CHAPITRE I
ELEMENTS DE LOGIQUE ET NOTION DES ENSEMBLES

A. ELEMENT DE LOGIQUE

Le but poursuivi par le cours de logique est d'étudier systématiquement la structure des propositions et les conditions générales de validité des raisonnements que l'on rencontre dans un discours scientifique. Mais, pour notre paragraphe, nous ne ferons ni un exposé d'ordre philosophique sur les lois de la pensée, ni une étude de la logique, mais tout simplement une description élémentaire des règles et symboles couramment utilisés dans les raisonnements mathématiques.
Ainsi, pour établir une théorie mathématique même élémentaire et en langage usuel, il faut disposer au départ des divers éléments ci-après :

1. Termes Primitifs

Les termes primitifs sont posés à priori, donc on ne peut pas les définir.
Par exemple : ensemble, élément, point, plan, …, etc.

2. Assemblage

Un assemblage est une suite finie des mots et des signes de ponctuation.

Exemple :
a) Trois est un nombre naturel pair ;
b) Tu mal, venir pas.

3. Enoncé

Un énoncé est un assemblage qui est correctement construit.
a) Trois est un nombre naturel pair ;
b) La terre est plate ;
c) La Reine d'Angleterre est une belle femme ;
d) Kinshasa est la capitale de la République Démocratique du Congo.

4. Axiome

Un axiome est un énoncé qu'on admet sans démonstration. D'une manière générale, les axiomes sont des règles décrivant les modalités d'emploi des termes primitifs pour former des énoncés ou des notions dérivées.

B. CALCUL DES PROPOSITIONS

1. Définition

Une proposition logique ou une proposition est un énoncé (P) qui est soit vrai, soit faux et qui ne peut pas être à la fois vrai et faux.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

2. Exemples

a) Kinshasa est la capitale politique de la République Démocratique du Congo.
b) 1 est le plus grand nombre naturel.
c) Kanku est la plus belle femme du monde.
d) t est une valeur de 8 dans IN.

a) et b) sont des propositions tandis que c) et d) ne les sont pas car les avis sont partagés pour ces deux derniers exemples.

3. Valeur de vérité d'une proposition

Il n'y a que deux valeurs de vérité possible : le vrai ou le faux. Soit P une proposition, la valeur de P est soit vrai noté v ou 1 si P est un énoncé vrai, soit faux noté f ou 0 si P est un énoncé faux.

Remarque :

1. Toute proposition a, par définition, une valeur de vérité et une seule.
2. Si ℓ désigne une collection des propositions et $\sqrt{a^2}$ ensemble des valeurs de vérité d'une proposition donnée ie $\sqrt{a} = \{v, f\}$ ou $\sqrt{a} = \{1,0\}$, alors on peut définir une application (h) de la manière suivante :
   $h : \ell \to \sqrt{a^2}$
   $$\text{p} \to \text{h(P)} = \begin{cases} \text{1 si p est une proposition vraie} \\ \text{0 si p est une proposition fausse} \end{cases}$$

Ainsi h(P) désignera dans notre cours la valeur de vérité d'une proposition donnée P. dès lors, on peut écrire : h(« Kinshasa est la capitale politique de la R.D.C ») = v ; pour dire que Kinshasa est la capitale de la R.D.C. est une proposition vraie.

Table de vérité d'une proposition P

Soit une proposition « P », on sait que « p » a deux valeurs de vérité possible. On l'écrit de la façon suivante :

h (P)
V
f

Table de vérité de deux propositions P et Q

Si on a deux propositions P et Q, il faut alors quatre lignes pour épuiser toutes les possibilités d'agencement des Vrais et des Faux, ie.

h (P)	h (Q)
v	v
v	f
f	v
f	f

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Table de vérité de trois propositions P,Q et R

Si on a trois propositions P,Q et R, il faut alors huit lignes ie

h (P)	h (Q)	h (R)
v	v	v
v	f	f
v	v	v
v	f	f
f	v	v
f	v	f
f	f	v
f	f	f

4. Définition

Deux propositions P et Q sont dites logiquement équivalentes et on écrit $P \equiv Q$ ssi elles ont la même valeur de vérité, ie $P \equiv Q$ ssi h(P)=h(Q).

N.B. : Dans la suite de notre cours, les lettre V et F désignerons respectivement la proposition vraie et la proposition fausse. Ainsi, h(V) = 1 et h(F) = 0.

C. CONNECTEURS LOGIQUES

Le but de ce paragraphe est d'abord de construire de nouvelles propositions à partir des propositions et des opérations logiques données et ensuite d'étudier leur valeur de vérité en fonction des valeurs de vérité des propositions du départ.

Définition 1 : Une proposition est dite composée quand au moins l'une de ses parties propres constitue une proposition par elle-même.

Donc une proposition composée comprend deux ou plusieurs propositions simples liées par des particules appelées connecteurs.

Définition 2 : Un connecteur logique ou opération logique est une fonction de vérité qui, pour chaque agencement possible des valeurs de vérité des composantes, attribue une et une seule valeur de vérité à la proposition composée.

Si θ désigne un connecteur logique, et $\wp$ une collection des propositions alors on a :

$$\theta = \wp \times \wp \to \wp$$
$$(P, Q) \mapsto \theta(P, Q) = P\,\theta\,Q, \text{ tel que } h(P\,\theta\,Q) \text{ dépend de } h(P) \text{ et de } h(Q)$$

Ainsi, la proposition $P\,\theta\,Q$ et dite composée et sa valeur de vérité dépend de celles de P et Q. Il suit qu'entre deux propositions données, on peut définir 16 connecteurs logiques.

Pour ce qui nous concerne, nous n'étudierons que les principaux à savoir : la conjonction, la disjonction, la négation, l'implication, la bi-implication, la disjonction exclusive, la tautologie et l'antilogie.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

1. La conjonction logique

a) Définition

La conjonction logique notée « $\wedge$ » est une application de $\wp \times \wp$ dans $\wp$ qui au couple des propositions (P, Q) associe la proposition $P \wedge Q$ (lire P et Q) vraie si P et Q les sont simultanément, fausse dans le cas contraire, ie la conjonction de deux propositions simples amène une proposition composée qui est vraie dans le seul cas où toutes les composantes sont vraies.

b) Table de vérité de P & Q

h (P)	h (Q)	h (Q)
v	v	v
v	f	f
f	v	f
f	f	f

c) Remarque

Il ressort de cette définition que si h(P) = h(Q) et h(R) = h(T) alors $h(P \wedge R) = h(Q \wedge T)$.

d) Exemples

a) h (« 3 divise 6 et 6 est pair ») = 1.
b) h (« 3x4=12 et 12 est un nombre premier ») = 0.
c) h (« 5 est pair et 5 est impair ») = 0.

e) Théorèmes

La conjonction ($\wedge$) vérifie les propriétés suivantes :

C_1. ($\wedge$) est improprement commutative ie.

$\forall$ P,Q, deux propositions, on a : $h(P \wedge Q) = h(Q \wedge P)$

C_2. ($\wedge$) est improprement associative ie.

$\forall$ P,Q,R trois propositions, on a : $h[P \wedge (Q \wedge R)] = h[(P \wedge Q) \wedge R]$

C_3. ($\wedge$) est improprement idempotente, ie.

$\forall$ P une proposition, on a : $h(P \wedge P) = h(P)$

C_4. La proposition V est l'élément neutre de ($\wedge$) dans $\wp$ ie.

$\forall$ P, proposition, on a : $h(P \wedge V) = h(P)$

C_5. La proposition F est l'élément absorbant de ($\wedge$) dans $\wp$ ie.

$\forall$ P, proposition, on a : $h(P \wedge F) = h(F) = 0$

Preuve de C_1, C_2, C_3, C_4 et C_5 à l'aide de la table de vérité.
Montrons par exemple C_1 et C_4.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Preuve de C_1

h (P)	h (Q)	h ($P \wedge Q$)	h ($Q \wedge P$)
v	v	v	v
v	f	f	f
f	v	f	f
f	f	f	f

Preuve de C_4

h (P)	h (v)	h ($P \wedge v$)
v	v	v
f	v	f

f) Définition

Soient $P_1, P_2, \ldots, P_k$, k propositions avec $k \geq 2$, alors par récurrence sur $k \in IN - \{1\}$, on a :

$$P_1 \wedge P_2 \wedge \ldots \wedge P_k = (P_1 \wedge P_2 \wedge \ldots \wedge P_{k-1}) \wedge P_k$$

g) Propriétés

Soient $P_1, P_2, \ldots, P_k$, k propositions avec $k \geq 2$, si $T = P_1 \wedge P_2 \wedge \ldots \wedge P_k$, alors
h(T) = 1 si $\forall i \in \{1,2,\ldots,k\}$, on a h($P_i$) = 1
h(T) = 0 si il existe $i \in \{1,2,\ldots,k\}$, tel que h(P_i) = 0

2. La disjonction logique

a) Définition

La disjonction logique notée (v) est une application de $\wp \times \wp$ dans $\wp$ qui au couple des propositions (P, Q) associe la proposition $P \vee Q$ (lire P ou Q) fausse si P et Q les sont simultanément, vraie dans les cas contraires, i.e. la disjonction de deux propositions simples amène une proposition composée qui est fausse dans le seul cas où toutes les composantes sont fausses.

b) Table de vérité de P & Q

h (P)	h (Q)	h (Q)
v	v	v
v	f	v
f	v	v
f	f	f

c) Remarque

Il ressort de cette définition que :
si h(P) = h(Q) et h(R) = h(T) alors $h(P \vee R) = h(Q \vee T)$.

d) Exemples

1) h (5 divise 7 dans IR ou 7 est multiple de 3 dans IR) = 1.
2) h (9 est pair ou 9 est impair) = 1.
3) h (le District de Tshilenge se trouve dans la province de l'Equateur et Bandundu est le chef-lieu de Mbandaka) = 0.

e) Théorèmes

La disjonction ($\vee$) vérifie les propriétés suivantes :

d_1. (v) est improprement commutative.
d_2. (v) est improprement associative.
d_3. (v) est improprement idempotente.
d_4. La proposition F est l'élément neutre de (v) dans $\wp$
d_5. La proposition V est l'élément absorbant de (v) dans $\wp$

Preuve de d_1, d_2, d_3, d_4 et d_5 au TP l'aide des tables des vérités. Montrons que par exemple la propriété d_2 à l'aide de table de vérité où

Pour trois propositions P, Q et R, on a : $h[P \vee (Q \vee R)] = h[(P \vee Q) \vee R]$

h (P)	h (Q)	h (R)	h (PvQ)	h (QvR)	$h[P \vee (Q \vee R)]$	$h[(P \vee Q) \vee R]$
v	v	v	v	v	v	v
v	v	f	v	v	v	v
v	f	v	v	v	v	v
v	f	f	v	f	v	v
f	v	v	v	v	v	v
f	v	f	v	v	v	v
f	f	v	f	v	v	v
f	f	f	f	f	f	f

f) Définition

Soient P_1, P_2, …, P_k, k propositions avec k $\geq$ 2, alors par récurrence sur k $\in$ $IN^* - \{1\}$, on a :

$P_1 \vee P_2 \vee ... \vee P_k = (P_1 \vee P_2 \vee ... \vee P_{k-1}) \vee P_k$

g) Proposition

Soient P_1, P_2, …, P_k, k k propositions avec k $\geq$ 2, si T = $P_1 \vee P_2 \vee ... \vee P_k$, alors

h(T) = 1 si $\exists i \in \{1,2,...,k\}$, tel que h($P_i$) = 1

h(T) = 0 si $\forall i \in \{1,2,...,k\}$, on a h($P_i$) = 0

La preuve de cette proposition découle de la définition de la disjonction.

h) Théorèmes

Pour P, Q et R trois propositions, on a :

P_1. $h[P \wedge (Q \vee R)] = h[(P \wedge Q) \vee (P \wedge R)]$
P_2. $h[P \vee (Q \wedge R)] = h[(P \vee Q) \wedge (P \vee R)]$
P_3. $h[P \wedge (Q \wedge R)] = h[(P \wedge Q) \wedge (P \wedge R)]$
P_4 $h[P \vee (Q \vee R)] = h[(P \vee Q) \vee (P \vee R)]$

Preuve de P_1 à l'aide de la table de vérité

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

h (P)	h (Q)	h (R)	h (QvR)	$h\left[(P \wedge (Q \vee R)\right]$	h (P $\wedge$ Q)	h (P $\wedge$ R)	$h\left[(P \wedge Q) \wedge (P \vee R)\right]$
v	v	v	v	v	v	v	v
v	v	f	v	v	v	f	v
v	f	v	v	v	f	v	v
v	f	f	f	f	f	f	f
f	v	v	v	f	f	f	f
f	v	f	v	f	f	f	f
f	f	v	v	f	f	f	f
f	f	f	f	f	f	f	f

Preuve de P_4

En vertu de l'idempotence, de la commutativité et de l'associativité de $\vee$ dans $\wp$, on a :

$$\begin{aligned} h[P \vee (Q \vee R)] &= h[(P \vee P) \vee (Q \vee R)] \\ &= h[P \vee (P \vee Q) \vee R] \\ &= h[P \vee (Q \vee P) \vee R] \\ &= h[(P \vee Q) \vee (P \vee R)] \end{aligned}$$

3. La négation logique

a) Définition

Soit P une proposition, la négation de P notée 1P ou $\overline{P}$ est l'énoncé « non P », vrai si P est une proposition fausse, faux si P est une proposition vraie.

Ainsi, la négation logique est une application τ définie comme suit :

$$\tau : \wp \to \wp$$

$$p \to \tau(P) = \overline{p}$$

b) Table de vérité de (aP)

h (P)	h (1P)
1	0
0	1

c) Remarque

Si h (P)=h (Q), alors h (1P)=h (1Q).

d) Exemples

1. Soient a et b deux nombres naturels,

   i. $h\left(\overline{a = b}\right) = h(a \neq b)$

   ii. $h\left(\overline{a \leq b}\right) = h(a \succ b)$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

2. Soit la proposition P : « Kabeya est un fleuve », alors la négation de P est la proposition : « Kabeya n'est pas un fleuve ». Ou encore : il est faux de dire que Kabeya est un fleuve.

e) Théorème

Pour une proposition P, on a :

n_1 : $h\left(\overline{\overline{P}}\right)=h(P)$

n_2 : $h\left(P\wedge\overline{P}\right)=0$

n_3 : $h\left(P\vee\overline{P}\right)=1$

Montrer aux exercices n_1, n_2 et n_3 à l'aide de table de vérité.

4. La conditionnelle

a) Définition

La conditionnelle logique $(\rightarrow)$ est une application de $\wp\times\wp$ dans $\wp$ qui, au couple des propositions (P, Q) associe la proposition $(P\rightarrow Q)$ (lire si P, …, alors Q ou P implique Q) fausse si P est vraie et Q est fausse, vraie dans les autres cas.

b) Table de vérité de (P & Q)

h (P)	h (Q)	h $(P\rightarrow Q)$
1	1	1
1	0	0
0	1	1
0	0	1

c) Remarque

La proposition $P\rightarrow Q$ est logiquement équivalente à la proposition $\overline{P}\vee Q$, ie $\forall P,Q\in\wp$, on a : $h(P\rightarrow Q)=h\left(\overline{P}\vee Q\right)$; (n)

d) Exemples

1. h (6x2 = 3 $\rightarrow$ divise (6) = 1
2. h (0$\in\varnothing$ $\rightarrow$ 0 est impair) = 1
3. h (3 est un naturel impair $\rightarrow$ 3 divise 11dans IN) = 0

e) Théorèmes

i_1 : h (P$\rightarrow$P) = 1.
i_2 : h (P$\rightarrow$V) = 1.
i_3 : h (P$\rightarrow$F) = h ($\overline{P}$).
i_4 : h (V$\rightarrow$P) = h (P).
i_5 : h (F$\rightarrow$P) = 1.

Preuve

i_1 : h (P$\rightarrow$P) = h ($\overline{P}\vee P$)=1 en vertu de la relation (n) du point 4. c) et (n_3) du point 3. e)

i_3 : h (P$\rightarrow$F) = h ($\overline{P}\vee F$) = h ($\overline{P}$) car F élément neutre de (v) dans $\wp$

i_5 : h (F $\rightarrow$ P) = h ($V \vee P$) = h (V) = 1 car la proposition V est un élément absorbent de (v) dans $\wp$.

i_2 et i_4 aux exercices.

f) Définition

1. Soient P et Q deux propositions, alors la proposition $Q \rightarrow P$ est la réciproque de la proposition $P \rightarrow Q$ et on a : $h(P \rightarrow Q) \neq h(Q \rightarrow P)$.
   En effet, supposer que $h(P \rightarrow Q) = 0$, cela signifie que h (P) = 1 et h (Q) = 0 entraînant que $h(Q \rightarrow P) = 1$
2. soient P et Q deux propositions, alors la proposition $\overline{Q} \rightarrow \overline{P}$ est la contraposée de la proposition $P \rightarrow Q$.

g) Proposition

Pour P, Q deux propositions, on a : $h(P \rightarrow Q) = h(\overline{Q} \rightarrow \overline{P})$ ie $h(P \rightarrow Q) = h(\overline{Q} \rightarrow \overline{P})$.

Preuve

En vertu de ce qui a précédé,

On a : $h\left(\overline{Q} \rightarrow \overline{P}\right) = h\left(\overline{\overline{Q}} \vee \overline{P}\right) = h\left(Q \vee \overline{P}\right) = h(\overline{P} \vee Q) = h(P \Rightarrow Q)$

h) Théorèmes

Pour P, Q et R trois propositions, on a :

P_1 : $h[P \rightarrow (Q \vee R)] = h[(P \rightarrow Q) \wedge (P \rightarrow R)]$

P_2 : $h[(P \wedge Q) \rightarrow R] = h[(P \rightarrow R) \vee (Q \rightarrow R)]$

P_3 : $h[P \rightarrow (Q \vee R)] = h[(P \rightarrow Q) \vee (P \rightarrow R)]$

P_4 : $h[(P \vee Q) \rightarrow R] = h\left[(P \rightarrow R) \wedge (Q \rightarrow R)\right]$

Preuve

P_1. On a, d'après I.1.3.4. (3) (n) et P_2 de I.1.3.2. (8) que

$$h\left[P \rightarrow (Q \wedge R)\right] = h\left[\overline{P} \vee (Q \wedge R)\right] = h\left[\left(\overline{P} \vee Q\right) \wedge \left(\overline{P} \vee R\right)\right] = h\left[(P \rightarrow Q) \wedge (P \rightarrow R)\right]$$

P_4. On a, d'après I.1.3.4. (3) (n) et L_2 de Morgan, voir I.1.6. (4), que :

$$h\left[(P \vee Q) \rightarrow R\right] = h\left[\left(\overline{P \vee Q}\right) \vee R\right] = h\left[\left(\overline{P} \wedge \overline{Q}\right) \vee R\right]$$

$= \mathrm{h}\left[\left(\overline{\mathrm{P}} \vee R\right) \wedge \left(\overline{Q} \vee R\right)\right]$, en vertu de P_2 de la conditionnel (8).

$$= h\left[(P \rightarrow R) \wedge (Q \rightarrow R)\right]$$

Montrer P_2 et P_3 aux exercices.

i) Exercices

La conditionnelle logique est-elle improprement associative ?

j) Remarque

L'usage répandu en mathématique du connectif « IMPLICATION » est de n'écrire que les propositions vraies.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Ainsi, si dans une théorie, on écrit $P \Rightarrow Q$ (lire P implique Q), cela signifie que la proposition implicative $P \to Q$ est vraie.

D'où une implication logique notée $(\Rightarrow)$ est une proposition composée qui a comme connectif principal une conditionnelle et qui est toujours vraie.
Il s'ensuit que $P \Rightarrow Q$ et $P \to Q$ ont même évaluation (1011).
Si elles sont différentes au point de vue nature, on doit les identifier au point de vue valeur de vérité.

N.B. : On fait la même remarque pour la bi-implication notée $\Leftrightarrow$, (lire bi-implique), qui est une proposition composée ayant comme connectif principal une bi-conditionnelle et ayant toujours la valeur vraie.

5. La bi – conditionnelle

a) Définition

La bi-conditionnelle notée ($\leftrightarrow$) est une application de $\wp \times \wp$ dans $\wp$ qui, au couple des propositions (P, Q) associe la proposition $P \leftrightarrow Q$ (lire P bi-implication Q ou P si et seulement si Q) vrai si P et Q ont une même valeur de vérité, fausse dans les autres cas.

Remarque : La bi-conditionnelle logique des propositions P et Q est la proposition P implication Q et Q implication P ie $h[P \leftrightarrow Q] = h[(P \to Q) \wedge (Q \to R)]$ ou
$P \leftrightarrow Q \equiv (P \to Q) \wedge (Q \to R)$

b) Table de vérité de Pa) Q

h (P)	h (Q)	h $(P \leftrightarrow Q)$
1	1	1
1	0	0
0	1	0
0	0	1

c) Exemples

1. h (3 divise 9 si et seulement si 9 est multiple de 3) = 1
2. h (5-1 = 4 $\leftrightarrow$ 4+1 = 6) = 0
3. h (Kinshasa est en R.D.C $\leftrightarrow$ Pointe Noire est au Gabon) = 0

d) Exercices

1. Construire la table de vérité de la proposition composée suivante : « Je bois de l'eau si et seulement s'il pleut et que je ne suis pas fâché ».
2. Montrer que, pour P et Q deux propositions, on a :
   i. $h(P \leftrightarrow Q) = h(Q \leftrightarrow P)$
   ii. $h[P \leftrightarrow (Q \leftrightarrow R)] = h[(P \leftrightarrow Q) \leftrightarrow R]$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

6. La disjonction exclusive

a) Définition

La disjonction exclusive notée ($\veebar$) est une application de $\wp\times\wp$ dans $\wp$ qui, au couple des propositions (P, Q) associe la proposition $(P \veebar Q)$ (lire soit P, soit Q), vraie si P et Q ont des valeurs différentes de vérité et fausse dans les autres cas.

b) Table de vérité de $P \veebar Q$

h (P)	h (Q)	h $(P \veebar Q)$
1	1	0
1	0	1
0	1	1
0	0	0

c) Exemple

« Je reste dormir à la maison ou je vais étudier à l'Université de Kinshasa ».
On constate que le connecteur « ou », utilisé est la disjonction exclusive.
Prendre P pour la proposition : « je reste dormir à la maison » et pour Q la proposition : »je vais étudier à l'université de Kinshasa ».

Pour avoir la proposition composée sous la forme $(P \veebar Q)$.

a. Si h(P) = 1 et h(Q) = 1, alors h($(P \veebar Q)$) = 0 car on ne peut pas au même moment rester dormir à la maison et aller étudier à l'Université de Kinshasa.
b. Si h(P) = 1 et h(Q) = 0, alors h($(P \veebar Q)$) = 1.

d) Proposition

Soient P et Q deux propositions, alors $h(P \vee Q) = h\left(\overline{P \leftrightarrow Q}\right)$.
Preuve aux exercices à l'aide de table de vérité.

7. Tautologie et anthologie

a) Définition (tautologie)

Une proposition composée est une tautologie si elle est vraie quelles que soient les valeurs de vérité de ses composantes.
Par exemples, pour deux propositions P et Q,

1. La proposition $(P \to Q) \to (\overline{P} \vee Q)$ une tautologie car $h[(P \to Q) \to (\overline{P} \vee Q)] = 1$. On peut alors écrire $(P \to Q) \Leftrightarrow (\overline{P} \vee Q)$.
2. La proposition $\overline{P \vee Q} \to \overline{P} \wedge \overline{Q}$ est aussi une tautologie et on peut écrire : $\overline{P \vee Q} \Leftrightarrow \overline{P} \wedge \overline{Q}$.

b) Définition (antilogie)

Une proposition composée est une antilogie ou une contradiction si elle est fausse quelles que soient les valeurs de vérité des composantes.
Par exemple, pour une proposition P, la proposition $P \wedge \overline{P}$ est une antilogie.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

c) Remarque

Dans la proposition : $P \Rightarrow Q$, puisqu'elle est une tautologie, alors P est l'hypothèse et Q est la thèse.

D. PREDICAT OU FORME PROPOSITIONNELLE

1. Définition

Tout énoncé qui contient une ou plusieurs variables et qui devient une proposition selon les valeurs attribuées à cette(s) variable(s) est appelé prédicat ou ferme propositionnelle. Noter que ces variables sont à prendre dans un ensemble appelé univers.

2. Définition (Univers de la variable)

L'univers d'une variable d'un prédicat ou forme propositionnelle est un ensemble des valeurs que l'on peut donner aux formes variables d'un prédicat pur obtenir une proposition. L'univers d'une variable est arbitraire et est toujours donné avec la forme propositionnelle. En notant par E l'univers d'une variable quelconque et par P(x) le prédicat dépendant de x, avec $x \in E$. On a, pour $a \in E$, que : « P(a) » est une proposition si h[P(a)] = 1, alors on dit que la proposition « P(a) » est satisfaite ou réalisée pour x = a.

Exemples :

a) Soit P(x) : « x est un diviseur de 32 », un prédicat défini sur IN, alors pour x=1, on obtient la proposition P(1) = « 1 est diviseur de 32 ». Sa valeur de vérité est vrai.
   Pour x = 2, on obtient la proposition P(2) = « 2 est diviseur de 32 ». Sa valeur de vérité est vrai.
   Pour x = 3, obtient la proposition P(3) = « 3 est un diviseur de 32 ». Sa valeur de vérité est faux, car 3 ne divise pas 32 dans IN.
b) Soit P(x) : « $\sqrt{x-4} < 3$ » un prédicat défini sur $A = [4;+\infty[\subset IR$
   Alors h[P(4)] = 1 car la proposition P(4) : 0 < 3 est vraie.
   Remarquer que l'ensemble IR n'est pas l'univers de ce prédicat car pour x = 0, P(0) n'a pas de sens dans IR.

3. Classe d'un prédicat

a) Définition

Soit P(x) un prédicat défini sur E$\neq \varnothing$, on appelle classe de P(x) ou ensemble solution de P(x) notée Ep, le sous-ensemble de E formée des éléments a de E tels que la proposition P(a) est vraie.

$$Ep = \{a \in E : h[P(a)]\} = 1$$

b) Exemples

1. Soit P(x) : $x^2 - 4 \leq 0$, un prédicat défini sur IR, déterminer alors la classe de P(x) notée IRp.
   On a : IRp = $\{[a \in IR : h_2[P(a)]] = 1\}$

$= \{a \in IR : a \quad - 4 \leq 0\}$

$= [-2{,}2]$

D'où IRp = $[-2{,}2]$

2. Soit Q(x) : $\sqrt{5-x} > 2$, un prédicat sur A $\subset$ IR. Déterminer A et A_Q.

On sait que A est formé des éléments x de IR pour lesquels le prédicat Q(x) a un sens.

b.1. $A = \{x \in IR : 5 - x \geq 0\} = \{x \in IR : x \leq 5\} =]-\infty;5]$

b.2.

$A_Q = \{a \in A : h[Q(a)] = 1\}$

$= \{a \in A : \sqrt{5-a} > 2\}$

$=]-\infty;1[$

c) Exercices

Déterminer la classe et l'ensemble univers des prédicats suivants.

a) $T(x) : \sqrt{3x+1} - x = 7$

b) $R(x) : x + \sqrt{x^2 - 10x + 9} > x + 2\sqrt{x^2 - 10x + 9}$

4. Opérations logiques

Soient P(x) et Q(x) deux prédicats définis sur $E \neq \emptyset$.

a) Définition (la conjonction des prédicats)

La conjonction de P(x) et Q(x) est le prédicat $P(x) \wedge Q(x) \equiv (P \wedge Q)(x)$.

Si on note par $E_{P \wedge Q}$ la classe de $P(x) \wedge Q(x)$, on a alors :

$E_{P \wedge Q} = \{a \in E : h[(P \wedge Q)(a)] = 1\}$

$= \{a \in E : h[P(a) \wedge Q(a)] = 1\}$

$= \{a \in E : h[P(a)] = 1 \text{ et } \mathrm{h}[\mathrm{Q}(\mathrm{a})] = 1\}$

$= \{\mathrm{a} \in \mathrm{E} : \mathrm{a} \in \mathrm{Ep} \text{ et } \mathrm{a} \in \mathrm{E_Q}\}$

$= Ep \cap E_Q$

D'où $Ep \wedge E_Q = Ep \cap E_Q$

b) Définition (la disjonction des prédicats)

La disjonction des prédicats est le prédicat $P(x) \vee Q(x) \equiv (P \vee Q)(x)$.

Montrer aux exercices que $E_{P \vee Q} = Ep \cup E_Q$ avec $E_{P \vee Q}$ la classe de $(P \vee Q)(x)$.

c) Définition (la négation de P(x)

La négation de P(x) est le prédicat $\overline{P(x)} = \overline{P}(x)$

En notant la classe de $\overline{P}(x)$ par $E_{\overline{P}}$, on a :

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

$$E_{\overline{P}} = \left\{ a \in E : h\left[\overline{P}(a) \right] = 1 \right\}$$
$$= \left\{ a \in E : h\left[P(a) \right] = 0 \right\}$$
$$= \left\{ \mathrm{a} \in \mathrm{E{:}a} \notin \mathrm{Ep} \right\}$$
$$= \mathrm{E - E_p}$$

d) Définition (l'implication des prédicats)

L'implication des prédicats P(x) et Q(x) est le prédicat.
$P(x) \Rightarrow Q(x) \equiv (P \Rightarrow Q)(x) \equiv (\overline{P} \vee Q)(x)$ en vertu de ce qui a précédé,
Si $Ep \Rightarrow P$ est la classe de $(P \Rightarrow Q)(x)$, alors
$Ep \Rightarrow Q = E_{\overline{P}} \cup E_Q = (E - Ep) \cup E_Q$
Déterminer aux exercices la classe de $P(x) \Leftrightarrow Q(x) \equiv (P \Leftrightarrow Q)(x)$.

e) Exemples

Soient P(x) : $x \succ 1$ et Q(x) : $x \leq 3$ deux prédicats définis sur IR.
Déterminer $IR_{P \wedge Q}$, $IR_{\overline{P}}$ et $IR_{P \Rightarrow Q}$
On a :

- $IR_{P \wedge Q} = IR_P \cap IR_Q = (]1;+\infty[) \cap (]-\infty;3]) =]1;3]$
- $IR_{\overline{P}} = IR - IR_P = (]-\infty;+\infty[) - (]1;+\infty[) =]-\infty;1]$
- $IR_{P \Rightarrow Q} = IR_{\overline{P}} \cup IR_Q = (]-\infty;1]) \cup (]-\infty;3]) =]-\infty;3]$

E. QUANTIFICATEURS

Il peut arriver dans l'énoncé d'une proposition que : l'on ait besoin d'indiquer une quantité.
Par exemple : tous les nombres naturels non nuls sont impaires ou il existe certaines femmes qui ont des yeux rouges.
On remarque que ces propositions portent en elles-mêmes une notion de quantité. Dans ce paragraphe, nous allons indiquer les symboles représentant des quantités que nous appelons quantificateurs. On distingue trois principaux.

1. Définition (Quantificateur existentiel)

Soit P(x) un prédicat défini sur $E \neq \varnothing$, alors l'énoncé : « il existe au moins un élément x de E vérifiant P(x) » est une proposition que l'on note par : « $\exists x \in E : P(x)$ ».
Le symbole $\exists$ représente le quantificateur existentiel qui se lit : « il existe au moins ». Ainsi, la proposition : « $\exists x \in E : P(x)$ est vraie si la clase du prédicat P(x) est non vide, soit $Ep \neq \varnothing$ » ie $h[\exists x \in E : P(x)] = 1$ si $Ep \neq \varnothing$.

2. Définition (Quantificateur universel)

Soit P(x) un prédicat défini sur $E \neq \varnothing$, alors l'énoncé :
« Pour tout élément x de E, on a P(x) » est une proposition que l'on note par
«$\forall x \in E : P(x)$ ». Le symbole $\forall$ représente le quantificateur universel qui se lit : « pour tout » ou « quelque soit ». La proposition : $\forall x \in E : P(x)$ est vraie si la clase du prédicat P(x) est égal à l'univers de P(x), soit $Ep = E$ ie $h[\forall x \in E : P(x)] = 1$ si $Ep = E$.

3. Définition (Quantificateur d'unicité)

Pour un prédicat P(x) défini sur $E \neq \varnothing$, l'énoncé : « il existe un et un seul élément x de E vérifiant P(x) » est une proposition que l'on note par : $h(\exists! x \in E : P(x)) = 1$ ssi Ep est un ensemble singleton.

4. Exemples

a) Soit $P(x) : x^2 - 4 \geq 0$, un prédicat défini sur IR,
Calculer $h[\forall x \in IR : P(x)] = ?$
Déterminons d'abord IRp
On sait que $IRp = [a \in IR : a^2 - 4 \geq 0] =]-\infty ; -2] \cup [2 ; +\infty[$
Comme IRp$\neq$IR, alors $h[\forall x \in IR : P(x)] = 0$
Remarquer $h[\forall x \in IR : x^2 + 4 \geq 0] = 1$ car IRp=IR.

b) Calculer $h[\exists x \in IR : x^2 - 4 \geq 0] = ?$
Puisque, d'après ce qui précède : $IRp =]-\infty ; -2] \cup [2 ; +\infty[\neq \varnothing$
Alors $h[\exists x \in IR : x^2 - 4 \geq 0] = 1$
Par contre $h[\exists! x \in IR : x^2 - 4 \geq 0] = 0$ car IRp n'est aps un ensemble singleton
Remarquer que $h[\exists! x \in IN : x^2 - 4 = 0] = 1$ car INp = {1} avec INp la classe du prédicat P(x) : « x – 4 = 0 » défini dans IN.

5. Proposition

Soit P(x) un prédicat défini sur $E = \varnothing$, alors

5.1. $\forall x \in \varnothing : P(x)$ est vraie ie $h[\forall x \in E : P(x)] = 1$.

5.2. $\exists x \in \varnothing : P(x)$ est fausse ie $h[\exists x \in E : P(x)] = 0$.

Preuve de 5

On sait que $Ep = \varnothing p = \{x \in \varnothing : P(x)\} = \varnothing$. Comme $Ep = \varnothing = E$, alors $\forall x \in E : P(x) = 1$ et $\exists x \in E : P(x) = 0$.

6. Proposition

Soit P(x) un prédicat défini sur $E \neq \varnothing$, alors $h[(\forall x \in E : P(x)) \Rightarrow (\exists x \in E : P(x)] = 1$

Preuve

Supposer que $\forall x \in E : P(x) = 1$ et montrer que $\exists x \in E : P(x) = 1$.
Puisque, $h(\forall x \in E : P(x)) = 1$, alors Ep = E.
Or $E \neq \varnothing$ par hypothèse, donc $Ep \neq \varnothing$ entraînant que $h(\exists x \in E : P(x)) = 1$.

7. Théorème

Soit P(x) un prédicat défini sur $E \neq \varnothing$, alors

7.1. $h[\overline{\forall x \in E : P(x)}] = h[\exists x \in E : \overline{P}(x)]$

7.2. $h[\overline{\exists x \in E : P(x)}] = h[\forall x \in E : \overline{P}(x)]$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Preuve de 7

Supposer que $h\left[\overline{\forall x \in E : P(x)}\right] = 1$ et montrer que $h\left[\exists x \in E : \overline{P}(x)\right] = 1$.

Puisque $h\left[\overline{\forall x \in E : P(x)}\right] = 1$, alors $h(\forall x \in E : P(x)) = 0$, ie Ep = E ou $E - Ep \neq \emptyset$. Sachant que $E - Ep = E_{\overline{P}}$, alors $E_{\overline{P}} \neq \emptyset$, d'après ce qui précède, il suit que $h\left[\exists x \in E : \overline{P}(x)\right] = 1$. Cqfd.

Par exemple :

a) $h\left(\overline{\forall x \in IR : x^2 - 5 \leq 0}\right) = h\left(\exists x \in IR : x^2 - 5 > 0\right)$.

b) $h\left(\overline{\text{toutes les femmes ont les yeux blonds}}\right)$ = h(certaines femmes n'ont pas des yeux blonds).

8. Ordre des Quantificateurs

Il faut respecter l'ordre des quantificateurs dans une expression qui en contient plusieurs. Les quantificateurs de même nature permutent, tandis que qu'en général, les quantificateurs de nature différente ne permutent pas.

ie:

8.1. $h(\forall x \in E, \forall y \in E : P(x, y) = h(\forall y \in E, \forall x \in E : P(x, y))$

8.2. $h(\exists x \in E, \exists y \in E : P(x, y)) = h(\exists y \in E, \exists x \in E : P(x, y))$

8.3. $h(\forall x \in E, \exists y \in E : P(x, y)) = h(\exists y \in E, \forall x \in E : P(x, y))$

Illustrons 8.3 par l'exemple ci-dessous.

Considérons l'ensemble IN muni de la relation : « est inférieur à » : notée (<). On constate que : $h\left(\forall n \in IN ; \exists a \in IN : \text{ tel que: n < a}\right) \neq h\left(\exists a \in IN : \forall n \in IN, \text{ on a: n < a}\right)$.

Car pour la première proposition, IN n'a pas de plus grand élément et pour la deuxième : a est le plus grand élément de IN. La première proposition est vraie, par contre, la seconde est fausse.

9. Remarques

Soient $E \neq \emptyset \neq F$ et P(x, y) un prédicat à deux variables défini sur $E \times F \neq \emptyset$ alors on se propose d'étudier la valeur de vérité des propositions suivantes :

$A_1 \equiv \forall x \in E, \forall y \in F : P(x, y);$

$A_2 \equiv \exists x \in E, \exists y \in F : P(x, y);$

$A_3 \equiv \forall x \in E, \exists y \in F : P(x, y);$

$A_4 \equiv \exists x \in E, \forall y \in F : P(x, y);$

Etudions alors la valeur de vérité de A_1, on procédera de même pour A_2, A_3 et A_4.

h (A_1) = $h(\forall x \in E, \forall y \in F : P(x, y))$

= $h(\forall y \in F : P(x, y))$ avec x une constante

= $h(\forall y \in F : P_x(y))$, x constante et y variable.

On se ramène ainsi à un prédicat d'une variable (y). Si $F_{P_x} = F$, alors $h(\forall y \in F : P_x(y)) = 1$, entraînant que $h(\forall x \in E, \forall y \in F : P(x, y)) = 1$, sachant que F_{P_x} est la classe du prédicat $P_x(y)$.

Exemple

Calculer $h\left(\forall x \in IR, \exists y \in IR : 2x + 3y > 0\right)$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

D'après ce qui précède, on a :

$h(\forall x \in IR, \exists y \in IR : 2x+3y \succ 0) = h(\exists y \in IR : 2x+3y > 0)$

Poser $P(x, y) \equiv 2x+3y > 0$, un prédicat à une variable définie sur IR et x est une constante.

$$IR_p = \{ y \in IR : 2x+3y > 0 \}$$
$$= \left\{ y \in IR : y > -\frac{2x}{3} \right\}$$
$$= \left] -\frac{2x}{3} ; +\infty \right[\neq \varnothing, \forall x \in IR$$

Comme $IR_P \neq \varnothing$, alors $h(\exists y \in IR / P(x, y)) = 1$ quelque $x \in IR$ entraînant que $\forall x \in \mathbb{R}$, $\exists y \in \mathbb{R}$: $2x+3y > 0$. Calculer aux exercices

$h(\exists x \in IR, \forall y \in IR : y^2 - xy + 4 \geq 0) = ?$

F. LOIS, PRINCIPES ET REGLES DE LA LOGIQUE

1. Principe de la contradiction

a) Définition

Pour toute proposition P, on a : $h(P \wedge \overline{P}) = 0$

Une proposition est contradictoire si $h(P) = h(\overline{P})$

2. Principe du tiers-exclu

Pour toute proposition P, on a : $h(P \vee \overline{P}) = 1$

3. Principe de la contraposition

Pour deux propositions P et Q, on a : $h(P \Rightarrow Q) = (\overline{Q} \Rightarrow \overline{P})$

Preuve

Supposer que $h(P \Rightarrow Q) = 0$ et montrer que $h(\overline{Q} \Rightarrow \overline{P})$.

En effet, $h(P \Rightarrow Q) = 0$ implique que $h(P) = 1$ et $h(Q) = 0$.

Or, $h(P) = 1$ et $h(Q) = 0$ entraîne $h(\overline{P}) = 0$ et $h(\overline{Q}) = 1$ donc $h(\overline{Q} \Rightarrow \overline{P}) = 0$.

4. Lois de De Morgan

Pour P et Q, deux propositions, on a :

L_1 : $h(\overline{P \vee Q}) = h(\overline{P} \wedge \overline{Q})$

L_2 : $h(\overline{P \wedge Q}) = h(\overline{P} \vee \overline{Q})$

Preuve à l'aide de la table de vérité.

5. Lois d'absorption

Pour P et Q, deux propositions, on a :

L_1 : $h[P \vee (P \wedge Q)] = h(P)$

L_2 : $h[P \wedge (P \vee Q)] = h(P)$

Preuve à l'aide de la table de vérité.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

6. Règle de Modus Ponens

Pour deux propositions P et Q, on a :
Si $h(P)=1$ et $h(P \Rightarrow Q)=1$, alors $h(Q)=1$

Preuve
D'après I.1.3.4.3., (n), on a : Voir hypothèse ci-dessus ;
$1 = h(P \Rightarrow Q) = h(\overline{P} \vee Q) = h(Q)$ car $h(\overline{P}) = 0$.
D'où $h(Q)=1$.

7. Règles disjonction des cas

Pour P et Q deux propositions, on a :
Si $h(P \Rightarrow Q)=1$ et $h(\overline{P} \Rightarrow Q)=1$, alors $h(Q)=1$.

Il faut montrer à l'aide de table de vérité que la proposition $[(P \Rightarrow Q) \wedge (\overline{P} \Rightarrow Q)] \Rightarrow Q$ est une tautologie.
Illustrons cette règle de disconjonction de cas par un exemple.
Considérer trois ensembles non vides A, B et C tels que : $(A \cap B) \subset (A \cap C)$ et $(A \cup B) \subset (A \cup C)$, et montrer que $B \subset C$, ou $\forall a : a \in B \Rightarrow a \in C$.

- Si $a \in A$, $a \in A \cap B$ par définition, alors $a \in A \cap C$ par hypothèse, donc $a \in C$.
- Si $a \notin A$, $a \in A \cup B$ par définition, alors $a \in A \cup C$ par hypothèse, donc $a \in C$.

Pour se conformer à I.1.5 (7), prendre : P : « $a \in A$ » et Q : « $a \in C$ ».

8. Loi du Syllogisme hypothétique

Pour trois propositions P, Q et R, on a :
$h\{[(P \Rightarrow Q) \wedge (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)\} = 1$

G. METHODES DES RAISONNEMENTS MATHEMATIQUES

1. Raisonnement par implication

Raisonner par implication c'est remplacer l'implication proposée par un certain nombre d'implications successives dont la vérité est facile à établir ou elle est déjà établie. [On compose l'implication (les implications) obtenue(s), avec des règles I.1.6 (6) et (7)].

2. Raisonnement par contre exemple

Le raisonnement par contre exemple est un raisonnement le plus clair et convaincant. On considère un énoncé (P) donnant une propriété universelle de certains éléments d'une théorie δ et on se propose de démontrer que P est faux. Pour cela, il faut exhiber un élément de la théorie δ vérifiant $\overline{P}$.

Exemples :

a. Soit l'énoncé P : « Tout nombre naturel n qui est à la fois divisible par 2 et par 8 est divisible par 16 ». montrons que P est faux.
   Il existe un naturel 24 tel que 2 divise 24, 8 divise 24 et pourtant 16 ne divise pas 24.
b. « Tout groupe fini est commutatif ». ceci est faux car il existe un groupe (S_3, O), avec S_3 ensemble de permutations d'un ensemble à 3 éléments, non commutatif et pourtant fini car son cardinal est 6.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

3. Raisonnement par absurde

a) Proposition

Dans une théorie δ si une proposition P est contradictoire, alors tout énoncé Q est contradictoire.
En effet, supposons que P et $\overline{P}$ soient vraies à la fois et considérer une proposition Q dans δ, on constate que l'implication $\overline{P} \Rightarrow (P \rightarrow Q)$ est vraie, puisque $\overline{P}$ est vraie par hypothèse, alors $P \rightarrow Q$ est aussi vraie entraînant que Q est vraie, car P est vraie par hypothèse. Donc, dans δ, Q, un énoncé quelconque est vrai, il en est de même de $\overline{Q}$. Cqfd.

b) Principe de raisonnement par absurde

Si dans une théorie δ, on veut montrer que la proposition P est vraie, par absurde. On suppose que P est une proposition fausse, ie $\overline{p}$ est une proposition vraie et on forme la théorie δ' obtenue en adjoignant $\overline{p}$ à la théorie δ on montre qu'un énoncé Q de δ est contradictoire dans δ'. Il s'ensuit que la proposition $\overline{p}$ est à rejeter et le principe du tiers exclu établi que P est vraie.

c) Exemple

Considérer l'ensemble IR muni de la relation « est inférieur ou égal à » et montrer par absurde que $0 \leq 1$. Pour cela, supposer que $\overline{0 \leq 1} \equiv 0 > 1$; (i) est vrai, comme $0 > 1$, d'après l'hypothèse d'absurdité, alors $0 + (-1) > 1 + (-1)$ est vrai, soit $(-1) > 0$. $(-1) > 0 \Rightarrow (-1).(-1) > 0$, ie $1 > 0$; (ii). On abouti ainsi à une contradiction car on a à la fois voir (i) et (ii) $0 > 1$ et $1 > 0$. Cette contradiction provient du fait qu'on avait supposé que $\overline{0 \leq 1} \equiv 0 > 1$ est vrai.

Donc $0 \leq 1$.

4. Raisonnement récurrence

Le principe consiste à établir qu'un prédicat où intervient une variable n ; avec n un entier naturel, est vrai pour tout n.
ie $\forall n \in IN : P(n)$ est vrai.
Pour cela, il faut :
(1°) Etablir que pour n = 0 ; n = 1 ; n = 2 ;…, les propositions P(0), P(1), P(2) sont vraies.
(2°) Supposer que P(n) est vrai jusqu'à l'ordre $k \in IN$ (hypothèse de récurrence), et montrer que P(n) reste aussi vrai jusqu'à l'ordre (k + 1).
(3°) D'où $\forall n \in IN : P(n)$ est vrai.

a) Exemple

Etablir par le raisonnement de récurrence sur IN^* que la somme de n premiers nombres naturels non nuls est : $\frac{n(n+1)}{2}$

ie $1 + 2 + ... + n = \frac{n(n+1)}{2}$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Il faut montrer que pour tout élément (n) de IN^* :

$P(n) = \frac{n(n+1)}{2}$ est vraie, avec P(n) la somme de n premiers nombres naturels non nuls.

1°. Pour n = 1, n =2 et n = 3, les propositions P(1), P(2) et P(3) sont vraies car :

n = 1 ; P(1) = 1

n = 2 ; P(2) = 1 + 2 = 3 = $\frac{2(2+1)}{2}$

n = 3 ; P(3) = 1 + 2 + 3 = 6 = $\frac{3(3+1)}{2}$

2°. Supposer que P(n) est vraie jusqu'à l'ordre k, avec $k \leq n$, ie $P(k) = 1 + 2 + ... + \frac{k(k+1}{2}$ et montrer que P(n) est vraie jusqu'à l'ordre (k + 1) ie

$P(k+1) = \frac{(k+1)(k+2)}{2}$ .Or

$$\begin{aligned} P(k+1) &= 1 + 2 + ... + k + (k+1) \\ &= P(k) + (k+1) \\ &= \frac{\mathrm{k}(\mathrm{k}+1)}{2} + (k+1) \\ &= \frac{(\mathrm{k}+1)(k+2)}{2} \end{aligned}$$

Donc, $P(k+1) = \frac{(k+1)(k+2)}{2}$ est vraie.

