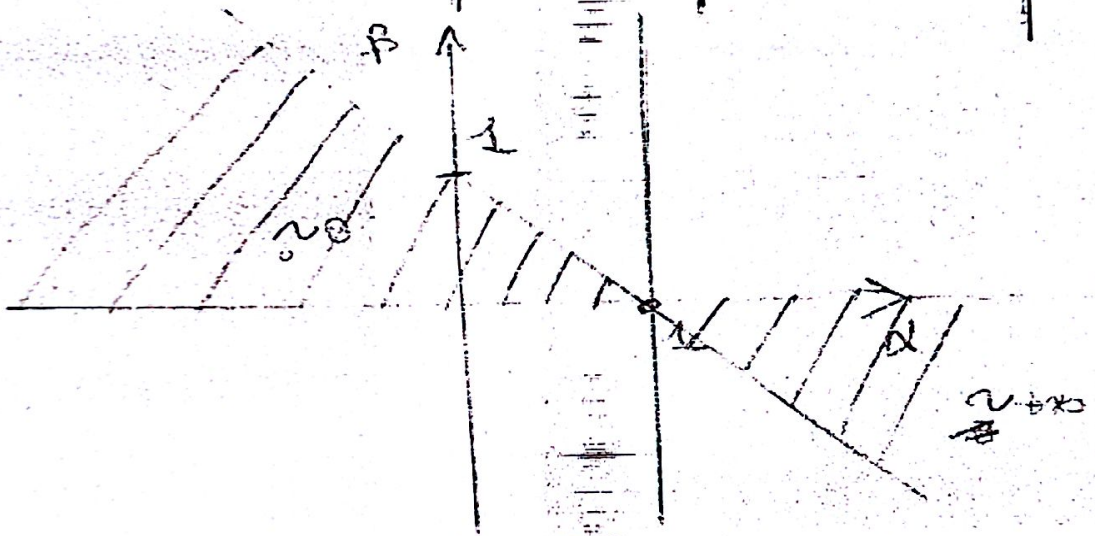
donc $I(\alpha, \beta)$ est $\begin{cases} \text{cv} & \text{si } \alpha + \beta > 1 \\ \text{div} & \text{si } \alpha + \beta \leq 1 \end{cases}$

si $\beta = 0 \quad f(x) = \frac{1}{2x^\alpha}$ d'où $I(\alpha, \beta)$ est $\begin{cases} \text{cv} & \text{si } \alpha > 1 \\ \text{div} & \text{si } \alpha \leq 1 \end{cases}$

$\beta < 0$ $f(x) \sim \frac{1}{x^\alpha}$ d'où $I(\alpha, \beta)$ est $\begin{cases} \text{CV} & \text{si } \alpha > 1 \\ \text{Div} & \text{si } \alpha \leq 1 \end{cases}$

Tableau Bilan

	$\underset{0}{\overset{a}{\sim}} f(x)$	$\underset{0}{\overset{+\infty}{\sim}} f(x)$	cdt ^o CV $\underset{0}{\sim}$	cdt ^o div $\underset{0}{\sim} \overset{+\infty}{\sim}$
$\beta > 0$	$\frac{1}{x^\alpha}$	$\frac{1}{x^{\alpha+\beta}}$	$\alpha < 1$	$\alpha + \beta > 1$
$\beta = 0$	$\frac{1}{2x^\alpha}$	$\frac{1}{2x^\alpha}$	$\alpha \leq 1$	$\beta > 1$
$\beta < 0$	$\frac{1}{x^{\alpha+\beta}}$	$\frac{1}{x^\alpha}$	$\alpha + \beta \leq 1$	$\alpha > 1$



b) 3 points à celui qui l'a 'bordé'.

1- On suppose que f_n converge uniformément vers f sur B , par définition on a: $\forall \varepsilon > 0 \exists n_0 \in \mathbb{N}^*$ tel que $\forall n > n_0 \Rightarrow |f_n(x) - f(x)| < \varepsilon$ et $\forall x \in B$

$$d_n = \sup \{ |f_n(x) - f(x)|, x \in B \} \quad n \in \mathbb{N}^*$$

$$d_n \leq \varepsilon \quad \text{d'où} \quad \lim_{n \rightarrow \infty} d_n = 0$$

Inversement supposons $\lim_{n \rightarrow \infty} d_n = 0$. On a alors

$$|f_n(x) - f(x)| \leq \sup \{ |f_n(x) - f(x)| : x \in B \} < \varepsilon$$

pour n suffisamment grand et pour $x \in B$, ce qui signifie que $\{f_n\}$ est uniformément convergente vers f sur B .

2- Etant donné $\varepsilon > 0$

$$|f_n(x) - f(x)| < \frac{\varepsilon}{2} \quad \text{et} \quad |g_n(x) - g(x)| < \frac{\varepsilon}{2}$$

pour n suffisamment grand et $\forall x \in A$ on a

$$|f_n(x) + g_n(x) - (f(x) + g(x))| \leq |f_n(x) - f(x)| + |g_n(x) - g(x)| < \varepsilon$$

pour n suffisamment grand et $\forall x \in A$

3- Soient $f_n(x) = x \left(1 - \frac{1}{n}\right)$ et $g_n(x) = \frac{1}{x^2}$

$f_n(x)$ et $g_n(x)$ sont deux suites uniformément convergentes vers $f(x) = x$ et $g(x) = \frac{1}{x^2}$ respectivement

$$\text{se plus} \quad f_n(x) g_n(x) = \frac{1}{x} \left(1 - \frac{1}{n}\right)$$

$$d_n = \sup \left\{ \left| \frac{1}{n} g(x) - \frac{1}{x} \right| \mid x \in]0, 1[\right\} = +\infty \quad (n \in \mathbb{N})$$

et donc la convergence n'est pas uniforme

Exercice III

Soit l'application de $\mathbb{R}^2 \rightarrow \mathbb{R}$ définie par

$$\begin{cases} f(x, y) = xy \sin\left(\frac{1}{x^2+y^2}\right) & (x, y) \neq (0, 0) \\ f(0, 0) = 0 \end{cases}$$

- 1 - Montrons que f est différentiable en tout point de :
- sur $\mathbb{R}^2 \setminus \{(0, 0)\}$ f est de classe C^1 , donc différentiable
 - Différentiabilité en $(0, 0)$

$$\frac{\partial f}{\partial x}(0, 0) = \lim_{x \rightarrow 0} \frac{f(x, 0) - f(0, 0)}{x} = \lim_{x \rightarrow 0} \frac{0}{x} = 0$$

$$\frac{\partial f}{\partial y}(0, 0) = \lim_{y \rightarrow 0} \frac{f(0, y) - f(0, 0)}{y} = \lim_{y \rightarrow 0} \frac{0}{y} = 0$$