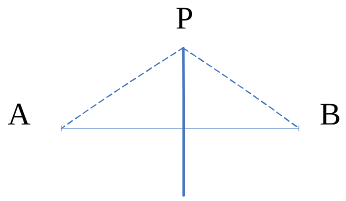
D'où $\forall n \in IN^*; P(n) = \frac{n(n+1)}{2}$ est vraie.

5. Raisonnement par contraposition

Si dans une théorie τ , on veut démontrer l'implication $P \Rightarrow Q$ on peut, dans la même théorie, démontrer la contraposée $\overline{Q} \Rightarrow \overline{P}$.

a) Exemple

« Tout point équidistant des extrémités d'un segment $[AB]$ appartient à la médiatrice de ce segment ».



La contraposée de cette proposition composée est la suivante :

« Tout point n'appartient pas à la médiatrice d'un segment $[AB]$ n'est pas équidistant des extrémités de ce segment ».

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

H. LA THEORIE DES ENSEMBLES

1. Généralités

Comme nous l'avons dit à l'introduction de cet ouvrage, les notions d'ensemble, élément, appartenance sont des notions primitives, donc on ne peut pas les définir.
Mais, nous allons donner une présentation élémentaire et signifiée des axiomes qui précisent les principales notions ensemblistes.
Remarquer tout d'abord que la notion d'ensemble est issue de la notion de collection, mais toute collection n'est pas un ensemble.

2. Ensemble, élément et appartenance

Soit E, un ensemble et a un objet, l'énoncé :
« a est un élément de E » est une proposition.
Si h (a est un élément de E) = 1, alors on écrit : $a \in E$
Si h (a est un élément de E) = 0, alors on écrit : $a \notin E$
Le symbole $\in$ est le signe d'appartenance qui se lit : « est un élément de » ou « appartient à ».
On désigne les éléments d'un ensemble par des lettres minuscules et on désigne un ensembles par une lettre majuscule.

3. Ecriture d'un ensemble en extension

On dit qu'un ensemble est défini (déterminé) en extension si on connaît la liste de ses éléments, laquelle liste est placée entre accolades.
Par exemple : $A = \{a, ei, o, u, y\}$. Ce fait est justifié par l'axiome d'extensionalité. Si un ensemble E ne contient que 2 éléments, soient a et b avec $a \neq b$ ie $E = \{a, b\}$, on dit que E est un ensemble pair.
Si dans la paire $\{a, b\}$, on a : a = b, alors l'ensemble $\{a; a\}$ ou $\{b; b\}$ ne contenant qu'un seul élément sera noté : $\{a\}$ ou $\{b\}$ et appelé ensemble singleton.
D'où l'axiome 1 affirmant l'existence d'un ensemble.

Axiome 1
Pour tout objet a, il existe un ensemble $\{a\}$, qui admet a pour seul élément. On dit donc que : $a \in \{a\}$.

4. L'égalité de deux ensembles

Deux ensembles E et F sont égaux, ce qu'on écrit E = F si et seulement s'ils ont les mêmes éléments.

Exemples

a. $Z_+ = N$
b. Soient trois ensembles A, B et C définis en extension comme suit : $A = \{2,4,6,8\}$; $B = \{8,2,4,6\}$ et $C = \{4,6,8,9\}$, alors $A = B$ et $A \neq C$ car il existe $2 \in A$ et $2 \notin C$.

5. L'inclusion

Soient A et E deux ensembles, on dit que A est inclus dans E si tout élément de A est aussi élément de E.

On dit parfois que A est sous-ensemble de E ou est une partie de E et on écrit $A \subset E$ (lire A est inclus dans E). Ainsi, $A \subset E$ si $\forall x : x \in A \Rightarrow x \in E$. Il s'en suit que
$E = F \Leftrightarrow E \subset F$ et $F \subset E$.

6. Ensemble des parties d'un ensemble

Axiome 2 dit axiome d'un ensemble des parties
Soit E, un ensemble, il existe un nouvel ensemble appelé ensemble des parties de E, formé de tous les sous-ensembles de E. cet ensemble est noté par $\wp_E$ (lire P rond de E).
Ainsi, si A est une partie de E, a un élément de A, b un élément de E, on a :

$$A \subset E \Leftrightarrow A \in \wp_E ; a \in A$$
$$\{b\} \subset E \Leftrightarrow \{b\} \in \wp_E$$

Exemple
Soit $A = \{a; b\}$ un ensemble pair, alors :
$\wp_A = \{\varnothing; \{a\}; \{b\}; A\}$

$$\wp_{\wp_E} = \begin{Bmatrix} \varnothing, \{\varnothing\}; \{\{a\}\}; \{\{b\}\} A; \{\{a\}, \{b\}\}; \{\varnothing; \{a\}\}; \{\varnothing, \{b\}\}, \{\varnothing, A\}, \{\{a\}, A\}; \{\{b\}, A\}, \\ \{\varnothing, \{a\}, \{b\}\}, \{\varnothing, \{b\}, A\}, \{\{a\}, \{b\}, A\}, \{\varnothing, \{a\}, A\} \wp_A \end{Bmatrix}$$

Remarquer que $\{a\} \neq \{\{a\}\}$ car $a \neq \{a\}$.

7. Définition d'un ensemble en compréhension

Axiome 3 (dit axiome de compréhension)
Soit E un ensemble non vide et P(x) un prédicat défini dans E, il existe un sous-ensemble E_P de E formé des éléments x de E vérifiant P(x).

Exemples

a) Soit P(x) : « $|x| < 5$ », un prédicat défini dans Z, alors :

$Z_P = \{x \in Z : P(x)\} \subset Z$

$= \{x \in Z : |x| < 5\}$ est la définition en comprehension de Z_P

$= \{-5; -4; -3; -2; -1; 0; 1; 2; 3; 4; 5\}$

On dit dans ce dernier cas qu'on a défini l'ensemble Z_P en extension.

b) Soit Q(x) : « x est un diviseur de 32 », un prédicat défini dans IN, alors $IN_Q = \{x \in IN : \text{x est un diviseur de } 32\} \subset IN$.

Cet ensemble est défini en extension comme suit :
$IN_Q = \{1,2,4,8,16,32\}$

8. L'ensemble vide

Soit E, un ensemble non vide et P(x) : « $x \notin E$ », un prédicat défini dans E, alors d'après l'axiome 3, il existe $E_P \subset E$ avec $E_P = \{x \in E : P(x)\} = \{x \in E : x \notin E\}$. Cet ensemble E_P ne contient aucun élément. On l'appelle ensemble vide et on le note par $\varnothing$. D'où $E_P = \varnothing$ et $\varnothing \subset E$.
Remarquer que, pour tout ensemble $E \neq \varnothing$, on a :
$\varnothing \subset E$ car $\forall a : a \in \varnothing \Rightarrow a \in E$. Cette proposition est vraie en vertu de I.1.3.4.5. (i5).

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

9. Complément d'un ensemble

a) Définition

Soient A et E deux ensembles non vides avec $A \subset E$ et P(x) : « $x \notin A$ », un prédicat défini dans E. d'après l'axiome 3, l'ensemble Ep existe avec :

$$Ep = \{x \in E : P(x)\} \subset E$$
$$= \{x \in E : x \notin A\} \subset E$$

Cet ensemble Ep est appelé complément de A dans E. on le note par C_E^A (lire complément de A dans E).

Ainsi, $C_E^A = \{x \in E : x \notin A\}$ et $u \in C_E^A \Rightarrow u \in E$ et $u \notin A$.

Par exemple, le complément de l'ensemble de nombres naturels impairs dans IN est l'ensemble de nombres naturels pairs.

b) Propriétés

Dans ce qui suit, on considéré E comme un ensemble référentiel non vide et $\wp_E$, l'ensemble des parties de E.

On définit un opérateur C dans $\wp_E$, par lequel le complément de X dans E est noté : C_E^x ou tout simplement CX.

$$C : \wp_E \to \wp_E$$
$$X \to CX = \{x \in E : x \notin X\}$$

Pour tout A, B et C élément de $\wp_E$, on a :

P$_1$. $C\varnothing = E$ et $CE = \varnothing$

P$_2$. $C(CA) = A$

P$_3$. $CA = CB \Rightarrow A = B$

P$_4$. $A \subset B \Rightarrow CB \subset CA$

Preuve

P$_1$. On sait que :

$$C\varnothing = \{x \in E : \overline{x \notin E}\} = \{x \in E : \overline{\overline{x \in E}}\} = \{x \in E : x \in E\} = E$$

et $CE = \{x \in E : x \notin E\} = \varnothing$.

P$_2$. Il faut montrer que $C(CA) = A$ ou $C(CA) \subset A$ et $A \subset C(CA)$ ou encore pour tout élément a de E, on a : $a \in C(CA) \Leftrightarrow a \in A$

En effet, $a \in C(CA) \Leftrightarrow a \notin CA$, par définition de complément d'un ensemble

$$\Leftrightarrow \overline{a \in CA}$$
$$\Leftrightarrow \overline{\overline{a \in A}}$$
$$\Leftrightarrow a \in A$$

P$_3$. Trivial en vertu de P$_2$ ci-dessus.

P$_4$. Montrons que, pour tout élément b de E :

$b \in CB \Rightarrow b \in CA$

Puisque $A \subset B$, par hypothèse, on a pour tout élément b : $b \in A \Rightarrow b \in B$, alors par contraposée, on obtient : $\forall b : b \notin B \Rightarrow b \notin A$ ie, $\forall b : b \in CB \Rightarrow b \in CA$ et $CB \subset CA$.

I. OPERATIONS SUR LES ENSEMBLES

1. La réunion des ensembles

a) Axiome4 (Axiome de la réunion)

Soient E et F, deux ensembles non vides, alors il existe un ensemble appelé E union F, formé des éléments qui appartiennent à au moins un des ensembles E, F.
On le note par $E \cup F$, et on lit : E union F.
Si $A \subset E$ et $B \subset E$, alors $A \cup B$ existe d'après l'axiome 4 ci-dessus, il est associé au prédicat $x \in A$ ou $x \in B$ dans E.
Ainsi, d'après l'axiome 3, on a :
$A \cup B = \{x \in E : x \in A \text{ ou } x \in B\} \subset E$
Ainsi, $x \in A \cup B \Rightarrow x \in A$ ou $x \in B$ et $x \notin A \cup B$ signifie d'après L_2 de de Morgan que $x \notin A$ et $x \notin B$.

b) Propriétés

Pour A, B et C, parties de E, un ensemble non vide, on a :
P_1. 1° $A \cup \emptyset = A$;
2° $A \cup E = E$
P_2. $A \cup A = A$
P_3. $A \cup B = B \cup A$
P_4. $A \cup (B \cup C) = (A \cup B) \cup C$
P_5. $A \cup C_E^A = B$

***Preuves* de P_5** car P_1, P_2, P_3 et P_4 se démontrent facilement à partir de la définition de $\cup$ et des propriétés de (v).
Pour P_5, il faut montrer que $\forall a \in E : a \in A \cup C_E^A \Leftrightarrow a \in E$
En effet :

$$a \in A \cup C_E^A \Leftrightarrow a \in A \text{ ou } a \in C_E^A$$
$$\Leftrightarrow a \in A \text{ ou } (a \in E \text{ et } a \notin A)$$
$$\Leftrightarrow (a \in E \text{ ou } a \in E) \text{ et } (a \in A \text{ ou } a \notin A), \text{ d'après } P_2 \text{ de I.1.3.2. (8)}$$
$$\Leftrightarrow a \in E \text{ et } a \in E, \text{ d'après } n_3 \text{ de I.1.3.3. (5)}$$
$$\Leftrightarrow a \in E, \text{ d'après } c_3 \text{ de I.1.3.1. (5)}$$

2. Intersection des ensembles

a) Définition

Soient A et B, deux ensembles non vides, alors il existe un nouvel ensemble appelé *A inter B* et formé des éléments qui appartiennent à la fois aux ensembles A et B.
On le note par $A \cap B$, et on lit : A inter B.
On constate que $A \cap B \subset A$ ou $A \cap B \subset B$
Définissons alors un prédicat P(x) : « $x \in B$ » dans A pour avoir d'après l'axiome 3, le sous-ensemble Ap, avec :

$Ap = \{x \in A : P(x)\} \subset A$
$\quad = \{x \in A : x \in B\} \subset \mathrm{A}$

Dès lors, si A et B sont deux sous-ensembles de E, alors $A \cap B$ existe d'après ce qui précède et il est déterminé par le prédicat P(x) : « $x \in A$ et $x \in B$ défini dans E ».

On a :
$A \cap B = \{x \in E : P(x)\}$
$\quad = \{\mathrm{x} \in \mathrm{E} : \mathrm{x} \in \mathrm{A} \text{ et } \mathrm{x} \in \mathrm{B}\}$

Il suit que :
1°. $x \in A \cap B \Rightarrow x \in A$ et $x \in B$
2°. $x \notin A \cap B \Rightarrow x \notin A$ ou $x \notin B$, et ce d'après L_1 de de Morgan.

b) Propriétés

P$_1$. $A \cap \varnothing = \varnothing$ et $A \cap E = A$
P$_2$. $A \cap A = A$
P$_3$. $A \cap B = B \cap A$
P$_4$. $A \cap (B \cap C) = (A \cap B) \cap C$
P$_5$. $A \cap C_E^A = \varnothing$

c) Théorème

Pour A, B et C, parties de E, E un ensemble non vide, on a :

P$_1$. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
P$_2$. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
P$_3$. $C_E^{A \cap B} = C_E^A \cup C_E^B$
P$_4$. $C_E^{A \cup B} = C_E^A \cap C_E^B$
P$_5$. $A \cap (A \cup B) = A$ et $A \cup (A \cap B) = A$
P$_6$. $A \cap (B \cap C) = (A \cap B) \cap (A \cap C)$
P$_7$. $A \cup (B \cup C) = (A \cup B) \cup (A \cup C)$

Preuve de P$_3$

Montrons que $\forall a \in C_E^{A \cap B} \Leftrightarrow a \in C_E^A$ ou $a \in C_E^B$.
En effet,
$\forall a, a \in C_E^{A \cap B} \Leftrightarrow a \notin A \cap B$
$\quad \Leftrightarrow a \notin A \text{ ou } a \notin B, \text{ d'après } \mathrm{L}_2 \text{ de de Morgan}$
$\quad \Leftrightarrow \mathrm{a} \in \mathrm{C}_\mathrm{E}^\mathrm{A} \text{ ou } \mathrm{a} \in \mathrm{C}_\mathrm{E}^\mathrm{B}$
$\quad \Leftrightarrow \mathrm{a} \in \left[\mathrm{C}_\mathrm{E}^\mathrm{A} \cup C_E^A\right]$. Cqfd

Pour prouver le reste des propriétés, utiliser les propriétés de la conjonction $(\wedge)$ et de la disjonction $(\vee)$, ainsi que les définitions de l'intersection et de l'union des ensembles.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

3. Différence des ensembles

a) Définition

Soient A et B deux ensembles et P(x) : « $x \notin B$ » un prédicat défini dans A, alors le sous-ensemble Ap existe d'après l'axiome 3 et on a :

$$Ap = \{x \notin A : P(x)\} \subset A$$
$$= \{x \in A : x \notin B\} \subset \mathrm{A}$$

Cet ensemble Ap est appelé différence des ensembles A et B. on le note par A-B (lire A moins B). Ainsi, $A - B = \{x : x \in A \text{ et } x \notin B\}$.

b) Remarque

Soient A et B deux ensembles non vides, alors $A - B = C_A^{A\cap B}$

Montrons que $\forall a : a \in C_A^{A\cap B} \Leftrightarrow a \in A \text{ et a} \notin \mathrm{B}$.

En effet, d'après L_2 de Morgan, le principe de la non contradiction et la distribution de la conjonction par rapport à la disjonction, on a :

$$a \in C_A^{A\cap B} \Leftrightarrow a \in A \text{ et a} \notin (\mathrm{A} \cap \mathrm{B})$$
$$\Leftrightarrow \mathrm{a} \in \mathrm{A} \text{ et } (\mathrm{a} \notin \mathrm{A} \text{ ou a} \notin \mathrm{B})$$
$$\Leftrightarrow (\mathrm{a} \in \mathrm{A} \text{ et a} \notin \mathrm{A}) \text{ ou } (\mathrm{a} \in \mathrm{A} \text{ et a} \notin \mathrm{B})$$
$$\Leftrightarrow \mathrm{a} \in \mathrm{A} \text{ et a} \notin \mathrm{B}, \text{ d'après } \mathrm{d}_4 \text{ de I.1.3.2. (5)}$$

D'où, $a \in C_A^{A\cap B} \Leftrightarrow a \in (A - B)$

c) Propriétés

Pour A et b deux parties d'un ensemble non vide E, on a :

P_1. $A - \varnothing = A$
P_2. $\varnothing - A = \varnothing$
P_3. $A - A = \varnothing$
P_4. $A - B \neq B - A$ si $A \neq B$
P_5. $A \cap (E - A) = \varnothing$
P_6. $A \cup (E - A) = E$

Preuve de P_5

Il faut montrer que : $\forall a : a \in A \cap (E - A) \Leftrightarrow a \notin E$

En effet,

$$a \in A \cap (E - A) \Leftrightarrow a \in A \text{ et a} \in (\mathrm{E} - \mathrm{A})$$
$$\Leftrightarrow \mathrm{a} \in \mathrm{A} \text{ et } (\mathrm{a} \in E \text{ et a} \notin \mathrm{A})$$
$$\Leftrightarrow (\mathrm{a} \in \mathrm{A} \text{ et a} \in E) \text{ et a} \notin \mathrm{A} \text{ en vertu de } \mathrm{c}_1 \text{ de I.1.2.1. (5)}$$
$$\Leftrightarrow \mathrm{a} \in \mathrm{A} \text{ et a} \notin \mathrm{A}$$
$$\Leftrightarrow \mathrm{a} \notin \mathrm{E}. \text{Cqfd}$$

Montrer les autres propriétés aux exercices.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

4. Différence symétrique

a) Définition

Soient A et B deux ensembles non vides, la différence symétrique des ensembles A et B, noté $A\Delta B$, (lire A delta B) est ensemble défini comme suit :

$$A\Delta B = \{x : (x \in A) \veebar (x \in B)\}$$
$$= \{x : (x \in A \text{ et } x \notin B) \text{ ou } (x \in B \text{ et } x \notin A)\}$$
$$= (A - B) \cup (B - A)$$

D'où $A\Delta B = (A - B) \cup (B - A)$

b) Remarque

Pour A et B deux parties quelconques de E, E ensemble non vide, on a :

$A\Delta B = (A \cup B) - (A \cap B)$

c) Propriétés

Pour A, B et C, parties d'un ensemble non vide E, on a :

P$_1$. $A\Delta\varnothing = A$
P$_2$. $A\Delta A = \varnothing$
P$_3$. $A\Delta B = B\Delta A$
P$_4$. $A\Delta(B\Delta C) = (A\Delta B)\Delta C$
P$_5$. $A \cap (B\Delta C) = (A \cap B)\Delta(A \cap C)$

Pour prouver toutes ces propriétés, utiliser la définition de (Δ) ainsi que les propriétés de $(\cap)$ et de $(\cup)$.

5. Généralisation de l'intersection et l'union

a) Définition (famille des parties d'un ensemble)

Soient E, un ensemble non vide et I un ensemble quelconque fini ou infini, on appelle famille des parties de E toute application

$$\varphi : I \to \wp_E$$
$$\text{i} \mapsto \wp(\text{i}) = X_i$$

On la note par $A = (X_i)_{i \in I}$ ou $A = \{X_i : i \in I\}$avec I, un ensemble des indices et $X_i \in \wp_E$.

Si $i \in IN$, alors $A = (X_i)_{i \in IN}$ est dit famille dénombrable des parties de E.

Si $i \in IR$, alors $A = (X_i)_{i \in IR}$ est dit famille non dénombrable des parties de E.

b) Exemples

1. En associant à tout nombre naturel k la partie $X_k = \{x \in IN : x \leq k\}$de IN. On définit ainsi une application φ de la manière suivante :

   $$\varphi : IN \to \wp_{IN}$$
   $$\text{k} \mapsto \text{X}_\text{k} = \{x \in IN : x \leq k\}$$

   Alors $A = (X_k)_{k \in I}$ ou $A = \{X_0, X_{2i}, X_{3i}, ..., X_k\}$ est une famille des parties de IN.

Remarquer par exemple que : $X_2 = \{x \in IN : x \leq 2\} = \{0,1,2\}$ et $X_3 = \{x \in IN : x \leq 3\} = \{0,1,2,3\}$.

2. Dans IR, en associant à tout élément $s \in IN^*$ l'intervalle ouvert $Xs =]-s, s[\subset IR$; on obtient alors une famille $A = (Xs) = \{Xs =]-s, s[: s \in IN^*\}$, dénombrable des parties de IR.

3. On sait que dans IR², une droite passant par l'origine des axes est donnée par l'équation y = mx, avec $m \in IR$. Ainsi, en associant à tout réel m, une droite $D_m = y = mx$, on obtient alors une famille $A = \{D_m \equiv y = mx : m \in IR\}$ non dénombrable des parties de IR², qu'on appelle famille des droites du plan IR² passant par l'origine des axes, à l'exclusion de la droite x = 0.

c) Intersection et union d'une famille des parties d'un ensemble E

Soit $A = (X_i)_{i \in I}$, une famille des parties d'un ensemble non vide E, alors :

- L'intersection de A, notée : $\cap A = \bigcap_{i \in I} X_i$ est définie comme suit :

  $\cap A = \bigcap_{i \in I} X_i = \{x / \forall i \in I : x \in X_i\}$

  Ainsi, $y \in (\bigcap_{i \in I} X_i) \Rightarrow \forall i \in I, y \in X_i$

- L'union de A, notée : $\cup A = \bigcup_{i \in I} X_i$ est définie comme suit :

  $\cup A = \bigcup_{i \in I} X_i = \{x / \exists i \in I : x \in X_i\}$

  Il suit que $z \in (\bigcup_{i \in I} X_i) \Rightarrow \exists i \in I, z \in X_i$.

d) Recouvrement d'une partie d'un ensemble

Soit $\mathcal{A} = (X_i)_{i \in I}$ une famille des parties E et $A \subset E$, on dit que $\mathcal{A}$ est un recouvrement de A si A $\subset (\cup \mathcal{A})$

e) Partition d'un ensemble

Soit E, un ensemble non vide, on appelle partition d'un ensemble E tout recouvrement ($\wp$) de E dont les éléments sont 2 à 2 disjoints et chacun étant différent de l'ensemble vide ie ($\wp$) est une partition de E si :

i) $\forall X \in \wp$: on a $X \neq \varnothing$

ii) $\forall X, X' \in \wp : X \neq X' \Rightarrow X \cap X' = \varnothing$

iii) $\bigcup_{X \in \wp} X = E$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

CHAPITRE II
RELATIONS ET APPLICATIONS

A. RELATIONS

1. Couple et produit cartésien

a) Couple

(1) Définition

Etant donné deux éléments x, y : on appelle couple x, y noté : (x, y) (Lire : couple x, y), l'ensemble : $\{\{x\},\{x,y\}\}$
i.e. (x, y) = $\{\{x\},\{x,y\}\}$

(2) Théorème

Soient deux couple (x, y) et (x', y')
Alors (x, y) = (x', y') ⇔ x = x' et y = y'
Démonstration
(i) ⟹ Montrons que : (x, y) = (x', y') ⟹ x = x' et y = y'

On sait d'après la définition du couple que : $(x,y)=\{\{x\},\{x,y\}\}=\{\{x'\},\{x',y'\}\}=(x',y')$ (j)

Deux cas sont possibles
1^er^ cas :
Supposons que : x = y la paire {x, y} = {x, x} = {x} et $\{\{x\},\{x,y\}\}=\{\{x\},\{x\}\}=\{\{x\}\}$
(j) devient $\{\{x\}\}=\{\{x'\}\{x',y'\}\}$ (k)
On arrive a une égalité entre deux ensemble dont le premier a un seul élément x et le second en a deux qui sont : {x'} et {x', y'}
Pour qu'il y ait égalité, il faut que : x' = y' car dans ce cas, {x',y'} = {x'} et , $\{x'\}$, {x',y'} = $\{\{x'\}\}$
Et k devient : $\{\{x\}\}=\{\{x'\}\}\Leftrightarrow\{x\}=\{x'\}\Leftrightarrow x=x'$

D'où $\left.\begin{array}{l} x=y \\ x'=y' \\ x'=x \end{array}\right\|\Leftrightarrow y'=x'=x=y$

2^e^ cas :
Supposons que x ≠ y, la relation (j) donne :$\{\{x\},\{x,y\}\}=\{\{x'\},\{x',y'\}\}$
⇔ (*1) $\{x\}=\{x'\}$ et $\{x,y\}=\{x',y'\}$
Ou
(*2) $\{x\}=\{x',y'\}$ et $\{x,y\}=\{x'\}$
En considérant (*1), on a : puisque {x} = {x'} et {x, y} = {x',y'}, que
x = x' et y = y'
D'où si x ≠ y et (x, y) = (x', y'), alors x = x' et y = y'
En considérant (*2), on a :
Pour avoir cette égalité, il faut que x = y, or par hypothèse, on a que x ≠ y,

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Donc x = y contredit notre hypothèse et ce cas est à rejeter,

- Si x = y et (x, y) = (x', y') alors x = x'
  Et y = y'
- Si x ≠ y et (x, y) = (x', y'), alors x = x'
  Et y = y'.

(ii) ⟹Montrons que : (x = x' et y = y') ⇒ (x, y) = (x', y')
Puisque x = x' et y = y', alors {x} = {x'} et {x, y} = {x', y'}
Donc $\{\{x\},\{x,y\}\} = \{\{x'\},\{x',y'\}\}$ et (x, y) = (x', y')

(3) Remarque

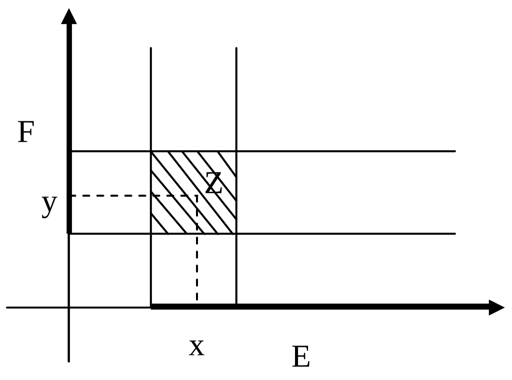
R_1 La définition du couple a été introduite pour démontrer le théorème ci haut.
R_2 Soit z = (x, y), alors x est la première projection de z et y est la deuxième projection. On note respectivement : x = Pr_1 z et y = Pr_2 z.
R_3 Si x ≠ y, alors (x, y) ≠ (y, x).
Les couples (x, y) et (y, x) sont dites couples transposé ou couple réciproques.
R_4 $\overline{[(x,y) = (x',y') \Leftrightarrow (x = x' \text{et } y = y')]} \equiv [(x,y) \neq (x',y') \Leftrightarrow (x \neq x' ou\ y \neq y')]$
Exemple : (3, x) ≠ (3, y) si x ≠ y (3,4) ≠(3,5).

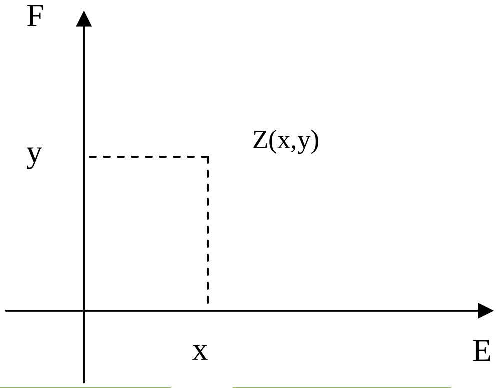
b) Le produit cartésien

(1) Axiome 5 (axiome produit)

Si E et F sont deux ensembles, il existe un ensemble constitué de tous les couples (x, y) tels que : x ∈ E et y ∈ F, qu'on appelle : produit cartésien de E par F et qu'on note par : E x F, ce qu'on lit : E <u>crois</u> F

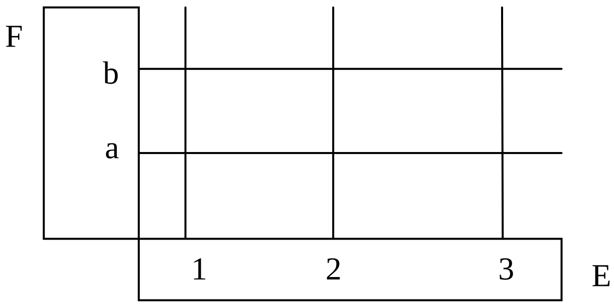
i.e. E x F = $\{(x,y) : x \in E,\ y \in F\}$ ou encore
E x F = $\{Z \mid \exists x \in E, \exists y \in F : Z = (x,y)\}$
$(Z \in E \times F \implies \exists\, x\, E, \exists\, y \in F : Z = (x,y))$





Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Exemple :
E = {1,2,3}
F = {a, b}
Alors E x F = {(1, a); (1, b); (2, a); (2, b); (3, a); (3, b)}



(2) Remarque

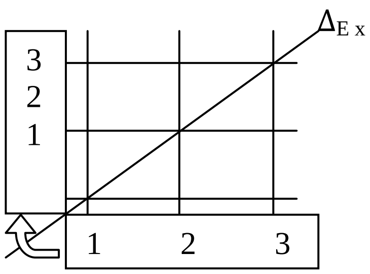
R_1 Si E = F, alors le produit cartésien de E par lui – même se note : E x E = E² (lire E deux)

Pour notre exemple :

E x E = {(1,1); (1,2); (1,3); (2,1); (2,2); (2,3); (3,1); (3,2); (3,3)}

- On appellera diagonale de l'ensemble E x E, noté $\Delta_{E \times E}$ l'ensemble de tout les couples de la forme (x, x) avec x ∈ E

  Pour notre exemple :
  $\Delta_{E \times E}$ = {(1,1), (2,2), (3,3)}
  $\Delta_{E \times E}$ = {(x, x): x ∈ E}



R_2 Soit $(A_i)_i \in [1,n] \subset \mathbb{N}$ une famille de n ensemble (A_1 , A_2 , A_3 , … , A_n) le produit cartésien de la famille $(A_i)_{i\in 1,n}$ se note $\bigcap_{i=1}^{n} A_i$ Produit cartésien d e la famille A_i , (A_i ensemble) avec i variant de 1 à n, n∈ ℕ

i.e. $\bigcap_{i=1}^{n} A_i = A_1 \times A_2 \times A_3 \times \dots \times A_n$

Soit $z \in \bigcap_{i=1}^{n} A_i \Longrightarrow \exists\, a_1 \in A_1, \exists\, a_2 \in A_2, \dots, \exists\, a_n \in A_n$ tel que z = (a_1 , a_2 , a_3 , … , a_n) qu'on appelle ***n – uplets***

(3) Proprieties

1. Si E' ⊂ E et F' ⊂ F, alors E' x F' ⊂ E x F

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Preuve:

Montrons que $\forall z'$: $z' \in E' \times F'$, alors $z' \in E \times F$

$z' \in E' \times F' \Longrightarrow \exists\, a' \in E'$, $\exists\, b' \in F'$: $z' = (a', b')$

$a' \in E'$ et $E' \subset E$, alors $a' \in E$ aussi $b' \in F'$ et $F' \subset F$, alors $b' \in F$

Donc $a' \in E$, $b' \subset F$, alors $(a', b') \in E \times F$

i.e. $z' \in E \times F$.

2. Si $E \neq \emptyset$ et $F \neq \emptyset$, alors E

En effet : $E \neq \emptyset \Longrightarrow \exists\, a : a \in E$

$F \neq \emptyset \Longrightarrow \exists\, b : b \in F$

Puisque $a \in E$, $b \in F$ alors $(a,b) \in E \times F$ et $E \times F \neq \emptyset$

3. Si $E \neq \emptyset$ alors $E \times \emptyset = \emptyset$

Démonstration

Supposons que $E \times \emptyset \neq \emptyset$,

D'après R_2, $\exists\, z : z \in E \times \emptyset$

$z \in E \times \emptyset \Longrightarrow \exists\, x \in E$, $\exists\, y \in \emptyset$ tel que $z = (x,y)$

Ce qui est absurde car $\emptyset$ n'a aucun élément. Alors, $E \times \emptyset \neq \emptyset$ et faux et $E \times \emptyset = \emptyset$ est vrai.

2. Relations binaires

a) Graphe

(1) Définition

Un graphe est un ensemble dont les éléments sont des couples. On le note par G.

Exemple

(3, 4), (5, 6), (7, 8) est un graphe.

Soit G un graphe, on note par :

- $pr_1\, G$ qu'on appelle $1^{ère}$ projection du graphe G, l'ensemble des premières projections des couples du graphe.
  i.e. $pr_1\, G = \{x : (x, y) \in G\}$
- $pr_2\, G$ qu'on appelle deuxième projection du graphe G, l'ensemble des deuxièmes projections des couples du graphe G
  i.e. $pr_2\, G = \{y : (x, y) \in G\}$

Pour notre exemple :

$pr_1\, G = \{3,5,7\}$ et $pr_2\, G = \{4,6,8\}$

(2) Remarque

i. Le produit cartésien de deux ensembles, donc un graphe.
ii. Un graphe est inclus dans le produit cartésien de $(pr_1\, G) \times (pr_2\, G)$

Exemple

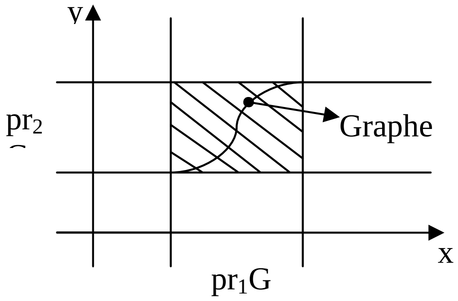
Soit $G = \{(3, a); (4, b); (5, b)\}$ un graphe quelconque.

Alors $pr_1\, G = \{3,4,5\}$

Et $pr_2\, G = \{a,b\}$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

D'où (pr_1 G) X (pr_2 G) = $\{(3,a); (3,b); (4,a); (4,b); (5,a); (5,b)\}$ et G ⊂ (pr_1 G) X (pr_2 G)



b) Définition d'une relation binaire entre deux ensembles

(1) Définition

Une relation binaires entre deux variables x et y décrivent respectivement deux ensembles A et B est une propriété définie sur A x B.
i.e. une propriété caractéristique des éléments d'une partie G de A x B. G s'appelle le graphe de la relation R souvent noté G_R. A (x,y) ∈ G_R , nous pouvons substituer la proposition équivalente suivante : « x et y vérifient la relation R » ce que l'on écrit en abrégé R(x,y) ou x R y. Ainsi, x R y ⟺ (x,y) ∈ G ou encor G = G_R = $\{(x,y): xRy\}$

De même $\overline{(xRy)} \Leftrightarrow (x,y) \in C^G_{AxB}$
Plus généralement, tout ce que nous avons dit des propriétés définies sur A x B ***est bien vrai*** des relations définies entre éléments de A et de B.
Soit « ≤ » (est inférieur ou égale à) une propriété définie sur A x B, avec A = $\{1,3,5,7\}$ et B = $\{2,0,6\}$
Alors G = $\{(1,2); (1,6); (3,6); (5,6)\}$ sont graphe.
On dit ici qu'on a défini une relation « ≤ » entre éléments de A et de B.

(2) Quelques définitions

Définition 1 : Deux relation R et R' entre éléments de A et B sont égales si elles ont les mêmes graphes. Soit G graphe de la relation R et G' graphe de la relation R'.
Alors : G = G' ⟺ $[\forall x \in A, \forall y \in B : (x,y) \in G \Leftrightarrow (x,y) \in G]$.

Définition 2 : la réciproque d'une relation binaire R entre élément de A et élément de B est la relation binaire entre élément de B et de A, noté R^{-1} et défini par :
∀(x,y) ∈ b x A : x R^{-1} y ⟹ y R x
C'est-à-dire (x,y) ∈ G^{-1} ⟹(y,x) ∈ G avec G = graphe de R G^{-1} = graphe de R'.

c) Relation binaire dans un ensemble

(1) Définition

a. Dans le cas ou A = B = E, on parle d'une relation binaire définie entre éléments de l'ensemble E ou tout simplement d'une relation définie sur (dans) un ensemble de E.
b. Exemple
   i. La relation « = » (est égale à) définie dans E ≠ ∅
      G = $\{(x,y) \in E^2 : x = y\} \equiv \{(x,x): x \in E\}$ = $\Delta_{E \times E}$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

ii. La relation “$\subset$” (lire est inclus dans) définie dans $P_{(E)}$ avec $E \neq \emptyset$. Son graphe G est défini en compréhension comme : $G = \{(A, B) \in \mathcal{P}_{(E)} X \mathcal{P}_{(E)} : A \subset B\}$ puisque $A = P_{(E)}$ alors $A \subset E$ et $B \in P_{(E)}$ alors $B \subset E$
Si $A \subset B$, alors $(A,B) \in G$.

En prenant par exemple $E = \{a,b,c\}$, alors $P_{(E)} = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, E\}$ les couples suivants satisfont à la relation « $\subset$ » définie dans $P_{(E)}$:
$(\emptyset,\emptyset)$, $(\square, \{a\})$, $(\{b\}, \{a, b\})$, $(\{c\}, E)$ …

(2) Qualité d’une relation dans un ensemble.

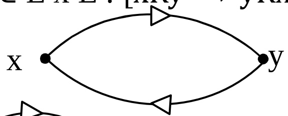
Définition

a. Soit R une relation définie dans $E \neq \emptyset$. Alors

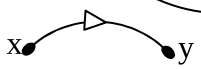
Définition 1 : R est dit réflexive si : $\forall x \in E : x R x$ i.e. $\Delta_{E \times E} \subset G$

Définition 2 : R est dit symétrique si : $\forall (x, y) \in E \times E : [xRy \Longrightarrow yRx]$

i.e. $\forall (x, y) \in E^2 : (x, y) \in G \Longrightarrow (y, x) \in G$

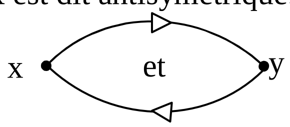


Si $\exists$ x, y $\in$ E tel que



Alors R est non symétrique.

Définition 3 : R est dit antisymétrique. Si $\forall x, y \in E : [(xRy \text{ et } yRx) \Longrightarrow x = y]$



$\Longrightarrow$ x = y

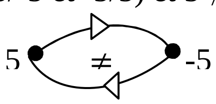
$\exists x,y \in E : [(xRy \text{ et } yRx) \text{ avec } x \neq y]$
Alors R est antisymétrique.

Définition 4 : R est dite transitive si
$\forall x,y \in E : xRy \text{ et } yRz \Longrightarrow xRz$.

b. Exemple :

1. « = » défini dans $\mathbb{N}$ ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$) est une relation qui est réflexive, symétrique et transitive
2. « $\leq$ » dans $\mathbb{Z}$ ($\mathbb{N}$, $\mathbb{Q}$, $\mathbb{R}$) est réflexive, antisymétrique et transitive.
3. « $\subset$ » dans $P_{(E)}$ est réflexive, antisymétrique et transitive
4. « // » (est parallèle à) définie dans D, avec D ensemble des droites du plan affine, est réflexive, symétrique et transitive.
5. « \ » (divise) dans $\mathbb{Z}$ est réflexive et transitive mais elle n’est pas symétrique.

Car $\exists$ 2, 4 $\in \mathbb{Z}$: 2 divise 4 et 4 ne divise pas 2. Elle n’est pas aussi symétrique
Car $\exists$ 5, -5 $\in \mathbb{Z}$: (5/-5 et -5/5) et $5 \neq -5$



(3) Relation d'équivalence

(a) Définition

Une relation R dans un ensemble est dite d'équivalence si elle est à la fois : réflexive, symétrique et transitive.
Soit R une relation d'équivalence. Pour traduire que le couple (x,y) vérifie la relation R, on remplace la notation générale x R y par :

$x \equiv y$ (module R) ce qu'on lit : « x est congru y modulo R »
« x est équivalent à y modulo R »

(b) Exemples

1. « = » est une relation d'équivalence dans E avec E ≠ □
2. « // » (est parallèle à) est une relation d'équivalence dans D
3. Dans $\mathbb{Z}$, on définit la relation R par : $x \, R \, y \Leftrightarrow P \backslash (x - y)$ [P divise $(x - y)$] avec $P \in \mathbb{N}^*$, $x, y \in \mathbb{Z}$

R est une relation d'équivalence qu'on appelle congruence modulo P. on peut alors écrire :
$x \equiv y$ (modulo P) $\Leftrightarrow P \backslash (x - y) \Leftrightarrow \exists\, q \in \mathbb{Z} : x - y = p \,.\, q$
d'où $\forall\, x, y \in \mathbb{Z} : x \equiv y$ (modulo P) $\Leftrightarrow \exists\, q \in \mathbb{Z}\; x - y = p \,.\, q$

Montrons que $(\equiv)$ est une relation d'équivalence dans $\mathbb{Z}$
$\forall x \in \mathbb{Z} : x \equiv x$ (modulo P) car $\exists\, q = 0 \in \mathbb{Z} : x - x = 0 = 0$. P est R est réflexive dans $\mathbb{Z}$

- $\forall x, y \in \mathbb{Z}$, montrons que : $x \equiv y$ (modulo P) $\Longrightarrow y \equiv x$ (modulo P).

En effet : $x \equiv y$ (modulo P) $\Leftrightarrow \exists\, q \in Z : x - y = p \,.\, q$
$-y + x = p.q$ (+ est commutative dans Z)
$-(y - x) = p.q$
$(y - x) = -(p.q)$
$y - x = p\,(-q)$.
Donc $\exists\, q' = -q \in Z$ tel que $y - x = p.q'$ et $y \equiv x$ (modulo P)
Ce qui prouve que R est symétrique dans R.

1) $\forall\, x, y, z \in Z$: si $x \equiv y$ (modulo P) et $y \equiv z$ (modulo P).

Alors $x \equiv z$ (modulo P)
En effet : $x \equiv y$ (modulo P) $\Leftrightarrow \exists\, q \in Z : x - y = p \,.\, q$ (i)
et $y \equiv z$ (modulo P) $\Leftrightarrow \exists\, q' \in Z : y - z = p \,.\, q'$ (ii).

2) Montrons qu'il existe $q'' \in Z : x - z = p \,.\, q''$

Puisque p divise $x - y$ et $y - z$, alors p divise aussi leurs somme.
i.e. $\exists\, q''' \in Z : x - y + y - z = p.q'''$
Or $x - y + y - z = p.q + p.q'$, ou $x - z = p(q + q')$
Donc il suffit d prendre $q''' = q'' = p + q' \in Z$ pour avoir $x - z = p.q''$ avec $q'' \in Z$ et $x \equiv z$ (modulo P).
Ce qui prouve que $\equiv$ est transitive dans Z

d) Classe d'équivalence

(1) Définition

Soit R une relation d'équivalence définie dans $E \neq \emptyset$ et soit $a \in E$, on appelle classe d'équivalence de a noté Cl(a) ou $\dot{a}$ l'ensemble des éléments $x \in E$ qui sont équivalents à a.

i.e. Cl (a) = $\dot{a} = \{D' \in E : aRx\}$

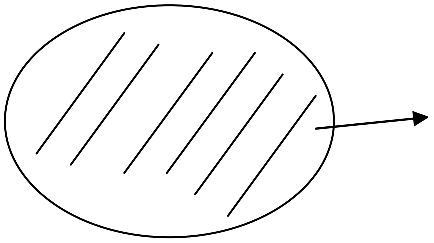
$= \{x \in E: a \equiv x \text{ (modulo R)}\}$

Exemples

La relation : « // » est une relation d'équivalence dans D.

Soit $D \in D$, Cl (D) = $\{D' \in D: D \,//\, D'\}$

Cl (D) s'appelle direction de la droite D.



(2) Propriétés

Soit R une relation d'équation définie dans $E \neq \emptyset$

P$_1$. $\forall a \in E$, $Cl(a) \neq \emptyset$

En effet, $\forall a \in E$, on a : a R a (R est réflexive) or a R a $\Longrightarrow a \in \dot{a}$ et $\dot{a} \neq \emptyset$

(L'élément a est dit représentant de la classe$\dot{a}$).

P$_2$. Si $a' \in$ Cl (a), alors Cl (a) = Cl(a')

En effet : soit $x \in Cl(a)$, il faut montrer que $x \in Cl(a')$

Par hypothèse : $a' \in Cl(a)$ et $x \in Cl(a)$

$\Longrightarrow$a R a' et a R x

$\Longrightarrow$a' Ra et a R x (R symétrique)

$\Longrightarrow$a' R x (R est transitive)

$\Longrightarrow x \in$ Cl (a')

Donc, on vient de montrer que $x \in Cl(a) \Longrightarrow x \in Cl(a')$

Soit $cl(a) \subset Cl(a')$

De même on établit que $Cl(a') \subset Cl(a)$, d'où l'égalité.

P$_3$. Deux classes distinctes sont disjointes.

Démonstration par contraposition

Montrons que si deux classes ne sont pas disjointes alors elles sont confondues.

Soit $\dot{a}$ et $\dot{b}$ deux classes d'équivalence modulo R ? Supposons $\exists\, x \in E : x \in \dot{a} \cap \dot{b}$

$\Longrightarrow x \in \dot{a}$ et $x \in \dot{b}$

$\Longrightarrow \dot{x} = \dot{a}$ et $\dot{x} = \dot{b}$ (d'après P$_2$)

$\Longrightarrow \dot{a} = \dot{b}$

(3) Théorème

Etant donné une relation d'équivalence R définie dans $E \neq \emptyset$, l'ensemble des classes d'équivalence modulo R forme une partition de E et réciproquement.

C'est-à-dire : toute partition de E définit une relation d'équivalence dans E.

Démonstration

3) $\Longrightarrow$) L'ensemble des classes d'équivalence modulo R est une partition de E

En effet, d'après P_1 et P_3, on a :

i. $\forall$ a $\in$ E : Cl(a) $\neq \emptyset$

ii. $\forall$ a,b $\in$ E : si $\dot{a} \neq \dot{b}$, alors $\dot{a} \cap \dot{b} = \emptyset$

Il faut alors montrer que l'union des classes d'équivalence modulo R donne E. ce qi est trivial, puisque tout élément a de appartient à au moins une classe d'équivalence (celle dont il est représentant) et à une seule d'après P_2

Donc l'union des classes d'équivalence modulo R dans E

4) $\Longleftarrow$ il faut montrer que toute partition de E définie une relation d'équivalence dans E

Soit P une partition de E, définissons une relation R dans E par :
$\forall$a, b $\in$ E : a R b ssi $\exists$ x $\in$ P : a $\in$ X et b $\in$ X
i.e. deux éléments a et b de E sont en relation R ssi a et b appartiennent à un même élément de P. Il faut montrer aux exercices que R ainsi définie dans E est une relation d'équivalence

Conclusion

La donnée d'une relation d'équivalence R dans E $\neq \emptyset$ est logiquement équivalente à la donnée d'une partition de E

(4) Ensemble quotient

(a) Définition

Soit R une relation d'équivalence dans E $\neq \emptyset$ on appelle ensemble quotient de E sur R l'ensemble des classes d'équivalence de E modulo R.

On note par $E/_R$ (lire E sur R)

Ainsi $E/_R = \{\dot{a}; a \in E\}$

$\forall$a $\in$ E : $\dot{a}$ $\in$ E, alors $\dot{a} \in P_{(E)}$ avec a $\in$ $\dot{a}$

De même, $\forall$ a $\in$ E : $\dot{a} \in E/_R$, alors $E/_R \in P_{(E)}$

Donc $E/_R \in \mathcal{P}_{\mathcal{P}_{(E)}}$

(b) Exemple

On a vu que la relation x ≡ y (modulo P) $\Leftrightarrow \exists$ k $\in \mathbb{Z}$: x – y = kp, k $\in \mathbb{Z}$ et p $\in \mathbb{N}^*$ est une relation d'équivalence dans $\mathbb{Z}$.

Soit x $\in \mathbb{Z}$, alors : Cl(x) = $\dot{x} = \{y \in \mathbb{Z} : x \equiv y \text{ (modulo P)}\}$

$$= \{y \in \mathbb{Z} : \exists k \in \mathbb{Z} : y - x = kp\}$$
$$= \{y \in \mathbb{Z} : \exists k \in \mathbb{Z} : y = x - kp\}$$
$$= \{y = x - kp : k \in \mathbb{Z}\}$$
$$= \{y = x + p.k : k \in \mathbb{Z}\}$$

Remarquer que $\forall$ x $\in \mathbb{Z}$, $\exists$ r, q $\in \mathbb{Z}$ unique tel que : x = p.q + r (avec $0 \leq r \leq p$), d'après la division euclidienne dans $\mathbb{Z}$

Alors : $x \doteq \dot{r}$ avec $r = \{0,1,2,3, \ldots (p-1)\}$ car x = pq + r $\Leftrightarrow$ x – r = p.q $\Leftrightarrow$ x ≡ r (modulo P)

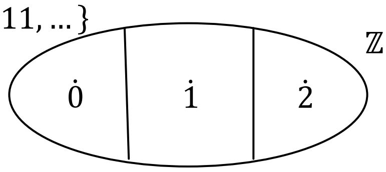
Alors l'ensemble quotient de $\mathbb{Z}$ par cette relation de congruence modulo P se note :

$$\mathbb{Z}/P\mathbb{Z} = \left\{\dot{0}, \dot{1}, \dot{2}, \ldots, \dot{\widehat{P-1}}\right\}$$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Cas particulier : prendre p = 3
Dans ce cas : $x \equiv y$ (modulo 3) $\Leftrightarrow \exists\, k \in \mathbb{Z} : x - y = 3k$
Alors $\mathbb{Z}/_{3}\,\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}\}$ avec (*) : $\dot{0} = \{\dots, -9\,, -6\,, -3\,,\ 0\,,\ 3\,, 6\,, 9, \dots\}$ensemble des multiples de 3
$-9 \equiv 0$ (modulo 3) car $\exists\, k = -3 : -9 - 0 = -3\,.\,3$
$-9 \equiv 9$ (modulo 3) car $\exists\, k = -6 : -9 - 9 = 3(-6)$
$\dot{1}$ = ensemble des multiples de 3 augmentés de 1
i.e. $\dot{1} = \{\dots, . -8\,, -5\,, -2\,, 1\,, 4\,, 7\,, 10, \dots\}$
$\dot{2} = \{\dots, -7\,, -4\,, -1\,, 2\,, 5\,, 8\,, 11, \dots\}$

Alors $\{\dot{0}, \dot{1}, \dot{2}\}$ est une partition de $\mathbb{Z}$



(5) Relation d'ordre

(a) Définition

Une relation binaire R défini dans $E \neq \emptyset$ est dit relation d'ordre si elle est à la fois réflexive, antisymétrique et transitive. Si R est une relation d'ordre définie dans E, alors au leu de x R y, on notera : « $x < y$ » (lire x précède y ou x est avant y) et sa réciproque se notera $y > x$ (lire y est après x)
Ainsi, un ensemble $E \neq \emptyset$, muni d'une relation d'ordre R dite un ensemble ordonné par R, ou tout simplement que E possède la structure d'ordre.

Exemples

i. La relation « $\leq$ »défini dans $\mathbb{N}$ ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$) est une relation d'ordre.
ii. La relation « $\subset$ » définie dans $P_{(E)}$ est une relation d'ordre.
iii. La relation / (divise) définie dans $\mathbb{N}^*$ par $\forall\, x,y \in \mathbb{N}^* : y = k.x$ est une relation d'ordre.

En effet, (*) $\forall\, x \in \mathbb{N}^* : x/x$? oui car $\exists\, k = 1 : x = 1.x$ et / est réflexive

(**) $\forall x, y \in \mathbb{N}^*$: si x/ y et y/x alors $x = y$
$x/y \Longrightarrow \exists\, k \in \mathbb{N}^* : y = k.x$ (i)
et $y/x \Longrightarrow \exists\, k' \in \mathbb{N}^* : x = k'y$ (ii)
(i) dans (ii) $\Longrightarrow x = k'(kx) = (k'.k)x$
Donc $x = (k'.k)x \Leftrightarrow k.k' = 1 \Leftrightarrow k = k' = 1$
Si $\left.\begin{matrix} k = 1, (i) y = x \\ k' = 1, (ii) x = y \end{matrix}\right| et\ /\ est\ \ antisymétrique.$

(***) $\forall\, x, y, z \in \mathbb{N}^*$ si x/y et $y/z \Longrightarrow x/z$
$x/y \Longrightarrow - \exists\, k \in \mathbb{N}^* : y = kx$ (i)
et $y/z \Longrightarrow \exists\, k' \in \mathbb{N}^* : z = k'y$ (ii)
(i) dans (ii) $\Longrightarrow z = k'.(k.x)$
$= (k'.k)\,.\,x$
i.e. $\exists\, k'' = k'.k \in \mathbb{N}^* : z = k''.\,x$, soit x/ z
Et / est transitive

Remarque
Si $x< y$ (x strictement inférieur à y) alors $x \leq y$ avec $x \neq y$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

(b) Ordre total et ordre partiel.

b_1 Soit R une relation d'ordre définie dans $E \neq \emptyset$, alors R est dite d'ordre total si :
$\forall$ x,y $\in$ E : on a $x < y$ ou $y < x$.
i.e. deux éléments quelconque de E sont toujours comparable par la relation d'ordre < si E est donné par une relation d'ordre ***total***, alors on dit que E est totalement ordonné.
Si il existe un couple (x,y) $\in$ E x E tel que x et y ne soient pas comparés par la relation <, on dit qu < est d'ordre partiel et un ensemble muni d'une relation d'ordre partiel est dit partiellement ordonné.

b_2 . ***Exemple***

1. La relation « $\leq$ » dans $\mathbb{N}$ est une relation d'ordre total car $\forall$ x, y $\in \mathbb{N}$, on a $x \leq y$ ou $y \leq x$.
   Par exemple, pour 3,5 $\in \mathbb{N}$ on a, $3 \leq 5$ et pour 6 et 2, on a $6 \leq 2$ ou $2 \leq 6$.
   N.B $x < y$ (lire x est inférieur à y) signifie que $x \leq y$ et $x \neq y$.
2. La relation « $\subset$ » dans $P_{(E)}$ avec $E \neq \emptyset$ est une relation d'ordre partiel. Car $\exists$ A, B $\in P_{(E)}$ tel que $A \not\subset B$ et $B \not\subset A$
   Par exemple : soit E = {a,b} alors $P_{(E)} = \{\emptyset, \{a\}, \{b\}, E\}$
   A = {a} , B = {b} $\in P_{(E)}$ tel que $\{a\} \not\subset \{b\}$ et $\{b\} \not\subset \{a\}$.
3. La relation divise « / » définie dans $\mathbb{N}^*$ est une relation d'ordre partiel car $\exists$ 2,3 $\in \mathbb{N}^*$ tel que 2 ne divise pas 3 et 3 ne divise pas 2

(c) Intervalles

a. Soit E un ensemble totalement ordonné par <, on appelle segment ou intervalle fermé noté $[a,b] = \{x \in E : a < x < b\}$.

L'intervalle ouvert noté : $]a, b[= \{x \in E : a < x < b$ avec $a \neq x$ et $b \neq x\}$
i.e. $]a, b[= [a, b] - \{a, b\}$
$[a, b[= \{x \in E : a < x < b$ avec $x \neq b\}$ appelé intervalle semi – ouvert à droite.
$]a, b] = \{x \in E : a < x < b$ avec $a \neq x\}$ appelé intervalle semi – ouvert a gauche.
$[a, \longrightarrow[= \{x \in E : a < x\}$ appelé section finissante fermée.
$]\longleftarrow , b] = \{x \in E : x < b\}$ appelé section commençante ouvert.
Dans $\mathbb{R}$ ordonné par $\leq$: $]a,b[= \{x \in \mathbb{R} : a \leq x \leq b$ avec $a \neq x$ et $x \neq b\}$
$= \{x \in \mathbb{R} : a < x < b\}$

b. Soit E un ensemble totalement ordonné par <. on appelle successeur de a $\in$ E tout élément a $\in$ E tel que $]a, a'[= \emptyset$, et prédécesseur de a tout élément a $\in$ E tel que : $]a, a[= \emptyset$
   Ces éléments s'il existe sont *toujours* unique.

c. Exemples

Dans $\mathbb{Z}$ ordonné par $\leq$, le successeur de -10 est -9 car $]-10 , -9[= \emptyset$
-11 est le prédécesseur de -10 car $]-11, -10[= \emptyset$
Le successeur de 4 est 5 car $]4,5[= \emptyset$
$\mathbb{R}$ et $\mathbb{Q}$ n'ont pas de successeur ni de prédecesseur.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

e) Eléments remarquable d'un ensemble ordonné ou d'une partie d'un ensemble ordonné.

(1) Définition

Soit $(E, \leq)$ un ensemble ordonné.
Définition 1 :
Un élément $M \in E$ et dit maximal si $x \in E$ et $x \geq M \Longrightarrow x = M$.

Définition 2 :
Un élément $m \in E$ est dit minimal si $x \in E$ et $x \leq m \Longrightarrow x = m$.

Remarque
R_1 Ces éléments n'existe pas toujours.
R_2 Un ensemble peut avoir plusieurs éléments maximaux (minimaux).

Exemple :
$\mathbb{N}^{**} = \mathbb{N} - \{0,1\}$, un ensemble ordonné par / (divise), on a $\leq y \Leftrightarrow x/y$
Soit un élément minimale de $\mathbb{N}^{**}$. i.e. si $x \in \mathbb{N}^{**}$: x/m alors $x = m$ à condition que m soit premier.

Définition 3 :
Un élément $g \in E$ est dit plus grand élément de E si $\forall x \in E : x \leq g$.
Un élément $p \in E$ est dit plus petit élément de E si $\forall x \in E ; p \leq x$.

Exemple :

i. 0 est le plus petit élément de $(\mathbb{N}, \leq)$ car $0 \leq x, \forall x \in \mathbb{N}$
ii. 1 est le plus petit élément de $(\mathbb{N}^*, \backslash)$ car $1\backslash x, \forall x \in \mathbb{N}^*$
iii. $\emptyset$ est le plus petit élément de $\left(\mathcal{P}_{(E)}, \subset\right)$car $\emptyset \subset A, \forall A \in P_{(E)}$
iv. E est le plus grand élément de $\left(\mathcal{P}_{(E)}, \subset\right)$ car $\forall A \in P_{(E)}, A \subset E$

Proposition 1
Si un ensemble ordonné E admet un plus grand (respectivement plus petit) élément, alors cet élément est unique.

Preuve
Soit $(E, \leq)$ un ensemble. Supposons qu'il existe g et g' plus grand élément de E,
Montrons que g = g'.
Mais g plus grand élément de E $\Longrightarrow \forall x \in E : x \leq g$ (i)
g' plus grand élément de E $\Longrightarrow \forall x \in E : x \leq g'$ (ii)

$$\left.\begin{array}{l}\text{puisque } g \in E, \text{d'après (ii)} g \leq g' \\ \text{et aussi } g' \in E, \text{d'après (i)} g' \leq g\end{array}\right\} \longrightarrow g = g' \text{car } \leq \text{ est antisymétrique.}$$

Proposition 2
Si un ensemble ordonné admet un plus grand élément alors cet élément est unique et c'est le seul élément maximal.

Preuve
Soit $(E, \leq)$ un ensemble ordonné. Soit $g \in E$ un plus grand élément de E

i.e. $\forall x \in E : x \leq g$ (i)
Soit $M \in E$ un élément maximal d'après (i)
Donc $M \leq g$ et d'après la définition de M on a $g = M$.

(2) Majorant – minorant d'une partie d'un ensemble ordonné.

(a) Définition

a. Soit E un ensemble ordonné par $\leq$ et A une partie de E, un élément $\alpha \in E$ est dit Majorant de A si $\forall x \in A$, on a : $x \leq \propto$
   - Si une partie A de E admet un majorant, alors on dit que A est une partie majorée de E.
   - Soit $\propto \in E$ un majorant de $A \subset E$, alors $\forall \propto' \in E$ avec $\propto' \geq \propto$, est un majorant de A dans E.

Exemples :
$(\mathbb{R}, \leq)$: soit $A =]-\infty ; 2[\subset \mathbb{R}$ quelques majorants de A sont : 2, 3,4,…
Si M est l'ensemble des majorants de A , alors $M = [2 , + \infty[$
Remarquez ici que 2 est un majorant de A car $\forall x \in A$: on a $x \leq 2$ et 3 est majorant de A car $3 \geq 2$.

b. Un élément $\beta \in E$ est dit minorant de $A \subset E$ si $\forall x \in A$, $\beta \leq x$.
   - Si une partie A de E admet un minorant, alors A est dit partie minoré de E.
   - Soit $\beta \in E$ un minorant, alors $\forall \beta' \in E$ tel que $\beta' \leq \beta$, β' est aussi un minorant de E.
      i. ***Exemple :***
         $B =]5, +\infty[\subset (\mathbb{R}, \leq)$
         5 est un minorant de B dans $\mathbb{R}$ car $\forall b \in B : 5 \leq b$
         4 est un minorant de B dans $\mathbb{R}$ car $4 \leq 5$.
         Si m est l'ensemble des minorants de B ; alors $m =]-\infty, 5]$
         Toute partie A de E majorée et minorée est dit bornée.
         i.e. $A \subset E$ est dite bornée si $\exists \propto, \beta \in E : \forall x \in A ; \beta \leq x \leq \alpha$
      ii. ***Exemple :***
         Tout intervalle de $\mathbb{R}$ est une partie bornée de $]2, 4[\subset \mathbb{R}$

(b) Bornes inférieures et supérieures d'une partie d'un ensemble ordonné

Soit $(E, \leq)$ un ensemble ordonné et $A \subset E$.

a. *Un élément $S \in E$ est dit borne supérieure de A dans E si les conditions suivantes sont vérifiées :*
   i. S soit un majorant de A dans E.
   ii. $\forall \propto \in E$ un autre majorant de A dans E, alors on a : $S \leq \alpha$

i.e. S est le plus petit des majorants de A dans E.

b. *Un élément $s \in E$ est dit borne inférieur de $A \subset E$ si les conditions suivantes sont vérifiées :*
   i. S soit un minorant de A dans E.
   ii. $\forall \beta \in E$ un autre minorant de A dans E, on a : $\beta \leq s$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

i.e. s es le plus grand des minorants de A dans E.

Il faut remarquer que :
1* Ces éléments n'existent pas toujours.
2* si ces éléments existent, ils sont uniques.

c. Notations

La borne supérieure d'une partie A de E se note : Sup_E^A (lire sup A dans E).
La borne inférieure d'une partie A de E se note : Inf_E^A (lire inf A dans E)
Si $\mathrm{Sup}_E^A \in A$, alors on peut aussi l'appeler le plus grand élément de A.

Exemple :

i. Soit E un ensemble totalement ordonné par < . soit a, b ∈ E avec a < b alors
inf {a,b} = a et sup {a,b} = b
ii. Soit $P_{(E)}$ ordonné par l'inclusion (⊂) : $\inf\{A,B\} = A \cap B$ *et* $\sup\{A,B\} = A \cup B$
$\forall A, B \in P_{(E)}$
iii. Soit ℕ* ordonné par la relation divise (/)
∀ x, y ∈ ℕ* : inf{x,y} = d.d.c (x,y) = x ⋀ y (lire x section y)
Sup {x,y} = p.m.c (x,y) = x ⋁y (x union y)

Exemples :

x = 15 D 15 = {1,3,5,15}
y = 20 D 20 ={1,2,4,5,10,20}
D 15 ∩ D 20 = {1,5} ⟹ d.d.c (15, 20) = 5
$M_{15}^* = \{15, 30, 45, 60, 75, 80, 105, 120,\dots\}$
$M_{20}^* = \{20, 40, 60, 80, 100, 120, \dots\}$
$M_{15}^* \cap M_{20}^* = \{60, 120,\dots\} \Longrightarrow$ p.m.c (15, 20) = 60
Sup {15, 20} = 60

Ou $\begin{array}{r||l} 15 & 3 \\ 5 & 5 \\ 1 & \end{array}$ $\begin{array}{r||l} 20 & 2 \\ 10 & 2 \\ 5 & 5 \\ 1 & \end{array}$

15 = 3 x 5 20 = 2² x 5
p.p.m.c (15, 20) = 3 x 5 x 2² = 60.

iv. Soit $A \subset \mathbb{R}$ avec $A = \{x \in \mathbb{R} : x^2 < 2\}$
$\mathrm{Sup}_{\mathbb{R}}^A = \sqrt{2}$, $\mathrm{Inf}_R^A = -\sqrt{2}$
Si x > 0 ; |x| = x et (i) $x < \sqrt{2}$.

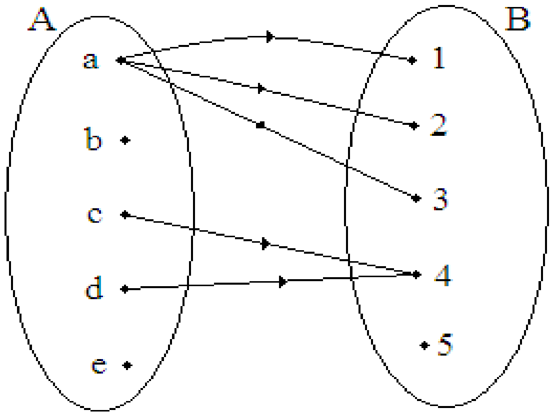
B. APPLICATIONS

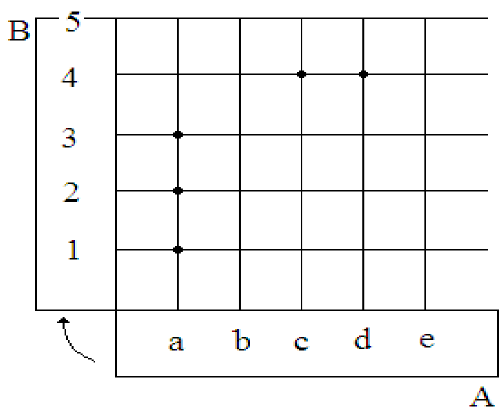
1. Correspondance entre ensembles A et B

a) Définition

Soit R, une relation binaire entre éléments x et y avec x ∈ A et y ∈ B dont G est le graphe. On appelle correspondance ente ensembles A et B, le triplet (A, B, G) où A est l'ensemble de départ ou source de la correspondance, B est l'ensemble d'arrivée ou But de la correspondance et G est le graphe de la correspondance.

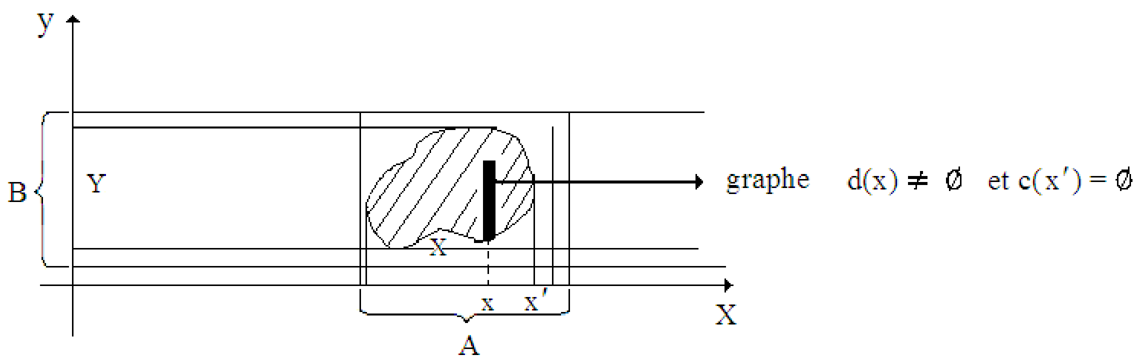
b) Exemples





(*) Soit x ∈ A, on appelle Coupe suivant x, notée C(x) l'ensemble des éléments y ∈ B tels que les couples (x, y) ∈ G,
ie. C(x) = {y ∈ B : (x, y) ∈ G}.
On appelle coupe suivant l'élément y ∈ B, l'ensemble des éléments x ∈ A tels que (x, y) ∈ G.
ie. C(y) = {x ∈ A : (x, y) ∈ G}.
Pour notre exemple : C(a) = {1, 2, 3}, C(b) = ∅.
C(1) = {a} et C(4) = {c, d}.
C(5) = ∅.

(**) L'ensemble de définition de la correspondance (A, B, G) est l'ensemble X ⊂ A des éléments x ∈ A tels que les couples suivant x ne soient pas vides.
ie. X = {x ∈ A : ∃ y ∈ B : (x, y) ∈ G}.
L'ensemble des valeurs de la correspondance (A, B, G) est l'ensemble Y ⊂ B tels que les coupes suivant y ∈ B ne soient pas vides.
ie. Y = {y ∈ B : ∃ x ∈ A : (x, y) ∈ G}.
Pour notre exemple : X = {a, c, d} et Y = {1, 2, 3, 4}.
Ainsi ∀ x ∈ X, on dit que la correspondance est définie et tout y ∈ Y est une valeur prise par la correspondance.



2. Correspondance fonctionnelle ou fonction

a) Définition

Une correspondance (A, B, G) est dite fonctionnelle par rapport à la deuxième variable y si pour tout élément $x \in A$, la coupe suivant x est un ensemble qui possède au *plus* un élément.

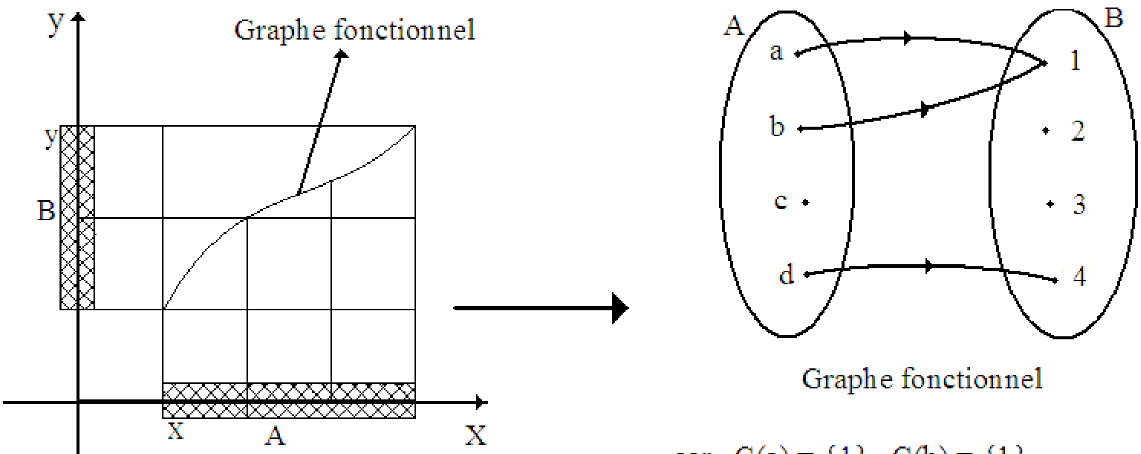
ie. $\forall x \in A, \forall y, y' \in B\ [(x, y) \in G \text{ et } (x, y') \in G \Leftrightarrow y = y']$ (i).

Si x → y, x → y' alors y = y', on peut encore traduire (i) par : $\forall x \in A, !y \in B : (x, y) \in G$.

(Le symbole ! se lit : il existe au plus).

Ainsi une telle relation s'appelle fonction définie dans A à valeurs dans B et l'expression (i) montre que le graphe G est fonctionnel.

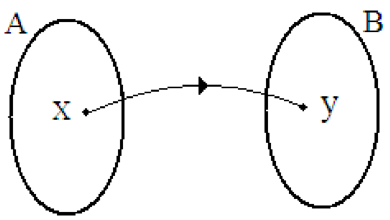
Exemples :



car $C(a) = \{1\}$, $C(b) = \{1\}$

$C(c) = \emptyset$ et $C(d) = \{4\}$

(*) L'unique élément $y \in B$ associé à x par une fonction, s'il existe, est appelé image de $x \in A$ par la fonction donnée ou valeur de la fonction au point x.



(**) Le sous-ensemble $D \subset A$ des éléments $x \in A$ ayant effectivement des images dans B s'appelle l'ensemble de définition ou domaine de définition d'une fonction.

$D = \{x \in A : \exists! y \in B : (x, y) \in G\}$. ($\exists!$ Se lit : « il existe un et un seul »).

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

b) Notation

Si on désigne par une lettre f ou g ou h une fonction de A vers B, on écrit symboliquement :

$f : A \to B$ ou $A \xrightarrow{f} B$

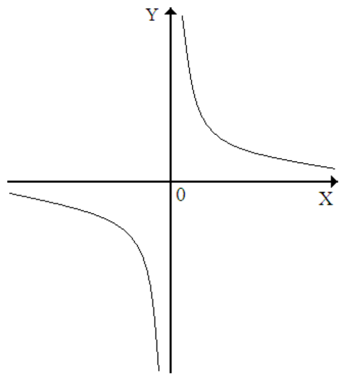
Alors l'unique élément $y \in B$ associé à x par la fonction s'il existe, est noté : f(x) (lire f de x ou image de x par la fonction f).

On écrit $f : A \to B$
$x \rightsquigarrow y = f(x)$

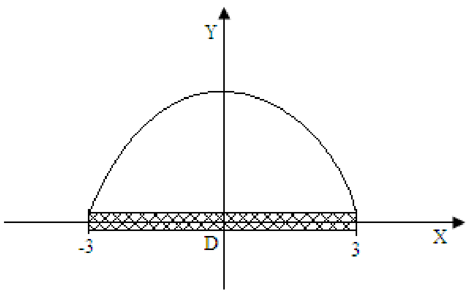
N.B. (1) pour qu'une fonction soit définir, il faut donc préciser son ensemble de départ A, son ensemble d'arrivée B et une loi liant tout $x \in A$ à l'élément associé $y \in B$.

Exemples :

i. $f : R \to R$
$x \rightsquigarrow f(x) = \frac{1}{x}$
D = R*.



ii. $f : R \to R$
$x \rightsquigarrow f(x) = \sqrt{9 - x^2}$
D= [-3, 3]



(2) Le graphe d'une fonction f de A vers B se note Gf avec $Gf = \{(x, y) \in A \times B : y = f(x)\}$
$= \{[x, f(x)] : x \in A\}$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

c) Image directe, Image réciproque d'une partie

(1) *Image Directe*

(a) Définition

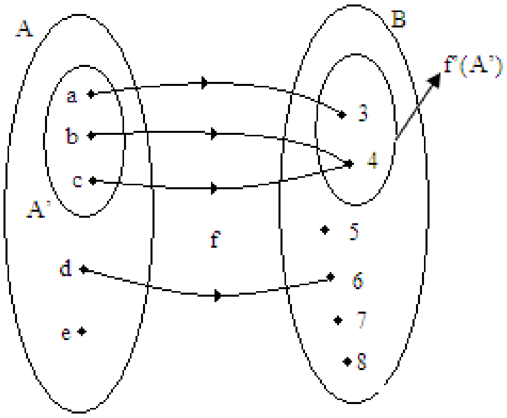
Soit : A $\to$ B

x ⇝ f(x), une fonction et A'$\subset$ A. On appelle image directe de la partie A de E par la fonction f, l'ensemble des éléments y $\in$ B images d'au moins un élément de A'.

On la note par $f^{\bullet}$(A') (lire f point de A').

Ainsi $f^{\bullet}(A') = \{y \in B : \exists x \in A' : y = f(x)\}$

ie. [$f^{\bullet}(A') \subset B$]



- Si A' = {b, d}, alors $f^{\bullet}$(A') = {4, 6}.
- Si A' = {a, b, c}, alors $f^{\bullet}$(A') = {3, 4}.

(b) Remarque

Soit f : A $\to$ B, une fonction

- Si $f^{\bullet}(\phi) = \phi$.
- Si A' = {a}, alors $f^{\bullet}$(A') a au plus un élément.

(c) Propriétés

Soit f : A $\to$ B, une fonction

- Si A'$\subset$ A'' $\subset$ A, alors $f^{\bullet}(A') \subset f^{\bullet}(A'')$

En effet soit Z $\in f^{\bullet}$(A'), montrons que Z $\in f^{\bullet}$(A'')

$Z \in f^{\bullet}(A') \Rightarrow \exists x \in A' : f(x) = Z$

$\Rightarrow \exists x \in A''$ (car A' $\subset$ A'') : f(x) = Z

$\Rightarrow \exists z \in f^{\bullet}(A'')$.

- S A' $\subset$ A, A'' $\subset$ A, alors $f^{\bullet}(A' \cap A'') \subset f^{\bullet}(A') \cap f^{\bullet}(A'')$.

En effet: Soit Z $\in f^{\bullet}(A' \cap A'')$, montrons que Z $\in f^{\bullet}(A') \cap f^{\bullet}(A'')$.

Mais $Z \in f^{\bullet}(A' \cap A'') \Rightarrow \exists x \in A' \cap A'' : f(x) = z$

$\Rightarrow \exists x \in A' : f(x) = z$ donc $z \in f^{\bullet}(A')$

et $\exists x \in A'' : f(x) = z$, donc $z \in f^{\bullet}(A'')$.

D'où Z $\in f^{\bullet}$(A') et Z $\in f^{\bullet}$(A''). ie. Z $\in f^{\bullet}(A') \subset f^{\bullet}(A'')$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

- Si A'$\subset$ A, A'' $\subset$ A, alors $f^{\bullet}$(A' $\cup$ A'') = $f^{\bullet}$(A') $\cup$ $f^{\bullet}$(A'')

A montrer aux exercices.

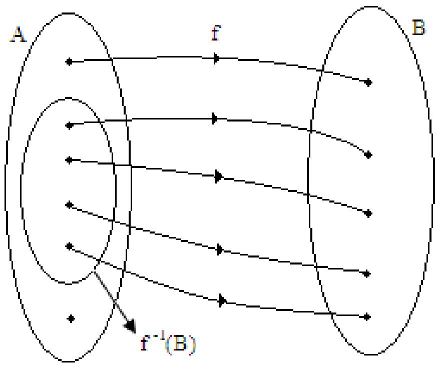
(2) Images réciproques

(a) Définition

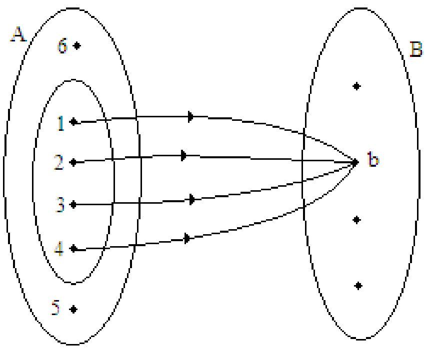
Soit f : A $\to$ B

x $\rightsquigarrow$ f(x), une fonction, et B' $\subset$ B, on appelle image réciproque d'une partie B' de B par la fonction f l'ensemble des éléments x $\in$ A tels que f(x) $\in$ B'. On la note par f^{-1} (B') (lire f moins un de B').

Ainsi f^{-1} (B') = {x $\subset$ A : f(x) $\subset$ B'} ie. f^{-1} (B') $\subset$ A.



Il faut remarquer que si B' = {y} ; alors f^{-1} = ({y}) peut se noter f^{-1} (y) et peut comporter plusieurs éléments.



Par exemple : f^{-1} (B) = {1, 2, 3, 4}.

(b) Propriétés

Soit f : A $\to$B, une fonction

- Si B' $\subset$ B'' $\subset$ B, alors f^{-1} (B') $\subset$ f^{-1} (B'')

En effet : Soit x $\in$ f^{-1} (B') $\Rightarrow$ f(x) $\in$ B'

$\Rightarrow$ f(x) $\in$ B''

Car B' $\subset$ B'' $\Rightarrow$ x $\in$ f^{-1} (B'').

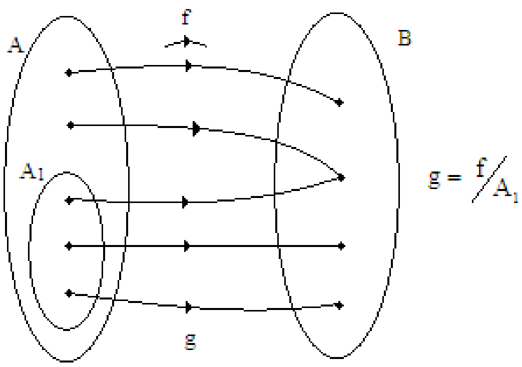
- Si B' $\subset$ B et B'' $\subset$ A alors $\begin{cases} f^{-1}(B' \cap B'') = f^{-1}(B') \cap f^{-1}(B'') \\ f^{-1}(B' \cup B'') = f^{-1}(B') \cup f^{-1}(B'') \end{cases}$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

(c) Restriction, Prolongement

Soit A, une ensemble non vide et soient $A_1 \subset A$ et A_2 un ensemble contenant A et $f : A \to B$, une fonction.

- La nouvelle fonction g de A1 vers B définie par $\forall x \in A_1$, $f(x) = g(x)$ s'appelle la restriction de f à A_1 et se note $f/_{A_1}$ = gr. $f/_{A_1}$ se lit f restreinte à A_1.



$A_1 \to B$
$x \rightsquigarrow g(x) = f(x)$

- Toute fonction h de A_2 vers B dont la restriction à A est la fonction f s'appelle prolongement de f à A_2.

C'est-à-dire $h : A_2 \to B$ est un prolongement de $f : A \to B$ si $h/_A = f$.

Il faut remarquer que la restriction d'une fonction est unique alors que plusieurs prolongements sont possibles.

Exemples :

$f : N \to N$

$$x \rightsquigarrow f(x) = \begin{cases} o \text{ si } n \text{ est pair} \\ 1 \text{ si } n \text{ est impair} \end{cases}$$

Soit P l'ensemble de nombres naturels pairs et I l'ensemble de nombres naturels impairs.

$g = f/_p : P \to N$

$n \rightsquigarrow f/_p(n) = 0$

$i = f/_I : I \to N$

$n \rightsquigarrow f/_I(n) = 1,$

- f est le prolongement de g à N, car

$g : P \to N$

$n \rightsquigarrow g(n) = 0$, d'où $g = f/_p$, en prolongeant g à N, on peut avoir f.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

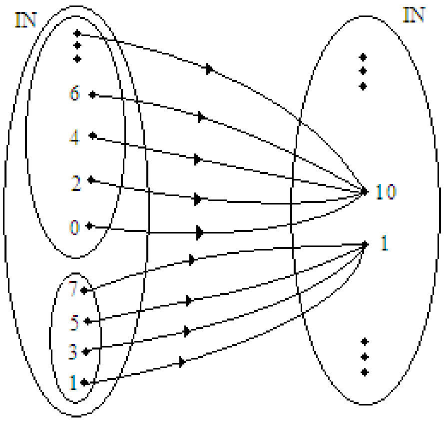
- On peut encore prolonger g à N en posant :

$k : N \rightarrow N$

$$x \rightsquigarrow k(x) = \begin{cases} 0 \text{ si n est pair} \\ 5 \text{ si n est impair} \end{cases}$$

Car ${}^{k}\!/\!{}_{p}$: $P \rightarrow N$.

$n \rightsquigarrow p(n) = 0$.



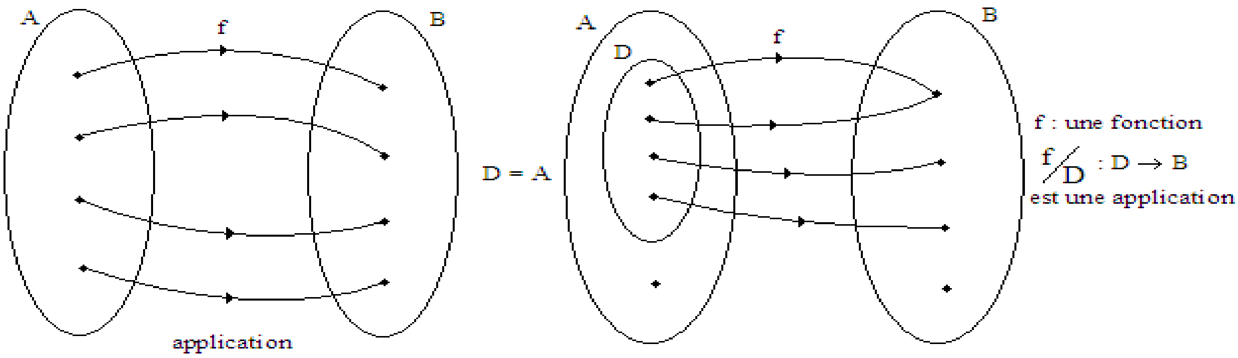
3. Applications

a) Définition

Soient A et B, deux ensembles non vides. On appelle application de A vers B toute fonction f de A vers B toute fonction f de A vers B (toute fonction f de A vers B) dont l'ensemble de définition est A.

Soit $f : A \rightarrow B$ une fonction dont $D \subset A$ est domaine de définition, alors la restriction de f à D est une application de D vers B.

D'où $f : A \rightarrow B$ est une application si $\forall x \in A, \exists y \in B : f(x) = y$.



Les applications de A vers B constituant un ensemble noté B^A ou App (A, B) c'est-à-dire B^A ou App (A, B) = {f : A $\rightarrow$ B : f est une app •}.

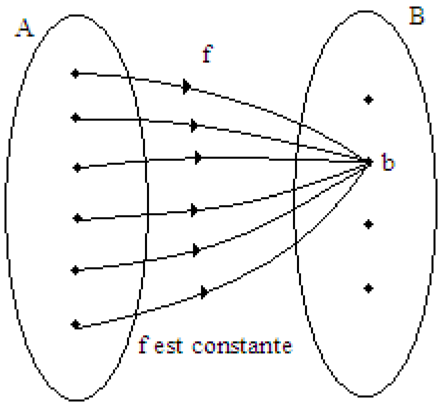
Ainsi $f \in B^A \Rightarrow f : A \rightarrow B$, est une application.

b) Exemples

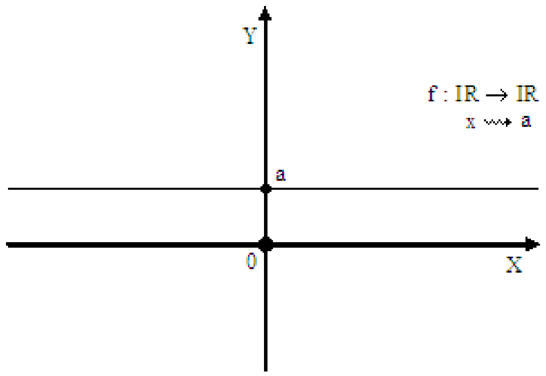
- *L'application constante*

f : A $\to$ B est constante ssi $\exists b \in B : \forall x \in A : f(x) = b$

1.



2.



- *L'application identique* sur l'ensemble A est l'application notée 1_A ou $id_A : A \to A$ est définie par $\forall x \in A : 1_A(x) = X$. C'est-à-dire :

$1_A : A \to A$

$x \rightsquigarrow 1_A(x) = x.$

- La fonction caractéristique d'une *Partie A de E* avec E ≠ 0 est l'application notée φ_A et définie par :

$\varphi_A : E \to \{0, 1\}$

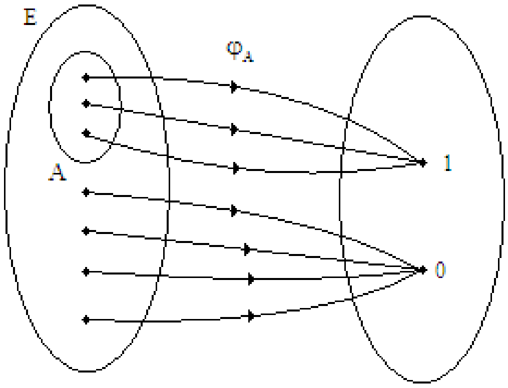
$$x \rightsquigarrow \varphi_A(x) = \begin{cases} 1 \text{ si } x \in A \\ 0 \text{ si } x \notin A \end{cases}$$

Donc c'est une application partielle de l'application

$\varphi : E \times \wp_{(E)} \to \{0,1\}$

$$(X, A) \rightsquigarrow \varphi_{(X,A)} = \begin{cases} 1 \text{ si } x \in A \\ 0 \text{ si } x \notin A \end{cases}$$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com



(*) En analyse mathématique, on appelle fonction numérique variable réelle toute application f définie d'une partie $E \subset R$ vers R.

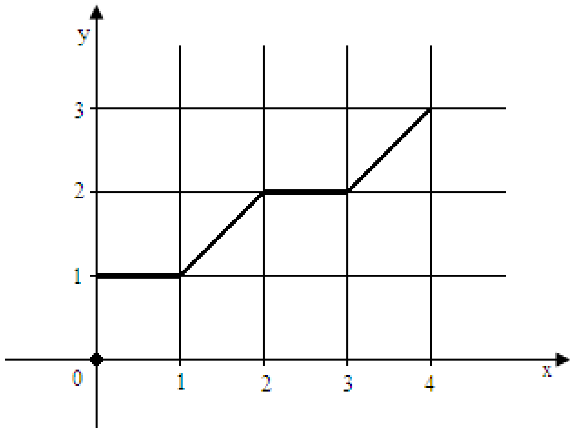
Exemples :
(1) La fonction logarithme Népérienne est notée ln.

$$\text{Avec ln : } \begin{array}{l} R_+^* \to R \\ x \to \ln x, \text{fonction numérique d'une variable réelle.} \end{array}$$

(2) $f : [1,4] \to R$

$$x \rightsquigarrow f(x) = \begin{cases} x \text{ si } 1 \leq x < 2 \\ 2 \text{ si } 2 \leq x \leq 3 \\ x/2 + 1/2 \text{ si } 3 \leq x \leq 4 \end{cases}$$

Son graphe est dessiné ci-dessous.

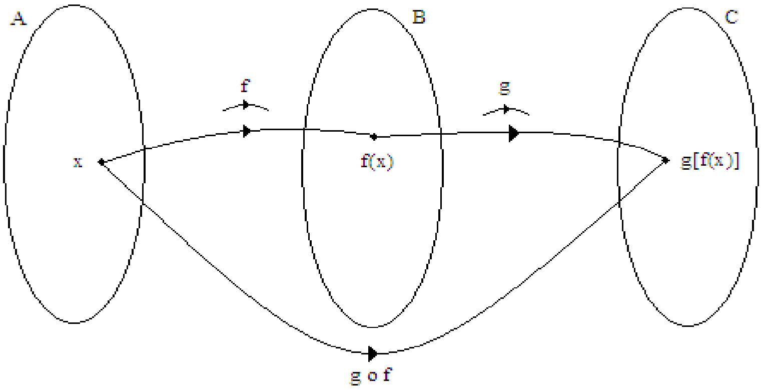


c) La composition des applications

(1) Définition :

Soient f : A → b et g : B → c, deux applications. La composée des applications f et g est l'application h = g o f de A vers C définie par :
∀x ∈ A : h(x) = (g o f)(x) = g[f(x)].

L'application g o f qui se lit g rond f est l'application composée de f suivie de g.



C'est –à dire : g o f : A $\rightarrow$ C

x $\rightsquigarrow$ (g o f)(x) = g[f(x)]

Exemples :

$$\mathbb{R} \xrightarrow{f} \mathbb{R} \xrightarrow{\sin} \mathbb{R}$$

x $\rightsquigarrow$ (x^2 + 4) $\rightsquigarrow$ sin (x^2 + 4)

sinof = sinf

Avec sin f : R $\rightarrow$ R

x $\rightsquigarrow$ sin f(x) = sin(x^2 + 4)

(2) Théorème.

La composition des applications est associative. C'est-à-dire $\boldsymbol{\forall f \in B^A, g \in G^B, h \in D^C}$, on a : (h o g) o d = h o (g o f).

En effet, soit x $\in$ A, posons y = f(x), z = g(y) et t = h(z)

Calculons, $\forall$x $\in$ A : [(h o g) o f(x)] et [h o (g o f)](x).

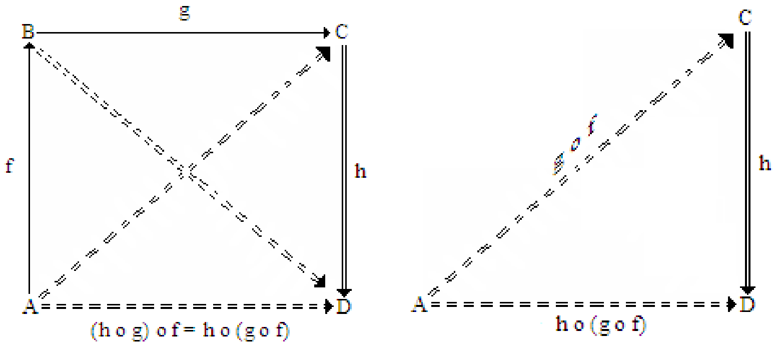
[(h o g) o f](x) = [(h o g)f(x)]
= [(h o g)(y)]
= {h [g(y)]}
= h (z)
= t

Donc [(h o g) o f(x)] = t **(i)**

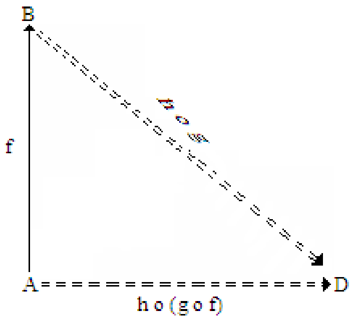
[h o (g o f)(x)] = h(g o f)(x)
= h{g[f(x)]}
= h[g(y)] = h(z) = t

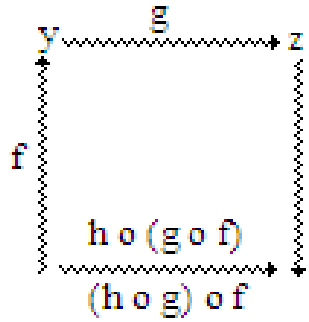
Donc [h o (g o f)](x) = t **(ii)**

D'où **(i)** et **(ii)** $\Rightarrow\forall$x $\in$ A, [(h o g) o f](x) = [h o (g o f)](x) et (h o g) o f = h o (g o f).



Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com





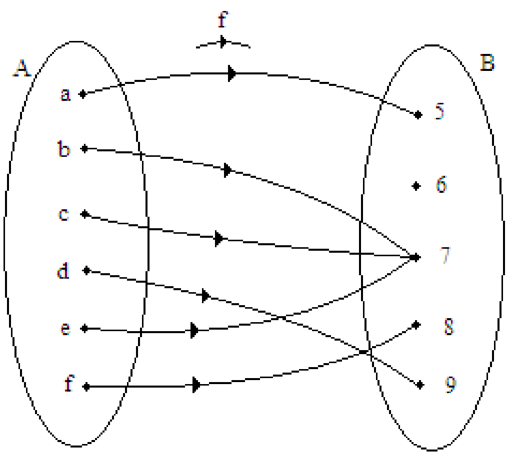
d) Classification des applications.