Posons $\varepsilon(h, k) = \frac{f(ah, ak) - f(0, 0) - \left[\frac{\partial f}{\partial x}(0, 0)h + \frac{\partial f}{\partial y}(0, 0)k \right]}{\sqrt{h^2 + k^2}}$

$$0 \leq |\varepsilon(h, k)| = \frac{|h||k|}{\sqrt{h^2 + k^2}} \sin\left(\frac{1}{h^2 + k^2}\right)$$

$$\leq \sqrt{h^2 + k^2} \sin 1$$

$$\lim_{(h, k) \rightarrow (0, 0)} \sqrt{h^2 + k^2} \sin 1 = 0 \Rightarrow \lim_{(h, k) \rightarrow (0, 0)} \varepsilon(h, k) = 0$$

donc f est différentiable en $(0, 0)$ et la différentiel est

$$df_{(0,0)} : \mathbb{R}^2 \rightarrow \mathbb{R} \quad (h, k) \mapsto \frac{\partial f}{\partial x}(0, 0)h + \frac{\partial f}{\partial y}(0, 0)k$$

les dérivées partielles sont-elles continues?

$$\frac{\partial f}{\partial x}(x, y) = y \sin\left(\frac{1}{x^2+y^2}\right) - \frac{2x^2 y}{(x^2+y^2)^2} \cos\left(\frac{1}{x^2+y^2}\right)$$

$$\frac{\partial f}{\partial y}(x, y) = x \sin\left(\frac{1}{x^2+y^2}\right) - \frac{2y^2 x}{(x^2+y^2)^2} \cos\left(\frac{1}{x^2+y^2}\right)$$

Soit $\frac{1}{\sqrt{2\pi n}}$ une suite numérique telle que

$$\left(\frac{1}{\sqrt{2\pi n}}, \frac{1}{\sqrt{2\pi n}}\right) \rightarrow (0, 0) \text{ lorsque } n \rightarrow +\infty.$$

$$\frac{\partial f}{\partial x}\left(\frac{1}{\sqrt{2\pi n}}, \frac{1}{\sqrt{2\pi n}}\right) = \frac{\sqrt{2\pi n}}{2} (-1)^{n+1}$$

$\frac{\partial f}{\partial x}(0, 0)$ mais $\frac{\sqrt{2\pi n}}{2} (-1)^{n+1}$ n'admet pas de limite
 $n \rightarrow +\infty$ donc $\frac{\partial f}{\partial x}$ n'est pas continue en $(0, 0)$.

Idem pour $\frac{\partial f}{\partial y}$.

Exercice I Etudier la nature de la série numérique de terme général u_n dans chacun des cas suivants :

1) $u_n = (-1)^n (\sqrt{n^2 + 1} - n), \forall n \in \mathbb{N}$ (Criteres S.A)

2) $u_n = \left(\frac{an}{n+1}\right)^n, \forall n \in \mathbb{N}$ où a est un réel positif (Cauchy, desuons $a < a$)

3) $u_n = \frac{a^n}{(1+a)(1+a)^2 \dots (1+a)^n},$ où a est un réel positif (D'Alembert / avec limite)

Exercice II Soient a et b deux nombres réels tels que $0 < a < b$. On définit les suites (w_n) et (z_n) par

$w_0 = a, z_0 = b$ et $w_{n+1} = \sqrt{w_n z_n}, z_{n+1} = \frac{w_n + z_n}{2}, \forall n \geq 0$

1- Démontrer $\forall n \geq 0$ on a $w_0 \leq w_n \leq w_{n+1} \leq z_{n+1} \leq z_n \leq z_0$.

2- Démontrer que $z_n - w_n \leq \frac{z_0 - w_0}{2^n}, \forall n \geq 0$.

3- En déduire que les suites w_n et z_n sont convergentes et la ont même limite.

Exercice III Soit E un ensemble non vide.

1- Montrer que l'application définie sur $E \times E$ par

$d(x, y) = \begin{cases} 1 & \text{si } x \neq y \\ 0 & \text{si } x = y \end{cases}$ est une distance sur E .

est une distance sur E .

2- a- Quels sont les ouverts sur E ?

b- Quels sont les fermés sur E ?

3- On pose $d' = \frac{d(x, y)}{1 + d(x, y)}, \forall (x, y) \in E \times E$.

Montrer que d' est une distance sur E .

4- On suppose que $E = \mathbb{R}$, montrer que (\mathbb{R}, d) et (\mathbb{R}, d') sont des espaces métriques bornés dont on précisera le diamètre.

Exercice IV

Soit f une application continue de \mathbb{R} dans lui-même périodique de période 1. On suppose qu'il existe un couple (A, a) de nombres réels strictement positifs tel qu'au voisinage de 0, $|f(\cdot)| \simeq A|t|^a$. Pour tout entier $n \geq 1$, on note f_n la fonction définie sur l'intervalle $[0, +\infty[$ par la formule

$f_n(t) = f(\sqrt{t + n^2})$.

1- Montrer que la suite de fonctions $(f_n)_{n \geq 1}$ converge simplement vers 0 sur l'intervalle $[0, +\infty[$.

2- Montrer que la convergence n'est pas uniforme sur l'intervalle $[0, +\infty[$.

3- Déterminer les intervalles de $[0, +\infty[$ sur lesquels la convergence est absolue.

exercices: CAP/PC

preuve: Analyse

EXERCICE I

- 1) Critère de la suite Alternée $\sum u_n$ CV.
- 2) Critère Cauchy $\sum u_n$ CV si $a < 1$.
- 3) Critère d'Abel $\sum u_n$ CV.

EXERCICE II

$$\begin{cases} w_0 = a, & z_0 = b \\ w_{n+1} = \sqrt{w_n z_n} \quad \text{et} \quad z_{n+1} = \frac{w_n + z_n}{2} \quad \forall n \geq 0 \end{cases}$$

2) Montrons que $\forall n \geq 0$ on a:

$$w_0 \leq w_n < w_{n+1} < z_{n+1} < z_n \leq z_0$$

démonstration par récurrence

pour $n=0$ $w_1 = \sqrt{w_0 z_0}$ et $z_1 = \frac{w_0 + z_0}{2} < z_0$

Démontrons que $\sqrt{ab} < \frac{a+b}{2}$ (ie $w_1 < z_1$).

En élevant au carré on a:

$$4ab < (a+b)^2$$

soit $0 < a^2 - 2ab + b^2 = (a-b)^2$ ce qui est vrai

par suite

$$w_0 \leq w_0 < w_1 < z_1 < z_0 \leq z_0$$

Supposons l'inégalité vraie jusqu'à l'ordre $n-1$

$$w_0 \leq w_{n-1} < w_n < z_n < z_{n-1} \leq z_0$$

Mais comme précédemment nous avons

FIN

$W_n < \sqrt{W_n Z_n}$, $Z_{n+1} = \frac{W_n + Z_n}{2} < Z_n$ ainsi que $\sqrt{W_n Z_n} < \frac{W_n + Z_n}{2}$
 Par suite nous avons.

$$W_0 \leq W_{n-1} < W_n < W_{n+1} < Z_{n+1} < Z_n < Z_{n-1} \leq Z_0$$

soit $W_0 \leq W_n < W_{n+1} < Z_{n+1} < Z_n \leq Z_0$
 l'inégalité est vraie pour l'ordre n d'où le résultat.