(1) Introduction

(a) Equation

Soient A et B deux ensembles non vides et $f : A \rightarrow B$, une application.
Soit $y_0 \in B$, on appelle équation la forme propositionnelle $f(x) = Y_0$ **(i).**
Vraie pour certains éléments de A. $x \in A$ est appelé une inconnue de **(i)** et tout élément $x_0 \in f^{-1}(Y_0)$ est appelé solution de **(i)**.
Ainsi, résoudre **(i)**, c'est trouver toutes les valeurs $x_0 \in A$ qui sont éléments de $f^{-1}(Y_0)$, lesquelles valeurs sont appelées solutions de l'équation **(i).**
Si S est l'ensemble des solutions de l'équation $f(x) = Y_0$, alors $S = f^{-1}(Y_0)$.

(b) Exemples



- Soit $Y_0 = 7 \in B$, l'équation $f(x) = 7$ admet pour solution tout élément $x \in A$ tel que $x \in f^{-1}(7)$

Or, $f^{-1}(7) = \{b, c, e\}$, donc $S = f^{-1}(7) = \{b, c, e\}$ est l'ensemble des solutions de l'équation $f(x) = 7$

- Soit $Y_0 = 8 \in B$, l'ensemble des solutions de l'équation $f(x) = 8$ est :

$S = f^{-1}(8) = \{f\}$.

- Soit $Y_0 = 6 \in B$, l'équation $f(x) = 6$ admet pour ensemble des solutions $S = \Phi$ car $\nexists\, x \in A$ tel que $f(x) = 6$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

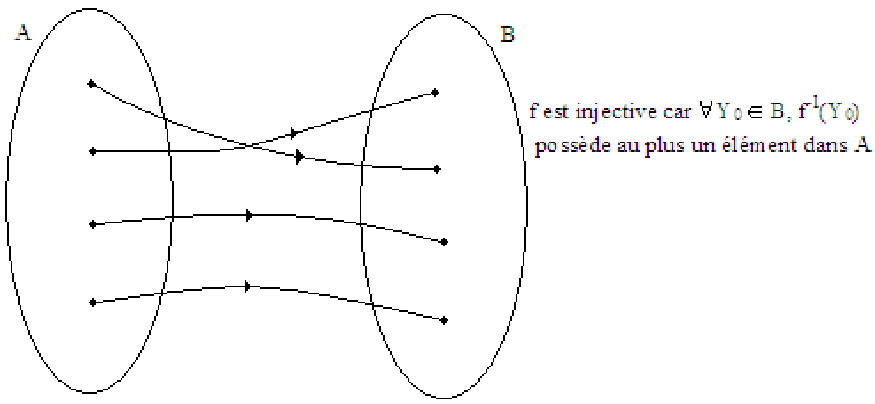
NB : cette notion d'équation va nous permettre de classifier les applications.

(2) Classification des applications.

(a) Application injectives ou injection

(i) Définition :

Soient 2 ensembles A et B non vides et $f : A \to B$, une application, on dit que f est injective ou une injection si $\forall Y_0 \in B$, l'équation $f(x) = Y_0$ admet au plus une solution dans A. Ie. $\forall Y_0 \in B$, $f^{-1}(Y_0)$ possède 0 ou 1 élément. En d'autre termes $f : A \to B$ est injective signifie que $\forall x, x' \in A : [x \neq x \Rightarrow f(x) = f(x')]$ ou par contraposée, $\forall x, x' \in A : [f(x) = f(x') \Rightarrow x = x']$
NB. $f : A \to B$ n'est pas injective signifie que :
$\exists x, x' \in A : [x \neq x$ et $f(x) = f(x')]$



(ii) Exemples

1° $f : N \to N$
$x \rightsquigarrow f(x) = x + 3$ est une injection car $\forall$ x, x' $\in$ N, $f(x) = f(x') \Rightarrow X = X'$
En effet $f(x) = f(x') \Leftrightarrow x + 3 = x' + 3 \Leftrightarrow x = x'$ comme 3 est régulier ou la loi (+) dans N

2° Soit $A \neq \Phi$ et $A' \subset A$, alors :
$\varphi : A' \to A$
$x \rightsquigarrow f(x) = x$ est une injection canonique

3° Soit $f : [0, \infty[\to R$
$x \rightsquigarrow f(x) = x^2$ est injective.
Par contre $f : R \to R$
$x \rightsquigarrow f(x) = x^2$ n'est pas injective car $\exists$ 1, -1 $\in$ R ; $f(1) = f(-1)$

(iii) Propriétés.

P_1 : la composée de deux injections est une injection.
En effet : soient $A \xrightarrow{f} B \xrightarrow{g} G$ deux injections, alors
$gof : A \to G$ est injective.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

$\forall x, x' \in A : x \neq x' \Rightarrow f(x) \neq f(x')$ (car f est injective).
$\Rightarrow g[f(x)] \neq g[f(x')]$ (car $f(x), f(x') \in B$ et g injection)
Donc $\forall x, x' \in A$, $x \neq x' \Rightarrow (g \circ f)(x) \neq (g \circ f)(x')$ et g o f est injective.

P$_2$ ou Lemme de Serre
Soient $A \xrightarrow{f} B \xrightarrow{g} G$, deux applications composables telles que g o f soit injective, alors f est injective.

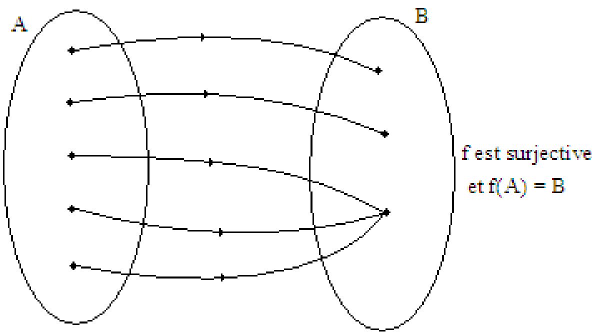
Démonstration par contraposition :
C'est-à-dire : f non injective $\Rightarrow$ g o f non injective.
En effet, f non injective $\Rightarrow \exists x, x' \in A : x \neq x'$ et $f(x) = f(x')$.
$f(x), f(x') \in B$, g fonction $\Rightarrow g[f(x)] = g[f(x')]$.
Donc $\exists x, x' \in A : x \neq x'$ et $(g \circ f)(x) = (g \circ f)(x')$.
Donc g o f est non injective.

P$_3$: Soit $f : A \to B$, une application, s'il existe une application
$g : B \to A$ telle que $g \circ f = 1_A$, alors f est injective.
En effet. Supposons qu'il existe $g : B \Rightarrow A$ telle que $g \circ f = 1_A$, montrons que f est injective.
Ie. $\forall x, x' \in A$, $f(x) = f(x') \Rightarrow g[f(x)] = g[f(x')]$. Car $f(x), f(x') \in B$ et g est une fonction.
Or $(g \circ f)(x) = g[f(x)] = 1_A = x$ et $(g \circ f)(x') = x'$
Donc $\forall x, x' \in A$; $f(x) = f(x') \Rightarrow x = x'$ et f est une injection.

(b) Application surjective ou surjection

(i) Définition :

Soient $A \neq \Phi$ et $B \neq \Phi$ et $f : A \to B$, une application. On dit que f est une surjection ou une application surjective si $\forall\, y_0 \in B$, l'équation $f(x) = y_0$ admet au moins une solution c'est à dire : $\forall y \in B, \exists x \in A : f(x) = y$, donc $f^{\bullet}(A) = B$
Dans ce cas, on dit que f est une application A sur B.



(ii) Exemples :

1° Soit $f : A \to B$ une application.
Alors $g : A \to f^{\bullet}(B)$
$x \rightsquigarrow g(x) = f(x)$ est une surjection

2° $f : R \to R_+$
$x \rightsquigarrow f(x) = |x|$, surjection.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

3° $P : E \to E/R$

$x \rightsquigarrow \dot{x}$ est une surjection canonique.

(iii) Propriétés

P_1 : La composée de deux surjections est une surjection.
En effet. Soient $A \xrightarrow{f} B \xrightarrow{g} C$, deux surjections.
Alors $g \circ f : A \longrightarrow C$ est une surjection.
$f : A \to B$ une surjection $\Rightarrow f^{\bullet}(A) = B$ (i)
$g : B \to C$ surjective $\Rightarrow g^{\bullet}(B) = C$ (ii)
$C \overset{(ii)}{=} g^{\bullet}(B) \overset{(i)}{=} g^{\bullet}[f^{\bullet}(A)] = (g^{\bullet} \circ f^{\bullet})(A) = (g \circ f)^{\bullet}(A)$
Donc $C = (g \circ f)^{\bullet}(A)$ et $g \circ f$ surjective.

P_2 ou Lemme de Serre :
Soit $A \xrightarrow{f} B \xrightarrow{g} C$, deux applications composables tels que g o f soit surjectives. Alors g est surjective.
En effet : $g \circ f : A \to C$ surjection $\Rightarrow \forall z \in C, \exists x \in A$,
Tel que $(g \circ f)(x) = g[f(x)] = z$
$x \in A$ et f une application $\Rightarrow f(x) = y$ existe dans B.
ie. $\exists y = f(x) \in B : g(y) = g[f(x)] = z$. Donc $\forall z \in C$,
$\exists y = f(x) \in B : g(y) = z$. Ce qui montre que g est surjective.

P_3 Soit $f : A \to B$, une application s'il existe $h : B \to A$ telle que $f \circ h = 1_B$, alors f est surjective.
En effet. Supposons qu'il existe $h : B \to A$ telle que $f \circ h = 1_B$ et montrons que $f : A \to B$ est surjective ou $\forall y \in B, \exists x \in A : f(x) = y$.
En effet $\forall y \in B$, $(f \circ h)(y) = f[h(y)] = 1_B(y) = y$.
Il suffit de prendre $z = h(y) \in A$ pour avoir f surjective.

(c) L'application bijective ou bijection

(i) Définition :

Soient $A \neq \Phi$ et $B \neq \Phi$ et $f : A \to B$, une application, on dit que f est une application bijective ou une bijection si f est à la fois injective et surjective.
Ainsi une application $f : A \to B$, bijective est parfois appelée application biunivoque et toute application biunivoque de l'ensemble A vers A lui-même est appelé permutation de l'ensemble.

(ii) Exemples :

1° Soit $b \in \mathbb{R}_+^* \setminus \{1\}$ et $f : \mathbb{R} \to \mathbb{R}_+^*$
$x \rightsquigarrow f(x) = b^x$ est une bijection.

2° $f : \mathbb{N} \to \mathbb{N}^*$
$n \rightsquigarrow n' = n + 1$, bijection.
$n' = n + 1$ s'appelle successeur de naturel n.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

(iii) Théorème

Une application $f : A \to B$ est bijective ssi $\forall y \in B$, l'équation $f(x) = y$ admet une solution et une seule et montrons que f est bijective.
Ce qui est trivial car f est à la fois injective et surjective.
$\Rightarrow$ Supposons que $f : A \to B$ est bijective et montrons que l'équation $f(x) = y$ admet une solution et une seule dans A, $\forall y \in B$.
En effet, $f : A \to B$ bijective $\Rightarrow$ f est surjective.
ie. $\forall y \in B, \exists x \in A : f(x) = y$. De plus, cet élément $x \in A$ est unique car f étant une application injective, $\forall x' \in A$ tel que $x \neq x'$ implique que $f(x) \neq f(x')$.
ie. $y \neq f(x')$. Donc x est unique.
D'où $\forall y \in B, \exists! x \in A : f(x) = y$

Nous venons de montrer que $f : A \to B$ est bijective ssi $\forall y \in B$, l'équation $f(x) = y$ admet une et une seule solution dans A.
Désignons là par $x = g(y)$, cela nous permet de définir une application de la manière suivante :
$g : B \to A$
$Y \rightsquigarrow g(y) = x$ qui est visiblement bijective car $\forall y \in B : f(x) = y \Leftrightarrow x = g(y)$

Montrons en effet que $g : B \to A$ est bijective ou

- g est surjective ou $\forall x \in A, \exists y \in B : g(y) = x$

En effet, $x \in A$ et $f : A \to B$, une application, cela signifie que $f(x)$ existe dans B.
Posons $f(x) = y \in B$, alors $\exists y = f(x) \in B : g(y) = x$.
D'où $\forall x \in A\ \exists y = f(x) \in B : g(y) = x$.

- g est injective ou $\forall y, y' \in B, g(y) = g(y') \Rightarrow y = y'$.

En effet, $\forall y, y' \in B, g(y) = g(y')$. ie. $x = x'$ avec $x, x' \in A$.
Or $f : A \to B$ étant une application, comme $x, x' \in A$ sont tels $x = x'$, donc $f(x) = f(x')$
ie. $y = y'$.
D'où $\forall y, y' \in B, g(y) = g(y') \Rightarrow y = y'$.

Conclusion :
L'application $g : B \to A$
$y \rightsquigarrow x$ est appelé réciproque de l'application bijective $f : A \to B$
$x \rightsquigarrow y$
On la note par f^{-1}. ie. $f^{-1} = g$
Ainsi une bijective $f : A \to B$ et sa réciproque $f^{-1} : B \to A$ peuvent se noter :

$$\mathbf{A} \underset{f^{-1}}{\overset{f}{\rightleftarrows}} \mathbf{B}$$

D'autres part : $\forall x \in A, \forall y \in B : f(x) = y \Leftrightarrow f^{-1}(y) = x$
NB : pour que f^{-1} existe, il faut d'abord que f soit bijective.

(iv) Propriétés

$\mathbf{P_1}$: Soit $f : A \to B$ une bijection et $f^{-1} : B \to A$, sa réciproque. Alors :
(i) $f \circ f^{-1} = 1_B$ et $f^{-1} \circ f = 1_A$.
En effet : $\forall y \in B : (f \circ f^{-1})(y) = f[f^{-1}(y)] = f(x)$ avec $y = f(x)$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Donc $\forall y \in B : (f \circ f^{-1})(y)$ et $f \circ f^{-1} = 1_B$.
(ii) $\forall x \in A : (f^{-1} \circ f)(x) = f^{-1}[f(x)] = f^{-1}(y)$ avec $f(x) = y$.
Donc $\forall x \in A : (f^{-1} \circ f)(x) = x \Rightarrow f^{-1} \circ f = 1_A$.

P_2 ou Lemme de Serre

Soient $A \xrightarrow{f} B \xrightarrow{g} C$, deux applications telles que g o f soit bijectives alors f est injective et surjective.
En effet : g o f bijective $\Rightarrow$ g o f injective et g o f surjective.
g o f injective $\Rightarrow$ f est injective (**P_2**).
et g o f surjective $\Rightarrow$ g est surjective (**P_2**).
D'où g est surjective et f est injective.

P_3 : Pour une application $f : A \to B$, il existe deux applications $g, h : B \to A$ telles que $f \circ g = 1_B$ et $h \circ f = 1_A$ ssi f est bijective.
Alors h = g

$$\begin{tikzcd} B \arrow[r, "g"] \arrow[rr, bend right, "f \circ g = 1_B"'] & A \arrow[r, "f"] \arrow[rr, bend right, "h \circ f = 1_A"'] & B \arrow[r, "g"] & A \end{tikzcd}$$

Preuve
$\Rightarrow$ Supposons qu'il existe $g, h : B \to A$ telles que $f \circ g = 1_B$ et $h \circ f = 1_A$, montrons que f est bijective.
En effet : $f \circ g = 1_B \Rightarrow$ f est surjective (**P_3**).
et $h \circ f = 1_A \Rightarrow$ f est injective (**P_3**).
D'où f est injective et surjective. ie. f est bijective.
$\Rightarrow$ Supposons que $f : A \to B$ est bijective, alors $\exists$f-1 : $B \to A$ telles que $f^{-1} \circ f = 1_A$
Et $f \circ f^{-1} = 1_B$ (**P_1**).
Donc il suffit de prendre $h = g = f^{-1}$.
Montrons que h = g sachant que f og = 1B et h o f = 1A.
$(h \circ f) \circ g = h \circ (f \circ g)$ ou $1_A \circ g = h \circ 1_B$

$$\left(\begin{tikzcd} B \arrow[r, "g"] \arrow[rr, bend right, "1_A \circ g = g"'] & A \arrow[r, "1_A"] & A \end{tikzcd}\right) \quad \left(\begin{tikzcd} B \arrow[r, "1_B"] \arrow[rr, bend right, "h \circ 1_B = h"'] & B \arrow[r, "h"] & A \end{tikzcd}\right)$$

P_4 : Soient $A \xrightarrow{f} B \xrightarrow{g} C$, deux bijections, alors g o f est aussi une bijection, et de plus $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.
Preuve
1° $g \circ f : A \to C$ bijective.
Car $f : A \to B$ bijective $\Rightarrow$ f injective et f surjective,
Et $g : B \to C$ bijective $\Rightarrow$ g injective et g surjective,
$\Rightarrow$ g o f injective et g o f surjective ;
$\Rightarrow$ g o f bijective.

2° Montrons que : $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.
En effet, f et g, bijectives $\Rightarrow f^{-1}$ existe et bijective.
$\Rightarrow g^{-1}$ existe et bijective.
D'autre part g o f bijective $\Rightarrow (g \circ f)^{-1}$ existe et bijective, de plus

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} (g^{-1} \circ g) \circ f$
$= f^{-1} \circ 1_B \circ f = (f^{-1} \circ 1_B) \circ f$
$= f^{-1} \circ f$
$= 1_A$
Donc $f^{-1} \circ g^{-1}$ est la réciproque de g o f que l'on note $(g \circ f)^{-1}$.
D'où $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

(d) Application involutives ou involutions

(i) Définition

Une application $f : A \to A$ ($A \neq \Phi$) est dite involutive ou une involution si $f \circ f = 1_A$.

(ii) Exemples

a. Soit $E \neq \Phi$, l'application $G_E : \wp_{(E)} \to \wp_{(E)}$
$A \rightsquigarrow G_E^A = [X \in E : K]$ est une involution car $G_E\left(G_E^A\right) = A$

b. L'application opposée : $Z \to Z$
$x \rightsquigarrow (oppx) = -x$ est une involution car $opp[opp(x)] = opp(-x)$
$= -(-x) = x$.

c. La conjugaison définie de $\mathbb{C} \to \mathbb{C}$
$Z \rightsquigarrow \overline{Z}$ est une involution car $\overline{\overline{Z}} = Z$
Soit $Z = x + yi$, alors $\overline{Z} = x - yi$, d'où $Z = \overline{\overline{Z}}$ et $\overline{\overline{Z}} = x + yi$.

(iii) Proposition

Toute involution est une bijection.
En effet, soit $f : A \to A$, une involution $\Rightarrow$ $f \circ f = 1_A$,
Or $f \circ f = 1_A \Rightarrow$ f est injective et f est surjective. Donc f est bijective.
Exercice : La composition de deux involutions est-elle une involution ?

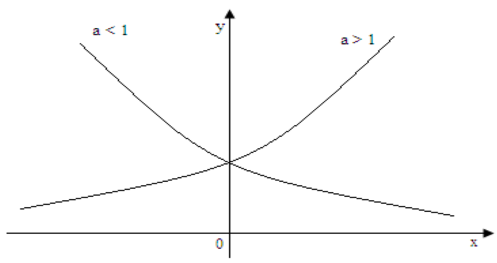
(e) Application croissantes et décroissantes

(i) Définition

Soient $(A, \leq)$ et $(B, \geq)$, deux ensembles ordonnée et f, une application. On dit que f est croissante si $\forall x_1, x_2 \in A, x_1 \leq x_2 \Rightarrow f(x_1) \leq f(x_2)$
Et on dit que f est décroissante si $\forall x_1, x_2 \in A, x_1 \leq x_2 \Rightarrow f(x_1) \geq f(x_2)$.
On dit que f est monotone si f est soit croissante soit décroissante.

Exemple

Soit $a \in \mathbb{R}_+^* \setminus \{1\}$ et $f : \mathbb{R} \to \mathbb{R}_+^*$
$x \rightsquigarrow f(x) = a^x$.



Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Alors f est croissante si a > 1 et décroissante si a < 1.
NB. Si $\forall x_1, x_2 \in A$, $x_1 > x_2 \Rightarrow f(x1) < f(x2)$, on dit que f est strictement croissante, de même f est strictement décroissante si $\forall x_1, x_2 \in A$, $x_1 < x_2 \Rightarrow f(x1) > f(x2)$.

C. DENOMBREMENT

1. Ensemble N

a) Ensemble équipotents

(1) Définition

Soient A et B, deux ensembles. On dit que A est équipotent à B ou que A et B sont équipotents ou encore que A et B ont même puissance s'il existe une bijection entre A et B.

(2) Exemples

a. N et P sont équipotents car $f : N \rightarrow P$
$n \rightsquigarrow 2n$ bijective.

b. A = {1, 2, 3} est équipotent à {{1, 2}, 3} car on peut établir une bijection entre ces deux ensembles par exemple : $1 \rightarrow \{1 ; 2\}$
$2 \rightarrow 3$
$3 \rightarrow 5$

NB. Tout ensemble qui est équipotent à N ou à une partie de N est di *dénombrable.*

Exemple
Soit V, l'ensemble des voyelles de l'alphabet français.
Alors V est dénombrable car $\exists f : V \rightarrow \{4, 9\} \subset n$ bijective.
V = { a, e, i, o, u, y} et {4, 9} = {4, 5, 6, 7, 8, 9}.

(3) Théorème

La relation « est équipotent à » définie entre les ensembles est une relation d'équivalence, c'est-à-dire $\forall A, B$, ensemble, on a A Eq B ssi il existe une bijection entre A et B.
Montrons que « Eq » est une relation d'équivalence ente les ensembles.

- Eq réflexive car $\forall A$, ensemble, on a A Eq A puisque $\exists 1_A : A \rightarrow A$ qui est bijective.
- Eq symétrique. ie. $\forall A, B$ ensembles, A Eq B $\Rightarrow$ B Eq A.

En effet, A Eq B $\Rightarrow \exists f : A \rightarrow B$ bijective.
$\Rightarrow f^{-1} : B \rightarrow A$ bijective.
$\Rightarrow$ B Eq A et *Eq* est symétrique.

- La transitivité de la relation « Eq » découle de la composition des bijections. Montrons en effet que $\forall A, B, C$ ensembles : si A Eq B et B Eq C alors A Eq C.

A Eq B $\Rightarrow \exists f : A \rightarrow B$ bijection.
B Eq C $\Rightarrow \exists g : B \rightarrow C$ bijection.
$\Rightarrow g \circ f : A \rightarrow C$ est bijective. ie. A Eq C et la relation Eq est transitive.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

(4) Cardinal d'un ensemble

(a) Définition

Soit A un ensemble, nous allons définir un nouvel objet mathématique appelé cardinal de l'ensemble A et noté card (A) ou ⋕A.
Soit A un ensemble, alors tous les ensembles équipotents à A appartiennent à une même classe d'équivalence qu'on appelle cardinal de A.

Ainsi, le cardinal d'un ensemble A est la classe d'équivalence de A par la relation d'équipotence. C'est donc une collection de tous les ensembles qui sont équipotents à A. D'où le cardinal d'un ensemble n'est pas un ensemble.
Remarque : Si E est un ensemble, alors card E = n existe et on l'appelle parfois nombre cardinal.

(b) Conséquences de la définition d'un cardinal

i. Soient A et B deux ensembles, alors card (A) = card (B) si A et B sont équipotents, i.e. il existe une bijection entre A et B.
ii. Le cas de l'ensemble vide.

L'ensemble vide est le seul et unique équipotent à $\emptyset$. Alors on pose traditionnellement que :

- *Card ($\emptyset$) = 0 nombre cardinal zéro*
- *$\forall a$, objet, l'ensemble $\{a\}$ existe et card ($\{a\}$) = 1 nombre cardinal 1.*

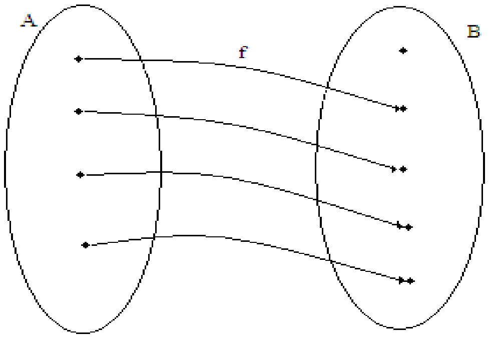
i.e. 1 est une collection de tous les ensembles singletons.
D'où card ($\{\emptyset\}$) = card ($\{0\}$) = card ($\{a\}$) = 1. Etc.
Par ailleurs, $0 \neq 1$ puisqu' il n'existe aucune bijection entre $\emptyset$ et un ensemble singleton. Puisque $0 \neq 1$, alors $\{0, 1\}$ est une paire et card ($\{0, 1\}$) = 2.
Signalons que les nombres cardinaux ne constituent pas un ensemble, mais cependant, on peut envisager des ensembles de cardinaux. D'où au paragraphe suivant, nous identifieront l'ensemble des entiers naturels à l'ensemble des cardinaux finis.

(c) Relations d'ordre définie entre les cardinaux

Soient A et B deux ensembles, nous pouvons nous trouver devant les situations suivantes :

- Soit que A et B sont équipotents
- Soit que l'un est équipotent à une partie de l'autre

Soit A cet ensemble qui est équipotent à une partie de B, cela signifie qu'il existe une injection entre A et B.



A est équipotent à $f'(A) \subset B$ car

$$g : A \to f'(A)$$
$$x \to g(x) = f(x) \text{ est bijective.}$$

Dès lors $f : A \to B$ est bijective.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

(i) Définition

Soient x et y deux cardinaux tels qu'il existe des ensembles X et Y avec x = card (X) et y = card (Y).
On dit que $x \leq y$ (lire x est inférieur ou égal à y) i.e. card (X) $\leq$ card (Y).
S'il existe une injection entre X et Y, montrons que la relation « $\leq$ » est une relation d'ordre :

i. $\forall$ x, cardinal, on a $x \leq x$, car il existe $1_x : X \to X$ qui est injective [x = card (X)] et « $\leq$ » est réflexive.
ii. $\forall$ A, B deux ensembles tels que card A $\leq$ card B et card B $\leq$ card A, alors card A = card B.

En effet :

card A $\leq$ card B $\Rightarrow \exists$ f : A $\to$ B injective *et*
card B $\leq$ card A $\Rightarrow \exists$ g : B $\to$ A injective.

Puisque f : A $\to$ B et g : B $\to$ A sont injectives, alors f : A $\to$ B est bijective. Donc A et B sont équipotents i. e. card A = card B et « $\leq$ » est antisymétrique.
D'où le théorème ci – dessous dit :

Théorème de CANTOR – BERNSTEIN
$\forall$ x, y deux cardinaux, si $x \leq y$ et $y \leq x$, alors $x = y$.

iii. $\forall$ A, B, C trois ensembles,
Si card (A) $\leq$ card B et card B $\leq$ card C, alors card A $\leq$ card C.

En effet :

card A $\leq$ card B $\Rightarrow \exists$ f : A $\to$ B injective

et

card B $\leq$ card A $\Rightarrow \exists$ g : B $\to$ A injective.

(f : A $\to$ B et g : B $\to$ C injectives) $\Rightarrow g \circ f$: A $\to$ C injective par suite card (A) $\leq$ card (C) et « $\leq$ » est transitive.
D'où (i), (ii) et (iii) $\Rightarrow$ la relation « $\leq$ » est d'ordre.
Cette relation « $\leq$ » est d'ordre total d'après le théorème de **ZERMELO** ci – dessous qu'on doit admettre.

Théorème de ZERMELO
$\forall$ x, y deux cardinaux, l'une des propositions suivantes : $x \leq y$ ou $y \leq x$ est vrai.

(ii) Remarques

Soient A et A' deux ensembles,

i. Si A' $\subset$ A, alors card A' $\leq$ A car il existe une injection canonique f : A' $\to$ A, qui à x associe x.
ii. Si A' $\subset$ A avec A' $\neq$ A.
Alors (card A' $\leq$ card A et card A' $\neq$ card A) se note card A' $<$ card A et le signe « $<$ » se lit « *est inférieur à* ».

D'où $x < y \Leftrightarrow x \leq y$ et $x \neq y$.
Remarquer que $0 \leq 1$ car $\emptyset \subset \{0\}$.

(d) Etudes des opérations x et + dans la collection des cardinaux

(i) Multiplication des cardinaux

(a) Préliminaire

Si A et A', B et B' sont des ensembles équipotents, alors A x B et A' x B' sont équipotents, alors A x B et A' x B' sont équipotents.

En effet,

A ε_q A' $\Longrightarrow \exists$ f : A → A'

x ⇝ f(x) bijective.

et

B ε_q B' $\Longrightarrow \exists$ g : B → B'

y ⇝ g(y) bijective.

Définissons l'application h de la manière suivante :

h : A x B → A' x B'

(x, y) ⇝ h(x, y) = (f(x), g(y)).

Puisque f et g sont bijectives, alors h l'est aussi et A x B est équipotent à A' x B'. D'où la définition suivante :

(b) Définition

***b*₁** Si x et y sont des cardinaux tels que x = card A et y = card B, alors par définition :

$x \times y$ = card (A x B).

La loi x s'appelle multiplication et $x \times y$ ou $x \cdot y$ est le produit de x et y.

***b*₂ Propriétés**.

1. La multiplication des cardinaux est associative et commutative.

N. B. : On sait que ∀ A, B ensembles, A x B ≠ B x A, mais l'application
f : A x B → B x A
(x, y) ⇝ (y, x) est bijective et A x B est équipotent à B x A.

2. Elle admet 1 pour élément neutre. i.e. ∀ x, cardinal : x . 1 = x.

En effet, soit un ensemble A tel que card A = x, si B = {a}, alors l'application
g : A x {a} → A
(x, a) ⇝ x est bijective.
Par conséquent, A x {a} ε_q A et card (A x {a}) = card A, soit $x \cdot 1 = x$.

3. 0 est un élément absorbant pour la loi "$\times$". i.e. ∀ x, cardinal ; on a : $x \cdot 0 = 0$, trivial car $A \times \emptyset$, ∀ A ensemble.

4. ∀ x, y, deux cardinaux :

$$\begin{cases} x.y=1 \Rightarrow x=1 \text{ et } y=1 \\ x.y=0 \Rightarrow x=0 \text{ ou } y=0. \end{cases}$$

5. La multiplication est distributive par rapport à l'addition *(exercice).*

(ii) L'addition des cardinaux

(a) Préliminaire

i. Soient A et A', B et B' des ensembles équipotents tels que $A \cap B = \emptyset$. Alors $A \cup B$ est équipotent à $A' \cup B'$.

En effet, soit $f : A \to A'$ une bijection et $g : B \to B'$ une bijection. Montrons que $A \cup B$ est équipotent à $A' \cup B'$.
Puisque $A \cap B = \emptyset$, alors définissons l'application h de la manière suivante :
$h : A \cup B \to A' \cup B'$

$$z \rightsquigarrow h(z) = \begin{cases} f(z) \text{ si } z \in A \\ g(z) \text{ si } z \in B \end{cases}.$$

Comme $A' \cup B' = \emptyset$, chaque élément de $A \cup B$ aura une image et une seule par h et réciproquement, ce qui prouve que h est une bijection et on a : $A \cup B \; \varepsilon_q \; A' \cup B'$.

ii. Si x et y sont des cardinaux, alors il existe des ensembles A' et B' tels que x = card (A') et y = card (B') avec $A' \cup B' = \emptyset$.

En effet, si x et y sont tels que card (A) = x et card (B) = y alors il suffit de prendre $A' = A \times \{0\}$ et $B' = B \times \{1\}$ car, dans ce cas, card $(A' \times \{0\}) = x$ et card $(B \times \{1\}) = 1$ avec $(A \times \{0\}) \cap (B \times \{1\} = \emptyset$.
D'où la définition suivante :

(b) Définition

Si x et y sont deux cardinaux tels que x et y sont deux cardinaux tels que x = card (A) et y = card (B), avec $A \cap B = \emptyset$, alors par définition : $x + y = \text{card}\,(A \cup B)$ avec $A \cap B = \emptyset$.
La loi (+) s'appelle addition des cardinaux ; x + y est la somme de x et y.

b_1 Propriétés.

1. L'addition des cardinaux est associative et commutative (exercice).
2. Elle admet 0 pour élément neutre i.e. $\forall$ x, cardinal : x + 0 = x. Si x = card (A), comme $A \cup \emptyset = A$, alors card $(A \cup \emptyset)$ = card (A), soit x + 0 = x.
3. $\forall$ x, y deux cardinaux, $x + y = 0 \Longrightarrow x = 0$ et $y = 0$. Ce qui est vrai car si x = card (A) et y = card (B), alors $A \cup B = \emptyset \Leftrightarrow A = \emptyset$ est $B = \emptyset$.

b_2 Théorème

Soit x et y deux cardinaux, alors $x \leq y$ ssi il existe un cardinal z tel que : x + z = y.

Preuve

i. $\Longrightarrow$ Supposons que $x \leq y$ et soit A, B deux ensembles tels que x = card A et y = card B. $x \leq y \Longrightarrow \exists\, f : A \to B$ injective. Comme $f : A \to f^{\circ}(A) = B' \subset B$ est bijective. i.e. card A = card B'.

Il suffit de considérer $z = ð_B^{B'}$, alors $z \cap B' = \emptyset$ et $z \cup B' = \emptyset$ et $z \cup B' = B$. En posant z = card(Z), alors card (B), soit x + z = y.

ii. $\Longleftarrow$ Supposons qu'il existe un cardinal z tel que : x + z = y et soit A, B et Z des ensembles tels que : card (A) = x, card (B) = y et card (Z) = z avec $A \cap Z = \emptyset$ puisque x + z = y, alors il existe une bijection entre $A \cup Z$ et B.

Soit $f : A \cup Z \to B$ cette bijection, alors la restriction de f à A est une injection de A vers B.D'où $x \leq y$.

NB : On sait que $\forall$ A, B, C des ensembles : $A \times (B \cup C) = (A \times B) \cup (A \times C)$
Si $B \cap C = \emptyset$ et $(A \times B) \cap (A \times C) = \emptyset$, alors card $[A \times (B \cup C)]$ = card $[(A \times B) \cup (A \times C)]$.
Soit $x \cdot (y + z) = xy + xz$, sachant que x = card (A), y = card (B) et z = card (C).

(e) Cardinaux Finis (Entiers Naturels).

(i) Théorème

$\forall$ x, y deux cardinaux, alors $x + 1 = y + 1 \Leftrightarrow x = y$.

- $x = y$, alors $x + 1 = y + 1$ (trivial).
- Soit x et y deux cardinaux tels que $x + 1 = y + 1$.

Si A et B sont deux ensembles tels que : x = card (A) et y = card (B), considérons deux éléments distincts i et j n'appartenant pas à $A \cup B$.
Alors : $x + 1$ = card (A') avec $A' = A \cup \{i\}$
$y + 1$ = card (B') avec $B' = B \cup \{j\}$.
Puisque $x + 1 = y + 1$, il existe une bijection f de A' vers B'.

Deux cas sont possibles :

- Si $f(i) = j$, alors f/A est une bijection de A vers B. D'où $x = y$.
- Si $f(i) \neq j$, soit $b = f(i)$ et $a = f^{-1}(j)$. Posons $A'' = A - \{a\}$ et $B'' = B - \{b\}$, alors l'application $h = f/A''$ est bijective de A'' vers B''.
- Si on prolonge h à A par $h(a) = b$, on obtient une bijection h de A vers B et $x = y$.

(ii) Cardinaux finis

(a) Définitions

Un cardinal n est fini ssi $n \neq n + 1$.

Exemples :

- 0 est un cardinal fini car $0 \neq 0 + 1 = 1$
- 1 est un cardinal fini car $1 \neq 1 + 1 = 2$.

Un cardinal non fini est dit infini.
Un ensemble est dit fini ou infini suivant que son cardinal est fini ou infini.
Un cardinal fini est aussi appelé un nombre naturel.
Si A est un ensemble fini, alors card (A) est appelé nombre d'éléments de A.
Si A est un ensemble infini, alors card (A) est appelé nombre transfini.

(b) Axiome de l'infini

Les cardinaux finis constituent un ensemble. Cet ensemble est désigné par N, qu'on appelle ensemble des cardinaux finis ou des nombres naturels.
Il est légitime d'écrire que : $0 \in \mathbb{N}$, $1 \in \mathbb{N}$.
NB : $\mathbb{N}^* = \mathbb{N} - \{0\}$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

(c) Ensemble infini des cardinaux finis

Propriétés

L'application f de $\mathbb{N}$ dans $\mathbb{N}$ définie par $\forall\, n \in \mathbb{N}$, $f(n) = n + 1$ est bijective de $\mathbb{N}$ dans $\mathbb{N}^*$.
i.e. $f : \mathbb{N} \to \mathbb{N}^*$
$n \rightsquigarrow n + 1$ est bijective.

En effet, il faut montrer que f est une application bijective.

i. F est une application si $\forall\, n \in \mathbb{N}$, $n + 1$ est un cardinal fini. Sachant que n est un cardinal fini, alors $n \neq n + 1$ entraîne $n + 1 \neq (n + 1) + 1$ car par contraposée,
$n + 1 =(n + 1) + 1 \Longrightarrow n = n + 1$
Vrai d'après le théorème d.5.a).
D'où $n + 1$ est un cardinal fini. De plus, $n + 1\neq 0$, puisque $1 \neq 0$.

ii. f est injective d'après le théorème d. 5. a).

iii. Montrons que f est surjective ou $\forall\, n \in \mathbb{N}^*$, $\exists\, m \in \mathbb{N} : f(m) = n$, i.e. $m + 1 = n$.
Soit $n \in \mathbb{N}^*$, alors il existe $A \neq \emptyset$, tel que $n = \text{card}\,(A)$.
$A \neq \emptyset \Longrightarrow \exists\, a \in A$, alors en posant $A' = A - \{a\}$, on a : $A = A' \cup \{a\}$ et $A' \cap \{a\} = \emptyset$, alors $\text{card}\,(A) = \text{card}\,(A' \cup \{a\})$.
Dès lors il existe m tel que : $n = m + 1$. C'est $m = \text{card}\,(A')$. m est un cardinal fini : si non $m + 1 = n$ ne serait pas un cardinal fini.

Définition

Pour tout cardinal fini n, le cardinal fini $n + 1$ est appelé le successeur de n.
Il faut noter que, $\forall\, n \in \mathbb{N}$, $n \leq n + 1$. Ainsi, dans $\mathbb{N}$:

i. Tout élément n a un successeur unique.
ii. Deux éléments différents ont des successeurs différents.
iii. Zéro n'est le successeur d'aucun élément.

D'où $\mathbb{N} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \ldots, \}$.

Conséquence

D'après ce qui précède, on a vu que $\mathbb{N}^* = \mathbb{N} - \{0\}$.
Sachant que $\mathbb{N}^* \cap \{0\} = \emptyset$, alors $\text{card}\,(N) = \text{card}\,(\mathbb{N}^* \cup \{0\})$
$= \text{card}\,(\mathbb{N}^*) + 1 \quad$ (i).

D'autre part, $\text{card}\,(\mathbb{N}) = \text{card}\,(\mathbb{N}^*)$ car il existe une bijection f de $\mathbb{N}$ vers $\mathbb{N}^*$ associant n à $n + 1$. D'où (i) devient : $\text{card}\,(\mathbb{N}) = \text{card}\,(\mathbb{N}) + 1$.

Par suite card $\mathbb{N}$ n'est pas un cardinal fini et $\mathbb{N}$ est un ensemble infini. En désignant le cardinal de $\mathbb{N}$ par $\mathcal{N}_\circ$ (lire aleph zéro), alors $\mathcal{N}_\circ$ est un nombre transfini et on a : $\mathcal{N}_\circ = \mathcal{N}_\circ + 1$.

Conclusion

Cette conséquence prouve que la définition d'un cardinal fini a un sens, car il existe au moins un ensemble de cardinal n tel que $n = n + 1$. Soit par exemple l'ensemble $\mathbb{N}$. D'où $\mathbb{N}$ est un ensemble infini et $\mathcal{N}_\circ$ est un nombre transfini.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

b) L'ensemble N

L'ensemble ℕ est l'ensemble des nombres naturels. On va le munir de la loi (+), de la loi (x) et de la relation d'ordre.

(1) Les propriétés de (+) dans ℕ

- (+) est associative, commutative et admet $0 \in \mathbb{N}$ comme élément neutre.
- Soit $x' \in \mathbb{N}^*$, $\exists\, x \in \mathbb{N} :\ x' + x = 0$
- Tout élément de ℕ est régulier pour l'addition, c'est – à – dire :
  $\forall\, x, y, z \in \mathbb{N}, x + y = y + z \Longrightarrow x = y.$

(2) Les propriétés de (·) dans ℕ

- (·) est commutative, associative et admet 1 pour élément neutre.
- 0 est un élément absorbant pour (·) dans ℕ : c'est – à – dire : $\forall\, n \in \mathbb{N} : n \cdot 0 = 0$
- $\forall\, x, y, z \in \mathbb{N}^* : x \cdot z = y \cdot z \Longrightarrow x = z.$
- De plus, la loi (·) est distributive par rapport à la loi (+) dans ℕ

(3) (ℕ,≤) est un ensemble totalement ordonné

a. $\forall\ a, b \in \mathbb{N} :\ a \le b \Leftrightarrow d \in \mathbb{N} : \boldsymbol{b = a + d}, \Longrightarrow \boldsymbol{d = b - a}$ qu'on appelle différence entre a et b.

b. $\forall A \subset \mathbb{N}$ $\boldsymbol{avec\ A \neq \emptyset}, \exists \boldsymbol{k} \in \boldsymbol{A}$; $\forall \boldsymbol{x} \in \boldsymbol{A}$, on a $k \le x$, donc k est le plus petit élément de A et en particulier, *0 est le plus petit élément de* **ℕ.**

c. $\forall a, b \in \mathbb{N}$ $\boldsymbol{avec\ a \le b}$
   $[a, b] = \{x \in \mathbb{N} : \boldsymbol{a \le x \le b}\}$ alors a est le plus petit élément de [a, b] et b est le plus grand élément de [a, b].

d. $\forall x \in \mathbb{N}^*, \exists\, x' = x+1$ qu'on appelle successeur de x.

e. $\forall x \in \mathbb{N}^*, \exists\, x' = x-1$ qu'on appelle prédécesseur de x.

f. $L'ensemble$ ℕ est *un ensemble infini* d'éléments, c'est – à – dire ℕ n'a pas un plus grand élément : car $\forall x \in \mathbb{N}, \exists \boldsymbol{y} \in \mathbb{N} : \boldsymbol{x \le y}.$

(4) Théorème

Soit $A \subset \mathbb{N}$, $(A \neq 0)$ tel que :

i. Avec $0 \in A$
ii. $\forall x \in A : x + 1 \in A$

Alors : A = **ℕ.**

Démonstration par absurde

Supposons $A \neq \mathbb{N}$ c'est – à – dire $\mathbb{N} \setminus A \neq \emptyset$ avec $\mathbb{N} \setminus A \subset \mathbb{N}$

D'après ***c.2.***, $\exists k \in \mathbb{N} \setminus A$ tel que $\forall x \in \mathbb{N} \setminus A, k \le x$, k est le plus petit élément de $\mathbb{N} \setminus A$.

Puisque $0 \in A$, alors 0 n'appartient pas à $\mathbb{N} \setminus A \Longrightarrow k \neq 0$. D'après ***c.5.***, k admet un prédécesseur qui est k – 1.

Sûrement que :

$k - 1 \notin \mathbb{N} \setminus A$ car $k - 1 < k$ *et k supposé le plus petit élément de* $\mathbb{N} \setminus A$,

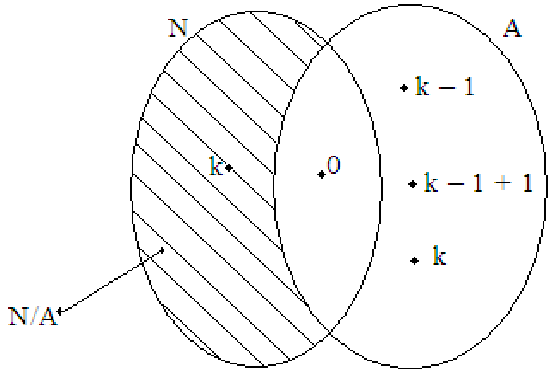
$\Longrightarrow k - 1 \in A.$

D' où finalement, on a : $k - 1 \notin \mathbb{N} \setminus A$ et $k - 1 \in A$, $k \notin A$ et $k \in \mathbb{N} \setminus A$.

Or $k - 1 \in A$ et $k \notin A$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

$\Downarrow$ *Hypothèse.*
$k - 1 + 1 \in A$, donc $k \in A$.
On arrive ainsi à une contradiction car on a supposé que $A \neq \mathbb{N}$.
Donc $A \neq \mathbb{N}$ est faux et $A = \mathbb{N}$ est vrai.



(5) Ensemble finis

i. Définition :

Un ensemble A est dit fini ou qu'il contient n éléments c'est – à – dire card A = n s'il existe une bijection entre A et [1, n] à n éléments.

ii. Exemple :

Soit A l'ensemble des lettres de l'alphabet français, alors A est fini car $\exists\, f : A \to [1, 26]$ bijective. $\Longrightarrow \#\, A = 26$.
Si V est l'ensemble des voyelles de l'alphabet français, alors V à six élément, car :
$\exists\, f : V \to [1, 6]$. *NB :* $[1, n] \in \mathbb{N}$.
Soient A et B deux ensembles finis.
Si $f : A \to B$ est injective alors card A $\leq$ card B
$f : A \to B$ est surjective alors card A $\geq$ card B
$f : A \to B$ est bijective alors card A = card B

2. Analyse Combinatoire

a) Nombre d'application d'ensemble fini vers un ensemble fini

(1) Théorème :

Soit A et B deux ensembles finis ayant respectivement p et n éléments. i.e. card A = p et card B = n.
Alors le nombre d'application de A vers B est n^p, ($p, n \in \mathbb{N}^*$). Ce qu'on écrit : card $(B^A) = n^p$.
Ainsi tout élément $h \in B^A$ s'appelle Arrangement avec répétition de p élément pris dans un ensemble à n éléments.

Démonstration par récurrence sur p

Soit $A = \{a_1, a_2, \ldots, a_p\}$ et $B = \{b_1, b_2, \ldots, b_n\}$, ces deux ensembles.

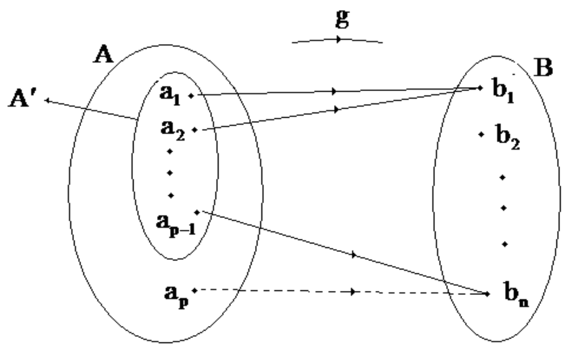
- Si p = 1, i.e. card A = 1, alors $A = \{a_1\}$ et le nombre d'applications de A vers B est n. Ce qu'on écrit : card $(B^A) = n^1 = n$ (vraie).

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

- ***Hypothèse de récurrence***

Supposons que cette formule est vraie jusqu'à l'ordre p – 1. I.e. le nombre d'élément d'un ensemble à (p – 1) éléments vers un ensemble à n éléments est n^{p-1}.
Montrons que le nombre d'application d'un ensemble à p éléments vers un ensemble à n éléments est n^p.

Soit $A' \subset A$ tel que $\text{card}\, A' = (p-1)$.
i.e. $A' = \{a_1, a_2, ..., a_{p-1}\}$. Alors $A = A' \cup \{a_p\}$.
Considérons une application $g : A' \longrightarrow B$. Alors g peut – être prolongée en une application de A vers B par la donnée d'une image à l'élément $a_p \in A$. Or a_p peut prendre n'importe quel élément de B pour image et comme B a pour cardinal n, alors on aura n prolongements distincts de $g \in B^{A'}$ en une application de A vers B.