2) Démonstration par récurrence

A l'ordre $n=0$ on a :

$$Z_0 - W_0 \leq \frac{Z_0 - W_0}{2}$$

Supposons que nous ayons.

$$\frac{W_n + Z_n}{2} - \sqrt{W_n Z_n} \leq \frac{Z_n - W_n}{2}$$

après simplification nous obtenons

$$-\sqrt{W_n Z_n} \leq -W_n \text{ ce qui est vérifié}$$

$$\text{d'où } Z_{n+1} - W_{n+1} \leq \frac{Z_n - W_n}{2} \leq \frac{Z_0 - W_0}{2^{n+1}}$$

ce qui démontre que

$$Z_n - W_n \leq \frac{Z_0 - W_0}{2^n} \quad \forall n \geq 0$$

$$\lim_{n \rightarrow \infty} \frac{1}{2^n} = 0 \text{ or } 0 \leq Z_n - W_n \leq \frac{Z_0 - W_0}{2^n}$$

Par passage à la limite on a :

$$0 \leq \lim_{n \rightarrow \infty} (Z_n - W_n) \leq \lim_{n \rightarrow \infty} \left(\frac{Z_0 - W_0}{2^n} \right) = 0$$

(9)

Il existe point (u_n) est \uparrow et (v_n) est \downarrow et $u_n < v_n$
 $\forall n \geq 0$. Ce sont des suites adjacentes par
suite elles convergent et admettent la même limite.

~~EXERCICE 1~~

EXERCICE III

Soit E un ensemble non vide

1. Montrons que l'application

$$d(x, y) = \begin{cases} 1 & \text{si } x \neq y \\ 0 & \text{si } x = y \end{cases} \text{ est une distance}$$

(i) $d(x, y) = 0 \Leftrightarrow y = x$ (séparation)

(ii) $d(x, y) = d(y, x) =$ (symétrie)

(iii) ~~x, y, z~~ x, y et z trois points ~~distincts~~ quelconques qcy
 $d(x, z) = \frac{1}{10}$; $d(x, y) = \frac{1}{10}$; $d(y, z) = \frac{1}{10}$. il est clair que
 $d(x, z) \leq d(x, y) + d(y, z)$.

2. a - les ouverts sur E

Les ouverts de E sont de la forme $\{x\} \forall x \in E$

b - les fermés sur E
Les fermés de E sont de la forme $\{x, y\} \forall x, y \in E$

3. On pose $d' = \frac{d(x, y)}{1 + d(y, x)}$, $\forall (x, y) \in E \times E$.

Montrer que d' est une distance sur E .

(i) Soient x, y deux points de E .

$$d'(x, y) = 0 \Rightarrow \frac{d(x, y)}{1 + d(y, x)} = 0 \Rightarrow d(x, y) = 0$$

$$\Rightarrow x = y$$

si $x = y \Rightarrow d'(x, y) = 0$ par def.

$$\text{d'où } d'(x, y) = 0 \Leftrightarrow x = y$$

(1)

ii) $d'(x, y) = d'(y, x)$ car d est une distance

iii) soit $f(t) = \frac{t}{1+t}$

$\forall t \in \mathbb{R}_+$, $f'(t) = \frac{1}{(t+1)^2} > 0$, d'où f est st \nearrow

$$d'(x, z) = \frac{d(x, z)}{1+d(x, z)} = f(d(x, z)).$$

~~$$f(d(x, z)) = f\left(\frac{d(x, y) + d(y, z)}{1+d(x, y) + d(y, z)}\right)$$~~

or $d(x, z) \leq d(x, y) + d(y, z)$

$$\begin{aligned} f(d(x, z)) &\leq f(d(x, y) + d(y, z)) = \frac{d(x, y) + d(y, z)}{1 + d(x, y) + d(y, z)} \\ &= \frac{d(x, y)}{1 + d(x, y) + d(y, z)} + \frac{d(y, z)}{1 + d(x, y) + d(y, z)} \end{aligned}$$

$$f(d(x, z)) \leq \frac{d(x, y)}{1 + d(x, y)} + \frac{d(y, z)}{1 + d(y, z)}$$

$$f(d(x, z)) \leq f(d(x, y)) + f(d(y, z))$$

$$d'(x, z) \leq d'(x, y) + d'(y, z) \quad (\text{inégalité triangulaire})$$

d'où d' est une distance sur E .

7 - On suppose que $E = \mathbb{R}$, montrons que (\mathbb{R}, d) et (\mathbb{R}, d') sont des espaces métriques bornés

(E)

exercice IV

Tout d'abord $f(0) = 0$ et par périodicité, si n , $f(n) = 0$. Puisque $f(0) = f(n)$, il en résulte que la suite $(f_n(0))_{n \geq 1}$ converge vers 0.

Maintenant si $t \in \mathbb{R}_*^+$.

$$f_n(t) = f(\sqrt{t+n^2}) = f(\sqrt{t+n^2} - n).$$

$$\text{or } \sqrt{t+n^2} - n = \frac{1}{n + \sqrt{t+n^2}} \underset{n \rightarrow +\infty}{\sim} \frac{t}{2n}.$$

On conclut $|f_n(t)| \underset{n \rightarrow +\infty}{\sim} A \left(\frac{t}{2n}\right)^\alpha$

ce qui prouve que la suite $(f_n(t))_{n \geq 1}$ converge vers 0. La suite $(f_n)_{n \geq 1}$ converge donc simplement vers 0 sur $[0, +\infty[$.

2) La fonction $|f| \underset{0}{\sim} A|t|^\alpha$, la fonction f n'est pas nulle: $\exists s \in [0, 1] \mid f(s) \neq 0$.

considérons la suite $(t_n)_{n \geq 1}$ où, $\forall n \geq 1$, $t_n = 2ns$

$$f_n(t_n) = f(\sqrt{t_n+n^2} - n) = f\left(\frac{2ns}{\sqrt{2ns+n^2}+n}\right).$$

comme $\lim_{n \rightarrow +\infty} \frac{2ns}{\sqrt{2ns+n^2}+n} = s$, par continuité de f au point s ,

$$\lim_{n \rightarrow +\infty} f_n(t_n) = f(s) \neq 0. \text{ ce qui}$$

prouve que la continuité n'est pas uniforme.

(6)

3^o Puisque $|f| \sim \pi |t|^\alpha$, alors $t \mapsto \frac{|f(t)|}{|t|^\alpha}$ est bornée sur le segment $[0, a]$, $|f(t)| \leq \pi |t|^\alpha$,
soit $a \in \mathbb{N}^+$, $\forall t \in [0, a]$ et $\forall n \geq 1$

$$0 \leq \sqrt{t+n^2} - n = \frac{t}{\sqrt{t+n^2} + n} \leq \frac{a}{2n}$$

On en conclut que, $\forall n \geq \frac{a}{2}$ et $\forall t \in [0, a]$
 $\sqrt{t+n^2} - n \in [0, 1]$ et donc

$$|f_n(t)| = |f(\sqrt{t+n^2} - n)| \leq \pi \left(\frac{t}{\sqrt{t+n^2} + n} \right)^\alpha \leq \pi \left(\frac{a}{2n} \right)^\alpha$$

donc la convergence est absolue sur le segment $[0, a]$.

I. ALGÈBRE (2h)

3pb I Soient E, F, G et H quatre ensembles non vides,

1+2 $f: E \rightarrow F; g: F \rightarrow G$ et $h: G \rightarrow H$.

Montrer que $(g \circ f$ et $h \circ g$ sont bijectives) si et seulement si $(f, g$ et h sont bijectives)

5,5pb II Donner la valeur de vérité (avec justification) des propositions suivantes :

- 1 1- Tout sous groupe H d'un groupe monogène $(G, .)$ est distingué dans $(G, .)$.
- 1 2- Si tout sous groupe H d'un groupe $(G, .)$ est distingué dans $(G, .)$ alors $(G, .)$ est monogène.
- 1 3- Tout groupe fini est cyclique.
- 1 4- Pour tout groupe fini $(G, .)$ d'ordre n , d'élément neutre e et pour tout $x \in G$, on a $x^n = e$.
- 1 5- Un anneau A non nul avec élément unité noté 1_A est de caractéristique zéro si et seulement si pour tout $n \in \mathbb{N}^*$, on a $n \cdot 1_A \neq 0_A$.

7pb III a) Soient $A(X) = X^4 - 9X^3 + 30X^2 - 44X + 24$,

$B(X) = X^3 - 5X^2 + 8X - 4$ et $C(X) = X^2 + X + 1$ dans $\mathbb{R}[X]$.

- 1 1- Montrer que $A(X)$ a un zéro multiple d'ordre 3 que l'on déterminera. Factoriser $A(X)$ dans $\mathbb{R}[X]$.
 - 1 2- Déterminer l'idéal de $\mathbb{R}[X]$ engendré par $A(X)$ et $B(X)$.
 - 1,5 3- Décomposer en éléments simples dans $\mathbb{R}(X)$ la fraction rationnelle $F(X) = \frac{B(X)}{A(X)C(X)}$
- b) Factoriser le polynôme $P(X) = 8X^3 - 36X^2 + 46X - 15 \in \mathbb{R}[X]$ sachant que ses zéros sont en progression arithmétique.

9pb IV Soient E un \mathbb{R} -espace vectoriel de dimension 3, $B = (e_1, e_2, e_3)$ une base de E sur \mathbb{R} , B^* la base duale de la base B, $u_1 = e_1 + 2e_2 - e_3$, $u_2 = 2e_1 + 3e_2$ et $u_3 = e_1 + 3e_2 - e_3$.

- 0,5 1- a) Montrer que $C = (u_1, u_2, u_3)$ est une base de E sur \mathbb{R} .
- 1 b) Déterminer les matrices de passage $P_{B \rightarrow C}$ de B à C et $P_{C \rightarrow B}$ de C à B.
- 1 2- Soit $C^* = (u_1^*, u_2^*, u_3^*)$ la base duale de la base C.
- 1 a) Déterminer les matrices de passage $P_{B^* \rightarrow C^*}$ de B^* à C^* et $P_{C^* \rightarrow B^*}$ de C^* à B^* .
- 0,5 b) En déduire C^* (en fonction des éléments de B^*)
- 3- Soient $v_1 = 5e_1 + 2e_2 + 4e_3$, $v_2 = 3e_1 + 2e_2$, $v_3 = e_1 + 2e_3$ et $F = \text{vect}(v_1, v_2, v_3)$ le sous-espace vectoriel de E engendré par v_1, v_2, v_3 .
- 1 Déterminer F° l'orthogonal de F (dans E^*) et un système d'équations cartésiennes de F dans la base B.

4- Soit $u \in E_{\mathbb{R}}(E)$ tel que $M(u, B) = \begin{pmatrix} 5 & 3 & 1 \\ 2 & 2 & 0 \\ 4 & 0 & 2 \end{pmatrix}$

- 1 i) Déterminer $M(u, C)$ la matrice de u dans la base C.
- 1 ii) Déterminer $\text{Im}(u)$ et $\text{Ker}(u)$ (dans la base B).
- 1 iii) Déterminer $M({}^t u, B^*)$ et $M({}^t u, C^*)$ où ${}^t u$ est la transposée de u.
- 1 iv) Déterminer $\text{Im}({}^t u)$ et $\text{Ker}({}^t u)$ (dans la base B^*).
- 0,5 5- a) Soit $v = 7e_1 + 14e_2 - e_3 \in E$. Déterminer les coordonnées de v dans la base C.
- 0,5 b) Soit $f = 7e_1^* + 14e_2^* - e_3^* \in E^*$. Déterminer les coordonnées de f dans la base C^* .

II. ANALYSE (2R)

Exercice 1.

Soit $f(x) = x^3 - 3x + 2$ et m un paramètre réel.

1. Etude et représentation graphique de f .
2. Déterminer le nombre de solution(s) réelle(s) de l'équation $x^3 - 3x + 2 - m = 0$.

Exercice 2.

Énoncer

- a) le théorème des valeurs intermédiaires;
- b) le théorème de Rolle;
- c) le théorème des accroissements finis.

Exercice 3. Déterminer une primitive de $f(x) = \frac{1}{1+x^4}$

Exercice 4. Calculer au moyen d'une intégrale l'aire d'un disque de rayon R .

Exercice 5 (suite de Fibonacci).

Déterminer la suite (u_n) définie par $u_0 = u_1 = 1$ et $u_{n+2} = u_{n+1} + u_n$
(on calculera u_n en fonction de n et on donnera $\lim u_n$).

Cours (partie)

I - Si f, g et h sont bijectives alors $g \circ f$ et $h \circ g$ sont bijectives car la composée de deux bijections est une bijection.

Inversement, supposons que $g \circ f$ et $h \circ g$ sont bijectives. Alors f est injective, g est surjective et injective, et h est surjective. Ainsi g est bijective.

Soit g^{-1} la bijection réciproque de g . $g^{-1} \circ (g \circ f) = f$ et la composée de deux bijections, f est donc bijective. De même $h \circ (g \circ g^{-1}) = h$ est bijective.

Ainsi f, g et h sont bijectives.

II - 1 - Vrai car tout groupe monogène est abélien et dans un groupe abélien, tout sous-groupe est distingué.

2 - Faux car $(\mathbb{C}, +)$ n'est pas monogène et tout sous-groupe de $(\mathbb{C}, +)$ est distingué dans $(\mathbb{C}, +)$.

3 - Faux car $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$ le groupe de Klein, n'est pas cyclique.

4 - Vrai car l'ordre de tout élément de (G, \cdot) divise $n = \text{l'ordre de } (G, \cdot)$.

5 - Vrai car A est de caractéristique zéro si et seulement si 1_A est d'ordre infini dans $(A, +)$ et 1_A d'ordre infini dans $(A, +)$ équivaut à : pour tout $n \in \mathbb{N}^*$, $n \cdot 1_A \neq 0_A$.