Toute application $f : A \longrightarrow B$ est ainsi obtenue, puisque sa restriction à A' est l'application g.
D'où le nombre d'applications de A vers B est égal au nombre d'applications de A' vers B multiplié par n (n est le nombre de prolongements).
Or $\text{card}\left(B^{A'}\right) = n^{p-1}$

$$\text{Donc } \text{card}\left(B^{A}\right) = \text{card}\left(B^{A'}\right).n = n^{p-1}.n = n^{p-1+1} = n^p$$

D'où $\text{card}\left(B^{A}\right) = n^p, \ \forall p, n \in \mathbb{N}^*$

(2) Exemples

i. Combien de nombres à quatre chiffres peut – on former avec le chiffre 5 ou le chiffre 6.

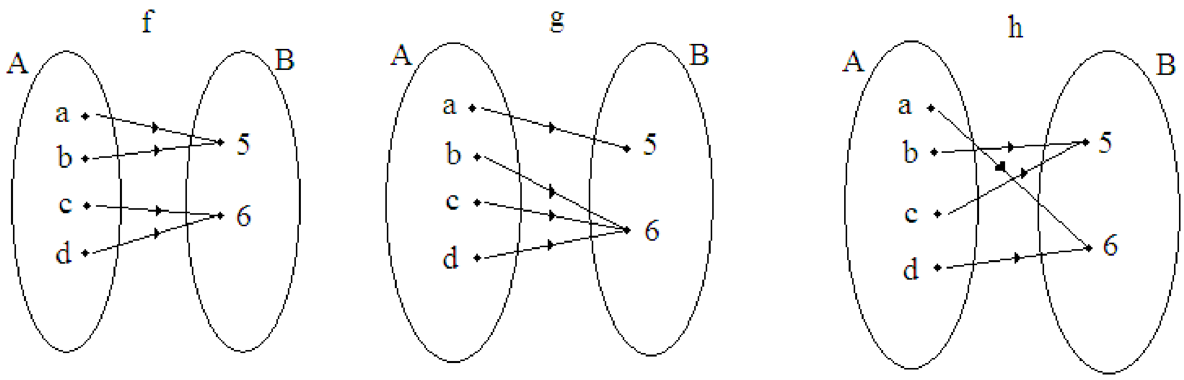
Solution :

Quelques exemples de ces nombres : 5566, 5555, 5665, 6665, … etc. Il y a autant de nombres à quatre chiffres formés avec les chiffres 5 ou 6 qu'il y a d'applications d'un ensemble à quatre éléments vers un ensemble à deux éléments.
Donc : $2^4 = 16$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Solution détaillée

Soit $A=\{a,b,c,d\}$; $B=\{5,6\}$ deux ensembles et $f : A \longrightarrow B$ une application.
Combien de telles applications y a – t – il ?
Comme $\text{card}\,A = 4$ et $\text{card}\,B = 2$, alors $\text{card}\left(B^A\right) = 2^4 = 16$.
Voici quelques – unes de ces applications :



ii. Etant donnés trois polynômes du premier degré en x et en y.

$$P_1 : a_1x + b_1y + c_1$$
$$P_2 : a_2x + b_2y + c_2$$
$$P_3 : a_3x + b_3y + c_3$$

On considère le système d'inéquations formé en faisant suivre chacun de ces polynômes du signe >0 ou du signe <0.
Combien de tels systèmes peut – on former ?

Solution :
Voici quelques exemples de tels systèmes d'inéquations :

$$\text{i)} \begin{cases} P_1 < 0 \\ P_2 < 0 \\ P_3 < 0 \end{cases} \qquad \text{ii)} \begin{cases} P_1 > 0 \\ P_2 < 0 \\ P_3 < 0 \end{cases} \qquad \text{iii)} \begin{cases} P_1 > 0 \\ P_2 > 0 \\ P_3 < 0 \end{cases}$$

Si $A=\{P_1, P_2, P_3\}$ et $B=\{>0, <0\}$, alors on peut établir $2^3 = 8$ applications entre ensembles A et B.
D'où on peut former huit systèmes d'inéquations avec ces trois polynômes.

iii. Si $\text{card}A = n$, $n \in \mathbb{N}$ et $f : A \longrightarrow \{0,1\}$ une application,

alors $\text{card}\,\text{App}\left[\left(A, \{0,1\}\right)\right] = 2^n$.

(3) Application : Le nombre des parties d'un ensemble fini

Soit A un ensemble à n éléments avec $n \in \mathbb{N}$
Problème : Calculer le cardinal de $P_{(A)}$.
Solution : Définir une application

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

$$\Gamma : P_{(A)} \to \mathrm{App}\left(A, \{0,1\}\right)$$
$$X \to \Gamma_X : A \to \{0,1\}$$
$$x \to \Gamma_X(x) = \begin{cases} 1 \text{ si } & x \in X \\ 0 \text{ si } & x \notin X \end{cases}$$

Où Γ_X est une application caractéristique de $X \subset A$.

i. Γ est bien définie car $\forall X \in \wp_{(A)}$, on doit toujours avoir Γ_X appelée *Fonction Caractéristique de X.* Il faut alors montrer que Γ est bijective.

ii. Γ est injective car $\forall X, X' \in \wp_{(A)}$, $X \neq X' \Rightarrow \Gamma_X \neq \Gamma_{X'}$.

En effet : $X \neq X' \Rightarrow \exists x \in A : x \in X$ et $x \notin X'$.
$x \in X \Rightarrow \Gamma_X(x) = 1$ et $\Gamma_{X'}(x) = 0$ car $x \notin X'$, avec $0 \neq 1$.

Donc $x \in A : \Gamma_X(x) - 0 \neq 0 = \Gamma_X(x)$ et Γ est injective.

iii. Γ est surjective par définition car $\forall g$, fonction caractéristique, il existe $X \subset A$, i.e. $X \in P_{(A)}$ tel que : $\varphi_X = g$.

Donc $\varphi_X = \Gamma_X$ puisque $\wp_{(A)}$ est en bijection avec App(A, $\{0,1\}$), i.e. $\wp_{(A)}$ est équipotent à App(A, $\{0,1\}$), alors card $\wp_{(A)} =$ card$\left[\mathrm{App}(A, \{0,1\})\right]$.

Or card$\left[\mathrm{App}(A, \{0,1\})\right] = 2^n$, donc card$\wp_{(A)} = 2^n$

Remarque : Si $A = \emptyset$, $\wp_{(\emptyset)} = \{\emptyset, \emptyset\} = \{\emptyset\}$ alors Card$\wp_{(\emptyset)} = 1$.

Or Card$\wp_{\emptyset} = 0$, donc card$\wp_{(\emptyset)} = 2^0 = 1$. D'où $\boxed{2^0 = 1}$.

b) Nombre d'injection d'un ensemble fini vers un ensemble fini (arrangement sans répétition)

(1) Etude d'un cas particulier

Soient $A = \{a_1, a_2, a_3\}$ et $B = \{b_1, b_2, b_3, b_4\}$ deux ensembles finis. Car card A = 3 et card B = 4.

Problème :
Déterminer le nombre d'injections de A vers B.
Soit f : A ⟶ B une injection et $a_1 \in$ A. Par f : a_1 a quatre possibilités d'avoir une image dans B. i.e. on peut envoyer a_1 sur b_1, soit sur b_2, soit sur b_3 ou soit sur b_4. Une fois l'image de a_1 fixée dans B pour que l'application obtenue soit injective. Ce qui fait 4 · 3 flèches au 1er étage. L'image de a_1 et celle de a_2 étant fixées dans B, alors a_3 restera avec deux possibilités d'avoir une image dans B.
Ce qui fait 4 · 3 · 2 flèches au deuxième étage. D'où autant de flèches c'est autant des injections qu'on peut établir entre ensembles A et B.
Or il y a 4 · 3 · 2 flèches, donc il y aura 4 · (4 – 1) · (4 – 2) = 4 · 3 · 2 = 24 injections entre A et B.
Présentons cette situation sous forme de schéma sagittal ci – dessous :

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

(2) Etude d'un cas général

Soient A et B deux ensembles finis ayant respectivement p et n éléments.

Prenons $A=\{a_1, a_2, a_3, ..., a_p\}$ et $B=\{b_1, b_2, b_3, ..., b_n\}$, (n, p ∈ ℕ*).

Problème : Calculer le nombre d'injections de A vers B.

Deux cas sont possibles :

1^er^ cas : si p > n, alors dans ce cas, il n'y a aucune injection entre A et B et le nombre d'injections est zéro.

2^ème^ cas : $p \leq n \ (1 \leq p \leq n)$

Désignons par I(A, B) l'ensemble des applications injectives de A vers B. Déterminons $\mathrm{card}[I(A,B)]$.

Soit $a_1 \in A$, alors a_1 a n possibilités d'avoir une image dans B. Une fois l'image de a_1 choisie, a_2 aura (n – 1) possibilités d'avoir une image pour que l'application obtenue soit injective. Ce qui donne n·(n – 1) flèches au 1^er^ étage.
Les images de a_1 et de a_2 étant fixées dans B, alors a_3 aura (n – 2) possibilités d'avoir une image pour la même raison que précédemment. Ce qui donne n·(n – 1) · (n – 2) flèches au 2^ème^ étage. Ainsi, au k^ième^ étage, le nombre de flèches partant d'un élément est (n – k + 1) et le nombre total de flèches à cet étage est n·(n – 1) · (n – 2) … (n – k + 1).
D'où le *théorème* suivant :
Le nombre d'injection d'un ensemble A vers un ensemble B avec $\mathrm{card}\, A = p$ et $\mathrm{card}\, B = n$, $(1 \leq p \leq n)$ est : $n(n-1)(n-2)\ldots(n-p+1)$ **.**

Démonstration.
Définitions :

Tout élément $h \in I(A, B)$ où A est un ensemble à p éléments et B un ensemble à n éléments, s'appelle ***Arrangement sans répétition de n éléments pris p à p*** $(1 \leq p \leq n)$**.**
I.e. Un arrangement de p éléments pris dans un ensemble à n éléments est une suite de p éléments d'un ensemble à n éléments. Il s'en suit qu'un arrangement de p éléments est un sous – ensemble rangé de p éléments d'un ensemble à n éléments.
Donc, le nombre d'injections d'un ensemble A à p éléments vers un ensemble B à n éléments est le » même que le nombre des arrangements de p élément pris dans un ensemble à n éléments.
Ce nombre ce note A_n^p ce qu'on lit : « A, n, p ».
Ainsi $A_n^p = \mathrm{card}[I(A,B)] = n \cdot (n-1) \cdot (n-2) \ \ldots \ (n-p+1)$
D'où $A_n^p = n \cdot (n-1) \cdot (n-2) \ \ldots \ (n-p+1)$ qui est donc un produit de p facteurs (naturels) consécutif dont le plus grand est n.

(3) Exemples

i. Les arrangements des lettres a, b, et c prises deux à deux sont : (a, b), (b, a), (a, c), (c, a), (b, c) et (c, b).
Le nombre total de ces arrangements est : $A_3^2 = 3 \times 2 = 6$

Solution détaillée

Soient $A=\{1,2\}$ et $B=\{a,b,c\}$ et $f: A \to B$, une application.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

On peut avoir les injections suivantes :

$f(1)=a$; $f(2)=b$ $f(1)=b$; $f(2)=a$ $f(1)=a$; $f(2)=c$ $f(1)=c$; $f(2)=a$ $f(1)=b$; $f(2)=c$ $f(1)=c$; $f(2)=b$.

Donc six injections correspondant à six arrangements.

ii. Combien de nombre à trois chiffres différents peut – on former avec les chiffres : 1, 2, 3, 4 et 5.

Solution :

Le problème revient à établir des injections entre un ensemble à trois éléments et un ensemble ayant pour éléments : 1, 2, 3, 4 et 5.

Donc $A_5^3 = 5\cdot 4\cdot 3 = 60$.

(4) Définitions :

Soit n ∈ ℕ, on appelle factorielle n, le nombre noté $n!$ (lire n factorielle) et définie de la manière suivante :

- $0! = 1$
- $1! = 1$

$\forall n \in IN^* \backslash \{1\} : n! = n.(n-1).(n-2)\ ...\ 3.2.1$

Exemples : $5! = 5.4.3! = 60.$

$$\text{Ainsi : } A_n^p = \frac{n!}{(n-p)!}$$

$$\text{car : } \frac{n!}{(n-p)!} = \frac{n(n-1)(n-2)...(n-p+1)(n-p)!}{(n-p)!}$$

$$= n(n-1)...(n-p+1)$$

$$= A_n^p$$

$$= \text{card}\, I(A,B) \text{ avec card} A = p \text{ et card} B = n$$

c) Nombre de bijections d’un ensemble fini vers un ensemble fini (permutations).

Soient A te B deux ensembles finis. Pour qu’il y ait une bijection entre A et B, il faut que A et B aient le même cardinal.

Soit n ce cardinal, c’est –à – dire $\text{Card}\, A = \text{Card}\, B = n$. On sait que toute bijection est en particulier une injection.

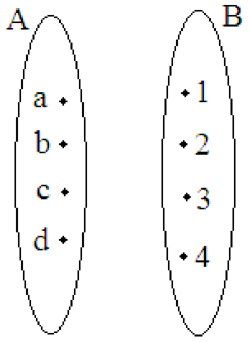
D’autre part, toute injection de A vers B est une bijection car ⋕A = ⋕ B, donc le nombre de bijections de A vers B est égal au nombre d’injections de A vers B. Or ce nombre est

$A_n^n = \dfrac{n!}{(n-n)!} = \dfrac{n!}{0!} = n!$. Donc le nombre de bijections de A vers B avec

$\text{Card}\, A = \text{Card}\, B = n$ est $n!$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Exemples :



Le nombre de bijection qu'il y a entre A et B est : A ! = 4 x 3 x 2 =24 i.e. 24 bijections entre A et B.

En particulier : si A = B, alors toute bijection de A vers A lui – même est appelée ***permutation*** de l'ensemble A.
Ainsi l'ensemble A ayant n éléments doit avoir $n!$ permutations. Et le nombre de permutations de l'ensemble A à n éléments se note : P_n.

Donc : $P_n = n!$, $(n \in IN^*)$.

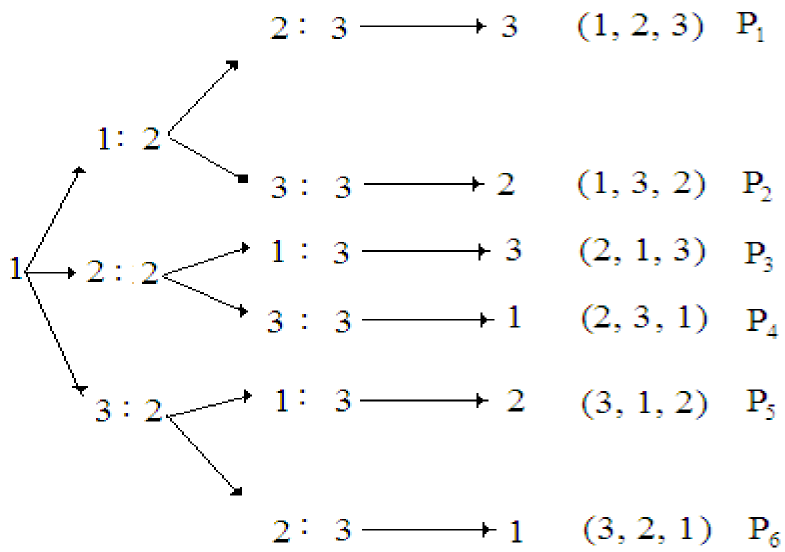
D'où le *théorème* suivant :

Le nombre de permutations de l'ensemble à n éléments est : $n! = P_n = A_n^n$ **.**

Exemples :

1) Donner les permutations de l'ensemble $A = \{1, 2, 3\}$.

   Total : $3! = 3 \times 2 = 6$ permutations de A. Ces permutations sont : $(1,2,3), (1,3,2), (2,1,3), (3,1,2)$ et $(3,2,1)$. Ci – dessous l'arbre des permutations de l'ensemble A.



2) Combien de mots peut – on former avec les lettres du mot « eau ». (chaque lettre étant prise une fois et une fois seulement).

Solution :

Soit $A = \{e, a, u\}$. Ces mots sont : eau, eua, aeu, aue, uae, uea.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Donc il y a $3!=6$ mots qu'on peut former avec les lettres du mot « eau ».

d) Nombre de partie a p éléments d'un ensemble a n éléments. (Combinaison sans répétition).

Soit A, un ensemble à n éléments (n ≥ 1) et soit $A' \subset A$, une partie à p éléments avec (p ≥ 0). *Problème :* L'ensemble A aura combien de parties à p éléments ?
Désignons par $P_p(A) \equiv$ l'ensemble des parties de A à p éléments, alors calculons $\mathrm{Card}(P_p(A))$.

- Si p = 0, il y a un et un seul sous – ensemble de A ayant 0 élément ………
  $\Rightarrow \mathrm{Card}(P_0(A)) = 1$
- $P > 0 (p \le n)$, soit $f : [1,p] \to A$, une injection, c.à.d. $f \in I([1,p], A)$

  f étant injective $\Rightarrow f([1,p]) \subset A$

  $\Rightarrow f([1,p])$ a p éléments

  $\Rightarrow f([1,p]) \in P_p(A)$

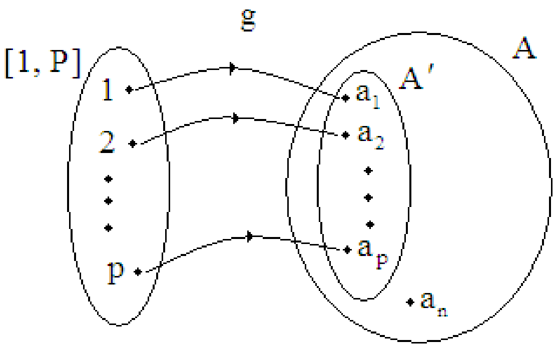
Soit $A' \in P_p(A) \Rightarrow A' \subset A$ et card $A' = p$.

Ainsi A' peut être obtenue comme image par f de $[1,p]$. i.e. $A' = f([1,p])$

Réciproquement

Soit $A' \in P_p(A)$, c.à.d. $A' \subset A$ et card $A' = p$, alors toute bijection.

$g : [1,p] \to A'$ est une injection de $[1,p] \to A$ et g détermine un arrangement de p éléments de A à n éléments.



g est une application injective.

Or il existe p! bijections entre $[A,p]$ et A', donc $P!$ injections de $[1,p] \to A$ engendrées par A'.

$$\text{D'où} : \mathrm{Card}\{I([1,p], A)\} = p!\,\mathrm{card}\,P_p(A).$$

$$\text{Soit card}\,P_p(A) = \frac{\mathrm{Card}\{I([1,p], A)\}}{P!}$$

$$= \frac{A_n^p}{P!}$$

$$\text{i.e. card}(P_p(A)) = \frac{\frac{n!}{(n-p)!}}{P!} = \frac{n!}{P!(n-p)!}$$

$$\text{D'où finalement} : \mathrm{Card}(P_p(A)) = \frac{n!}{P!(n-p)!}$$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

(1) Définition

Tout élément de $P_p(A)$ s'appelle une combinaison de n éléments pris p à p $(0 \le p \le n)$.
Donc, une combinaison de n éléments pris p à p est une **partie** à p éléments pris dans un ensemble à n éléments.
Ainsi le nombre des parties d'un ensemble à p éléments d'un ensemble à n éléments est le même que le nombre de combinaisons de n éléments pris p à p $(0 \le p \le n)$.

Ce nombre, on le note par : C_n^p ce qu'on lit « c. n. p. » ou par $\begin{pmatrix} n \\ p \end{pmatrix}$ ce qu'on lit n au – dessus de p.

Par suite :

$$C_n^p = \frac{n!}{P!(n-p)!} = \text{Card}\, P_p(A)$$

i.e. $C_n^p = \dfrac{n!}{P!(n-1)!}$

Exemples :

i. Les combinaisons des lettres a, b, c, d prises 2 à 2 sont :
(a, b), (a, c), (a, d), (b, c), (c, d).

D'après la formule on a : $C_4^2 = \dfrac{4!}{2!(4-2)!} = \dfrac{4!}{2!2!} = \dfrac{4\times3\times2}{2\times2} = 6$ combinaisons possibles.

ii. Soient $P = \{a, b, c, d, e, f\}$ l'ensemble de six points du plan affine P tels que trois d'entre eux ne soient pas alignés.

Calculer le nombre de triangles dont trois de ces points sont les sommets.

$$\text{Le nombre de triangles est} : C_6^3 = \frac{6!}{3!(6-3)!} = \frac{6\times5\times4}{3!} = 20$$

$$\text{Le nombre de droites est} : C_6^2 = \frac{6!}{2!4!} = \frac{6\times5\times4\times3\times2}{2\times4\times3\times2} = 15$$

(2) Propriétés

$P_1 : C_n^p = C_n^{n-1} \quad (p \le n)$

Effet : $C_n^{n-p} = \dfrac{n!}{(n-p)!(n-n+p)!}$

$$= \frac{n!}{(n-p)!\,p!} = \frac{n!}{p!(n-p)!} = C_n^p$$

$P_2 : C_{n-1}^{p-1} + C_{n-1}^p$

En effet : $C_{n-1}^{p-1} + C_{n-1}^p = \dfrac{(n-1)!}{(p-1)!(n-1-p+1)!} + \dfrac{(n-1)!}{p!(n-1-p)!}$

$$= \frac{(n-1)!}{(p-1)!(n-p)!} + \frac{(n-1)!}{p!(n-p-1)!}$$

$$= \frac{p(n-1)! + (n-1)!(n-p)}{p!(n-p)!}$$

$$= \frac{(n-1)!(p+n-p)}{p!(n-p)!} = \frac{(n-1)!n}{p!(n-p)!} = \frac{n!}{p!(n-p)!} = C_n^p$$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

(3) Triangle de PASCAL

La propriété P_2 conduit à la construction d'un tableau triangulaire appelé ***triangle de Pascal***. Les « 1 » qui bordent à gauche et à droite ce triangle sont les valeurs de C_n^0 et C_n^n car $C_n^0 = C_n^n = 1$.

Sur la première ligne, le seul élément « 1 » est la valeur de C_0^0.

Tout terme autre que les termes extrêmes s'obtient en additionnant le terme au – dessus et le terme à gauche de ce dernier.

Ainsi, le terme de rang p de la $n^{\text{ième}}$ ligne s'obtient en additionnant le terme de rang p – 1 et le terme de rang p de la $(n-1)^{\text{ième}}$ ligne.

D'où le tableau triangulaire ci – dessous :

$$
\begin{array}{llcl}
n & & & \\
0 & 1 & & C_0^0 \\
1 & 1 \quad 1 & & C_1^0 \quad C_1^1 \\
2 & 1 \quad 2 \quad 1 & & C_2^0 \quad C_2^1 \quad C_2^2 \\
3 & 1 \quad 3 \quad 3 \quad 1 & \text{ou} & C_3^0 \quad C_3^1 \quad C_3^2 \quad C_3^3 \\
\vdots & & & \vdots \\
n-1 & 1 \cdots C_{n-1}^{p-1} \quad C_{n-1}^{p} \cdots 1 & & \\
n & 1 \cdots \cdots \quad C_n^p \quad \cdots \quad 1 & & C_n^0 \quad C_n^1 \quad C_n^2 \cdots \quad \cdots \quad C_n^n
\end{array}
$$

(4) Binôme de NEWTON

(a) Généralités :

Dans tout anneau commutatif (A, +, ·) sont définies les expressions suivantes.

$\forall a, b \in A : (a+b)(a+b), (a+b)(a+b)(a+b)$.

Ainsi $\forall a, b \in A : (a+b)^2 = a^2 + ab + ba + b^2$

$$= a^2 + ab + ab + b^2$$

$$= a^2 + 2ab + b^2$$

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

Remarque :

Les coefficients $(1, 2, 3)$ et $(1, 3, 3, 1)$ qui interviennent respectivement dans les développements de $(a+b)^2$ et $(a+b)^3$ sont les termes de la **2ème** et **3ème** ligne du triangle de **Pascal**.

Nous nous proposons de développer : $(a+b)^n \ \forall a, b \in A, \ \forall n \in IN$.

(b) Développement de $(a+b)^n$

Théorème :

$\forall a, b \in A, \ \forall n \in IN$

$$(a+b)^n = a^n + C_n^1 \cdot a^{n-1} b + C_n^p \cdot a^{n-p} \cdot b^p + \cdots + b^n$$

$$= a^n + C_n^1 \cdot b \cdot a^{n-1} + C_n^p \cdot b^p \cdot a^{n-p} + \cdots + b^n$$

Ce que l'on condense en :

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

$$\boxed{(a+b)^n = \sum_{p=0}^{n} C_n^p a^{n-p} \cdot b^p}$$ formule du binôme de Newton. *Preuve aux exercices.*

Et les C_n^p s'appellent les coefficients binomiaux. Il faut savoir que ces coefficients binomiaux du développement de $(a+b)^n$ sont les termes de la $n^{ième}$ ligne du triangle de Pascal.

Quelques propriétés :

i. Le nombre des termes du développement de $(a+b)^n$ est $(n+1)$.
ii. La somme des exposants des termes en a et b est n.
iii. Les coefficients des termes équidistants des extrêmes dans le développement de $(a+b)^n$ sont égaux.

Remarque :

$$(a-b)^n = \left(a+(-b)\right)^n = \sum_{p=0}^{n} C_n^p (-b)^p \cdot a^{n-p}$$

$$\begin{aligned}(a-b)^4 &= \sum_{p=0}^{4} C_4^p (-b)^p \cdot a^{4-p} \\ &= C_4^0(-b)^0 a^4 + C_4^1(-b)^1 \cdot a^3 + C_4^2(-b)^2 a^2 \\ &= a^4 - 4a^3b + 6a^2b^2 - 4ab^3 + b^4\end{aligned}$$

D. LOIS DES COMPOSITIONS INTERNE ET EXTERNE

1. Lois de composition interne (LCI)

a) Généralités

(1) Définition

Soit $A \neq \Phi$. On appelle loi de composition interne dans A, toute application de A x A dans A.

Si f est cette application, ie. $f : A \text{ x } A \to A$

$$(a, b) \mapsto f(a,b) = c,$$

Alors f est dite loi de composition interne dans A et C est dit composé de a et b par la loi f.

Il est souvent commode de remplacer la notation f (a, b) par :

$a * b$ (lire a star b ou a étoile b), a T b (lire a truc b), a $\perp$ b (lire a anti-truc b), …où $(*)$, $(\perp)$, (T) sont des symboles opérationnels désignant chacun une loi de composition interne dans A.

Ainsi, dire que $(*)$ est une LCI dans A signifie que $* : A \text{ x } A \to A$

$$(a, b) \mapsto a * b = c.$$

(2) Remarques

R₁. Une LCI définie dans A est parfois dite loi partout définie dans A.

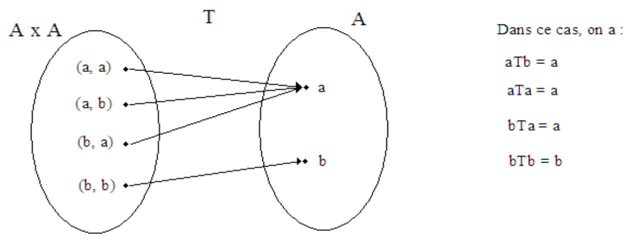
R₂. $(A, *)$ désignera une ensemble non vide A muni d'une loi de composition interne. Un tel couple est dit **magma**.

(3) Exemples

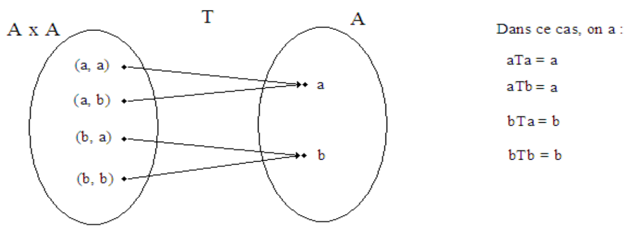
a) Définir une loi de composition interne dans A = {a, b}.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

b)
Soit (T) cette loi de composition interne dans A, alors
T : A x A $\rightarrow$ A avec A x A = {(a,a) , (a,b) (b,a) , (b,b)}
T peut être défini schématiquement par le diagramme sagittal ci – dessous



Ou



Donc on peut définir 16 lois de composition interne dans A = {a, b}

b) (+) et ($\bullet$) sont des LCI dans E = IN, Z, Q et IR car :

$+ : E \times E \rightarrow E$ et $\bullet : E \times E \rightarrow E$

$(a, b) \mapsto a + b = s$ $(a, b) \mapsto a \llcorner b = p.$

c) Les opération ensemblistes $\bigcap$, U et Δ sont des lois de composition interne dans P_E avec $E \neq \varnothing$

i.e. $\cap : P_E \times P_E \rightarrow P_E$

$(A,B) \rightarrow A \cap B = C$

$\cup : P_E \times P_E \rightarrow P$

$(A,B) \rightarrow A \cup B : C$

Illustration

Prendre A = {1,2} pour avoir $P_A = \{\varnothing, \{a\}, \{b\}, A\}$
On constate que pour

i. ($\cap$) par exemple que, $\{a\}, A \in P_A$: alors $\{a\} \cap A = \{a\} \in P_A$
$\{a\},\{b\} \in P_A : \{a\} \cap \{b\} = \varnothing \in P_A$

ii. ($\cup$) par exemple que : $\{b\}, A \in P_A : \{b\} \cup A = A \in P_A$
$\{a\},\{b\} \in P_A : \{a\} \cup \{b\} = A \in P_A$

d) Soit $E \neq \varnothing$ et $\beta(E,E) = \{p : E \rightarrow E : p$ est une permutation$\}$, alors la composition (o) des bijections est une loi de composition interne dans β (E,E) car la composée de deux bijection est une bijection.
$* : B(E,E) \times B(E,E) \rightarrow B(E,E)$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

$(f,g) \to f \circ g = h$

Par contre (-) n'est pas une loi de composition interne dans IN car $\exists 1,2 \in$ IN : $1 - 2 \notin$ IN
Aussi T définie comme suit n'est pas une loi de composition interne dans IN

T: IN x IN $\to$ IN

$(a,b) \to aTb = a^b$ car $\exists o \in$ IN : $oTo = 0^o \notin$ IN

Mais $\perp$ défini de la manière suivante : IN* x IN* $\to$ IN*

$(a,b) \to a \perp b = a^b$ est une loi de composition interne dans N*

Remarque

Si A est un ensemble fini d'éléments, on peut utiliser la table de Pythagore pour définir une loi de composition interne dans A. La 1[er] colonne et la 1[er] ligne de ce tableau reprennent les éléments de A.

a. Définir par exemple une loi de composition interne ($*$) dans A = {a,b}en utilisant la table de Pythagore, on a :

*	a	b
a	a	a
b	b	b

Ainsi $a * a = a$; $a * b = a$; $b * a = b$ et $b * b = b$

b. (+) Est – elle une loi de composition interne dans A = {1, 0,1} $\subset$ Z ?

Pour répondre a cette question, utilisons la table de Pythagore. On a :

+	1	0	-1
1		1	0
0	1	0	-1
-1	0	-1	

On constate que $1 + 1 \notin A$
Donc (+) n'est pas une loi de composition interne dans A

b) Partie stable, Partie permise et loi induite

Soit (E,*) un magma et $A \subset E$

(1) Partie stable

A est dite partie stable de E pour la loi de composition interne (*) si $A * A \subset A$, i.e. $\forall a,b \in A$ on a : $a * b \in A$

(2) Partie permise

A est dite partie permise de E pour la loi de composition interne si $A \times E \subset A$ et $E \times A \subset A$, i.e. $\forall a \in A$ on a : $\forall e \in A : a * e \in A$ et $e * a \in A$

(3) Loi induite

Soit (E,*) un magma et $A \subset E$, une partie stable de E pour la loi de composition interne (*). Alors la loi : (*') définie dans A de la manière suivante :

*' : A x A $\to$ A

$(a,b) \to a*'b = a*b$ est dite loi induite sur A par la loi de composition ($*$) de Z

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Exemples :

a. Considérons l'ensemble Z muni de deux loi,de composition interne (+) et (.) et
$A = pZ = \{pZ : z \in Z\}$ appelé ensemble des multiples de p avec $p\in IN$.

a_1 Montrons que A est une partie stable de Z pour les loi (+) et (.)

- En effet $\forall$ u, $v\in A$, montrons que $u + v\in A$

En effet :

- $u\in A \Rightarrow \exists z\in Z : u = pz$
- $v\in A \Rightarrow \exists z'\in Z : u = pz'$

Alors $u + v = pz + pz' = p(z+z') = pz''\in A$ avec $z'' = z + z'\in Z$

- Montrons que $\forall u,v\in A : u.v\in A$

En effet $u.v = pz . pz' = p(z.p.z') = p.z''\in A$ avec $z'' = z.p.z'\in Z$.

a_2 Montrons que A est une partie permise de Z pour (.) i.e. $\forall u\in A, \forall z\in Z : uz\in A$
En effet, $u\in A \Rightarrow \exists k\in Z : u = pk$
Il suit que $u.z = (p.k)z = p(k.z) = p.z' \in A$ avec $z'= k.z\in Z$
Donc $u.z \in A$.

a_3 A n'est pas partie permise de Z pour (+) car on peut trouver z dans Z et $u \in A$ tel que $u+z \notin A$

b. Considérons l'ensemble IR muni de deux loi de composition (+) et (.),
$IR+ = \{x\in IR : x\geq 0\}$ et $IR_- =\{x\in IR : x\leq 0\}$ respectivement ensemble des réel positifs et des réels négatifs.

b_1 IR_+ est une partie stable de IR pour les lois (+) et (.)
Car $\forall x, y\in IR_+$ $x+y \in IR_*$ et $x.y \in IR_+$
En effet $x, y \in IR \Rightarrow x\geq 0$ et $y\geq 0$
$\Rightarrow x + y\geq 0$ et $x.y\geq 0$
$\Rightarrow x + y\in IR_+$ et $x.y\in IR_+$

Par contre IR_+ n'est partie permise de IR ni pour la loi (+) ni pour la loi (.) car
$\exists(-5)\in IR$ et $3\in IR_+$ tel que : $-5 +3 = -2 \notin IR_+$ et $-5.3 = -15\notin IR_+$

b_2 IR_- est – elle partie stable de IR pour les lois (+) et (.) ?
Est – ce partie permise de IR pour les loi (+) et (.) ?

c) Qualité d'une loi de composition interne

Soit E un ensemble non vide muni de deux lois de composition interne $(*)$ et (T)

(1) Associativité

On dit que la loi $(*)$ est associative dans E si $\forall a, b, c\in E$, on a : $a* (b* c) = (a* b) * c$

(2) Commutativité

On dit que la loi $(*)$ est commutativité dans E si $\forall a, b\in E$, on a : $a* b = b* a$

N.B. si $(*)$ n'est pas commutative dans E et qu'il existe $a, b\in E$ tel que : $a* b = b* a$, on dit alors que a et b sont des éléments commutables ou permutables de E.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

(3) Distributivité d'une loi par rapport à une autre

On dit que la loi (T) est distributive par rapport à ($\ast$) si $\forall$ a, b, c$\in$ E, on a :
a T (b$\ast$c) = (a T b) $\ast$ (a T c) et (b$\ast$c) T a = (b T a) $\ast$ (c T a)

Exemples :

i. l'addition (+) et la multiplication (.) sont commutatives et associatives dans IN, Z, Q, et IR.

ii. ($\cap$),($\cup$) et (Δ) sont commutatives et associatives dans P_E avec E $\neq$ Ø.

iii. (.) est distributive par rapport à (+) dans IN, Z, Q et IR tout comme l' ($\cap$) est distributive par rapport à $\cup$ et Δ dans $P_{E.}$

iv. La loi T définie dans IN* par $\forall$ a,b$\in$ IN* : a T b = a^b n'est commutative car $\exists$ 2,3 $\in$ IN* : 2 T 3 $\neq$ 3T² i.e. 8 $\neq$ 9.

Mais $\exists$2,4 $\in$ IN* tel que 2 T 4 = 4 T 2 = 16
$\Rightarrow$2 et 4 sont des éléments commutables de IN*

TP : Soit IR l'ensemble de nombres réels muni de la loi ($\ast$) définitie comme suit :
$\forall$ a, b $\in$ IR : a$\ast$b = a + b + ab. ($\ast$) Est – elle commutative ? Associative ?
($\ast$) Est – elle distributive par rapport à (+) ?

d) Eléments remarquables d'une loi

Soit (E,*) un magma avec E $\neq$ Ø

(1) Élément neutre

On dit que l'ensemble E admet un élément neutre (n) pour la loi ($\ast$) si: $\forall$ x$\in$ E, on a :
x$\ast$n = x = n$\ast$x
Si x$\ast$n = x, alors n est l'élément neutre a droite de E.
Si n$\ast$x = x, alors n est l'élément neutre a gauche de E.
Si la loi ($\ast$) est commutative, alors il suffit de chercher soit l'élément neutre à droite, soit l'élément à gauche.

Propriété :
Si un ensemble E admet un élément neutre (n) pour ($\ast$), alors cet élément neutre est unique

(2) Elément symétrisable

(a) Définition :

Soit (E, $\ast$) un magma où ($\ast$) admet un élément neutre (n)
Alors x'$\in$ E est dit symétrique de x$\in$ E pour la loi ($\ast$) si x$\ast$x' = n = x'$\ast$x
Si x'$\ast$x = n, on dit alors que x' est le symétrique à droite de x
et x $\ast$x' = n, on dit alors que x' est le symétrique à gauche x
Si la loi ($\ast$) est commutative, alors il suffit de chercher soit le symétrique à droite, soit le symétrique gauche.

(b) Proposition :

Soit (E,$\ast$) un magma où ($\ast$) est associative et admet un élément neutre (n). Alors le symétrique d'un élément de E, s'il existe, est unique.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

(c) Vocabulaire

Un élément de E est dit symétrisable s'il admet son symétrique

Le symétrique d'un ensemble de E par

- La loi (+) est dite opposé,
- La loi (.) est dite inverse,
- La loi (o) est dite réciproque.

(d) Exemples

i. Soit (E = IN, Z, Q et IR, (+) et (.) deux loi de composition interne dans E alors
- 0 est l'élément neutre de E pour (+) car $\forall x \in E : x + 0 = x = 0 + x$
- 1 est l'élément neutre pour (.) dans E car $\forall x \in E : x .1 = x = 1 .x$

ii. Dans P_E muni des lois $(\cap)$,$(\cup)$ et (Δ),
- E est l'élément neutre pour $(\bigcap)$ car $\forall A \in P_E$: on a $A \bigcap E = A$.
- Ø est l'élément neutre pour $(\bigcup)$ car $\forall A \in P_E$: on a $A \bigcup Ø = A$
- Ø est l'élément neutre pour (Δ) car $\forall A \subset P_E$: on a $A \Delta Ø = A$ et le symétrique de $A \in P_E$ pour la loi (Δ) est A

iii. Soit (IR, $*$) un magma où $a * b = a + b + ab$ $\forall a,b \in$ IR
- Chercher l'élément neutre de IR par la loi ($*$).
- Chercher l'élément symétrique de $a \in$ IR par la loi ($*$) s'il existe.

Réponses :
- Soit $n \in$ IR l'élément neutre pour la loi de composition interne ($*$) s'il existe, alors $\forall a \in$ IR, on a : $a * n = a$
  En effet $a * n = a$ ssi $a + n + an = a \Leftrightarrow a + n (1 + a) = a \Leftrightarrow n(1 + a) = 0 \Leftrightarrow$ $\boxed{n = 0}$
  $\Rightarrow n = 0$ est l'élément neutre de IR pour la loi ($*$).

- Soit a', le symétrique de $a \in$ IR pour ($*$) s'il existe, alors $a * a' = 0$
  En effet, $a * a' = 0$ ssi $a + a' + aa' = 0$ ssi $a' + aa' = - a$ ssi $a'(1 + a) = - a$ ssi
  $a' = \dfrac{-a}{1+a}$ si $a \neq -1$. D'où le symétrique de $a \in$ IR est $\dfrac{-a}{1+a}$ si $a \neq -1$.

iv. Soit (F = IR x IR, T) un magma où (a, b) T (c, d) = (ac, bc + d). $\forall$ (a,b) , (c,d)$\in F^2$
- Chercher l'élément neutre de F pour la loi (T) s'il existe.
- Chercher l'élément symétrique de $(a, b) \in$ F s'il existe :

Recherche de l'élément neutre de F pour la loi (T) s'il existe.

Soit $(n,n') \in$ F l'élément neutre pour la loi (T), alors $\forall (a,b) \in$ F on a :

(a,b) T (n,n') = (a,b) T (a,b)

Résolvons la 1er équation : (a, b) T (n,n') = (a,b)

En effet, (a, b) T (n, n') = (a, b) $\Leftrightarrow$ (an, bn + n') = (a, b).

$$\Leftrightarrow \begin{cases} an=a \\ bn+n'=b \end{cases}$$

$$\Leftrightarrow \begin{cases} n=1 \\ n'=0 \end{cases}$$

$\Rightarrow$ (1, 0) est, l'élément neutre à droite de F pour la loi (T).

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Vérifions que (1, 0) est élément neutre à gauche de F pour la loi (T)
i.e. (1, 0) T (a, b) = (a, b).
En effet, (1, 0) T (a, b) = (1.a, 0.a + b) = (a, b).
D'où (1, 0) est l'élément neutre de F pour la loi (T)

Recherche de l'élément symétrique de (a,b)$\in$ F pour la loi (T)
Soit (a', b')$\in$ F l'élément symétrique s'il existe, (a,b) pour la loi (T), alors
(a, b) T (a', b') = (1,0) = (a', b') T (a, b)
Résolvons l'équation (a, b) T (a', b') = (1, 0)
En effet, (a, b) T (a', b') = (1, 0) $\Leftrightarrow$ (aa', ba' + b') = (1,0)

$$\Leftrightarrow \begin{cases} aa' = 1 \\ ba' + b' = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} a' = \frac{1}{a} & \text{si } a \neq 0 \\ b' = -\frac{b}{a} \end{cases}$$

Il s'en suit que si a $\neq$ 0, le couple $(\frac{1}{a}, -\frac{1}{b})$ est le symétrique à droite de (a, b) pour la loi T

comme $(\frac{1}{a}, -\frac{1}{b})$ T (a, b) = (1, 0), alors$(\frac{1}{a}, -\frac{1}{b})$ est aussi symétrique à gauche de (a, b)

D'où le symétrique de (a, b)$\in$ E est $(\frac{1}{a}, -\frac{1}{b})\in$ E si a $\neq$ 0

(3) Elément régulier ou simplifiable

Définition

Un élément r de E est dit régulier si $\forall$ a, b$\in$ E, on a :
$a * r = b * r \Rightarrow a = b$ et $r * a = r * b \Rightarrow a = b$.

(4) Elément idempotent

Définition

Un élément i de E est élément idempotent pour la loi ($*$) si $i * i = i$.
Noter que tout élément neutre (n) est idempotent car $n * n = n$.
Un ensemble peut avoir plusieurs éléments idempotents

(5) Elément absorbant ou singulier

Un élément $\in$ de E est dit absorbant ou singulier pour la loi ($*$) si$\forall$ a $\in$ E, on a :
$a * s = s = s * a$.
Notons que si un ensemble admet un élément absorbant, alors cet élément est unique

Exemple:

a. Dans (E = IN, Z, Q, IR,.)

0 est absorbant car $\forall$ a $\in$ E, a$\llcorner$0 = 0

b. Dans P $_E$ muni des lois ($\bigcap$) et (U),

- Φ est l'ensemble absorbant pour ($\bigcap$) car A$\bigcap \Phi = \Phi$, $\forall$ A $\in P_{E.}$
- E est l'ensemble absorbant pour (U) car A U E = E, $\forall$ A $\in P_{E.}$
- Chaque élément de P_E est idempotent pour (U), ($\bigcap$) car $\forall$ A$\in P_E$:

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

$A \cap A = A = A \cup A$.

c) Considérons l'ensembles IR muni de la loi ($*$) défini par $\forall$ a,b $\in$ IR : $a*b = a + b + ab$. Cherchons les éléments idempotents et singuliers de IR pour ($*$) s'ils existent.

(c_1) *Idempotent*:
Soit i $\in$ IR : i est idempotent, si $i*i = i$.
En effet: $i*i = i \Leftrightarrow i + i + ii = i \Leftrightarrow 2i + i^2 = i \Leftrightarrow i + i^2 = 0 \Leftrightarrow i(1 + i) = 0$
$\Leftrightarrow$ **i = 0** ou **i = -1**
Dou les éléments idempotents de (IR, $*$) sont 0 et -1.

(c_2) *élément absorbant :*
Soit S$\in$ IR. S est un élément absorbant de R par (*) la loi si $\forall$ a$\in$ IR : $a * s = s$
En effet $a * s = s \Leftrightarrow a + s + as = S \Leftrightarrow a(s + 1) = 0 \Leftrightarrow s = -1$
D'où (-1) est l'élément absorbant de (IR, $*$)

e) Loi Produit

(1) Définition

Soient (E, $*$) et (F, T) deux magma, avec $E \neq \Phi \neq F$.
Comme $E \neq \Phi \neq F$, alors **EXF = {(a, b) : a $\in$ E, b $\in$ F}** existe, alors
la loi (Δ) définie dans EXF par :
$\Delta : (E \times F) \times (E \times F) \longrightarrow E \times F$
$[(a, b), (c, d)] \longmapsto (a, b)\,\Delta\,(c, d) = (a*c, b\,T\,d)$, est dite **loi produit.**

(2) Remarques

R_1. Si ($*$) et (T) sont associatives et commutatives dans E et F, alors (Δ) l'est aussi dans E x F.
R_2. Si n est l'élément neutre de ($*$) dans E et n'est élément neutre de (T) dans F, alors (n, n') est l'élément neutre de (Δ) dans E x F.
R_3. Si a' est l'élément symétrique de a dans E pour la loi ($*$)et b' l'élément symétrique de b dans F pour la loi (T), alors (a', b') est le symétrique de (a, b) pour la loi (Δ) dans E x F.

(3) Exemples

a. Soient (Z, +) et (IR, +) deux magma. La loi (Δ) définie dans Z x IR par
$(a, b)\,\Delta\,(c, d) = (a + c, b + d)$ est une loi produit dont (0, 0) est l'élément neutre et (-a,-b) est le symétrique de (a, U) dans E, de même la loi (Δ) est commutative et associative.

b. Soient (Z, +) et (IR, •) deux magma.

i. La loi (Δ) définie dans F = Z x IR par $\forall$ (a, b) • (c, d) $\in$ F
$(a, b)\,\Delta\,(c, d) = (a + c, b.d)$ est une loi produit.

L'élément neutre de F pour la loi (Δ) est (0,1) et le symétrique de (a, b) $\in$ F pour la loi (Δ) est $(-a, \frac{1}{b})$ si $b \neq 0$.
De même (Δ) commutative et associative dans F.

ii. La loi (Δ) définie dans C = IR x IR par $\forall$ (a, b) • (c, d) $\in$ G :

(a, b) Δ (c, d) = (a.c, b.d) est une loi produit.

Montrer au TP que l'élément neutre de C pour la loi (Δ) est (1, 1) et le symétrique de (a, b) pour la loi (Δ) est $(\frac{1}{a}, \frac{1}{b})$ si $a \neq 0$, $b \neq 0$.

f) Loi Quotient

(1) Définition

Soit $(E, *, R)$ un triplet où $(*)$ est une loi de composition interne et R une relation d'équivalence. Puisque R est une relation d'équivalence dans E, alors E/R existe avec $E/R = \{\mathring{a} : a \in E\}$ appelé ensemble quotient de E par la relation R. Comme $(*)$ est une loi de composition interne dans E, on peut être tenté de définir une loi de composition interne dans E/R.