III a) 1 - $x_0 \in \mathbb{R}$ est zéro d'ordre 3 de $A(x)$ signifie que $A(x_0) = A'(x_0) = A''(x_0) = 0$ et $A'''(x_0) \neq 0$. Nous avons: $A(x) = x^4 - 9x^3 + 30x^2 - 44x + 24$

1) $A'(x) = 4x^3 - 27x^2 + 60x - 44$; $A''(x) = 12x^2 - 54x + 60$; $A'''(x) = 24x - 54$

Les zéros de $A''(x)$. $A''(x) = 6(2x^2 - 9x + 10)$. $A''(2) = 0$; $A'(2) = 32 - 108 + 120 - 44 = 0$, $A(2) = 16 - 72 + 120 - 88 + 24 = 0$. Il en résulte que $A(x) = (x-2)^3(x-3)$

2 - Nous avons $(A(x), B(x)) = (A(x) \wedge B(x))$

Nous avons $B(2) = 8 - 20 + 16 - 4 = 0$; $B'(x) = 3x^2 - 10x + 8$, $B'(2) = 12 - 20 + 8 = 0$

1) $B''(x) = 6x - 10 = 2(3x - 5)$. Ainsi $B(x) = (x-2)^2(x-1)$

$A(x) \wedge B(x) = (x-2)^2$. Alors $(A(x), B(x)) = (x-2)^2$

3 -
$$F(x) = \frac{(x-2)^2(x-1)}{(x-2)^3(x-3)(x^2+x+1)} = \frac{x-1}{(x-2)(x-3)(x^2+x+1)}$$

1)
$$F(x) = \frac{a}{x-2} + \frac{b}{x-3} + \frac{cx+d}{x^2+x+1}; \quad a = -\frac{1}{7}; \quad b = \frac{2}{13}$$

$\lim_{x \rightarrow +\infty} xF(x) = a + b + c = 0$; $c = -a - b = \frac{1}{7} - \frac{2}{13} = \frac{13 - 14}{91} = -\frac{1}{91}$

$F(0) = -\frac{1}{6} = -\frac{a}{2} - \frac{b}{3} + d$; $d = -\frac{1}{6} + \frac{a}{2} + \frac{b}{3} = -\frac{1}{6} - \frac{1}{14} + \frac{2}{39} = -\frac{17}{91}$

$\frac{1}{2}$

b) $P(x) = 8x^3 - 36x^2 + 46x - 15$

Soient x_1, x_2, x_3 les zéros de $P(x)$. Nous avons: $x_1 + x_2 + x_3 = 3x_2 = \frac{36}{8} = \frac{9}{2}$, soit

$x_2 = \frac{3}{2}$. $P(x) = 8(x - \frac{3}{2})(x^2 - 3x + \frac{5}{4}) = (2x - 3)(4x^2 - 12x + 5)$

$P(x) = (2x - 3)(2x - 1)(2x - 5)$

(1,5)

1- a) $\left(\begin{array}{ccc|c} 1 & 2 & -1 & u_1 \\ 2 & 3 & 0 & u_2 \\ 1 & 3 & -1 & u_3 \end{array} \right) \rightarrow \left(\begin{array}{ccc|c} 1 & 2 & -1 & u_1 \\ 0 & -1 & 2 & u_2 - 2u_1 \\ 0 & 1 & 0 & u_3 - u_1 \end{array} \right) \rightarrow \left(\begin{array}{ccc|c} 1 & 2 & -1 & u_1 \\ 0 & 1 & 0 & u_3 - u_1 \\ 0 & -1 & 2 & u_2 - 2u_1 \end{array} \right) \rightarrow$

$\left(\begin{array}{ccc|c} 1 & 2 & -1 & u_1 \\ 0 & 1 & 0 & u_3 - u_1 \\ 0 & 0 & 2 & u_3 + u_2 - 3u_1 \end{array} \right)$. Ainsi $e_2 = u_3 - u_1 = -u_1 + u_3$
 $e_3 = \frac{-3}{2}u_1 + \frac{1}{2}u_2 + \frac{1}{2}u_3$

$e_1 = u_1 - 2e_2 + e_3 = u_1 + 2u_1 - 2u_3 - \frac{3}{2}u_1 + \frac{1}{2}u_2 + \frac{1}{2}u_3 = \frac{3}{2}u_1 + \frac{1}{2}u_2 - \frac{3}{2}u_3$

(0,5) Il en résulte que $C = (u_1, u_2, u_3)$ est une base de E sur \mathbb{R} .

b) $P_{B \rightarrow C} = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 3 & 3 \\ -1 & 0 & -1 \end{pmatrix}$; $P_{C \rightarrow B} = \begin{pmatrix} \frac{3}{2} & -1 & -\frac{3}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} \\ -\frac{3}{2} & 1 & \frac{1}{2} \end{pmatrix}$

2- a) $P_{B^* \rightarrow C^*} = {}^t P_{C \rightarrow B} = \begin{pmatrix} \frac{3}{2} & 1 & -\frac{3}{2} \\ -1 & 0 & 1 \\ -\frac{3}{2} & \frac{1}{2} & \frac{1}{2} \end{pmatrix}$ 0,5

$P_{C^* \rightarrow B^*} = {}^t P_{B \rightarrow C} = \begin{pmatrix} 1 & 2 & -1 \\ 2 & 3 & 0 \\ 1 & 3 & -1 \end{pmatrix}$ 0,5

b) $C^* \begin{cases} u_1^* = \frac{3}{2}e_1^* - e_2^* - \frac{3}{2}e_3^* \\ u_2^* = \frac{1}{2}e_1^* + \frac{1}{2}e_3^* \\ u_3^* = -\frac{3}{2}e_1^* + e_2^* + \frac{1}{2}e_3^* \end{cases}$ 0,5

3- $\left(\begin{array}{ccc|c} 5 & 2 & 4 & v_1 \\ 3 & 2 & 0 & v_2 \\ 1 & 0 & 2 & v_3 \end{array} \right) \rightarrow \left(\begin{array}{ccc|c} 1 & 0 & 2 & v_3 \\ 5 & 2 & 4 & v_1 \\ 3 & 2 & 0 & v_2 \end{array} \right) \rightarrow \left(\begin{array}{ccc|c} 1 & 0 & 2 & v_3 \\ 0 & 2 & -6 & v_1 - 5v_3 \\ 0 & 2 & -6 & v_2 - 3v_3 \end{array} \right)$

2/3

$$5v_1 - v_2 + 3v_3 \text{ Ker } v_1 - v_2 - 2v_3 = 0, v_1 = v_2 + 2v_3$$

$$\text{vect}(v_1, v_2, v_3) = \text{vect}(v_2, v_3)$$

$$0 = \left\{ f = ae_1^* + be_2^* + ce_3^* \in E^* \mid f(v_2) = f(v_3) = 0 \right\}$$

$$= \left\{ f = ae_1^* + be_2^* + ce_3^* \in E^* \mid 3a + 2b = 0, a + 2c = 0 \right\}$$

$$= \left\{ f = ae_1^* + be_2^* + ce_3^* \in E^* \mid b = -\frac{3}{2}a, c = -\frac{a}{2}, a \in \mathbb{R} \right\}$$

$$F^0 = \text{vect}(2e_1^* - 3e_2^* - e_3^*)$$

$$F = \left\{ x = ae_1 + be_2 + ce_3 \in E \mid 2a - 3b - c = 0 \right\}$$

$$4- c) M(u, c) = P^{-1} M(u, B) P \text{ où } P = P_{B \rightarrow C}$$

$$M(u, c) = \begin{pmatrix} \frac{3}{2} & -1 & -\frac{3}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} \\ -\frac{3}{2} & 1 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 5 & 3 & 1 \\ 2 & 2 & 0 \\ 4 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 1 \\ 2 & 3 & 3 \\ -1 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 6 & \frac{13}{2} & \frac{17}{2} \\ 6 & \frac{27}{2} & \frac{15}{2} \\ -8 & -\frac{29}{2} & -\frac{21}{2} \end{pmatrix}$$

$$ii) \text{Im } u = F = \text{vect}(v_2, v_3)$$

$$\text{Comme } v_1 - v_2 - 2v_3 = 0, \text{ Ker } u = \text{vect}(e_1 - e_2 - 2e_3)$$

$$iii) M({}^t u, B^*) = {}^t M(u, B) = \begin{pmatrix} 5 & 2 & 4 \\ 3 & 2 & 0 \\ 1 & 0 & 2 \end{pmatrix}$$

$$M({}^t u, C^*) = {}^t M(u, c) = \begin{pmatrix} 6 & 6 & -8 \\ \frac{13}{2} & \frac{27}{2} & -\frac{29}{2} \\ \frac{17}{2} & \frac{15}{2} & -\frac{21}{2} \end{pmatrix}$$

$$iv) \text{Im } {}^t u = (\text{Ker } u)^0 = \text{vect}(e_1^* + e_2^*, -2e_1^* + e_3^*)$$

$$\text{Ker } {}^t u = (\text{Im } u)^0 = F^0 = \text{vect}(2e_1^* - 3e_2^* - e_3^*)$$

$$5- a) v = u_1^*(w)u_1 + u_2^*(w)u_2 + u_3^*(w)u_3 = -2u_1 + 3u_2 + 3u_3$$

$$b) f = f(u_1)u_1^* + f(u_2)u_2^* + f(u_3)u_3^* = 36u_1^* + 56u_2^* + 50u_3^*$$

EXERCICE 1

1) Soit

$$g(x) = \ln\left(1 + \frac{1}{x}\right) - \left(\frac{x-1}{2x^2}\right)$$

Etudier les variations et le signe de $g(x)$ suivant les valeurs de x dans \mathbb{R} .

2) Etudier et représenter graphiquement $f: \mathbb{R} \rightarrow \mathbb{R}$ telle que

$$f(x) = (x^2 - 1)\ln\left(1 + \frac{1}{x}\right)$$

On prouvera que

$$f'(x) = 2x g(x)$$

pour tout $x \in]-\infty, -1[\cup]0, +\infty[$.

EXERCICE 2

Soit $(f_n)_{n \in \mathbb{N}^*}$ la suite de fonctions définies sur $I =]-\pi, +\pi[$ par

$$f_n(x) = \frac{\sin^2(nx)}{n \sin x} \text{ si } x \neq 0 \text{ et } f_n(0) = 0$$

a) Etudier la convergence simple de $(f_n)_{n \in \mathbb{N}^*}$.

b) Etudier la convergence uniforme de $(f_n)_{n \in \mathbb{N}^*}$ dans chacun des cas suivants :

- i) Sur tout compacte de $]-\pi, +\pi[$ contenant zéro
- ii) Sur tout compacte de $]-\pi, +\pi[$ ne contenant pas zéro
- iii) $[\alpha, \pi[$ tel que $\alpha \in]-\pi, +\pi[$

EXERCICE 3

$$\text{Soit } I = \int_0^1 \frac{x \ln x}{(x^2+1)^2} dx$$

1) Justifier la convergence de I .

2) Calculer $I(a) = \int_a^1 \frac{x \ln x}{(x^2+1)^2} dx$ pour $a > 0$ en utilisant une intégration par partie puis en déduire I .

I. ALGÈBRE

Exercice 1

1- Décomposer en éléments simples dans $\mathbb{R}(X)$ la fonction rationnelle suivante :

$$f(x) = \frac{x - 1}{(x + 1)^2(x^3 + x^2 + x + 1)}$$

2- a) Décomposer en éléments simples la fraction rationnelle $\frac{1}{x(x+1)(x+2)}$

b) En déduire la limite de la suite $S_n = \sum_{k=1}^n \frac{1}{k(k+1)(k+2)}$

Exercice 2 : Logique

- 1- Soit $p \in \mathbb{N}$, un nombre premier. Montrer que p n'est pas un carré dans \mathbb{Q} .
- 2- Pour $m \in \mathbb{N}$, montrer que si $2^m - 1$ est un nombre premier alors m est un nombre premier.

Exercice 3

Soit A la matrice $\begin{pmatrix} -4 & -6 & 0 \\ 3 & 5 & 0 \\ 3 & 6 & 5 \end{pmatrix}$

- 1- Diagonaliser A
- 2- Calculer A^n en fonction de n.
- 3- On considère les suites $(u_n), (v_n)$ et (w_n) définies par leur premier terme u_0, v_0 et w_0 et les relations suivantes :

$$\begin{cases} u_{n+1} = -4u_n - 6v_n \\ v_{n+1} = 3u_n + 5v_n \\ w_{n+1} = 3u_n + 6v_n + 5w_n \end{cases}$$

Pour $n \geq 0$. On pose $X_n = \begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix}$. Exprimer X_{n+1} en fonction de A et X_n . En déduire

u_n, v_n et w_n en fonction de n.

CONCOURS D'ENTREE A LIENS (CAP/PC)

DISCIPLINE : MATHS

SESSION : 2015

EPREUVE

ADMISSIBILITE

EXERCICE 1

1) Soit $g(x) = \ln\left(1 + \frac{1}{x}\right) - \left(\frac{x-1}{2x^2}\right)$
des variations et le signe de $g(x)$ suivant
les valeurs de x dans \mathbb{R} .

$$\forall x \in Dg, Dg = \left\{ x \in \mathbb{R}, 1 + \frac{1}{x} > 0 \text{ et } x^2 \neq 0 \right\}$$

$$\Rightarrow \frac{x+1}{x} > 0 \text{ et } x \neq 0$$

	$-\infty$	-1	0	$+\infty$
$x+1$	-	0	+	+
x	-	0	+	+
$\frac{x+1}{x}$	+	0	-	+

$$\forall x \in Dg, Dg =]-\infty, -1[\cup]0, +\infty[$$

$$\text{on a } \lim_{x \rightarrow -\infty} g(x) = 0 \quad , \quad \lim_{x \rightarrow +\infty} g(x) = 0$$

$$\lim_{x \rightarrow -1^-} g(x) = -\infty \quad , \quad \lim_{x \rightarrow 0^+} g(x) = +\infty$$

g est une fonction continue et dérivable sur Dg
alors : $\forall x \in Dg, g'(x) = -\frac{x^2 + x + 2}{2x^3(x+1)}$

tableau de signe de $g'(x)$

x	$-\infty$	-1	0	$+\infty$
$g'(x)$	$-$	/	/	$-$

$\forall x \in]-\infty, -1[$, $g'(x) < 0 \Rightarrow g$ est strictement
décroissante sur $]-\infty, -1[$.

$\forall x \in]0, +\infty[$, $g'(x) < 0 \Rightarrow g$ est strictement
décroissante sur $]0, +\infty[$.

tableau de variation

x	$-\infty$	-1	0	$+\infty$
$g'(x)$	$-$	/	/	$-$
g	0	$-\infty$	$+\infty$	0

de signe de $g(x)$ suivant les valeurs de x dans \mathbb{R} .