Pour cela, il faut que $(*)$ soit compatible avec la relation (R), ie.
$\forall$ a, b, c, d $\in$ E : a R b et c R d $\Rightarrow$ $(a*c)$ R $(b*d)$

Dans ces conditions, on peut définir la loi $(\dot{*})$ dans E/R de la manière suivante :

$\forall\ \dot{a}, \dot{b} \in E/R : \dot{a} \,\dot{*}\, \dot{b} = \dot{\widehat{a * b}}$ et $(\dot{*})$ est dite loi quotient dans E/R.

(2) Remarque

Si $(*)$ est associative et commutative dans E, alors $(\dot{*})$ l'est aussi dans E/R.

Si n est l'élément neutre de $(*)$ dans E alors $\dot{n}$ est l'élément neutre de $(\dot{*})$ dans E/R.

Si x' st le symétrique de x dans E pour la loi $(*)$ alors $\dot{x}'$ est symétrique de $\dot{x}$ pour la loi $(\dot{*})$.

(3) Exemples

Considérons $(Z, +, x, \equiv [P])$ où la relation de congruence modulo p, avec $p \in$ IN*est définie par : $\forall$ x, y $\in$ Z : on a $x \equiv y\ [P]$ ssi $\exists k \in Z : x - y = kp$. Comme $(\equiv [P])$ est une relation d'équivalence alors $Z_P = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}, \ldots, \dot{\widehat{p-1}}\}$ existe. On peut alors définir une loi quotient dans Z_P.
Puisque (+) et (x) sont commutatives, alors elles sont compatibles avec $(\equiv [P])$.

Ce qui entraîne que les lois $(\dot{+})$ et $(\dot{x})$ peuvent être définies dans Z_P par $\forall\ \dot{a}, \dot{b} \in Z$:

On a : $\dot{a} \dot{+} \dot{b} = \dot{\widehat{a+b}}$ et $\dot{a}\ \dot{x}\ \dot{b} = \dot{\widehat{ab}}$.

Illustration : prenons p = 5 pour avoir $Z_5 = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{4}\}$ alors pour $\dot{3}, \dot{4} \in \mathbf{Z}_5$ on :

$\dot{3} \dot{+} \dot{4} = \dot{\widehat{3+4}} = \dot{2}$ et $\dot{3} \dot{x} \dot{4} = \dot{\widehat{3 x 4}} = \dot{2}$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

D’où la table de Pythagore pour les ($\dot{+}$) et ($\dot{x}$) dans $\mathbf{Z}_5$ est établie comme suit

$\dot{+}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{0}$
$\dot{2}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{0}$	$\dot{1}$
$\dot{3}$	$\dot{3}$	$\dot{4}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{4}$	$\dot{4}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$

$\mathbb{Z}_5$ $\mathbb{Z}_5$

et

$\dot{\times}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{1}$	$\dot{3}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{1}$	$\dot{4}$	$\dot{2}$
$\dot{4}$	$\dot{0}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

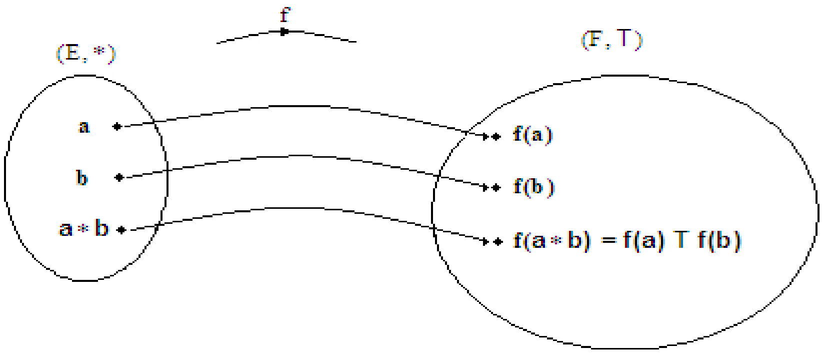
$\mathbb{Z}_5$ $\mathbb{Z}_5$

TP : Etablir le Table de Pythagore des lois ($\dot{+}$) et ($\dot{x}$) dans Z_3, Z_4, Z_5, Z_6 et Z_7.

g) Morphisme des Magmas

(1) Définition

Soient $(E, *)$ et (F, T) deux magma et $f : E \rightarrow F$, une application. f est dit morphisme des magma si $\forall$ a, b $\in$ E : on a : $f(a * b) = f(a)\ T\ f(b)$.



(2) Vocabulaire

Un morphisme injectif est dit monomorphisme, en abrégé mono.
Un morphisme surjectif est dit épimorphisme, en abrégé épi.
Un morphisme bijectif est dit isomorphisme, en abrégé iso.
Tout morphisme de E dans E est dit un endomorphisme, en abrégé endo, et tout endo bijectif est dit un automorphisme.

(3) Exemples

a. Soit a > 1 et a $\neq$ 1 l’application $\exp_a$; (IR, +) $\rightarrow$ ($\mathbb{R}^*_+$, •) :

$x \mapsto \exp_a(x) = a^x$ est un morphisme

Montrons que $\exp_a$ est un morphisme, ie. $\forall$ x, y$\in$ IR : $\exp_a(x + y) = \exp_a x . \exp_a y$.
En effet, $\exp_a(x + y) = a^{x+y} = a^x . a^y = \exp_a x . \exp_a y$ cqfd.

b. Soit f : ($\mathbb{R}^*_+$,•) $\rightarrow$ (IR, +)

$x \mapsto f(x) = \log_a x$ une application. Montrons que f est un morphisme avec a>1 et a $\neq$ 0.

En effet, $\forall x, y \in IR^*_+ : f(x.y) = \log_a(xoy) = \log_a x + \log_a y = f(x) + f(y)$

c. Soit p : (E, $*$) $\rightarrow$ (E/R, $\dot{*}$)

$a \quad \mapsto \quad p(a) = \dot{a}$ une application, montrons que p est un morphisme.

En effet, $\forall$ a, b$\in$ E : $p(a * b) = \overbrace{a * b}^{\bullet} = \dot{a} \dot{*} \dot{b} = p(a) \ \dot{*} \ p(b)$.

d. Par contre l'application f : (IR,+) $\to$ (IR,+)

$x \mapsto f(x) = ax + b$ n'est pas un endo

Car $\forall$ x, y $\in$ IR on a : $f(x+y) \neq f(x) + f(y)$.

En effet, $f(x+y) = a(x + y) + b = ax + ay + b = (ax + b) + ay = f(x) + ay \neq f(x) + f(y)$

(4) Théorème 1 sur les morphismes des magmas

Soient (E,$*$) et (F, T) deux magma et f : E $\to$ F un morphisme des magmas

1° f(E) est une partie stable de F pour la loi induite (T)

2° si (n) est l'élément neutre de E pour la loi ($*$) et (n') l'élément neutre deF pour la loi (T), alors f(n) = n'

3° si x' est le symétrique de x dans E pour ($*$), alors f(x') est le symétrie de f(x) dans f(E) pour (T) et on a : f(x') = [f(x)]'.

(5) Définition (noyau)

Soient (E,$*$), (F,T) deux magma ayant pour élément neutre respectif n et n' et f : (E,$*$) $\to$ (F, T) un morphisme

On appelle noyau de f noté Kerf l'ensemble des éléments de E qui ont pour image l'élément neutre (n') de F. ie. Kerf = {x$\in$ E : f(x) = n'}. Noter Kerf $\neq$ Ø car n $\in$ Kerf.

2. Loi de composition externe

a) Définition

Soient E $\neq$ Ø et K $\neq$Ø deux ensembles donnés.

On appelle loi de composition externe sur E à scalaires dans K toute application φ de K x E dans E, i.e.

φ : K x E $\to$ E

$(\alpha,\mu) \to \varphi(\alpha,\mu) = \alpha\mu$ dite multiplication externe.

$\mu\in$ E est dit vecteur et $\alpha \in$ K est dit scalaire

Exemples

a. Toute loi interne ($*$) dans E est externe dans E à scalaire dans E, i.e.

$* : E \times E \to E$

$(\alpha, \mu) \to \alpha * \mu$

b. Soit E l'ensemble des vecteurs libres de la géométrie plane, alors la multiplication d'un vecteur par un nombre réel est un vecteur, on définit une loi de composition externe sur E à scalaires dans IR, on a :

$* : IR \times E \to E$

$(\alpha, \vec{u}) \to \alpha.\vec{u} = \alpha\vec{u}$

L'application : Z x $Z_p \to Z_p$

$(z, \dot{a}) \to z\dot{a} = \overbrace{\alpha.u}^{\bullet}$ est une loi de composition interne sur Z_p à scalaires dans Z.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

b) Définition

E muni d'une loi de composition externe (.) à scalaires dans Z A est dite partie stable de E pour la loi de composition externe (.) si $\forall a \in K, \forall u \in A : au \in A$

c) Propriétés d'une une loi de composition externe

Soient (E, T, •) et (K, $\perp$) où (•) est une loi de composition externe dans E à scalaires dans K.

P_1 Si ($\perp$) est associative dans K, alors (.) est associative par rapport à ($\perp$) si $\forall \alpha,\beta \in K$, $\forall u \in E$:on a :$(\alpha \perp \beta).u = \alpha.(\beta.u)$

P_2 La loi de composition externe (•) est distributive par rapport à (T) de E si $\forall a, \forall u,v \in E$: on a $\alpha(uTv) = (\alpha u)\ T\ (\alpha v)$.

P_3 (•) est distributive par rapport aux lois internes (T) et ($\perp$) si $\forall \alpha, \beta \in K$, $\forall u \in E$: $(\alpha \perp \beta).u = (\alpha.u)\ T\ (\beta.u)$.

P_4 $\forall u \in E$, $1_k.u = u$.

CHAPITRE III
STRUCTURES ALGEBRIQUES

A. INTRODUCTION

Soit E un ensemble non vide. Si sur cet ensemble, on a défini :

- une ou plusieurs lois de composition (interne ou externe).
- une ou plusieurs relations,

On dit que E est muni d'une structure algébrique.
Donc conférer une structure algébrique à un ensemble non vide c'est munir cet ensemble d'une ou plusieurs lois de composition (interne ou externe) ou d'une ou plusieurs relations.
Dans notre cours, on va étudier les structures algébriques fondamentales à savoir : groupe, anneau, corps et espace vectoriel.
Mais, avant d'en arriver là, il faut savoir que :

1. ***Un groupoïde*** ou ***magma*** est un ensemble non vide muni d'une loi de composition interne.
2. ***Un Demi - groupe*** est un magma dont la loi de composition interne est associative.
3. ***Un Monoïde*** est un demi - groupe où la loi de composition interne admet un élément neutre.

   Si dans un monoïde chaque élément a son symétrique, alors ce monoïde devient un groupe.

   Exemple : (IN, +); (IN, $\cdot$); ($\mathbf{Z}$, +), ($\mathcal{P}_{E,}\cap$), ($\mathcal{P}_{E,}\cup$), ($\mathcal{P}_{E,}\Delta$), (Q, +), (Q, **.**), (IR, +) et (IR, **.**) sont des monoïdes.

B. GROUPE

1. Définition et propriétés

a) Définition :

Soit $G \neq 0$ et ($*$) une loi de composition interne définie dans G, alors (G, $*$) est dit groupe si :

i) ($*$) est associative, ie $\forall$ a, b, c $\in$ G, on a : $(a*b)*c = a*(b*c)$.

ii) ($*$) admet un élément neutre dans G, ie $\exists n \in G$ tel que $\forall x \in G$, on a : $x*n = x = n*x$.

iii) Chaque élément x de G admet son symétrique $x^{-1} \in G$. ie : $x*x^{-1} = n = x^{-1}*x$.

- Si ($*$) est commutative, alors (G,$*$) est dit groupe abélien ou groupe commutatif.
- Si G est un ensemble fini de cardinal n, ie #G = n, avec $n \in IN^*$, alors (G, $*$) est dit groupe fini d'ordre n.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

b) Exemples :

a) Le couple (E = $\mathbf{Z}$, Q, IR, +) est un groupe abélien d'élément neutre 0. Le symétrique de a étant (–a).

b) Le couple (F = Q^*, IR^*, •) est un groupe abélien d'élément neutre 1.

c) Soit le couple ($\mathbf{Z}$ xIR^*, Δ) où Δ est une loi produit définie par (a, b)Δ(c, d) = (a+c, b.d), alors ($\mathbf{Z}$ xIR^*, Δ) est un groupe abélien dont (0, 1) est l'élément neutre et le symétrique de (a, b) est (-a, $\frac{1}{b}$).

- Le couple (ExE, Δ) où (a, b)Δ(c, d) = (a+c, b+d) est un groupe abélien d'élément neutre (0,0) et le symétrique de (a, b) est (-a, -b).
- Le couple (FxF, Δ) où (a, b) Δ(c, d) = (a.c, b.d) est aussi un groupe abélien dont (1, 1) est l'élément neutre et $(\frac{1}{a}, \frac{1}{b})$ est le symétrique de (a, b).

d) Le couple ($\mathcal{P}_E$, Δ) est un groupe abélien ayant pour élément neutre $\varnothing$ et le symétrique de A$\in \mathcal{P}_E$ est A.

T.P. : 1. (IR, T) où aTb = a + b + ab est-ce un groupe ? Est-ce abélien ?

2. (IR^*xIR, $\perp$) où (a, b)$\perp$(c, d) = (ac, bc + d), est-ce un groupe ? Est-ce abélien ?

3. Soit B(E, E), l'ensemble des permutations de E et (o), loi de composition des applications. Montrer que (B(E, E), o) est un groupe non commutatif en général.

c) Propriété fondamentale d'un groupe

Soit (G, $*$) un groupe. Alors $\forall$ a, b$\in$ G, l'équation x$*$a = b ou a$*$x = b admet une solution et une seule en x$\in$ G.
En effet, a$\in$ G $\Rightarrow$ a^{-1} existe dans G.
Comme x$*$a = b, alors $(x*a)*a^{-1} = b*a^{-1} \Leftrightarrow x*(a*a^{-1}) = b*a^{-1} \Leftrightarrow x*n = b*a^{-1} \Leftrightarrow \boxed{x = b*a^{-1}}$.
Puisque $a^{-1}\in G$ et b$\in$ G, alors $x = b * a^{-1}\in G$, on montre de même que a $*$ x = b ssi $x = a^{-1}* b \in G$.

Exemple:
Résoudre dans:
a) (Z, +), l'équation : x + 3 = 7

Solution :
3$\in \mathbf{Z}$ $\Rightarrow$-3$\in \mathbf{Z}$, comme x + 3 = 7, alors x + 3 + (-3) = 7 + (-3) $\Leftrightarrow$ x + (3 – 3) = 7 – 3
$\Leftrightarrow$ x + 0 = 4
$\Leftrightarrow$ x = 4. D'où $S = \{4\}$

b) ($\mathcal{P}_E$, Δ), l'équation : A Δ X = B, pour A, B $\in \mathcal{P}_E$

Solution :

A$\in \mathcal{P}_E \Rightarrow$ le symétrique de A par la loi Δ est A.
Alors A Δ X = B $\Leftrightarrow$ A Δ (A Δ X) = A Δ B
$\Leftrightarrow$ (A Δ A) Δ X = A Δ B

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

$\Leftrightarrow \varnothing \Delta X = A \Delta B$

$\Leftrightarrow X = A \Delta B$. D'où $S = \{A \Delta B\}$

c) Dans (IN, +), l'équation x + 3 = 7.

$$x + 3 = 7 \Leftrightarrow x + 3 = 4 + 3$$
$$\Leftrightarrow x = 4.$$

NB : Corollaire : Dans un groupe, chaque élément est régulier. (Preuve au TP).

2. Sous – groupe

a) Définition :

Soient $(G, *)$ un groupe et $H \subset G$.

H est dit sous – groupe de G pour la loi induite $(*)$ si :

- $H \neq 0$.
- H est stable pour la loi $(*)$, ie $\forall$ a, b$\in$ H : $a*b \in H$.
- Chaque élément de H est symétrisable par la loi $(*)$ i.e. $\forall$ a $\in$ A : on a $a^{-1} \in H$.

b) Théorème :

Soient $(G, *)$ un groupe et $H \subset G$, alors $(H, *)$ est un sous – groupe de $(G, *)$ ssi

- $H \neq 0$.
- $\forall$ a, b$\in$ H : $a*b^{-1} \in H$. (Preuve au TP).

c) Remarque :

R₁. Tout sous – groupe H de G admet le même neutre (n) que le groupe $(G,*)$, ie $n \in H$.
Ainsi, dire que $H \neq \varnothing$ revient à monter que $n \in H$.

R₂. $(\{n\}, *)$ et $(G, *)$ sont aussi des sous – groupes de $(G,*)$ dits sous-groupes triviaux de $(G,*)$.

d) Exemples :

a) Soit $(\mathbf{Z}, +)$, un groupe, alors, tout sous – groupe de $\mathbf{Z}$ et de la forme :
$H = p\mathbf{Z} = \{p.z : z \in \mathbf{Z}\}$, dit ensemble des multiples de p avec $p \in$ IN.
Si p = 0, alors $H = 0\mathbf{Z} = \{0\}$.
Si p = 1, alors $H = 1\mathbf{Z} = \mathbf{Z}$.
$\Rightarrow \{0\}$ et $\mathbf{Z}$ sont les deux sous – groupes triviaux de $(\mathbf{Z}, +)$.

Montrons que $(H = p\mathbf{Z}, +)$ est un sous – groupe de $(\mathbf{Z}, +)$.

1. $H \neq \varnothing$ car $0 \in H$ parce que 0 = p.0 avec $z = 0 \in \mathbf{Z}$
2. H est une partie stable de $\mathbf{Z}$ pour (+) car $\forall$ u, v$\in H = p\mathbf{Z}$: $u + v \in H$. *Déjà démontré.*
3. $\forall u \in H$: montrons que $-u \in H$.
   En effet $u \in H \Rightarrow \exists z \in \mathbf{Z}$: u = pz.
   $u = pz \Rightarrow -u = -(pz) = p(-z)$.
   Comme $-z \in \mathbf{Z}$, alors $-u = p(-z) \in H$. Ce qui entraîne que $(-u) \in H$.

En particulier, $(2\mathbf{Z} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}, +)$ est un sous – groupe de $(\mathbf{Z}, +)$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

($3\mathbf{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$, +) est sous – groupe de ($\mathbf{Z}$, +).
En général, ($p\mathbf{Z} = \{\ldots, -4p, -3p, -2p, -p, 0, p, 2p, 3p, 4p, \ldots\}$, +) est un sous – groupe de ($\mathbf{Z}$, +).

b) On sait que (IRxIR, Δ) où (a, b) Δ(c, d) = (a + c, b + d) est un groupe abélien dont (0, 0) est l'élément neutre et (-a, -b) est le symétrique de (a, b).
Soient $E = \{(a, b)\in IR^2 : a + b = 0\}$ et $F = \{(a, b)\in IR^2 : a + b = 1\}$, deux sous-ensembles de IRXIR.
b$_1$. Montrons que (E, Δ) est un sous – groupe de (IR^2, Δ).
i) On constate $E \neq \varnothing$ car $(0, 0)\in E$ parce que 0 + 0 = 0.
ii) $\forall$ u = (a, b), v = (c, d)$\in$ E : (a, b) Δ (c, d)$\in$ E
En effet (a, b)$\in$ E $\Rightarrow$ a + b = 0 et
(c, d)$\in$ E $\Rightarrow$ c + d = 0.
Montrons que (a, b) Δ(c, d) = (a + c, b + d) $\in$ E , ie (a + c) + (b + d) = 0.
En effet (a + c) + (b + d) = a + (b + c) + d = (a + b) + (c + d) = 0 + 0 = 0
iii) $\forall$ (a, b) $\in$ E : $(a, b)^{-1}\in E$.
En effet : (a, b)$\in$ E et $E\subset IR^2 \Rightarrow (a, b)\in IR^2$
$\Rightarrow (a, b)^{-1}\in IR^2$, ie $(-a, -b)\in IR^2$.
Montrons que (-a, -b) $\in$ E ou –a + (-b) = 0.
On a : -a + (-b) = –a –b = - (a + b) = -0 = 0.
(i), (ii) et (iii) étant vérifiés, (E, Δ) est donc un sous – groupe de (IR^2, Δ).

b$_2$. (F, Δ) est – il un sous – groupe de (IR^2, Δ)?
Réponse : ($F = \{(a, b)\in IR^2, a + b = 1\}$, +) n'est pas un sous-groupe de (IR^2, +) car $(0, 0)\notin F$ parce que 0 + 0 = 0 et $0 \neq 1$.

TP : a) ($G = \{(a, b)\in IR^2 : a + 3b = 0\}$, +) est-ce un sous-groupe de (IR^2, +).
b) ($H = \{(a, b)\in IR^2 : a = 0\}$, +) est-ce un sous-groupe de (IR^2, +).
c) ($N = \{(a, 0): a\in IR\}$, +) est-ce un sous-groupe de (IR^2, +).
d) ($M = \{(a, b)\in IR^2 : b = 4a\}$, +) est-ce un sous-groupe de (IR^2, +).

e) Théorème :

Soit (G, $*$) un groupe, H et H' deux sous – groupes de G. Alors :
$*$ $H\cap H'$ est aussi un sous – groupe de G pour la loi ($*$).
$*$ H + H' = {u + u' : u$\in$ H, u'$\in$ H'} est aussi un sous – groupe de G pour la loi ($*$). Preuve au TP.

f) Sous – groupe distingué

(1) Définition :

Soit (G,$*$) un groupe non commutatif et $D\subset G$ un sous – groupe de G, alors (D, $*$) est dit sous – groupe distingué de G si : $\forall$ x$\in$ E :

$$x * D = D * x \Leftrightarrow x * D * x^{-1} = D$$
$$\Leftrightarrow x * D * x^{-1} \subset D$$
$$\Leftrightarrow D \subset x^{-1} * D * x$$

(2) Remarque :

R$_1$. Si (G,$*$) est un groupe abélien, alors tout sous – groupe de G est distingué.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

R_2. Quelque soit un groupe G, tout groupe trivial de G est distingué.

Exercice :
Considérons le groupe $(IR^* x\ IR, \perp)$ où $(a, b) \perp (c, d) = (ac, bc + d)$.
L'ensemble $F = \{(a, b) \in IR^* xIR : b = 0\}$ est – il un sous – groupe distingué de $IR^* x\ IR$ pour la loi $\perp$?

g) Relation d'équivalence relative à un Sous – groupe

(1) Notion :

Soit $(G, *)$ un groupe abélien et $H \subset G$, un sous – groupe de G, définissons une relation R dans G par $\forall\ a, b \in G$ on a : a R b ssi $a * b^{-1} \in H$ et montrons au T.P. que R ainsi définie est une relation d'équivalence dans G qu'on notera désormais par R_H.
Ainsi, la relation R_H est définie dans G par : $\forall\ a, b \in G$, on a : a R_H b ssi $a * b^{-1} \in H$.
Cherchons la classe d'équivalence de a par R_H.

Soit $a \in G$: $cl(a) = \dot{a} = \{x \in G : x * a^{-1} \in H\}$
$= \{x \in G : \exists h \in H : x * a^{-1} = h\}$
$= \{x = a * h : h \in H\}$
$= a * H.$

$Cl\ (a) = \dot{a} = a * H = H * a = \{h * a : h \in H\} \subset G$. Car $*$ est commutative.
Le quotient de l'ensemble G par la relation R_H noté $G/R_H \cong G/H$ est défini comme suit : $G/H = \{\dot{a} = a * H : a \in G\}$.
Comme $(*)$ est commutative, alors R_H est compatible avec $(*)$. Ce qui implique qu'on peut définir une loi quotient $(\dot{*})$ conférant aussi à G/H la structure d'un groupe quotient commutatif. Cette loi est définie de la manière suivante :

$$\forall\ \dot{a},\ \dot{b} \in G/H : \dot{a} \dot{*} \dot{b} = \dot{\overline{a * b}}$$

(2) Théorème de Lagrange

L'ordre d'un sous – groupe d'un groupe fini est un diviseur de l'ordre de ce groupe.

(3) Exemple :

Soit $(\mathbf{Z}, +)$, un groupe abélien. On sait que $H = p\mathbf{Z}$ est un sous – groupe de $\mathbf{Z}$ pour la loi (+), avec $p \in IN$.
Définir R_H dans Z par $\forall\ a, b \in \mathbf{Z}$ on a : a R b ssi $a - b \in H = p\mathbf{Z}$
ssi $\exists\ z \in \mathbf{Z} : a - b = pz$
Donc a R b ssi $\exists z \in \mathbf{Z} : a - b = pz$ ce qui est une relation de congruence modulo p. Il vient que l'ensemble quotient de $\mathbf{Z}$ par la relation R_H noté $\mathbf{Z}/R_H \equiv \mathbf{Z}/p\mathbf{Z}$ est donné par $\mathbf{Z}/p\mathbf{Z} = \{a + p\mathbf{Z} : a \in \mathbf{Z}\} = \{p\mathbf{Z}\ ;\ 1 + p\mathbf{Z}\ ;\ 2 + p\mathbf{Z}\ ;\ \dots\ ;\ (p-1) + p\mathbf{Z}\}$
$= \{\dot{0}, \dot{1}, \dot{2}, \dots, \dot{\overline{p-1}}\}$
$= \mathbf{Z}_p.$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Noter que $\forall a \in \mathbf{Z}$, cl (a) = $\dot{a} = \dot{a} + p\mathbf{Z} = \{a + pz : z \in Z\}$

$\Rightarrow (\mathbf{Z}/p\mathbf{Z}, \dot{+})$ est un groupe quotient abélien et $(\mathbf{Z}/p\mathbf{Z} - \{\dot{0}\}, \dot{x})$ est aussi un groupe quotient abélien si p est un nombre naturel premier.

Cas particuliers

Prendre P = 6, pour avoir $\mathbf{Z}/6\mathbf{Z} = \{6\mathbf{Z}, 6\mathbf{Z} + 1, 6\mathbf{Z} + 2, 6\mathbf{Z} + 3, 6\mathbf{Z} + 4, 6\mathbf{Z} + 5\}$

$= \{\dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{4}, \dot{5}\}$

$= \mathbf{Z}_6 \qquad \# \mathbf{Z}_6 = 6$

Si H est un sous – groupe de $\mathbf{Z}_6$ alors, $\# H \in \mathcal{D}_6 = \{1, 2, 3, 6\}$

Ainsi tout sous – groupe de $\mathbf{Z}_6$ est de la forme $H_p = p\mathbf{Z}_6$, avec $p \in \mathcal{D}_6 = \{1, 2, 3, 6\}$.

Si p = 1, $H_1 = \mathbf{Z}_6 = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{4}, \dot{5}\}$, sous-groupe trivial.

p = 2, $H_2 = 2\mathbf{Z}_6 = \{\dot{0}, \dot{2}, \dot{4}\}$, sous-groupe trivial.

p = 3, $H_3 = 3\mathbf{Z}_6 = \{\dot{0}, \dot{3}\}$, sous-groupe trivial.

p = 6, $H_6 = 6\mathbf{Z}_6 = \{\dot{0}\}$, sous-groupe trivial.

Comme $(\mathbf{Z}_6, \dot{+})$ est un groupe abélien et $(2\mathbf{Z}_6, \dot{+})$ par exemple un sous-groupe de $\mathbf{Z}_6$, alors

$\mathbf{Z}_6 / 2\mathbf{Z}_6 = \{\dot{a} + 2\mathbf{Z}_6 : \dot{a} \in \mathbf{Z}_6\}$.

TP : Quotienter aux exercices $\mathbf{Z}_6$ par $3\mathbf{Z}_6$? ; $6\mathbf{Z}_6$?

3. Morphisme de groupe

a) Définition :

Soient $(G,*)$, (F, T), deux groupes et $f : G \to F$ une application.
f est dite morphisme de groupes si $\forall x, y \in G$, on a : $f(x * y) = f(x) \, T \, f(y)$.

b) Exemples :

Soit $(G, *)$ un groupe non commutatif d'élément neutre . Alors

$\forall a \in G$, L'application $f_a : (G, *) \to (G, *)$

$x \to f_a(x) = a * x * a^{-1}$ est un endo des groupes.

Montrer que f est morphisme des groupes, ie $\forall x, y \in G : f_a(x * y) = f_a(x) * f_a(y)$

En effet, $f_a(x * y) = a * (x * y) * a^{-1} = a * (x * n * y) * a^{-1} = a * [x * (a^{-1} * a) * y] * a^{-1}$

$= (a * x * a^{-1}) * (a * y * a^{-1})$

$= f_a(x) * f_a(y)$.

D'où, $f_a(x * y) = f_a(x) * f_a(y)$ cqfd.

c) Théorème sur les morphismes des groupes

Soient $(G, *)$, (F, T) deux groupes de neutres respectifs n et n' et $f : G \to F$, un morphisme, alors :

i) $f(n) = n'$ et $f(x^{-1}) = [f(x)]^{-1}$
ii) $Kerf = \{x \in G : f(x) = n'\}$ un sous – groupe de $(G, *)$
iii) $F(E) = Imf = \{f(x) : x \in G\}$ est un sous – groupe de (F, T). (preuve TP)

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Preuve de **ii)**

- Montrons que (Kerf,$*$) est un sous – groupe distingué de (G, $*$)

  1° Kerf $\neq 0$ car $n \in$ Kerf parce que f(n) = n!

  2° $\forall x, y \in$ Kerf : $x * y^{-1} \in$ Kerf, ie $f(x * y^{-1}) = n'$

En effet, $f(x * y^{-1}) = f(x) \mathrm{T} f(y^{-1}) = f(x) \mathrm{T} [f(y)]^{-1} = n' \mathrm{T} (n')^{-1} = n' \mathrm{T} n' = n'$.

$f(x * y^{-1}) = n'$

- Montrons que Kerf est distingué, ie $\forall a \in G$: $a *$ Kerf = Kerf $* a \Leftrightarrow a*$ Kerf $* a^{-1} \subset$ Kerf.

Où $\forall u \in$ Kerf : $a * u * a^{-1} \in$ Kerf. Pour cela, calculons $f(a * u * a^{-1})$.

On a : $f(a * u * a^{-1}) = f(a) \mathrm{T} f(u) \mathrm{T} f(a^{-1})$

$= f(a) \mathrm{T} n' \mathrm{T} [f(a)]^{-1}$

$= f(a) \mathrm{T} [f(a)]^{-1}$

$= n'$ ***cqfd***.

d) Corollaire :

Soient (G, *), (F, *) 2 groupes d'éléments neutres respectifs n et n' et
$f : (G,*) \to (F, \mathrm{T})$ un morphisme.

Alors f est injectif ssi Kerf ={n}.

Si Kerf = {n}, alors f est injectif.

Montrons $\forall x, y \in G : f(x) = f(y) \Leftrightarrow x = y$.

En effet, $f(x) = f(y) \Leftrightarrow f(x) \mathrm{T} [f(y)]^{-1} = n'$

$\Leftrightarrow f(x) \mathrm{T} f(y^{-1}) = n'$

$\Leftrightarrow f(x * y^{-1}) = n'$

$\Leftrightarrow x * y^{-1} \in$ Kerf = {n}

$\Leftrightarrow$ x * y-1 = n

$\Leftrightarrow x = y$.

C. ANNEAU

1. Définition et éléments d'un anneau

a) Définition :

Soient $A \neq 0$, ($*$) et (T) deux lois de composition internes définies dans A, alors le triplet (A, $*$, T) est dit anneau si :

i) (A, $*$) est un groupe abélien
ii) (A, T) est un demi – groupe, ie T est associatif
iii) (T) est distributive par rapport à ($*$).

$*$ si (T) est commutative, alors (A, $*$, T) est un anneau commutatif.

$*$ si (T) admet un élément neutre de A, alors cet élément est dit unité de l'anneau et est noté par 1_A.

Dans ce cas, A est dit anneau unitaire ou initial.

Par conséquent, l'élément neutre de la loi ($*$) est dit zéro de l'anneau. On le note par 0_A.

b) Exemples :

a) ($\mathbf{Z}$, +, •) est un anneau commutatif unitaire de zéro 0 et d'élément unité 1.
b) ($\mathcal{P}_E$, Δ, $\cap$) est un anneau commutatif et unitaire de zéro $\varnothing$ et d'élément unité E.
c) (IR ; Q ; +, •) sont aussi des anneaux commutatifs et unitaires.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

d) [$\mathcal{F}$(A, IR), +, •] est un anneau commutatif dont le zéro est la fonction Θ et l'unité est la fonction J définies comme suit, sachant que $\mathcal{F}$(A, IR) est l'ensemble des fonctions numériques d'une variable réelle.

$$\Theta : A \subset IR \to IR \qquad \text{et } J : A \subset IR \to IR$$
$$x \mapsto \Theta(x) = 0 \qquad\qquad x \mapsto J(x) = 1$$

e) $(Z_p = \{\dot{0}, \dot{1}, \dot{2}, \ldots, \dot{p-1}, \dot{+}, \dot{x}\}$ est aussi un anneau commutatif et unitaire dont le zéro est $\dot{0}$ et l'élément unité est $\dot{1}$.

f) (ZxZ, +, •) où (a, b) + (c, d) = (a + c, b + d) et (a, b) • (c, d) = (ac, bd) est un anneau commutatif et unitaire de zéro (0, 0) et d'élément unité (1, 1).

Par contre,

1. (IN, +, •) n'est pas un anneau car (IN, +) n'est pas un groupe.
2. (IR^*, •, +) n'est pas un anneau car (+) n'est pas distributive par rapport à (•).

Exercice :

(IR^*xIR, $\perp$, •) où (a, b) $\perp$ (c, d) = (ac, bc + d) et (a, b) • (c, d) = (ac, bd) est – il un anneau ? est – ce unitaire ?

c) Eléments remarquables

(1) Diviseurs de zéro

Soit (A, +, •) un anneau de zéro noté (0). S'il existe a, b$\in$ A :
a • b = 0 avec a $\neq$ 0 et b $\neq$ 0.
Alors a et b sont dits diviseurs de zéro.

Exemple :

Considérons l'anneau $(Z_6, \dot{+}, \dot{x})$. On constate qu'il existe

$*\ \dot{2}, \dot{3} \in Z_6 : \dot{2}\ \dot{x}\ \dot{3} = \dot{0}$ avec $\dot{2} \neq \dot{0}$ et $\dot{3} \neq \dot{0}$. Ce qui implique que : $\dot{2}$ et $\dot{3}$ sont des diviseurs de zéro.

d) Anneau d'intégrité

On appelle anneau d'intégrité tout anneau commutatif non réduit au {0} et dépourvu des diviseurs de zéro.
ie (A, +, •) est dit anneau intègre si :
$\forall$ a, b$\in$ A on a : a • b = 0 $\Rightarrow$ a = 0 ou b = 0 où $\forall$ a, b$\in$ A : a $\neq$ 0 et a • b = 0 $\Rightarrow$ b = 0

Exemple :

a) On sait que (Z ; Q ; IR, +, •) sont des anneaux intègres car $\forall$ a, b$\in$ Z, Q, IR on a :
a • b = 0 $\Rightarrow$ a = 0 ou b = 0.

b) Si p est premier, alors (Z_p, +, •) est un anneau intègre. Car il n'existe pas a, b$\in$ **Z** tel que a • b = p.

e) Eléments inversibles d'un anneau

Soit (A, +, •) un anneau unitaire et u$\in$ A, s'il existe $u^{-1} \in$ A tel que u • u^{-1} = 1 = u^{-1}• u, alors u est dit élément inversible de A.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Si on note par s(A) l'ensemble des éléments symétrisables (inversibles) de A, alors [s(A), •] est un groupe.

Exemple :

a) On sait que (**Z** , +, •) est un anneau unitaire alors les éléments inversibles de **Z** sont 1 et (-1). S(Z) = {1, -1}. D'où $(S/\mathbf{Z},.\bullet)$ est un groupe abélien.

b) On sait aussi que (IR, +, •) est un anneau unitaire, alors S(IR) = IR^*.
D'où $\left(S(IR) = IR^*,.\right)$ est un groupe abélien.

2. Sous – anneau

a) Définition :

Soient (A, ∗, T) un anneau et A' ⊂ A, on dit que A' est un sous – anneau de (A, ∗, T) si

i) (A',∗) est un sous – groupe de (A, ∗)
ii) A' est une partie stable de A pour la loi (T) ;

En d'autre terme, (A', ∗, T) est dit sous – anneau de (A, ∗, T) si :

i) A' ≠ ∅
ii) ∀ a, b∈ A', a $*b^{-1}$∈ A'
iii) ∀ a, b∈ A', a T b∈ A'.

b) Remarque

∀ $A^{'}$, sous – anneau de A, on a : 0_A∈ A'
⇒ {0_A} et A sont des sous – anneaux triviaux de A pour les lois (∗) et (T).

c) Exemples :

a) (Z, +, •) est un anneau, alors tout sous – anneau de Z est de la forme pZ, alors p∈ IN.
i.e. (pZ, +, •) est un sous – anneau de (Z, +, •) car :

i) (pZ, +) est un sous – groupe de (Z, +) et
ii) pZ est stable pour la loi (•) de Z.

b) Soients (E = ZxZ, +, •) où (a, b) + (c, d) = (a + c, b + d) et (a, b) • (c, d) = (ac, bd) est un anneau.
E_1 = {(a, b)∈ ZxZ : a = b} et E_2 = {(a, b)∈ ZxZ : a + b = 0} deux sous – ensemble de E.

b_1. Montrer que (E_1, +, •) est un sous – anneau de (E, +, •).

i) E_1 ≠ ∅ car (0, 0)∈ E_1 parce que 0 = 0
ii) ∀ (a, b), (c, d)∈ E_1 : [(a, b) + (-c, -d)]∈ E_1.
On sait que [(a, b) + (-c, -d)] = (a – c, b – d) alors [(a, b) + (-c , -d)]∈ E_1,
ie. (a – c) , b – d) ∈ E_1 ssi a – c = b – d .
Comme (a, b)∈ E_1 alors a = b
et (c, d)∈ E_1 alors c = d ⇒ a – c = b – d cqfd.
iii) ∀(a, b), (c, d)∈ E_1 : (a, b) • (c, d)∈ E_1.

Montrons que (a, b) • (c, d) = (ac, bd)∈ E_1, ie. ac = bd.
En effet, (a, b)∈ E_1 ⇒ a = b et (c, d)∈ E_1 ⇒ c = d ⇒ ac = bd cqfd.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Donc $(E_1, +, \bullet)$ est un sous – anneau de $(E, +, \bullet)$.
b_2. $(E_2, +, *)$ est un sous – anneau de $(E, +, *)$? À travailler aux exercices

3. Idéal d'un anneau

Soient $(A, *, T)$ un anneau, I_g, I_d et I trois sous – ensembles de A.

a) Définitions :

- On dit que $(I_g, *, T)$ est un idéal à gauche de $(A, *, T)$ si :
  i) $I_g \neq \varnothing$;
  ii) $\forall$ x, $y \in I_g$: $x * y^{-1} \in I_g$;
  iii) $\forall x \in I_g$, $\forall a \in A$: $x \, T \, a \in I_g$.

- On dit que$(I_d, *, T)$ est un idéal à droite de $(A, *, T)$ si :
  i) $I_d \neq \varnothing$;
  ii) $\forall$ x, $y \in I_d$: $x * y^{-1} \in I_d$;
  iii) $\forall x \in I_d$, $\forall a \in A$: $a \, T \, x \in I_d$.

- On appelle idéal bilatère de A tout idéal I de A à la fois idéal à gauche et à droite, ie $(I, *, T)$ est idéal bilatère ou tout simplement idéal de $(A, *, T)$ si :
  i) $I \neq 0$;
  ii) $\forall$ x, $y \in I$: $x * y^{-1} \in I$;
  iii) $\forall x \in I$, $\forall a \in A$: $x \, T \, a \in I$ et $a \, T \, x \in I$.

b) Remarque :

Si A est un anneau commutatif, alors tout idéal I est bilatère.

c) Théorème :

Tout idéal bilatère I de A est un sous – anneau de A, mais la réciproque n'est pas toujours vrai.

d) Exemples :

a) Soit $(Z, +, \bullet)$, un anneau commutatif,
Alors tout idéal de Z est de la forme pZ, avec $p \in IN$ car :
  i) $(pZ, +)$ est un sous – groupe de $(Z, +)$
  ii) $\forall z \in Z$, $\forall u \in pZ$, on a $z \bullet u \in pZ$.

b) Soit $(E = ZxZ, +, \bullet)$ un anneau.
Le sous – ensemble $E_1 = \{(a, b) \in ZxZ : a = b\}$ de E est – il un idéal de $(E, +, .)$?
On sait que $(E_1, +)$ est un sous – groupe de $(E, +)$, voir l'exemple précédent.
Vérifions iii), ie $\forall (x, y) \in E$, $\forall (a, b) \in E_1$: $(x, y) . (a, b) \in E_1$?
On sait que $(x, y) . (a, b) = (x .a, y .b) \in E_1 \Leftrightarrow xa = yb$.
$(a, b) \in E_1 \Rightarrow a = b$.
On constate que $xa = yb$ si $x = y$. Ce qui n'est pas le cas en général.
Donc $xa \neq yb$ en général entraînant que $(x, y) \bullet (a, b) \notin E_1$.
Et E_1 n'est pas un idéal de $(E, +, \bullet)$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

4. Morphisme d'anneaux

a) Définition :

Soient (A, $*$, T) et (B, $\Delta, \perp$) deux anneaux et f : A $\rightarrow$ B une application. Alors f est dite un morphisme d'anneaux si :

i) f est un morphisme des groupes (A, $*$) et (B, Δ).

ii) f est morphisme des demi – groupes (A, T) et (B, $\perp$), en d'autres mots f est un morphisme d'anneau si $\forall$ a, b$\in$ A,

- f (a $*$ b) = f(a) Δ f(b)
- f(a T b) = f(a) $\perp$ f(b).

b) Théorème sur le morphisme d'anneaux

Soient (A, +, •), (B, +, T) deux anneaux de zéros respectifs 0_A et 0_B et f : A $\rightarrow$ B, un morphisme. Alors :

i) $f(0_A) = 0_B$ et f(-x) = -f(x)

ii) Imf = f(A) = {f(a) : a$\in$ A}est un sous – anneau de (B, +, T)

iii) Kerf = {a$\in$ A : f(a) = 0_A}est un idéal bilatère de (A, +, •).

Preuve de ce théorème aux exercices.

D. CORPS

1. Définition :

On appelle corps tout anneau (K) unitaire dont chaque élément distinct de 0_K est symétrisable par la 2^e loi de composition interne, ie (K, $*$, T) est dit corps si :

i) (K, $*$, T) est un anneau unitaire de zéro noté 0_k

ii) $\forall$ u$\in$ K^*= K - {0_K}, u est symétrisable par la loi de composition (T).

En d'autre terme, (K, $*$, T) est corps si :

i) (K, $*$) est un groupe abélien d'élément neutre (0_K)

ii) (K^* = K - {0_K},T) est un groupe

iii) (T) est distributive par rapport à ($*$).

Si (T) est commutative, alors (K, $*$, T) est dit corps commutatif ou champs.

$\forall$ K, corps on a : $0_k$$\in$ K et $1_K$$\in$ K appelés respectivement zéro et unité du corps K.

2. Exemples :

a) (Q ; IR, +, •) sont des champs car :

i) (Q ; IR, +) est un groupe abélien

ii) (Q^* ; IR^*, •) est un groupe abélien

iii) (•) est distributive par rapport à (+).

b) Soit (IRxIR, +, x) un triplet où (+) et (x) sont deux lois de compositions internes définies par : (a, b) + (c, d) = (a + c, b + d) et (a, b) x (c, d) = (ac – bd, ad + bc)

Montrons que (IR^2, +, x) est un champ.

i) (IR^2, +) est un groupe abélien de neutre (0, 0) et le symétrique de (a, b) est (-a, -b).

ii) [$(IR^2)^*$ = IR^2 - {(0, 0)}, x] est un groupe abélien d'élément neutre (1, 0). Le symétrique de (a, b) $\in$ $(IR^2)^*$ est $\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

En effet si (x, y) est le symétrique de (a, b)$\in (IR^2)^*$, alors (x, y) x (a, b) = (1, 0) $\Leftrightarrow$ (xa – yb, xb + ya) = (1, 0)

$\Leftrightarrow \begin{cases} xa - yb = 1 \\ xb + ya = 0 \end{cases}$ On obtient un système de deux équations à deux inconnues qu'on resoue par la méthode de Cramer. Pour cela, calculons Δ_s, Δ_a et Δ_b.

On a : $\Delta_s = \begin{vmatrix} a & -b \\ b & a \end{vmatrix} = a^2 + b^2$; $\Delta_a = \begin{vmatrix} 1 & -b \\ 0 & a \end{vmatrix}$ = a et $\Delta_b = \begin{vmatrix} a & 1 \\ b & 0 \end{vmatrix}$ = -b, alors

$x = \dfrac{\Delta_a}{\Delta_s} = \dfrac{a}{a^2 + b^2}$ et $y = \dfrac{\Delta_b}{\Delta_s} = \dfrac{-b}{a^2 + b^2}$, avec $a^2 + b^2 \neq 0$ car (a, b) $\in (IR^2)^*$.

iii) (x) est distributive par rapport à (+). *A montrer aux exercices.*

Par contre, (Z, +, •) n'est pas un corps car (Z, •) n'est pas un groupe.

Exercices :

a) Le triplet (IR, +, $*$) où $a * b = a + b + ab$ et ($*$), l'addition habituelle dans IR est – il un corps ? Justifier.

b) (IRxIR, +, •) où (+) et (•) sont des lois produits, est – il un corps ? Justifier.

3. Propriétés :

P$_1$. Tout corps K est un anneau intègre, ie $\forall$ a, b$\in$ K :

a • b = 0 $\Rightarrow$ a = 0 ou b = 0. Ou $\forall$ a, b$\in$ K, si a $\neq$ 0 et a • b = 0, alors b = 0

P$_2$. Dans un corps (K, +, •), toute équation x • a = b ou a • x = b avec a$\in K^*$ admet une solution et une seule dans K.

En effet, x • a = b $\Leftrightarrow$ x = b • $a^{-1} = \dfrac{b}{a}$ d'où $\boxed{\dfrac{b}{a} = b.\dfrac{1}{a}}$ appelé rapport ou quotient.

avec a^{-1} l'inverse de a car a $\neq$ 0 et a $\in$ K

Exemple :

On sait que (Z_5, +, •), avec Z_5 = {0, 1, 2, 3, 4} est un corps commutatif car 5 est premier alors l'équation 3x = 2 admet une solution et une seule dans Z_5.

En effet, 3$\in Z_5 \Rightarrow$ inv. (3) = 2 $\in Z_5$. Il vient que 3x = 2 $\Leftrightarrow$ 2(3x) = 2 • 2 $\Leftrightarrow$ x = 4.

D'où S = {4}. Remarquer que 2, 3$\in Z_5 \Rightarrow \dfrac{2}{3} \in Z_5$.

En effet $\dfrac{2}{3} = 2 \bullet 3^{-1} = 2 \bullet 2 = 4$. D'où $\dfrac{2}{3} = 4$.

***Exercice** :*

Dans le corps (Z_7, +, •), calculer $\dfrac{3}{2}$; $\dfrac{4}{5}$; $\dfrac{5}{6} + \dfrac{4}{3} + 6 = ?$

Corollaire :

$\forall$ a, b $\in$ K, $\forall$ b, d $\in$ K* : $\dfrac{a}{b} = \dfrac{c}{d} \Leftrightarrow a \bullet b = c \bullet d$

Preuve aux exercices.