• $\forall x \in]-\infty, -1[$, g est continue et strictement \searrow
et obtient que des valeurs négatives pour
tout $x \in]-\infty, -1[$ alors $\forall x \in]-\infty, -1[$, $g(x) < 0$

• $\forall x \in]0, +\infty[$, g est continue et strictement \searrow
et obtient que des valeurs positives pour
tout $x \in]0, +\infty[$ alors $\forall x \in]0, +\infty[$, $g(x) > 0$.

$$2) f: \mathbb{R} \rightarrow \mathbb{R}, f(x) = (x^2 - 1) \ln\left(1 + \frac{1}{x}\right)$$

$$\forall x \in Df, Df =]-\infty, -1[\cup]0, +\infty[$$

$$\text{on a } \lim_{x \rightarrow -\infty} f(x) = -\infty, \quad \lim_{x \rightarrow -1} f(x) = 0$$

$$\lim_{x \rightarrow 0} f(x) = -\infty \quad \text{et} \quad \lim_{x \rightarrow +\infty} f(x) = +\infty$$

$$\forall x \in Df, f'(x) = 2x g(x) \quad (\text{A prouver})$$

D'où le signe de $f'(x)$ dépend du signe de $x \mapsto 2x$ et $g(x)$.

tableau de signe

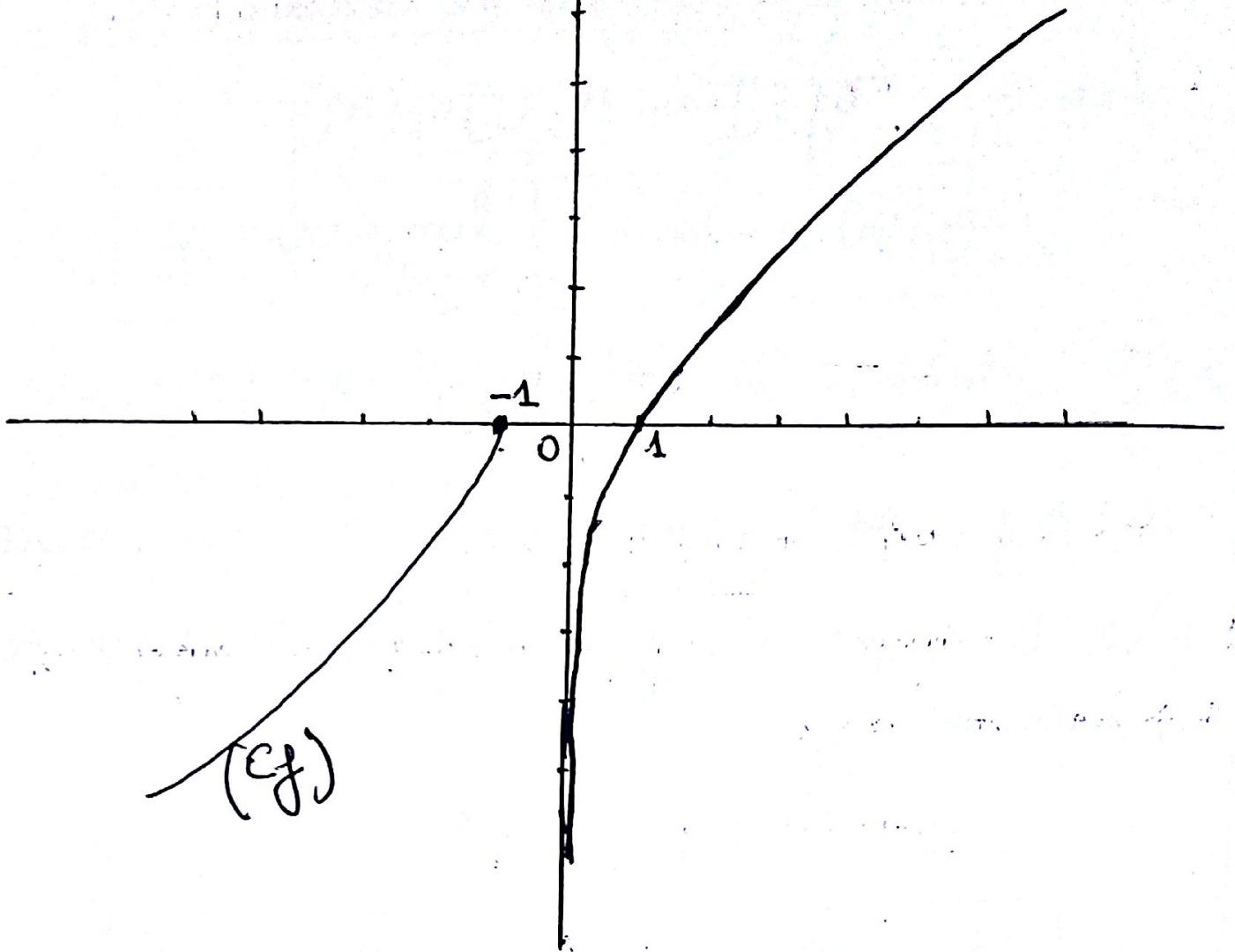
x	$-\infty$	-1	0	$+\infty$
$2x$		-	/	+
$g(x)$		-	/	+
$f'(x)$	+	/	/	+

$\forall x \in]-\infty, -1[, f'(x) > 0 \Rightarrow f$ est strictement croissante sur $]-\infty, -1[$

$\forall x \in]0, +\infty[, f'(x) > 0 \Rightarrow f$ est strictement croissante sur $]0, +\infty[$.

NB: Faites passer les asymptotes, les branches paraboliques et les tangentes.

$$f(1) = 0$$



EXERCICE 2 : Soit $(f_n)_{n \in \mathbb{N}^*}$ la suite de fonctions définies sur $I =]-\pi, +\pi[$ par

$$f_n(x) = \frac{\sin^2(nx)}{n \sin x} \quad \text{si } x \neq 0 \quad \text{et } f_n(0) = 0$$

a) de convergence simple de $(f_n)_{n \in \mathbb{N}^*}$

• Pour $x = 0$, on a $f_n(0) = 0$ et $\lim_{n \rightarrow +\infty} f_n(0) = 0$

• Pour $x \in]-\pi, \pi[\setminus \{0\}$, on a $\lim_{n \rightarrow +\infty} f_n(x) =$

$$= \lim_{n \rightarrow +\infty} \left| \frac{\sin^2(nx)}{n \sin x} \right| = \lim_{n \rightarrow +\infty} \frac{|\sin^2(nx)|}{n |\sin x|} \leq \lim_{n \rightarrow +\infty} \frac{1}{n |\sin x|}$$

$$\text{or } \lim_{n \rightarrow +\infty} \frac{1}{n |\sin x|} = 0 \quad \text{Alors } \lim_{n \rightarrow +\infty} f_n(x) = 0$$

Donc $(f_n)_{n \in \mathbb{N}^*}$ converge simplement sur $]-\pi, \pi[$

b) la convergence uniforme de $(f_n)_{n \in \mathbb{N}}$

i) Sur tout compacte de $] -\pi, +\pi[$ contenant zéro :

soit $[\alpha, \beta] \subset] -\pi, \pi[$ un compacte de $] -\pi, \pi[$ on a $0 \in [\alpha, \beta]$