P$_3$. Tout anneau unitaire, intègre et ayant un nombre fini d'éléments est un corps si p est premier, alors (Z_p, +, •) est un anneau unitaire, intègre et ayant p éléments, donc d'après P_3 : (Z_p , + , •) est un corps.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Exemple :
On sait que si p est premier, alors (Z_p, +, •) est un anneau intègre. Cet anneau est unitaire et a un nombre fini d'éléments.
Donc, en vertu de P_3 ci – dessus, on peut conclure que (Z_p, +, •) est un corps.

4. Sous - corps

Soit (K, +, •) un corps et $L \subset K$, alors (L, +, •) est dit sous - corps de (K, +, •) si :

i. (L, +) est un sous – groupe de (K, +)
ii. ($L^* = L - \{0_k\}$, •) est un sous – groupe de (K^*, •)

En d'autres termes, (L, +, •) est un sous corps de (K, +, •) si :

- $L \neq \emptyset$
- $\forall$ x, y$\in$ L : $x - y \in L$
- $\forall$ x, y $\in$ L^*, $x.y^{-1} \in L^*$

Théorème :
Les seuls idéaux d'un corps K sont les idéaux triviaux de K, à savoir $\{0_k\}$ et K lui-même. Preuve aux exercices.

E. ESPACE VECTORIEL

1. Définition et exemples

a) Définition :

Soient (K, +, •) un corps commutatif dont le zéro est (0_k) et l'unité (1_k) et $E \neq \emptyset$ muni d'une loi interne (+) et une loi externe (•) à scalaire dans K. Alors le triplet (E, +, •) est dit espace vectoriel sur K ou K – espace si :

i. (E, +) est un groupe abélien d'élément neutre 0_E
ii. La loi de composition externe (•) définie comme suit $f : K \times E \rightarrow E$
$(\alpha, \mu) \rightarrow \alpha \bullet \mu$

Vérifier les propriétés suivantes : $\forall$ α, $\beta \in K$, $\forall$ u, v $\in$ E,

P_1. $\alpha (u + v) = \alpha u + \alpha v$ et $(u + v) \bullet \alpha = u \alpha + v \alpha$
P_2. $(\alpha + \beta) u = \alpha u + \beta v$ et $u(\alpha + \beta) = u\alpha + u\beta$
P_3. $\alpha(\beta u) = (\alpha\beta) u$
P_4. $1_k \bullet u = u$

Les éléments $\alpha \in K$ sont dits des scalaires, tandis que tout élément de E est dit vecteur.

b) Exemples :

1) (E = {0}, +, •) est un espace vectoriel sur K
2) Tout corps commutatif (K, +, •) est un espace vectoriel sur sois – même. Donc
   - (IR, +, •) est un IR – espace car (IR, +, •) est un corps commutatif.
   - (Q, +, •) est un Q – espace car (Q, +, •) est un corps commutatif.
3) Le triplet (IR², +, •) où la loi interne (+) et la loi externe (•) à scalaire dans IR sont définies comme suit : $\forall$ (a, b), (c, d) $\in IR^2$ et $\forall$ $\alpha \in$ IR :
   (a, b) + (c, d) = (a + c, b + d) et α(a,b) = (αa,αb) est un IR – espace
   i. On sait que (IR², +) est un groupe abélien
   ii. La loi externe (•) : IR² x IR → IR²
   [α, (a, b)] → α (a, b) = (αa, αb) doit vérifier :
   $\forall$ α, $\beta \in$ IR, $\forall$ (a, b) , (c, d) $\in$ IR² :

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

P_1. α [(a, b) + (c, d)] = α (a, b) + α (c, d)

En effet (.) α[(a, b) + (c, b)] = α (a + c, b + d)

= [α (a + c), α (b + d)]

= (αa + αc, αb + αb)

= (αa, αb) + (αc, αd)

= α (a, b) + α (c, d) ***cqfd***

Montrer P_2, P_3 et P_4 aux exercices.

D'une manière générale, $\forall$ n$\in$ N^*, (R^n, +, •) est un espace vectoriel sur R avec (+) et (•) définies dans IR* comme suit :
$\forall$ (a_1, …, a_n) ; (b_1, …, b_n) $\in$ R^n, $\forall$ α $\in$ R :
(a_1, … , a_n) + (b_1, …, b_n) = (a_1 + b_1, …, a_n + b_n)
α (a_1, …, a_n) = (αa_1, …, αa_n).

Cas particuliers :
(R^3, +, •) est un R-espace.
(R^4, +, •) est un R-espace.

A $\neq$ Ø, F (A, R) = {f : A $\rightarrow$ R : f est une fonction numérique}

4) [F (A, R), +, •] où (+) est définie par $\forall$ f, g $\in$ F (A, R) : f + g $\in$ F (A, R) et on a :
(f + g) (x) =f(x) + g(x) et la loi externe (•) définie dans F(A, R) à scalaires dans K par
$\forall$ α $\in$ K,
$\forall$ f $\in$ F (A, R), on a : αf $\in$ F (A, R)
Noter que : $\forall$ x $\in$ A : (αf) (x) = α f (x).

c) Remarque :

Soit (E, +, •) un K-espace d'élément neutre (0_E).
$\forall$ α $\in$ K : α • 0_E = 0_E et $\forall$ u $\in$ E : u • 0_K = 0_K
Ainsi, $\forall$ α $\in$ K, $\forall$ u $\in$ E : αu = 0_E $\Leftrightarrow$ α = 0_K ou u = 0_E.
De ce qui précède, on constate que il n'y a aucun inconvénient de représenter le zéro K(0_K) et le zéro (0_E) par le même symbole 0. Ce qu'on fera désormais et 1_K et 1_E par 1.

2. Sous – espace vectoriel

a) Définition

Soit E un K – espace et S $\subset$ E.
S est dit sous-espace vectoriel de E sur K si :
i) (S, +) est un sous-groupe de (E, +)
ii) S est une partie stable de E par la loi externe (·)
i.e. (S, +, •) est un sous-espace vectoriel de (E, +, ·) si :

- S $\neq$ Ø
- $\forall$ x, y $\in$ S : x – y $\in$ S
- $\forall$ α $\in$ K, $\forall$ x $\in$ S : αx $\in$ S.

b) Théorème

Soit E un K – espace et S $\subset$ E.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

S est dit sous-espace vectoriel de E pour les lois (+) et (·) de E, ssi $\forall$ α, β $\in$ K, $\forall$ x, y $\in$ S on a : $\alpha x + \beta y \in S$ avec $S \neq \emptyset$.

c) Remarques

R_1 : $\forall$ S un sous-espace vectoriel de E, on a : $0 \in S$. ce qui entraîne que {0} est un sous-espace vectoriel de E. E est aussi un sous-espace vectoriel de E lui même
On dit alors que {0} et E sont des sous-espaces vectoriels triviaux de E.
Tout sous – espace vectoriel de E autre que {0} et E est dit sous – espace vectoriel propre de E.

R_2 : $\forall$ S, un sous-espace vectoriel de E, on a :$\{\emptyset\} \subset S \subset E$.

d) Proposition

Soit E un K – espace et M un sous-ensemble de E vérifiant :

i) $M \neq \emptyset$
ii) $\forall$ x, y $\in$ M : $x + y \in M$
iii) $\forall \alpha \in K$, $\forall x \in M : \alpha x \in S$.

Alors M est un sous – espace vectoriel de E.

e) Théorème

Soient E un K – espace, S et S' deux sous-espaces vectoriels de E. Alors :
i) $S \cap S'$est aussi un sous-espace vectoriel de E.
ii) $S + S' = \{s + s' : s \in S, s' \in S'\}$ est aussi un sous – espace vectoriel de E.

f) Somme directe

Soient E un K – espace, S et S' deux sous-espaces de E. Alors S et S' forment la somme directe de E ssi :
i) $S \cap S' = \{o\}$
ii) $S + S' = E$.

Si S et S' forment la somme directe de E, alors on peut écrire : $S \oplus S' = E$.
Ainsi $\forall u \in E$, $\exists! \, s \in S$, $\exists! \, s' \in S'$ tel que : $u = s + s'$.

g) Exemples

- Soient (E, +, •) un K – espace et $u \in E^*$, alors

$D = \{\alpha u : \alpha \in K\}$ est un sous-espace vectoriel de E appelé droite vectorielle engendrée par le vecteur u.

Preuve
Montrer que (D, +, ·) est un sous – espace vectoriel de (E, +, •)
i) $D \neq \emptyset$ car $0 \in D$. En effet, $\exists \alpha = 0 \in K : 0 = 0 \bullet \alpha$
ii) $\forall$ x, y $\in$ D : $x - y \in D$
En effet, $x \in D \Rightarrow \exists \alpha \in K : x = \alpha u$ et $y \in D \Rightarrow \exists \beta \in K : y = \beta u$
Alors $x - y = \alpha u - \beta u = (\alpha - \beta)\, u = \lambda u$, avec $\lambda = \alpha - \beta \in K$.
$\Rightarrow x - y \in D$.
iii) $\forall \lambda \in K$, $\forall x \in D$, on a : $\lambda x \in D$
En effet, $x \in D \Rightarrow \exists \alpha \in K : x = \alpha.u$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Alors, $\lambda x = \lambda\ (\alpha u) = (\lambda\alpha)\ u = m \bullet u$, avec $m = \lambda\alpha \in K$

- Soit ($E = IR^2, +, \bullet$) est un espace vectoriel sur IR,

$E_o = \{(a, o) : a \in IR\} \subset E$
$E^o = \{(0, b) : b \in IR\} \subset E$
$E' = \{a, b) : a + 3b = 0\} \subset E$

•1. Montrer que E_o, E^o et E' sont des sous espaces vectoriel de IR².

On peut montrer que E^0, E_0 et E' sont engendrés par un vecteur non nul u de E

i) $E_o = \{(a, 0) : a \in IR\}$
$= \{a(1, 0) : a \in IR\}$
$= \{a, u : a \in IR\}$ avec $u = (1, 0)$.

$\Rightarrow E_o$ est un sous espace de IR², en vertu de l'exemple (7a) ci – dessus

ii) $E^o = \{(o, b) : b \in IR\}$
$= \{b(0, 1) : b \in IR\}$
$= \{b \bullet v : b \in IR\}$ avec $v = (0, 1)$

$\Rightarrow E^0$ est un sous – espace vectoriel de E car E^0 est engendré par le vecteur v.

iii) $E' = \{(a, b) \in IR^2 : a + 3b = 0\}$
$= \{(a, b) \in IR^2 : a = -3b\}$
$= \{(-3b, b) : b \in IR\}$
$= \{b(-3, 1) : b \in IR\}$
$= \{b\omega : b \in IR\}$ avec $\omega = (-3, 1)$, ce qui prouve en vertu de l'exemple (7a) ci – dessus que E' est un espace vectoriel dans E

•2. Déterminer $E \cap E^o$

Pour cela, prenons $(a, b) \in IR^2$. Alors $(a, b) \in E_\circ \cap E^o \Leftrightarrow (a, b) \in E_o$ et $(a, b) \in E^o$
$\Leftrightarrow b = 0$ et $a = 0$
$\Leftrightarrow a = b = 0$

D'où $E_o \cap E^o = \{(0, 0)\}$ est un sous – espace vectoriel de E

•3. Déterminer $E^0 + E_0$.

On a : $E^o + E_o = \{(a, 0) + (0, b) : a, b \in IR\}$
$= \{(a, b) : a, b \in IR\}$
$= IR^2$

D'où E_o et E^o forment la somme directe de IR². On peut écrire alors que $\forall (a, b) \in IR^2$, on a : $(a, b) = (a, 0) + (0, b)$ avec $(a, 0) \in E_0$ et $(0, b) \in E^0$

- Soit ($F = IR3, +, \bullet$) est un IR – espace et

$F^o = \{(a, b, c) \in IR^3 : b = c = 0\} \subset F$
$F_o = \{(a, b, c) \in IR^3 : a = 0\} \subset F$
$F' = \{(a, b, c) \in IR^3 : a + b + c = 0\}$
$F'' = \{(a, b, c) \in IR^3 : a + 2c = 0\}$

•1. Montrons par exemple que F' est un sous – espace vectoriel de F:

i) $F' \neq \emptyset$ car $\exists (0,0,0) \in IR^3 : 0 + 0 + 0 = 0$ Donc $(0, 0, 0) \in F'$

ii) $\forall (a, b, c); (a', b', c') \in F'$ Montrer que $(a, b, c) + (a', b', c') \in F'$

En effet, $(a, b, c) \in F' \Rightarrow a + b + c = 0$
Et $(a', b', c') \in F' \Rightarrow a' + b' + c' = 0$

$$[(a,b,c)+(a',b',c')] \in F' \Leftrightarrow (a+a',b+b',c+c') \in F'$$
$$\Leftrightarrow (a+a')+(b+b')+(c+c')=0$$

En effet, $(a + a') + (b + b') + (c + c') = a + a' + b + b' + c + c'$
$= (a + b + c) + (a' + b' + c') = 0 + 0 = 0$

iii) $\forall\ \alpha \in IR, \forall (a,b,c) \in F'$: on a: $\alpha\,(a, b, c) \in F'$

En effet, $(a, b, c) \in F' \Rightarrow a + b + c = 0$

Or $\alpha(a, b, c) = (\alpha a\ ,\ \alpha b,\ \alpha c)$,

Donc $\alpha(a, b, c) \in F' \Leftrightarrow (\alpha a,\ \alpha b,\ \alpha c) \in F' \Leftrightarrow \alpha a + \alpha b + \alpha c = 0$

En effet, $\alpha a + \alpha b + \alpha c = \alpha(a + b + c) = \alpha\,.\,0 = 0$ car $a + b + c = 0$ par hypothèse.

•2. *Montrer aux exercices* que F°, F_0 et F'' sont les sous – espaces vectoriel de F

•3. F° et F_0 ; F_0 et F' forment – ils la somme directe de F ? Justifiez

3. Combinaison linéaire, Base et Dimension

Soient E un K – espace et $\mathscr{A} = \{v_1, v_2, \ldots, v_n\}$ une famille de n vecteurs

a) Définitions

1. On appelle *combinaison linéaire* de $\mathscr{A}$ en abrégé *combili* de A, tout vecteur de E de la forme $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n$ avec : $\alpha_1, \alpha_2, \ldots \alpha_n \in K$

Remarque :

R1. Le vecteur nul (0) est une combili de $\mathscr{A}$ car $0 = 0v_1 + 0v_2 + \ldots + 0v_n$

R2. Un vecteur quelconque v_2 de $\mathscr{A}$ peut aussi s'écrire comme *combili* de $\mathscr{A}$,
i.e. $v_2 = 0v_1 + 1v_2 + \ldots + 0v_n$

R3. L'ensemble des *combili* de $\mathscr{A}$ forment ce qu'on appelle engendré de $\mathscr{A}$ noté par Eng($\mathscr{A}$),
Ainsi, $\text{Eng}(\mathscr{A}) = \{v = \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n : \alpha_1, \alpha_2, \ldots \alpha_n \in K\}$

Théorème :

Eng($\mathscr{A}$) est un sous – espace vectoriel de E.

Preuve aux exercices

Noter que $\text{Eng}(\mathscr{A}) \neq \emptyset$ car $0 \in \text{Eng}(\mathscr{A})$

En effet, $0 = 0v_1 + 0_2\, v_2 + \ldots + 0v_n$ avec $0 \in K$

b) Famille génératrice

$\mathscr{A}$ est dite famille génératrice de E ssi tout vecteur de E peut s'écrire comme combili de $\mathscr{A}$, i.e. $\forall\ v \in E$; $\exists\ \alpha_1, \alpha_2, \ldots, \alpha_n \in K$ tel que : $v = \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n$.

c) Famille libre ou famille linéairement indépendante

$(\mathscr{A})$ est dite famille libre ou linéairement indépendante de E si la combinaison linéaire de la famille $(\mathscr{A})$ est nulle alors tous les scalaires sont nuls. i.e. Si $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n = 0$ alors, $\alpha_1 = \alpha_2 = \ldots = \alpha_n = 0$.

Dans le cas contraire i.e $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n = 0$ avec $\alpha_1 \neq 0$ ou $\alpha_2 \neq 0$ ou…ou $\alpha_n \neq 0$
Alors la famille $\mathscr{A}$ est dite liée ou linéairement dépendante.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

d) Base

$(\mathscr{A})$ est dite base de E ssi $\mathscr{A}$ est à la fois famille génératrice et libre de E.
Si $\mathscr{A} = \{v_1, v_2, \dots, v_n\}$ es une base de E, alors tout vecteur v de E s'écrit d'une manière unique comme *combili* de $\mathscr{A}$, i.e. $\forall\, v \in E, \exists\, !\ \alpha_1, \alpha_2, \dots, \alpha_n \in K$ tel que :
$v = \alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_n v_n$.

e) Exemples

1) Soit (IR , +, •), un IR – espace et $\mathscr{A} = \{5\}$ une famille qui a un vecteur 5

Ecrire 7 comme *combili* de $\mathscr{A}$.

7 s'écrit comme *combili* de $\mathscr{A}$ ssi $\exists \alpha \in$ IR tel que 7 = 5.

On prend $\alpha = \frac{7}{5}$ car $7 = 5 \bullet \frac{7}{5}$

i) $\mathscr{A} = \{5\}$ est – elle génératrice de IR ?

Ou $\forall\, u \in \text{IR}, \exists\, ?\ \alpha \in \text{IR} : u = 5 \bullet \alpha$ oui car $\alpha = \frac{u}{5} \in \text{IR}$

Donc $\mathscr{A} = \{5\}$ est une famille génératrice de IR (i)

ii) $\mathscr{A} = \{5\}$ est – elle libre ? i.e. $5 \bullet \alpha = 0 \overset{?}{\Rightarrow} \alpha = 0$

En effet, $5\alpha = 0 \Rightarrow \alpha = 0$ car $5 \neq 0$ et $\mathscr{A} = \{5\}$ et libre (ii)

D'où (i) et (ii) $\Rightarrow \mathscr{A} = \{5\}$ est une base de IR. On peut montrer que $\forall\, u \in$ IR*, la famille {u} est une base de IR.

2) Soient (IR², +, •) est un IR – espace et

$\mathscr{A} = \{v_1 = (1, 2) ; v_2 = (2, 1)\}$ une famille de deux vecteurs de IR².

$\bullet_1$ Ecrire v = (3, 4) $\in$ IR² comme *combili* de $\mathscr{A}$,

v = (3, 4) s'écrit comme *combili* de $\mathscr{A}$ si $\exists\, a, b \in$ IRtel que :

$(V) = av_1 + bv_2$

$$V = av_1 + bv_2 \Leftrightarrow (3, 4) = a(1, 2) + b(2, 1)$$
$$\Leftrightarrow (3, 4) = (a, 2a) + (2b, b)$$
$$\Leftrightarrow (3, 4) = (a + 2b, 2a + b)$$

$$\Leftrightarrow \begin{cases} a + 2b = 3 \\ 2a + b = 4 \end{cases} \Leftrightarrow \begin{cases} a = \frac{5}{3} \\ b = \frac{2}{3} \end{cases}$$

D'où $\exists\, a = \frac{5}{3}, b = \frac{2}{3} \in$ IR tell que : $(3,4) = \frac{5}{3}(1,2) + \frac{2}{3}(2,1)$

- $\mathscr{A}$ est – elle une famille génératrice de IR² ?

$\forall\, v = (x, y) \in$ IR² : $\exists ?\ a, b \in \text{IR} : v = av_1 + bv_2$

$v = av_1 + bv_2 \Leftrightarrow (x, y) = (a + 2b, 2a + b)$

$\Leftrightarrow \begin{cases} a + 2b = x \\ 2a + b = y \end{cases}$ Ce qui est un système de deux équations à deux inconnues à résoudre par la méthode de cramer.

On a : $\Delta_s = -3$; $\Delta_a = x - 2y$ et $\Delta_b = -2x + y$ entraîne que

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

$$\alpha = \frac{\Delta_a}{\Delta_s} = \frac{x-2y}{-3} = \frac{2y-x}{3} \ ; \qquad b = \frac{\Delta_b}{\Delta_s} = \frac{-2x+y}{-3} = \frac{2x-y}{3}$$

$$\Rightarrow (x, y) = \frac{-x+2y}{3} v_1 + \frac{2x-y}{3} v_2$$

- $\mathscr{A}$ est une famille libre car $av_1 + bv_2 = 0 \Rightarrow a = b = 0$

  Alors $\mathscr{A} = \{v_1 = (1, 2), v_2 = (2, 1)\}$ est une base de IR² car elle est à la fois une famille libre et génératrice de IR^2.

Exercices :

La famille $\mathscr{A}_1 = \{v_1 = (2, -1) ; v_2 = (3, 7)\}$ est – elle une base de IR² ?

La famille $\mathscr{A}_2 = \{v_1 = (1, 1, 1) ; v_2 = (1, 0, -1), v_3 = (1, 4, -2)\}$ est – elle une base de IR^3 ?

f) Théorème

Tout espace vectoriel E admet une base. Si, une base de E possède n vecteurs, alors toutes les bases de E auront chacune n vecteurs.

On appelle dimension de E le nombre de vecteurs d'une base de E

On note par dim(E) la dimension de E

Si une base de E est infinie, alors, toutes les bases de E sont infinies et E est dit espace vectoriel de u dimension infinie.

i. On sait que E = {0} est un espace – vectoriel sur K.
   Sa base est Ø et sa dimension est 0

- dim(IR) = 1car toute famille composée d'un nombre réel non nul u est une base de IR.

Noter que la base canonique de IR est {1} car $\forall x \in IR : x = x.1$

- dim(IR²) = 2 car toute base de IR² ne peut avoir que deux vecteurs

Noter que $B = \{e_1 = (1, 0) ; e_2 = (0, 1)\}$ est la base canonique de IR² car $\forall (x, y) \in$ IR² ; on a : $(x, y) = x.e_1 + y.e_2$

ii. $Dim(IR^3) = 3$ et $B = \{u_1 = (1, 0, 0) , u_2 = (0, 1, 0) , u_3 = (0, 0, 1)\}$ est la base canonique de IR^3 car $\forall (x, y, z) \in IR^3$, on a : $(x, y ,z) = xu_1 + yu_2 + zu_3$

D'où d'une manière générale la base canonique de IR^n est :

$B = \{e_1 = (1, 0,…, 0) ; e_2 = (0, 1,…, 0) ; … ; e_n = (0, 0, …, 0, 1)\}$

Soit $B = \{u = (1, -1, 0) ; v = (1, 0, -1)\}$ une famille des vecteurs de IR^3

Cherchons Eng(B)

On sait que $Eng(B) = \{au + bv : a, b \in IR\}$

Soit $(x, y, z) \in IR^3$. $(x, y, z) \in Eng(B) \Leftrightarrow (x, y, z) = au + bv$

$\Leftrightarrow a(1, -1, 0) + b(1, 0, -1) = (x, y, z) \Leftrightarrow (a + b, -a, -b) = (x, y, z)$

$$\Leftrightarrow \begin{cases} a+b=x \\ -a=y \\ -b=z \end{cases} \Leftrightarrow \begin{cases} a+b=x \\ a=-y \\ b=-z \end{cases} \Leftrightarrow -y-z=x \Leftrightarrow x+y+z=0$$

D'ou $\boxed{Eng(B) = \{(x, y, z) \in IR^3 : x + y + z = 0\}}$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

g) Exemples

Dans l'espace IR^3, considérons le sous – ensemble

$F = \{(a, b, c) \in IR^3 : a + c = 0\}$

- Montrer que F est un sous – espace vectoriel de IR^3
- Chercher dim(F)

On a $F = \{(a, b, c) \in IR^3: a + c = 0\}$

$= \{(a, b, c) \in IR^3: a = -c\}$

$= \{(-c, b, c): b, c \in IR\}$

$= \{(-c, 0, c) + (0, b, 0): b, c \in IR\}$

$= \{c(-1, 0, 1) + b(0, 1, 0): b, c \in IR\}$

$= \{cu + bv : b, c \in IR\}$

$= Eng(\{u, v\})$ avec $u = (-1, 0, 1)$ et $v = (0, 1, 0)$

$\Rightarrow$ F est un K – espace vectoriel de IR^3 engendré par les vecteurs u et v de IR^3.

$\Rightarrow$ La famille $\{u = (-1,0,1); v = (0,1,0)\}$ est une base de F et par conséquent la dimension de F est 2.

h) Remarques

Soit E un K – espace de dimension n.

R_1. Toute famille de m vecteurs de E telle que m > n n'est pas génératrice de E

R_2. Toute famille libre à e vecteurs telle que e < n est une partie d'une base de E

R_3. Toute famille libre à n vecteurs est une base de E

i) Théorème

Soient E un espace de dimension n sur K et S, S' deux sous – espaces vectoriels de E. Alors

i. $\dim(S) \leq \dim(E)$

ii. $\dim(S+S') = \dim(s) + \dim(S') - \dim(S \cap S')$

iii. si $\dim(S) = \dim(E)$ alors $S = E$

Exemples :

On sait que $E_o = \{(a, 0) : a\in IR\} = \{a(1, 0) : a\in IR\}$ et

$E^o = \{(0, b) : b\in IR\} = \{b(0, 1) : b\in IR\}$ sont deux espaces vectoriels de IR². Alors $E_o \cap E^o$ et $E° + E_0$ sont aussi des sous – espaces de IR².

Comme $\dim(E_0) = 1$ et $\dim(E°) = 1$ et $\dim(E° \cap E_0) = 0$

Alors $\dim(E_o + E^o) = \dim E_o + \dim E^o - \dim(E_o \cap E^o)$

$= 1 + 1 - 0$

$= 2$

D'où $E_0 + E^0 = IR^2$

4. Application linéaire ou morphisme d'espace vectoriels

a) Définition

Soient (E, +, •), (F, +, •) deux espaces vectoriels sur K et $f : E \to F$, une application. f est dite une application linéaire si $\forall \alpha\in K$, $\forall x, y \in E$:

i. $f(x+y) = f(x) + f(y)$
ii. $f(\alpha \bullet x) = \alpha \bullet f(x)$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

b) Théorème

Soient E, F, deux K – espaces et $f : E \to F$, une application.
f est une application linéaire ssi $\forall\, \alpha, \beta \in K$, $\forall\, x, y \in E$:

$$f(\alpha x + \beta y) = \alpha f(x) + \beta f(y)$$

Preuve aux exercices

c) Exemples

1. Soit $f : IR^2 \to IR^3$

$(x, y) \to f(x, y) = (x - y, 2x - y, 3x + 2y)$, une application

Montrer que f est linéaire

$\forall\, \alpha \in IR$, $\forall\, (x, y), (x', y') \in IR^2$;

- $f[(x, y) + (x', y')] = f(x + x', y + y')$
$= [(x+x')-(y+y'), 2(x+x')-(y + y'), 3\,(x + x')+2(y + y')]$
$= [x + x' - y - y', 2x + 2x' - y - y', 3x + 3x' + 2y + 2y']$
$= [(x-y) + (x'-y'), (2x-y)+(2x' -y') , (3x+2y)+(3x'+2y')]$
$= (x - y, 2x - y, 3x + 2y) + (x' \;\; y', 2x' - y', 3x' + 2y')$
- $f[\alpha\,(x, y)] = f(\alpha x, \alpha y) = (\alpha x - \alpha y, 2\alpha x - \alpha y, 3\alpha x + 2\alpha y)$
$= \alpha\,(x - y, 2x - y, 3x + 2y)$
$= \alpha f(x,y)$.

2. Soit $g : IR^2 \to IR^2$

$(x, y) \to g(x, y) = (x + 3y, x - y + 5)$, une application

Montrer aux exercices que f n'est pas une application linéaire

d) Définitions

Soient E, F deux espaces vectoriels sur K et $f : E \to F$ une application linéaire :

i. alors le noyau de f noté KerF est défini par
$$\mathrm{Kerf} = \{x \in E : f(x) = 0_f\} \subset E.$$

ii. L'image de f notée Imf est définie comme suit : $\mathrm{Imf} = f(E) = \{f(x) : x \in E\} \subset F$.

Exemples :

Déterminer Kerf si $f : IR^2 \to IR^2$

$(x, y) \to f(x, y) = (x - y, x + y)$ est une application linéaire

On a $\mathrm{Kerf} = \{(x, y) \in IR^2 : f(x, y) = 0_{IR^2}\}$
$= \{(x, y) \in IR^2 : (x - y, x + y) = (0, 0)\}$.

Or $(x - y, x + y) = (0, 0) \Leftrightarrow \begin{cases} x - y = 0 \\ x + y = 0 \end{cases} \Leftrightarrow \begin{cases} x = 0 \\ y = 0 \end{cases}$

Donc $\mathrm{Kerf} = \{(0, 0)\}$

e) Théorème 4 sur le morphisme d'espace vectoriels

Soient E, F, deux K – espace et $f : E \to F$, une application linéaire, alors

i. $f(0_F) = 0_F$ et $f(-x) = -f(x)$.
ii. si S est un sous espace vectoriel de E, alors f(S) est un sous espace vectoriel de F.
iii. Kerf est un sous – espace vectoriel de E.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

iv. Imf est un sous – espace vectoriel de F.

Preuve aux exercices

f) Rang d'une application linéaire

Soit $f : E \to F$, une application linéaire. On appele rang de f, noté r_g (f) la dimension de Imf.

i.e. $r_g(f) = \dim(Imf)$

g) Théorème

Soit E, un espace vectoriel sur K de dimension n, F un K – espace et $f : E \to F$, une application linéaire. Alors,

$$\boxed{\dim(E) = \dim(Kerf) + \dim(Imf)}$$

h) Corollaire

Soient E, F deux K – espaces et $f : E \to F$, une application linéaire

i. f est injective $\Leftrightarrow$ Kerf = $\{0_E\}$

ii. f est surjective $\Leftrightarrow$ Imf = F , i.e dim(Imf) = dim(F)

Par exemple : $f : IR^2 \to IR^2$

$(x, y) \to f(x, y) = (x - y, x + y)$ une application linéaire.

Déterminer le rang de f

On sait que Kerf = {(0, 0)}. Ce qu entraîne que dim(Kerf) = 0

D'après le théorème ci – dessus, on a :

$\mathrm{Dim}(IR^2) = \dim(Kerf) + \dim(Imf) \Leftrightarrow 0$

$2 = 0 + \dim(Imf) \Leftrightarrow \dim(Imf) = 2$

D'où $r_g(f) = \dim(Imf) = 2 = \dim(IR^2)$

On peut conclure, voir l'exemple précédent que f est à la fois injective et surjective.

Par exemple, pour l'application linéaire f définie comme suit :

$f : IR^2 \to IR^2$

$(x, y) \to f(x, y) = (x - y , x + y)$, déterminons le rang de f.

On sait que : Kerf = {(0, 0)}. Ce qui entraîne que dim Kerf = 0.

D'après le théorème ci – dessus, on a :

$\dim(IR^2) = \dim(Kerf) + \dim(Imf) \Leftrightarrow$

$2 = 0 + \dim(Imf)$

Soit $\dim(Imf) = r_g(f) = 2$

On peut donc conclure, d'après le corollaire ci – dessus que f est à la fois injective et surjective.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

CHAPITRE IV
L'ENSEMBLE DES NOMBRES COMPLEXES

A. INTRODUCTION

Soit $f : \mathbb{R} \to \mathbb{R}$

$x \mapsto f(x) = ax^2 + bx + c$, une fonction du second degré en x, avec $a \in \mathbb{R}^*, b, c \in \mathbb{R}$. Si $f(x) = 0$, ie $ax^2 + bx + c = 0$, on obtient alors une équation du second degré en x dont l'existence des solutions dépend de signe de $\Delta = b^2 - 4ac$. On sait par ailleurs que, si $\Delta \prec 0$ ie $(b^2 - 4ac) \prec 0$ ie $b^2 \prec 4ac$, alors l'équation $ax^2 + bx + c = 0$ n'a pas des solutions dans $\mathbb{R}$ car les nombres négatifs n'ont pas des racine carrés dans $\mathbb{R}$. D'où, il faut construire un ensemble E, incluant l'ensemble $\mathbb{R}$ (plus exactement ayant un sous-ensemble isomorphe à $\mathbb{R}$) et qui, muni de deux lois de compositions interne (+) et (.) soit un corps commutatif et tel que tout nombre réel, même négatif soit le carré dans E.

C'est cet ensemble E qu'on appelle ***ensemble des nombres complexes*** et qu'on note par $\mathbb{C}$.
Ce problème sera traité comme si on fait une extension du corps $\mathbb{R}$ par adjonction du symbole i tel que $i^2 + 1 = 0$, ie $i^2 = -1$.

Remarquer à cet effet que c'est Bombelli, mathématicien Italien qui fut le premier à utiliser l'objet $i = \sqrt{-1}$, qui par définition vérifie $i^2 = -1$. Comme il traitait cet objet comme un nombre, cela lui a permis de le composer avec les nombres réels, en prenant chaque fois soin de remplacer i^2 par -1 dans des calculs. Noter que ce calcul se faisait dans un corps, dit extension du corps $\mathbb{R}$ ou corps engendré par i sur $\mathbb{R}$ et noté par $\mathbb{R}[i]$.

Ainsi, pour deux réels x et y, on a, puisque $(\cdot)$ est commutative, associative et distributive par rapport à (+) dans $\mathbb{R}$:

- $(ix)y = i(xy)$
- $(ix)(iy) = -(xy)$
- $ix + iy = i(x + y)$
- $x(iy) = (xi)y = (ix)y = i(xy)$

Vérifier aux exercices que $(\mathbb{R}[i], +, .)$ est un anneau commutatif et $\mathbb{R}$ est un sous-anneau de $\mathbb{R}[i]$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

B. CONSTRUCTION DE $\mathbb{C}$ ET OPERATIONS

1. Construction de l'ensemble des nombres complexes

a) Théorème

L'ensemble $\mathbb{R}X\mathbb{R}$ muni de deux lois de compositions internes (+) et $(\cdot)$ définies comme suit :

$\forall (a,b),(a',b') \in \mathbb{R}^2$, on a :

- $(a,b)+(a',b')=(a+a',b+b')$
- $(a,b).(a',b')=(aa'-bb',ab'+a'b)$ est un corps commutatif dont le sous-corps décrit par les éléments de la forme $(a,0)$ avec $a \in \mathbb{R}$, est isomorphe à $\mathbb{R}$.

Cet ensemble $\mathbb{R}X\mathbb{R}$ est appelé : ensemble des nombres complexes et noté plus tard par $\mathbb{C}$. Ainsi, un couple ordonné (a,b) des nombres réels est dit nombre complexe. Remarquer que$\forall (a,b),(a',b') \in \mathbb{R}X\mathbb{R}: (a,b)=(a',b') \Leftrightarrow a=a' et\ b=b'$.

Preuve

Montrons que :

- $(\mathbb{R}^2,+,.)$ un corps commutatif.
  On sait d'après III.4.1. [2(6)] que $(\mathbb{R}^2,+,.)$ est un corps commutatif dont le zéro est le couple (0,0), l'unité est le couple (1,0), l'opposé de couple $(a,b) \in \mathbb{R}^2$ est le couple $(-a,-b)$ et le symétrique de couple $(a,b) \neq (0,0)$ est le couple $\left(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2}\right)$.
- On sait aussi, d'après III.4.2. [2(6)] que :
  $\mathbb{C}_0=\mathbb{R}X\{0\}=\{(a,b); a \in \mathbb{R}\}$ est un sous-corps de $(\mathbb{R}^2,+,.)$.
- ***Immersion de $\mathbb{R}$ dans $\mathbb{R}^2$ ou isomorphisme entre $\mathbb{R}$ et $\mathbb{C}_0$***

Définissons une application f de la manière suivante :

$$f: \mathbb{R} \to \mathbb{C}_0$$
$$a \mapsto f(a)=(a,0)$$

f ainsi définie est trivialement bijective et de plus, un morphisme des corps. Montrons à cet effet que :$\forall a,b \in \mathbb{R}: f(a+b)=f(a)+f(b)\ et\ f(a.b)=f(a).f(b)$

En effet, $f(a+b)=(a+b,0)=(a,0)+(b,0)=f(a)+f(b)$

et $f(a.b)=(a.b,0)=(a,0).(b,0)=f(a).f(b)$

D'où f est un isomorphisme des corps. C'est cet isomorphisme f qui nous permet d'immerger $\mathbb{R}$ dans $\mathbb{R}^2$ en identifiant $\mathbb{R}$ à $\mathbb{C}_0$ en posant, $\forall a \in \mathbb{R}; (a,0)=a$. En particulier $(1,0)=1$ et $(0,0)=0$. Puisque $\mathbb{C}_0 \subset \mathbb{R}^2$ est bien un sous-corps de $\mathbb{R}^2$ et $\mathbb{R}$ isomorphe à $\mathbb{C}_0$, alors $\mathbb{R} \subset \mathbb{R}^2$. $\mathbb{R}$ est bien un sous-corps de l'ensemble des complexes $\mathbb{R}^2$ et on a : $\mathbb{R} \simeq \mathbb{C}_0$ et

$\mathbb{C}_0 \subset \mathbb{R}^2 \Rightarrow \mathbb{R} \subset \mathbb{R}^2$. On dit alors qu'on a plongé ou immergé $\mathbb{R}$ dans le corps des complexes. D'où $\mathbb{R}$ est un sous-corps de $\mathbb{R}^2$.

b) Remarque

On sait d'après ce qui précède que, $\forall \alpha \in \mathbb{R}$, on a $\alpha = (\alpha, 0)$

Alors $\forall (a,b) \in \mathbb{R}^2, \alpha.(a,b) = (\alpha.0).(a,b) = (\alpha a - 0, \alpha b - 0) = (\alpha a, \alpha b)$

Ainsi, $\forall (a,b) \in \mathbb{R}^2, \alpha \in \mathbb{R}^2$, on a : $\alpha.(a,b) = (\alpha a, \alpha b)$. Ce qui est bien une loi externe $(\cdot)$ définie dans $\mathbb{R}^2$à scalaire dans $\mathbb{R}$.

i.e. $\cdot : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2$

$[\alpha, (a,b) \longmapsto \alpha(a,b) = (\alpha a, \alpha b)]$

Cette loi externe $(\cdot)$ munit le groupe additif $(\mathbb{R}^2, +)$ d'une structure d'espace vectoriel sur le corps des réels, de dimension 2. D'où le théorème suivant :

c) Théorème

L'ensemble $\mathbb{C} = \mathbb{R}^2$, muni d'une loi additive (+) et d'une loi externe $(\cdot)$ définie ci-dessus est un espace vectoriel sur le corps des réels, de dimension 2.

Preuve

- Comme $(\mathbb{R}^2, +)$ est un groupe abélien, montrons que la loi externe $(\cdot)$ vérifie les propriétés suivantes :

P$_1$. $\forall \alpha, \beta \in \mathbb{R}, \forall (a,b) \in \mathbb{R}^2, (\alpha, \beta)(a,b) = \alpha(a,b) + \beta(a,b)$

En effet,

$$(\alpha+\beta)(a,b) = \left[(\alpha+\beta)a, (\alpha,\beta)b\right] = (\alpha a + \beta a, \alpha b + \beta b)$$
$$= (\alpha a, \alpha b) + (\beta a, \beta b) = \alpha(a,b) + \beta(a,b)$$

P$_2$. $\forall \alpha \in \mathbb{R}, \forall (a,b), (a'b')) \in \mathbb{R}^2, \alpha[(a,b) + (a',b')] = \alpha(a,b) + \alpha(a',b')$

En effet,

$$\alpha\left[(a,b)+(a',b')\right] = \alpha(a+a', b+b') = \left[\alpha(a+a')\right], \alpha(b,b')]$$
$$= (\alpha a + \alpha a', \alpha b + \alpha' b) = (\alpha a + \alpha b) + (\alpha a', \alpha b')$$
$$= \alpha(a,b) + \alpha(a',b')$$

P$_3$. $\forall \alpha, \beta \in \mathbb{R}, \forall (a,b) \in \mathbb{R}^2, \alpha[\beta(a,b)] = (\alpha, \beta)(a,b)$

En effet, $\alpha\left[\beta(a,b)\right] = \alpha(\beta a, \beta b) = \left[\alpha(\beta a), \alpha(\beta b)\right] = \left[(\alpha\beta)a, (\alpha\beta)b\right] = \alpha\beta(a,b)$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

P$_4$. $\forall(a,b)\in\mathbb{R}^2$, on a : $1_{\mathbb{R}}(a,b)=(1.a,1.b)=(a,b)$

Montrons maintenant que la dimension de $\mathbb{R}^2$ est 2.

On sait que les couples (1,0) et (0,1) constituent un système des générateurs de l'espace vectoriel $\mathbb{R}^2$ sur $\mathbb{R}^2$. Donc, $S=\{Z_1=(1,0),Z_2=(0,1)\}$ est une base de $\mathbb{R}^2\simeq\mathbb{C}$ appelée base canonique de $\mathbb{C}\simeq\mathbb{R}^2$ car $\forall(a,b)\in\mathbb{R}^2$ on a $(a,b)=aZ_1+bZ_2$ et si $aZ_1+bZ_2=0$, alors a = b = 0. Comme $cardZ=2$ alors $\dim(\mathbb{R}^2)=2$.

Puisque $\mathbb{R}^2$ est un espace vectoriel sur $\mathbb{R}$ et $S=\{Z_1=(1,0);Z_2=(0,1)\}$ sa base, alors $\forall(a,b)\in\mathbb{R}^2$, on a, en vertu de l'immersion de $\mathbb{R}$ dans $\mathbb{C}$, que :

$$\begin{aligned}(a,b)&=a.(1,0)+b.(0,1)\\&=a.1+b.(0,1)\\&=a+b.(0,1)\end{aligned}$$

ie $(a,b)=a+b.(0,1)$;(s). En posant traditionnellement le couple $(0,1)=i$, (s) devient $(a,b)=a+bi$ et $a+bi\in\mathbb{R}^2$.

Ainsi, $\forall Z\in\mathbb{R}^2: Z=a+bi$ avec $a,b\in\mathbb{R}$ et $i=(0,1)$.

En d'autres termes, on remarque que :

$\forall a\in\mathbb{R},(0,1).(a,0)=(0-0,0+a)=(0,a)$, ie $i.a=(0,a)$. Le nombre complexe $i.a$ est nommé « imaginaire pur ». Comme, pour $(a,b)\in\mathbb{R}^2,(a,b)=(a,0)+(0,b)$, alors on obtient, d'après ce qui précède, que : $(a,b)=(a,0)+(0,b)=a+bi$, soit $(a,b)=a+bi$ (λ)

D'où $\mathbb{C}=\{Z=a+bi:\ a,b\in\mathbb{R}\}$, i étant égal à (0,1).

<u>N.B.</u> : Quelques propriétés des nombres complexes.

i. $\forall Z=a+bi, Z'=a'+b'i\in\mathbb{C}; a+bi=a'+b'i\Leftrightarrow a=a' \text{ et } b=b'$

ii. $\forall Z=a+bi\in\mathbb{C}; a+bi=0\Leftrightarrow a=0 \text{ et } b=0 \text{ ie } 0=0+0i$

iii. $\forall Z=a+bi\in\mathbb{C};$ si $b=0$ alors $Z=a$ est nommé un nombre réel.

En désignant par $\mathrm{Re}(Z)$ la partie réelle de Z, alors on a : $\mathrm{Re}(Z)=a$.

iv. $\forall Z=a+bi\in\mathbb{C};$ si $a=0$ alors $Z=bi$ est nommé un nombre "imaginaire pur".

En désignant par $\mathrm{Im}(Z)$ la partie imaginaire de Z, alors on a : $\mathrm{Im}(Z)=bi$ ou par abus de langage, on écrit aussi $\mathrm{Im}(Z)=b$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

d) Règles de calculs de i

Comme $i=(0,1)$, calculons alors i^2.

On a : $i^2=(0,1)^2=(0,1).(0,1)=(0-1,0+0)=(-1,0)=-1$. D'où $i^2=-1$.

De plus $i^3=-i$ et $i^4=1$.

En effet, $i^3=i^2.i=(-1).i=-i$ et $i^4=i^2.i^2=(-1).(-1)=1$.

D'où, en général, $\forall n\in\mathbb{N}^*$, on a :

$i^{4n}=1; i^{4n+1}=i; i^{4n+2}=-1$ et $i^{4n+3}=-i$

2. Opération dans $\mathbb{C}$

a) Addition dans $\mathbb{C}$

(1) Définition

L'addition (+) est définie dans $\mathbb{C}$ par

$\forall Z=a+bi, Z'=a'+b'i\in\mathbb{C}, Z+Z'=(a+a')+(b+b')i$.

En effet, on a, d'après V.2.1. (1) et de la relation (λ) que :

$$\begin{aligned}(a+bi)+(a'+b'i)&=(a,b)+(a',b')=(a+a',b+b')=(a+a',0)+(0,b+b')\\&=(a+a')+(b+b')i\end{aligned}$$

(2) Théorème

$(\mathbb{C},+)$ est un groupe abélien dont l'élément neutre est le nombre complexe nul $(0+0i=O)$ et l'opposé de $Z=a+bi$ étant $-Z=-a-bi$. Preuve aux exercices.

(3) Conséquences de la structure de groupe additif

$\forall t,t'\in\mathbb{C}, \exists! Z\in\mathbb{C}$ tel que : $t+Z=t'$.
En effet, d'après la conséquence de III.2.1. (3), on a :
$t+Z=t'\Leftrightarrow Z=t'+(-t)$. Par conséquent, le nombre complexe $t'+(-t)$, est appelé différence de t' et t. On a alors $t'-t=t'+(-t)$.
D'où retrancher un nombre complexe équivaut à ajouter son opposé. Par exemple, soit à calculer $(2+4i)-(5-6i)=?$
On a :
$(2+4i)-(5-6i)=(2+4i)+(-5+6i)=[2+(-5)]+(4+6)i=-3+10i$
D'où $(2+4i)-(5-6i)=-3+10i$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

b) La multiplication des nombres complexes

(1) Définition

La multiplication (.) dans $\mathbb{C}$ est une loi interne définie par
$\forall Z = a + bi, Z' = a' + b'i \in \mathbb{C} : Z.Z' = (a+bi)(a'+b'i) = (aa' + bb') + (ab' + a'b)i$

En effet, d'après V.2.1. (3) et la relation (λ), on a :

$$\begin{aligned} Z.Z' &= (a+bi)(a'+b'i) = (a,b).(a',b') \\ &= (aa'-bb', ab'+a'b) = (aa'-bb') + (ab'+a'b)i \end{aligned}$$

Théorème

$(\mathbb{C}^*, .)$ est un groupe abélien dont l'élément neutre est le complexe $1 = 1 + 0i$ et l'inverse de $Z = a + bi \in \mathbb{C}^*$ est $\dfrac{1}{Z} = \dfrac{1}{a+bi} = \dfrac{a-bi}{a^2+b^2}$

Preuve aux exercices.

Par exemple, pour $2 + 4i \in \mathbb{C}^*$; $\frac{1}{2+4i} = \frac{2-4i}{2^2+4^2} = \frac{2-4i}{20}$

Montrer que $\dfrac{1}{3+5i} = \dfrac{3-5i}{34}$

(2) Conséquence de la structure de groupe multiplicatif

$\forall t, t' \in \mathbb{C}^*, \exists!\, Z \in \mathbb{C}^*$ tel que $t.Z = t'$.

En effet, d'après la conséquence de III.2.1. (3), on a : $t.Z = t' \Leftrightarrow Z = \frac{1}{t}t'$

Par suite, ce complexe $\frac{1}{t}t'$ est appelé quotient de t' par t et noté par $\dfrac{t'}{t}$. Dès lors diviser t' par t équivaut à multiplier t' par l'inverse de t, ie $\dfrac{t'}{t} = t'.\dfrac{1}{t}$.