• On suppose que $0 \neq \beta$

On sait que pour montrer la convergence unifiée sur I . On recherche une suite $x_n \in I$ tel que $|f_n(x_n) - f(x_n)| < \epsilon_n$ et $\lim_{n \rightarrow +\infty} \epsilon_n = 0$

On peut prendre $x_n = \frac{\pi}{2n}$. A partir d'un certain rang $x_n \in [\alpha, \beta]$

$$|f_n(x_n) - f(x_n)| = \left| \frac{\sin^2(n x_n)}{n \sin x_n} \right| = \left| \frac{\sin^2\left(\frac{\pi}{2}\right)}{n \sin \frac{\pi}{2n}} \right| = \frac{1}{n \left| \sin \frac{\pi}{2n} \right|}$$

$$\text{or } 0 < \sin \frac{\pi}{2n} \leq \frac{\pi}{2n} \Leftrightarrow 0 < n \sin \frac{\pi}{2n} \leq \frac{\pi}{2}$$

$$\Rightarrow \frac{2}{\pi} \leq \frac{1}{n \sin \frac{\pi}{2n}}$$

$$\text{D'où } |f_n(x_n) - f(x_n)| = \frac{1}{n \left| \sin \frac{\pi}{2n} \right|} \geq \frac{2}{\pi}$$

$$\frac{2}{\pi} \leq |f_n(x_n) - f(x_n)| \leq \sup_{x \in I} |f_n(x) - f(x)|$$

$$\text{d'où } \lim_{n \rightarrow +\infty} \sup_{x \in I} |f_n(x) - f(x)| \geq \frac{2}{\pi}$$

D'où pas de convergence uniforme sur $[\alpha, \beta]$

On suppose $0 \neq \beta$
 On prend $x_n = -\frac{\pi}{2n}$, à partir d'un certain
 rang $x_n \in [\alpha, \beta]$:

$$|f_n(x_n) - f(x_n)| \geq \frac{2}{\pi}$$

D'où pas de convergence uniforme sur $[\alpha, \beta]$.

Conclusion : Pas de convergence uniforme de
 $(f_n)_{n \in \mathbb{N}}$ sur tout compact de $] -\pi, +\pi[$ contenant 0

ii) Sur tout compact de $] -\pi, +\pi[$ ne contenant pas
 zéro.

$$\text{on a } |f_n(x) - f(x)| = \left| \frac{\sin^2(nx)}{n \sin x} \right| \leq \frac{1}{n |\sin x|}$$

La fonction $x \mapsto \frac{1}{|\sin x|}$ est continue sur $[\alpha, \beta]$, donc
 elle admet un maximum M . (ce, $\exists M \in \mathbb{R}^+$,
 $\forall x \in [\alpha, \beta], \frac{1}{|\sin x|} \leq M$).

$$\text{Ainsi } \forall x \in [\alpha, \beta], |f_n(x) - f(x)| \leq \frac{1}{n} \times \frac{1}{|\sin x|}$$

$$|f_n(x) - f(x)| \leq \frac{M}{n} \longrightarrow 0 \text{ si } n \longrightarrow +\infty$$

Ce qui prouve que $(f_n)_{n \in \mathbb{N}}$ converge uniforme
 sur $[\alpha, \beta]$ ne contenant pas zéro.

iii) $[\alpha, \pi[$ tel que $\alpha \in] -\pi, +\pi[$

$$\text{Posons } x_n = \pi - \frac{\pi}{2n} \xrightarrow{n \rightarrow +\infty} \pi$$

Comme $\alpha < \pi$ alors $\exists n_\alpha \in \mathbb{N} \mid \forall n \geq n_\alpha, \alpha < x_n$
 or $\pi - \frac{\pi}{2n} < \pi$; Alors $\exists n_\alpha$ tel $\forall n \geq n_\alpha,$
 $x_n = \pi - \frac{\pi}{2n} \in [\alpha, \pi[$

$$\begin{aligned} |f_n(x_n) - f(x_n)| &= \left| f_n\left(\pi - \frac{\pi}{2n}\right) \right| = \left| \frac{\sin^2\left(n\pi - \frac{\pi}{2}\right)}{n \sin\left(\pi - \frac{\pi}{2n}\right)} \right| \\ &= \frac{1}{n \sin \frac{\pi}{2n}} \geq \frac{2}{\pi} \end{aligned}$$

alors $\frac{2}{\pi} \leq |f_n(x_n) - f(x_n)| \leq \sup_{x \in I} |f_n(x) - f(x)|$

D'où $\lim_{n \rightarrow +\infty} \sup_{x \in I} |f_n(x) - f(x)| \geq \frac{2}{\pi}$

$\Rightarrow \lim_{n \rightarrow +\infty} \sup_{x \in I} |f_n(x) - f(x)| \neq 0$

Par conséquent pas de convergence uniforme sur $[\alpha, \pi[$ avec $\alpha \in]-\pi, \pi[$.

Exercice 3 : Soit $I = \int_0^1 \frac{x \ln x}{(x^2+1)^2} dx$

1) de convergence de I

Posons $f(x) = \frac{x \ln x}{(x^2+1)^2}$ continue et positive sur $]0, 1]$

on a $\frac{x \ln x}{(x^2+1)^2} \underset{0}{\sim} x \ln x$ or $\int_0^1 x \ln x dx = -\frac{1}{4}$

d'où convergente alors I est convergente

$$2) \text{ Calculons } I(a) = \int_a^1 \frac{x \ln x}{(x^2+1)^2} dx \text{ pour } a > 0$$

$$\text{Posons } u = \ln x \Rightarrow u' = 1/x$$

$$v' = \frac{x}{(x^2+1)^2} \Rightarrow v = -\frac{1}{2} x \frac{1}{(x^2+1)}$$

$$I(a) = \left[-\frac{\ln x}{2(x^2+1)} \right]_a^1 + \frac{1}{2} \int_a^1 \frac{1}{x(x^2+1)} dx$$

$$I(a) = \frac{\ln a}{2(a^2+1)} + \frac{1}{2} \int_a^1 \left(\frac{1}{x} - \frac{x}{x^2+1} \right) dx$$

$$I(a) = \frac{\ln a}{2(a^2+1)} + \frac{1}{2} \left[\ln x \right]_a^1 - \frac{1}{2} \left[\frac{1}{2} \ln(x^2+1) \right]_a^1$$

$$I(a) = \frac{\ln a}{2(a^2+1)} + \frac{1}{2} (-\ln a) - \frac{1}{4} \ln(2) + \frac{1}{4} \ln(a^2+1)$$

$$I(a) = \frac{\ln a}{2(a^2+1)} - \frac{1}{2} \ln a + \frac{1}{4} \ln \left(\frac{a^2+1}{2} \right)$$

La dérivée de I

$$I = \lim_{a \rightarrow 0} I(a) = \frac{1}{4} \ln \left(\frac{1}{2} \right)$$

$$\text{done } \underline{I = \frac{1}{4} \ln \left(\frac{1}{2} \right)}$$