Par exemple,

$$\begin{aligned} \frac{3+4i}{2-5i} &= (3+4i)\cdot\frac{1}{2-5i} = (3+4i)\left(\frac{2+5i}{4+25}\right) \\ &= (3+4i)\left(\frac{2+5i}{29}\right) = \frac{1}{29}(3+4i)(2+5i) \end{aligned}$$

D'où $\dfrac{3+4i}{2-5i} = \dfrac{-14+23i}{29}$

Conclusion

Comme la multiplacition (.) est distributive par rapport à (+) dans $\mathbb{C}$. On conclut, d'après V.2.2.1 (2) et V.2.2.2 (2) que :

- $(\mathbb{C}, +, .)$ est un corps commutatif non ordonné, car aucun ordre dans $\mathbb{C}$ ne peut conférer à $\mathbb{C}$ la structure de corps ordonné. En effet, il existe $i \in \mathbb{C}$ tel que $i^2 = -1$ et pourtant dans un corps ordonné, tout nombre élevé au carré est positif.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

- $\mathbb{C}_0 = \mathbb{R}X\{0\} \cong \mathbb{R}$ est un sous corps de $\mathbb{C}$ pour les lois induites (+) et (.). remarquer que $\mathbb{C}^0 = \mathbb{R}X\{0\} = \{(0,b): b \in \mathbb{R}\} = \{bi: b \in \mathbb{R}\}$ a une structure maximale d'un groupe abélien pour la loi (+) car la loi (.) n'est pas interne dans $\mathbb{C}^0$.

Exercice

Montrer que $(\mathbb{C}_0, +, .)$ et $(\mathbb{C}^0, +, .)$ où (.) est une loi externe à scalaires dans $\mathbb{R}$, sont des sous-espaces vectoriels de $\mathbb{C}$ et on a : $\mathbb{C}_0 \oplus \mathbb{C}^0 = \mathbb{C}$.

c) Retour sur le problème posé

Le problème posé, à l'introduction de l'ensemble des complexes, nous a conduit à construire et à structurer l'ensemble $\mathbb{C}$. Il reste à montrer que l'ensemble $\mathbb{C}$ est bien la solution de ce problème. Or $(\mathbb{C}\ ,+,.)$ est un corps commutatif dont $(\mathbb{R},+,.)$ est sous-corps, donc il reste à établir que :

$\forall b \in\ \mathbb{R}$, il existe au moins $Z \in \mathbb{C}$ tel que $Z^2 = b$, (∂)

Or $Z \in \mathbb{C} \Rightarrow \exists x, y \in \mathbb{R}$ tel que $Z = x + yi$, donc $Z^2 = (x + yi)^2 = (x^2 + y^2) + 2xyi$ comme $b = b + 0i$, alors l'équation (∂) devient :

$$(x^2 + y^2) + 2xyi = b + 0i \Rightarrow \begin{cases} x^2 - y^2 = b \\ 2xy = 0 \end{cases} \Rightarrow \begin{cases} x^2 - y^2 = b \\ xy = 0 \end{cases} ,(\partial')$$

Puisque $x, y \in \mathbb{R}$ et $x.y = 0$, alors x = 0 et y = 0 car $\mathbb{R}$ est un corps ; donc le système (∂') se décompose en :

$$(\partial_1') \begin{cases} x^2 - y^2 = b \\ x = 0 \end{cases} \text{ et } (\partial_2') \begin{cases} x^2 - y^2 = b \\ y = 0 \end{cases}$$

Le système (∂_1') entraîne que x = 0 et $y^2 = -b$.

- Ainsi, si $b \in \mathbb{R}_+^*$, alors $y^2 = -b$ est une équation impossible dans $\mathbb{R}$. Ce qui est en fait le problème posé.
- Si $b \in \mathbb{R}_-^*$ puisque x = 0, alors $y^2 = -b$ entraîne que $y = \pm\sqrt{-b}$

  On vérifie que $Z = x + yi = 0 \pm i\sqrt{-b} = \pm i\sqrt{-b}$ satisfait l'équation (∂) .

Pour le système (∂_2'), puisque y = 0, alors $x^2 = b$ ssi $x = \pm\sqrt{b}$ si $b \in \mathbb{R}_+$, car dans le cas contraire, ie $b \in \mathbb{R}_-^*$, l'équation $x^2 = b$ est impossible dans $\mathbb{R}$.

On vérifie aussi que $Z = x + yi = 0 \pm i\sqrt{b} = \pm i\sqrt{b}$ satisfait l'équation (∂) .

D'où le corps $\mathbb{C}$ ainsi construit est solution du problème posé car pour $b \in \mathbb{R}$, l'équation

$$Z^2 = b \Leftrightarrow \begin{cases} Z = \pm\sqrt{b}, & si\ b \in \mathbb{R}_+^* \\ Z = \pm\sqrt{-b}, & si\ b \in \mathbb{R}_-^* \end{cases}$$

Par exemple, $Z^2 = -5 \Leftrightarrow Z = \pm i\sqrt{-(-5)} = \pm i\sqrt{5}$ et $Z^2 = 5 \Leftrightarrow Z = \pm\sqrt{5}$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

d) Nombres complexes conjugués

(1) Définition

Soit $Z = a + bi$, un nombre complexe, le conjugué de Z noté $\overline{Z}$ est le complexe $a - bi$ ie pour $Z = a + bi \in \mathbb{C}$, alors $\overline{Z} = a - bi$.

Par exemples : $\overline{1+i} = 1 - i$ et $\overline{5} = -5$ et $\overline{-5i} = 5i$.
Si $Z = a + bi$, alors $\overline{Z} = a - bi$ et on a :
$Z + \overline{Z} = 2a = 2\operatorname{Re}(Z)$ et $Z \cdot \overline{Z} = a^2 + b^2$, donc $Z + \overline{Z} \in \mathbb{R}$ et $Z.\overline{Z} \in \mathbb{R}$.

Ainsi, un nombre complexe Z est réel si $Z = \overline{Z}$ et il est imaginaire si $Z + \overline{Z} = 0$ ie $Z = -\overline{Z}$.

(2) Propriétés

P$_1$. L'application g : $\mathbb{C} \to \mathbb{C}$
$Z \to g(Z) = \overline{Z}$ est une involution

ie $g \circ g = id_{\mathbb{C}}$

En effet, montrons que $\forall Z \in \mathbb{C}, (g \circ g)(Z) = Z$ où $\overline{\overline{Z}} = Z$.

$(gog)(Z) = id_{\mathbb{C}} \Leftrightarrow g\left[g(Z)\right] = Z \Leftrightarrow g\left(\overline{Z}\right) = Z \Leftrightarrow \overline{\overline{Z}} = Z$

D'où, $\forall Z \in \mathbb{C}$, on a : $\overline{\overline{Z}} = Z$.

P$_2$. L'application g : $\mathbb{C} \to \mathbb{C}$
$Z \to g(Z) = \overline{Z}$ est un morphisme

Montrons que $\forall Z, Z' \in \mathbb{C}; g(Z + Z') = g(Z) + g(Z')$ et $g(Z.Z') = g(Z).g(Z')$.

En effet, pour $Z = a + bi, Z' = a' + b'i \in \mathbb{C}$, on a :

$$g(Z + Z') = \overline{Z + Z'} = \overline{(a+bi) + (a'+b'i)} = \overline{(a+a') + (b+b')i}$$
$$= (a+a') - (b+b')i = (a-bi) + (a'-b'i) = g(Z) + g(Z')$$

et

$$g(Z.Z') = \overline{Z.Z'} = \overline{(a+bi).(a'+b'i} = \overline{(aa'-bb') + (ab'+a'b)i}$$
$$= (aa'-bb') - (ab'+a'b)i = aa' - bb' - ab'i - a'bi$$
$$= (a-bi).(a'-b'i) = \overline{Z}.\overline{Z'} = g(Z).g(Z')$$

D'où, $\forall Z, Z' \in \mathbb{C}, \overline{Z + Z'} = \overline{Z} + \overline{Z'}$ et $\overline{Z.Z'} = \overline{Z}.\overline{Z'}$.

P$_1$ et P$_2$ $\Rightarrow$ l'application g est un automorphisme de ($\mathbb{C}$, +, $\cdot$).

P$_3$. $\forall Z \in \mathbb{C}^*, g\left(\frac{1}{Z}\right) = \frac{1}{g(Z)}$, ie $\overline{\left(\frac{1}{Z}\right)} = \frac{1}{\overline{Z}}$.

En effet, $Z \in \mathbb{C}^* \Rightarrow Z$ est inversible, ie $\exists \frac{1}{Z} \in \mathbb{C}^*$ tel que $Z.\frac{1}{Z} = 1$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Ou, d'après P_2 ci-dessus, $g\left(Z.\frac{1}{Z}\right)=g(1) \Leftrightarrow g(Z).g\left(\frac{1}{Z}\right)=1 \Leftrightarrow g\left(\frac{1}{Z}\right)=\frac{1}{g(Z)}$

D'où, $\overline{\left(\frac{1}{Z}\right)}=\frac{1}{\overline{Z}}$

e) Norme algébrique d'un nombre complexe

(1) Définition

On appelle norme algébrique d'un nombre complexe Z, notée N(Z), le nombre réel positif $Z.\overline{Z}$, ie $N(Z)=Z.\overline{Z}$.

On définit ainsi une application : $N: \mathbb{C} \to \mathbb{R}_+$

$$Z \to N(Z) = Z\,.\,\overline{Z}$$

Pour $Z=a+bi \in \mathbb{C}$, on a : $N(Z)=Z.\overline{Z}=a^2+b^2$, ie $N(a+bi)=a^2+b^2$.

Par exemples : $N(1)=1; N(4+3i)=16+9=25$ *et* $N(6i)=36$.

(2) Propriétés

P_1. $\forall Z \in \mathbb{C}, N(Z)=0 \Leftrightarrow Z=0$

En effet, pour $Z=a+bi \in \mathbb{C}$, on a :

$$N(Z)=0 \Leftrightarrow a^2+b^2=0 \Leftrightarrow a^2=0 \text{ et } b^2=0$$

$$\Leftrightarrow a=b=0 \Leftrightarrow 0=0+0i.$$

D'où, $Z=0=0+0i$.

P_2. L'application : $N: \mathbb{C} \to \mathbb{R}_+$

$Z \to N(Z) = Z\,.\,\overline{Z}$ est un morphisme des groupe

Ou $\forall Z, Z' \in \mathbb{C}, N(Z.Z')=N(Z).N(Z')$

En effet,

$$N(Z.Z')=(Z.Z').\left(\overline{Z.Z'}\right)=(Z.Z')\left(\overline{Z}.\overline{Z'}\right)=\left(Z.\overline{Z}\right)\left(Z'.\overline{Z'}\right)$$

$=N(Z).N(Z')$; vraie en vertu de P_2 de V.2.2.4 (2)

f) Calcul de l'inverse d'un nombre complexe

La norme algébrique de $Z \in \mathbb{C}$ nous permet de calculer l'inverse de Z et de retrouver son existence.

- Soit Z un nombre complexe inversible, ie $Z \neq 0$ et $\exists t \in \mathbb{C}^*$ tel que : $Z.t=1$.

  Comme N est un morphisme des groupes, alors $N(Z.t)=N(1) \Leftrightarrow N(Z).N(t)=1$. Ce qui prouve que Z inversible dans $\mathbb{C}$ *et* $N(Z)$ est inversible dans $\mathbb{R}_+^*$.

- Supposons maintenant que, pour $Z \in \mathbb{C}^*$, N(Z) est inversible dans $\mathbb{R}_+^*$, ie $N(Z)\neq 0$ et $\exists \frac{1}{N(Z)} \in \mathbb{R}_+^*$ tel que $N(Z).\frac{1}{N(Z)}=1.(\delta)$, comme $N(Z)=Z.\overline{Z}$, alors (δ) devient $\left(Z.\overline{Z}\right).\frac{1}{Z.\overline{Z}}=1$ ou $Z.\left(\overline{Z}.\frac{1}{Z.Z'}\right)=1$, soit $Z.\left(\overline{Z}.\frac{1}{N(Z)}\right)=1$ entraînant que :

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

$\overline{Z}.\dfrac{1}{N(Z)}$ est l'inverse de Z. en notant l'inverse de Z par $Z^{-1}=\dfrac{1}{Z}$, on obtient : $Z^{-1}=\dfrac{1}{Z}=\dfrac{\overline{Z}}{N(Z)}=\dfrac{\overline{Z}}{Z.\overline{Z}}$.

D'où, $\forall Z\in\mathbb{C}^*;\dfrac{1}{Z}=\dfrac{\overline{Z}}{N(Z)}$ et $\forall Z\in\mathbb{C}^*,\forall t\in\mathbb{C}$, on a :

$\dfrac{t}{Z}=t\cdot\dfrac{1}{Z}=\dfrac{t.\overline{Z}}{Z.\overline{Z}}$ ie $\dfrac{t}{Z}=\dfrac{t.\overline{Z}}{Z.\overline{Z}}$

Par exemple : $\dfrac{2+4i}{2-3i}=\dfrac{(3+4i)(2+3i)}{(2-3i)(2+3i)}=\dfrac{-6+17i}{13}$

g) Module ou valeur absolue d'un nombre complexe

(1) Définition

On appelle valeur absolue ou norme géométrique d'un nombre complexe Z, notée $|Z|$ ou V(Z) le nombre réel positif $\sqrt{Z.\overline{Z}}$. La valeur absolue d'un nombre complexe Z est la racine carrée arithmétique de la norme algébrique de Z.

On écrit alors ; pour $Z\in\mathbb{C};|Z|=V(Z)=\sqrt{N(Z)}=\sqrt{Z.\overline{Z}}$.

On définit ainsi une application :$V:\mathbb{C}\to\mathbb{R}^*_+$

$$Z\mapsto V(Z)=|Z|=\sqrt{Z.\overline{Z}}$$

Par exemple,$|3-6i|=\sqrt{(3-6i)(3+6i)}=\sqrt{9+36}=\sqrt{45}$ et

$$|a+bi|=\sqrt{(a+bi)(a-bi)}=\sqrt{a^2+b^2}$$

D'où, pour $Z=a+bi\in\mathbb{C}$, on a $|Z|=\sqrt{a^2+b^2}$

(2) Propriétés

P$_1$. L'application V : $\mathbb{C}\to\mathbb{R}^*_+$

Z $\to$ V(Z) = $|Z|$ = $\sqrt{N(Z)}$ est un morphisme des groupes pour la loi multiplicative.

Montrons que $\forall Z,t\in\mathbb{C}:V(Z.t)=V(Z).V(t)$.

En effet, $\forall Z,t\in\mathbb{C}$, on sait que $|Z|^2=Z.\overline{Z}$ et $|t|^2=t.\overline{t}$, alors d'après P$_2$ de V.2.2.4.,

$|Z.t|^2=(Z.t)(\overline{Z.t})=(Z.\overline{Z})(t.\overline{t})=|Z|^2.|t|^2=(|Z|.|t|)^2$

Soit$|Z.t|^2=(|Z|.|t|)^2$. En prenant les racines carrées dans $\mathbb{R}_+$ de 2 membres de cette égalité, on obtient :

$\sqrt{|Z.t^2|}=\sqrt{(|Z|.|t|)^2}\Leftrightarrow|Z.t|=|Z|.|t|$

D'où, $\forall Z,t\in\mathbb{C},|Z.t|=|Z|.|t|$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Conséquence

Si t est l'inverse de $Z \in \mathbb{C}^*$, ie $t = \frac{1}{t}$, alors $t.Z = \left(\frac{1}{Z}.Z\right) = 1$. Comme l'application $V = |\ \ |$ est un morphisme pour la loi interne $(.)$, on a : $\left|Z.\frac{1}{Z}\right| = |1|$ ssi $|Z|.\left|\frac{1}{Z}\right| = 1$ ssi $\left|\frac{1}{Z}\right| = \frac{1}{|Z|}$.

D'où, $\forall Z \in \mathbb{C}^*$, on a $\left|\frac{1}{Z}\right| = \frac{1}{|Z|}$.

P$_2$. $\forall Z \in \mathbb{C}, |Z| = 0 \Leftrightarrow Z = 0$, ce qui est évident d'après P$_1$ de V.2.2.5 (2).

P$_3$. $\forall Z \in \mathbb{C}, |Z| = |\overline{Z}| = |-Z|$, ce qui est vrai, d'après la définition de la valeur absolue d'un nombre complexe.

P$_4$. $\forall Z \in \mathbb{C}$, on a $\operatorname{Re}(Z) \le |Z|$.

En effet, pour $Z = a + bi \in \mathbb{C}$, on a : $|Z| = \sqrt{a^2 + b^2} \in \mathbb{R}_+^*$.

Comme $a \in \mathbb{R}$, alors $a \le |a|$. De plus $\sqrt{a^2} \le \sqrt{a^2 + b^2} = |Z|$ donc $a^2 \le \sqrt{a^2 + b^2} = |Z|$, or $\operatorname{Re}(Z) = a$, donc $\operatorname{Re}(Z) \le |Z|$.

P$_5$. $\forall Z, t \in \mathbb{C}, |Z + t| \le |Z| + |t|$. Cette inégalité est nommée : inégalité de Minkowski.

Preuve

En effet, par définition de la valeur absolue, on a :

$$|Z + t|^2 = (Z + t)\left(\overline{Z + t}\right) = (Z + t)\left(\overline{Z} + \overline{t}\right) = Z.\overline{Z} + t.\overline{Z} + Z.\overline{t} + t.\overline{t}$$

$$= |Z|^2 + |t|^2 + 2\operatorname{Re}\left(Z.\overline{t}\right)$$ car $Z.\overline{t}$ et $t.\overline{Z}$ sont conjugués.

$$\le |Z|^2 + |t|^2 + 2|Z|.|t|$$

Car d'après P_4, P_1 et P_3 ci-dessus,

$\operatorname{Re}\left(Z.\overline{t}\right) \le \left|Z.\overline{t}\right| = |Z|.\left|\overline{t}\right| = |Z|.|t|$, ie $\operatorname{Re}\left(Z.\overline{t}\right) \le |Z|.|t|$

On obtient ainsi, $|Z + t|^2 \le |Z|^2 + 2|Z|.|t| + |t|^2 = \left(|Z| + |t|\right)^2$, soit $|Z + t|^2 \le \left(|Z| + |t|\right)^2$ et en prenant les racines carrées de deux membres de cette inégalité dans $\mathbb{R}_+$, on obtient : $|Z + t| \le |Z| + |t|$, d'où la thèse.

Montrer aux exercices que $\forall Z, t \in \mathbb{C}, \left||Z| + |t|\right| \le |Z - t|$.

Conclusion

L'ensemble $\mathbb{C}$, muni des lois internes (+) et (.) et de la valeur absolue $(|\ \ |)$ est dit corps valué.

C. PLAN COMPLEXE

1. Représentation géométrique des nombres complexes

Dans ce paragraphe, nous allons nous permettre de donner une représentation tant vectorielle que ponctuelle d'un nombre complexe.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

a) Représentation vectorielle

Soient $\mathcal{V}_2$ un IR-espace euclidien, de dimension 2,

ie $\mathcal{V}_2 = \mathbb{R} - espace\ \mathbb{R}^2$ et $B = \{\overrightarrow{e_1}, \overrightarrow{e_2}\}$ sa base orthonormée $(*)$, alors

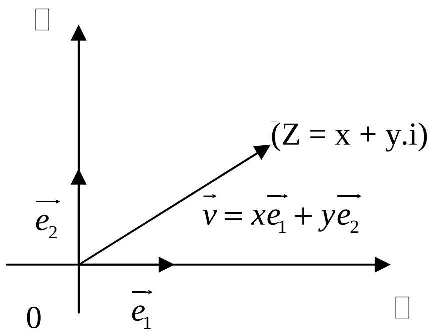
$\forall \vec{v} \in \mathcal{V}_2, \exists x, y \in \mathbb{R}$ tels que : $\vec{v} = x\overrightarrow{e_1} + y\overrightarrow{e_2}$:

x, y $\in$ IR $\Rightarrow$ x + yi $\in \mathbb{C}$

Il vient alors qu'à tout nombre complexe $Z = x + yi$, on associe le vecteur $\vec{v} \in V_2$ des composantes scalaires x et y dans la base B. Ce qui nous permet de définir une application : f : $\mathbb{C} \rightarrow \mathcal{V}_2$

$$Z = x + yi \mapsto f(Z) = \vec{v} = x.\overrightarrow{e_1} + y.\overrightarrow{e_1}$$

Cette application f est bijective de part sa définition.
Par exemple, $f(1) = \overrightarrow{e_1}$ et $f(i) = \overrightarrow{e_2}$.



Définitions

- Le nombre complexe $Z = x + yi$ s'appelle mesure complexe ou affixe du vecteur $\vec{v} = x\overrightarrow{e_1} + y\overrightarrow{e_2}$.
- Le vecteur $\vec{v} = x\overrightarrow{e_1} + y\overrightarrow{e_2}$ est le vecteur image de nombre complexe $Z = x + yi$. On note par $\left[\vec{v}\right]$ la mesure complexe du vecteur $\vec{v}$, alors $\left[\vec{v}\right] = Z \in \mathbb{C}$ ie $\left[x\overrightarrow{e_1} + y\overrightarrow{e_2}\right] = x + yi$. Ainsi, $\left[\overrightarrow{e_1}\right] = 1$; $\left[\overrightarrow{e_2}\right] = i$ et $\left[3\overrightarrow{e_1} + 2\overrightarrow{e_2}\right] = 3 + 2i$.

b) Représentation ponctuelle

Soit E_2, un R-espace affine euclidien de dimension 2 défini relativement à l'espace verctoriel V_2, rapporté à un repère orthonormé $\left(0, \overrightarrow{e_1}, \overrightarrow{e_2}\right)$. A tout nombre complexe Z, on associe un point M de E_2 de coordonnées cartésiennes x et y. Ceci nous permet de définir une application f de la manière suivante :

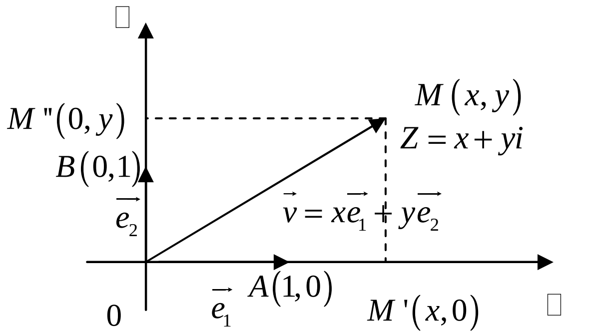
$$f : \mathbb{C} \rightarrow E_2$$

$$Z = x + yi \mapsto f(Z) = M(x, y)$$

f ainsi définie est une bijection.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Par exemple, $f(1) = A(1,0)$; $f(i) = B(0,1)$ et $f(0) = O(0,0)$



Ce dessin montre qu'à un nombre complexe $Z = x + yi$, on associe le point M(x,y) et à ce point M(x,y), on associe le vecteur $\overrightarrow{OM} = x\vec{e_1} + y\vec{e_2}$.

- ***Définition***

Le nombre complexe $Z = x + yi$ s'appelle affixe du point M(x,y), ie mesure complexe du vecteur $\overrightarrow{OM}$ et M(x,y) est dit point image de nombre complexe $Z = x + yi$.

- ***Définition*** (distance de deux points)

Soient M(x,y) et M'(x',y') deux points de E_2, images respectives de $Z = x + yi$ et $Z' = x' + y'i$, alors la distance entre M et M', notée d(M,M') est la valeur absolue de (Z.Z') ie $d(M,M') = |Z - Z'| = |(x - x') + (y - y')i| = \sqrt{(x - x')^2 + (y - y')^2}$ et $(\mathcal{V}_2, d)$ est dit espace vectoriel métrique.

Comme M(x,y) est le point image de $Z = x + yi$ et $Z = x + yi$ est la mesure complexe du vecteur $\overrightarrow{OM}$, alors, $|Z| = \left\|\overrightarrow{OM}\right\| = d(O,M) = \sqrt{x^2 + y^2}$, avec $\left\|\overrightarrow{OM}\right\|$ la norme vectorielle de $\overrightarrow{OM}$.

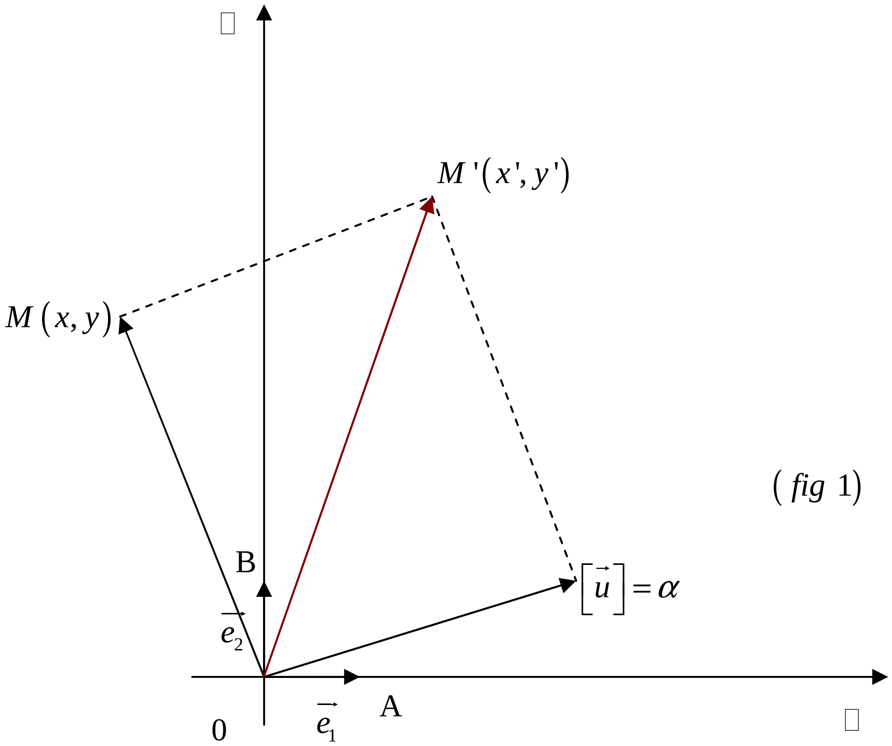
c) Remarque

Soit $\vec{u} \in \mathcal{V}_2$, si $\left[\vec{u}\right] = \alpha$, avec $\alpha = a + bi$, alors l'application de $\mathbb{C}$ dans $\mathbb{C}$ qui à $Z \in \mathbb{C}$ associe $\alpha + Z$, se traduit sur le point M d'affixe Z par la translation $t_{\vec{u}}$ ie si $\vec{u} \in V_2$ est tel que $\left[\vec{u}\right] = \alpha$, avec $\alpha \in \mathbb{C}$, alors

$$t_{\vec{u}} : E_2 \to E_2$$
$$M \to t_{\vec{u}}(M) = M' \text{ à condition que } \overrightarrow{MM'} = \vec{u}$$

est une translation associée au vecteur $\vec{u}$.

En effet, si $\left[\vec{u}\right] = \alpha = a + bi$, $\left[\overrightarrow{OM}\right] = Z = x + yi$ et $\left[\overrightarrow{OM'}\right] = Z' = x' + y'i$, ie $\vec{u} = a\vec{e_1} + b\vec{e_2}$, $\overrightarrow{OM} = x\vec{e_1} + y\vec{e_2}$ et $\overrightarrow{OM'} = x'\vec{e_1} + y'\vec{e_2}$, alors $\overrightarrow{OM} + \overrightarrow{MM'} = \overrightarrow{OM'} \Leftrightarrow \overrightarrow{MM'} = \overrightarrow{OM'} - \overrightarrow{OM}$ ou $\overrightarrow{OM'} - \overrightarrow{OM} = \vec{u}$ car $\overrightarrow{MM'} = \vec{u}'$. (fig 1)



En projetant le vecteur $\vec{u}$ respectivement sur d_1 et d_i avec d_1 et d_i droites vectorielles engendrées respectivement par $\vec{e_1}$ et $\vec{e_2}$, on obtient : $x'-x=a$ et $y'-y=b$ équivalant à $(x'-x, y'-y)=(a,b)$ ou $(x'-x)+(y'-y)i=a+bi$ ou encore $(x'+yi)-(x+y'i)i=a+bi$. Soit $x'+y'i=(a+bi)+(x+yi)$ ie $Z'=\alpha+Z$.

On constate que, $\forall \alpha \in \mathbb{C}$, l'application

$t_\alpha : \mathbb{C} \rightarrow \mathbb{C}$

$Z \mapsto t_\alpha(Z) = \alpha + Z$ est une translation de $\mathbb{C}$ associée à α.

Notons par $\mathcal{T}$ l'ensemble des translations du plan E_2 associées aux nombres complexes, ie $\mathcal{T} = \{t_\alpha : \mathbb{C} \rightarrow \mathbb{C} : t_\alpha$ est une translation de $\mathbb{C}$ associée à $\alpha \in \mathbb{C}\}$.

d) Théorème

(1) ($\mathcal{T}$, o) est un groupe abélien.

Preuve

- Montrons d'abord que la loi (o) est interne dans $\mathcal{T}$ ou $\forall \alpha, \beta \in \mathbb{C}, t_\alpha o t_\beta = t_\partial$ avec $\partial \in \mathbb{C}$.

  En effet effet,

  $\forall \alpha, \beta \in \mathbb{C}, \forall Z \in \mathbb{C} : (t_\alpha o t_\beta)(Z) = t_\alpha[t_\beta(Z)] = t_\alpha(\beta+Z) = \alpha + (\beta+Z) = (\alpha+\beta)+Z = t_{\alpha+\beta}$

  Prendre alors $\alpha+\beta=\partial \in \mathbb{C}$ pour avoir $t_\alpha + t_\beta = t_{\alpha+\beta}$ et la loi (o) est interne dans $\mathcal{T}$.
- Comme l'addition est associative et commutative dans $\mathbb{C}$, alors la loi (o) l'est aussi dans $\mathcal{T}$.
- La translation t_o est l'élément neutre de la loi (o) dans $\mathcal{T}$ car $\forall \alpha \in \mathbb{C}, t_\alpha o t_\beta = t_\alpha$.

  En effet, $t_\alpha o t_o = t_{\alpha+o} = t_\alpha$.
- Aussi pour $\alpha \in \mathbb{C}$, $t_{-\alpha}$ est la réciproque de t_α dans $\mathcal{T}$ pour la loi interne (o) car $t_\alpha o t_{-\alpha} = t_o$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

En effet, $t_\alpha o t_{-\alpha} = t_{\alpha+(-\alpha)} = t_o$.

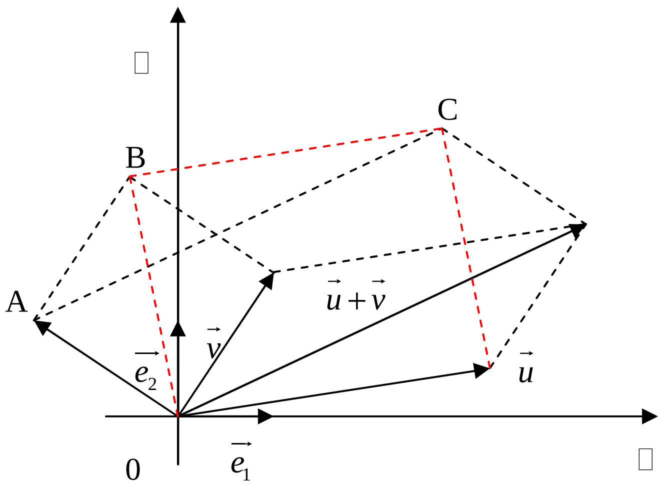
(2) L'ensemble ($\mathbb{C}$, +) est un groupe commutatif isomorphe à ($\mathcal{T}$,0) avec $\mathcal{T}$ l'ensemble des translations du plan affine associé au vecteur $\vec{u}$ de, dont la mesure complexe est le nombre complexe α.

Preuve

Soit $\vec{u} \in V_2$ tel que $\left[\vec{u}\right] = \alpha \in \mathbb{C}$, montrons que l'application

$$t : (\mathbb{C}, +) \to (\mathfrak{I}, o)$$
$$\alpha \mapsto t_\alpha = t_{\vec{u}} : E_2 \to E_2$$
$$M \mapsto t_{\vec{u}}(M) = M'$$

ssi $\overrightarrow{MM'} = \vec{u}$, est un isomorphisme des groupes abéliens.
En effet, t est bijective de part sa définition. De plus, $\forall \alpha, \beta \in \mathbb{C}, t_{\alpha+\beta} = t_\alpha o t_\beta$.
En effet, $\forall \vec{u}, \vec{v} \in V_2$ tels que $\left[\vec{u}\right] = \alpha$ et $\left[\vec{v}\right] = \beta$, avec $\forall \alpha, \beta \in \mathbb{C}$, on a :
$t_{\alpha+\beta} = t_{\vec{u}+\vec{v}} = t_{\vec{u}} \circ t_{\vec{v}} = t_\alpha \circ t_\beta$. (fig 2).
Ce résultat nous permet de conclure que l'addition des nombres complexes est interprétée dans le plan affine E_2 par la composition des translations de E_2 ou par l'addition vectorielle dans V_2.



(fig 2)

Posons $t_{\vec{u}+\vec{v}}(A) = C$ et $t_{\vec{v}}(A) = B$.

Montrons sur le dessin que : $t_{\vec{u}+\vec{v}}(A) = C$

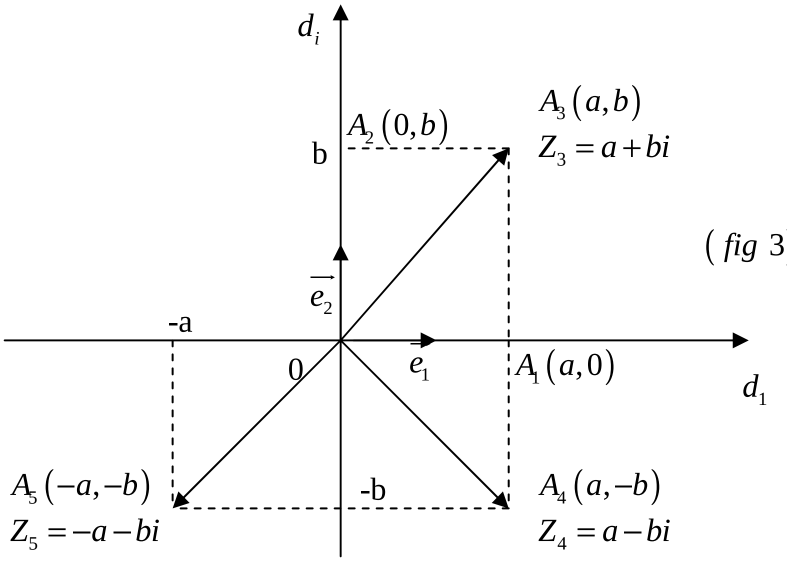
D'autre part, l'application bijective :

$$f : E_2 \to \mathbb{C}$$
$$(x, y) \mapsto f(x, y) = x + yi$$

est un isomorphisme d'espaces vectoriels, ie $\mathbb{C}$ et E_2 sont isomorphes. C'est donc cet isomorphisme f, qui nous permet alors d'identifier les deux R-espaces vectoriels $\mathbb{C}$ et E_2, avec E_2 le plan affine réel relativement à R-espace vectoriel V_2, et l'interprétation de

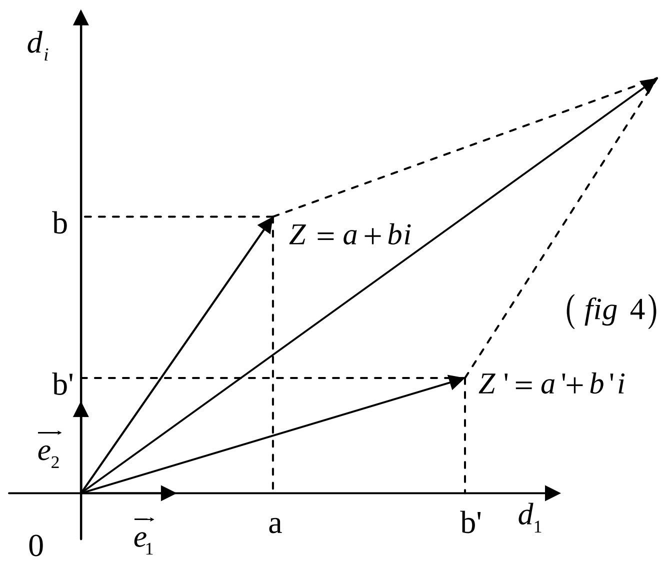
l'addition des nombres complexes par la composition des translations ponctuelles de E_2 ou l'addition vectorielle dans V_2, sont souvent appelées PLAN COMPLEXE ou PLAN D'ARGAND - GAUSS. Ainsi, pour $(x, y) \in E_2$, $f(x, y) = x + yi \in \mathbb{C}$ est appelé point du plan complexe $\mathbb{C}$.
Représentons, par exemple, dans le plan complexe $\mathbb{C}$ les images des nombres complexes suivants :

1) $Z_1 = a; Z_2 = bi; Z_3 = a + bi; Z_4 = a - bi$ et $Z_5 = -a - bi$; (fig 3).
2) $Z'' = Z + Z'$ avec $Z = a - bi$ et $Z' = a' + b'i$. (fig 4)



$(fig\ 3)$

On constate sur cette fig 1 que A_3 et A_4 points images respectifs de $Z_3 = a + bi$ et $Z_4 = a - bi$ sont symétriques par rapport à la droite d_1 engendrée par le vecteur $\vec{e_1}$.



$(fig\ 4)$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

2. Homothétie

a) Définition

Soit $a \in \mathbb{C}$, l'application

$$h_a : \mathbb{C} \to \mathbb{C}$$
$$Z \mapsto h_a(Z) = aZ$$
est appelée une homothétie de rapport a.

Si $a \in \mathbb{C}^*$, l'homothétie h_a est bijective. Elle est même un morphisme de groupe additif $(\mathbb{C},+)$. Donc h_a est un automorphisme de $(\mathbb{C},+)$ si $a \in \mathbb{C}^*$.

Noter par $H = \left\{ h_a : \mathbb{C} \to \mathbb{C} : h_a \text{ homothetie de } \mathbb{C} \text{ de rapport } a \in \mathbb{C}^* \right\}$, alors (H,o) est un groupe abélien dont l'élément neutre est $h_1 = id_{\mathbb{C}}$ et la réciproque de $h_a \in H$ est $h_{\frac{1}{a}} \in H$ car

$h_a o h_{\frac{1}{a}} = h_{\left(a.\frac{1}{a}\right)} = h_1$.

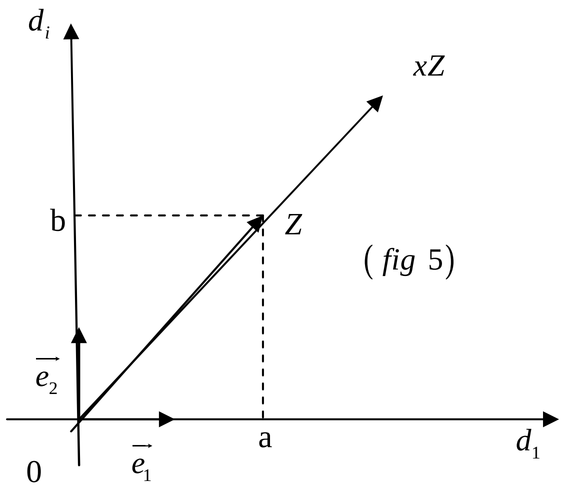
b) Théorème

(H,o) est un groupe abélien isomorphe à $(\mathbb{C}^*,.)$.

En effet, définir une application h de la manière suivante :

$$h : (\mathbb{C}^*,.) \to (H,o)$$
$$a \mapsto h_a : \mathbb{C} \to \mathbb{C}$$
$$\mathrm{Z} \mapsto h_a(Z) = aZ$$

et montrer aux exercices que h ainsi définit est un isomorphisme sachant que $Z = a + bi$ est un point du plan complexe $\mathbb{C}$, représenter dans ce même plan complexe $\mathbb{C}$ le point $x.Z$, avec $x \in \mathbb{R}_+^*$. (fig 5).



Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

3. Similitudes du plan complexe $\mathbb{C}$

a) Définition

Soit ∂ un nombre complexe non nul, l'application

$$s_\partial : \mathbb{C} \to \mathbb{C}$$
$$Z \mapsto s_\partial(Z) = \partial.Z$$

s'appelle similitude du plan complexe $\mathbb{C}$, associée à ∂.

Montrons que $\forall \partial \in \mathbb{C}^*$, s_∂ est une permutation de $\mathbb{C}$ ou d'après $\forall t \in \mathbb{C}$, l'équation $s_\partial(Z) = t$ admet une solution et une seule dans $\mathbb{C}$.

$s_\partial(Z) = t$ ssi $\partial.Z = t \Leftrightarrow Z = \partial^{-1}.t = \frac{1}{\partial}.t$. D'où $\exists ! Z = \frac{1}{\partial}.t \in \mathbb{C}$ tel que $s_\partial(Z) = t$ et s_∂ est une permutation de $\mathbb{C}$.

Si on note par $S = \{s_\partial : \mathbb{C} \to \mathbb{C} : s_\partial$ est une similitude du plan complexe $\mathbb{C}$, associé à $\partial\}$, alors S est un groupe abélien pour la loi interne (o) des compositions des similitudes de $\mathbb{C}$. D'où le théorème ci-dessous.

b) Théorème

(1) (S, o) ***est un groupe abélien.***

- Montrons que $\forall \partial, \lambda \in \mathbb{C}^*, s_\partial o s_\lambda = s_\alpha$ avec $\alpha \in \mathbb{C}^*$.

  En effet, $\forall Z \in \mathbb{C} : (s_\partial o s_\lambda)(Z) = s_\partial[s_\lambda(Z)] = s_\partial(\lambda Z) = \partial(\lambda Z)$
  $$= (\partial\lambda) Z = s_{\partial\lambda}$$

  Comme $\partial, \lambda \in \mathbb{C}^*$ et $\partial.\lambda$ aussi, prendre alors $\alpha = \partial.\lambda$ et (o) est une loi interne dans S. Ainsi, $\forall \partial, \lambda \in \mathbb{C}, s_\partial o s_\lambda = s_{\partial\lambda}$.
- D'autre part, pour $\partial = 1 \in \mathbb{C}^*$, la similitude $s_1 = id_{\mathbb{C}}$ est l'élément neutre de S pour la loi (o) et $s_{\frac{1}{\partial}} = s_{\partial^{-1}}$ est la réciproque de s_∂ pour la loi (o) dans S.
- De plus, la loi (o) est commutative et associative dans S car la loi (.) l'est aussi dans $\mathbb{C}$.

(2) L'application s est isomorphe des groupes abéliens

$$s : (\mathbb{C}^*, .) \to (S, o)$$
$$\partial \mapsto s_\partial : \mathbb{C} \to \mathbb{C}$$
$$Z \mapsto s_\partial(Z) = \partial Z$$

ie $\mathbb{C}^*$ est isomorphe à (S, o). Preuve aux exercices.

Conclusion :

Cet isomorphisme va nous permettre d'interpréter la multiplication des nombres complexes par la composition des similitudes dans le plan complexe $\mathbb{C}$.

Remarquer que si ∂ est un nombre complexe de module égale à 1, alors la similitude s_∂ devient alors une rotation de $\mathbb{C}$ associé à ∂ . On la note par r_∂ . Ainsi, pour ∂ un nombre complexe de module égal à 1, l'application

$$r_\partial : \mathbb{C} \to \mathbb{C}$$
$$Z \mapsto r_\partial(Z) = \partial Z$$

s'appelle rotation de $\mathbb{C}$ associée à ∂ .

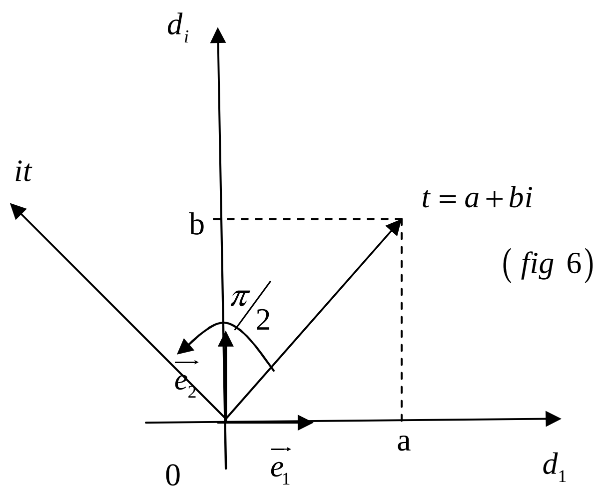
Si $R = \{ r_\partial : \mathbb{C} \to \mathbb{C} : r_\partial$ est une rotation de $\mathbb{C}$ associée à ∂, avec $\partial \in \mathbb{C}$ tel que $|\partial| = 1 \}$ alors (R, o) est un groupe abélien.

Représentation dans le plan complexe $\mathbb{C}$

a) Le point $Z = it$ avec $t = a + bi \in \mathbb{C}$. (fig 4).
b) Le point $Z'' = Z.Z'$ avec $Z = a + bi$ et $Z' = a' + b'i$, élément de $\mathbb{C}$. (fig 6).

Solution

a) Comme $Z = r_i(t)$, avec $t = a + bi$, commençons d'abord par représenter le point dans le plan complexe $\mathbb{C}$ et ensuite le point $Z = r_i(t)$ s'obtiendra par une rotation de centre O et d'angle $\pi/2$ de t.



$(fig\ 6)$

b) Pour représenter le point image de $Z'' = Z.Z'$ dans le plan complexe, procédons comme suit, au lieu et place de la composition des similitudes de plan complexe $\mathbb{C}$.

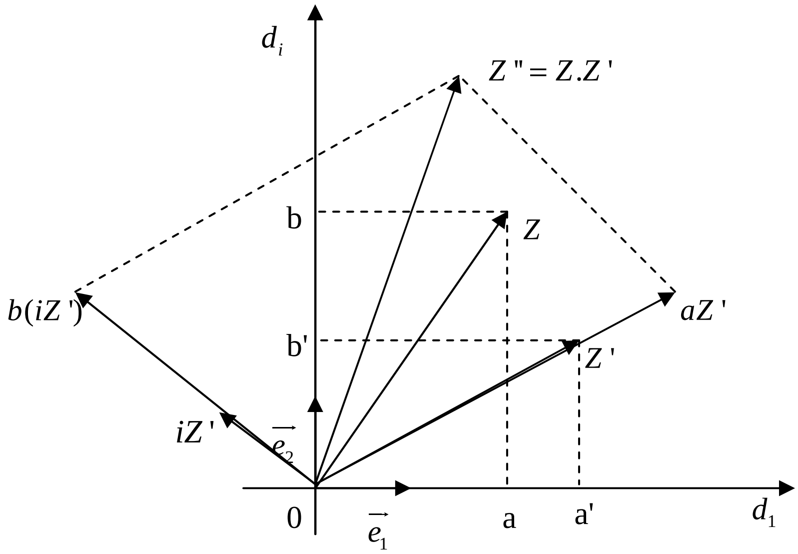
$$Z'' = Z.Z' = (a + bi)(a' + b'i) = a(a' + b'i) + bi(a' + b'i)$$
$$= h_a(Z') + h_b(iZ') = h_a(Z') + h_b[r_i(Z')]$$

Avec h_a, h_b homothésies de $\mathbb{C}$ de rapports respectifs a et b, r_i , rotation de $\mathbb{C}$ associée à $i \in \mathbb{C}$. Représentons d'abord Z' et $r_i(Z') = iZ'$ dans le plan complexe $\mathbb{C}$, puis

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

$h_a\left(Z'\right) = aZ'$ et $h_b\left[r_i\left(Z'\right)\right] = b\left(iZ'\right)$ et ensuite l'addition des vecteurs permettra d'indiquer le point $Z'' = Z.Z'$. (fig 7).

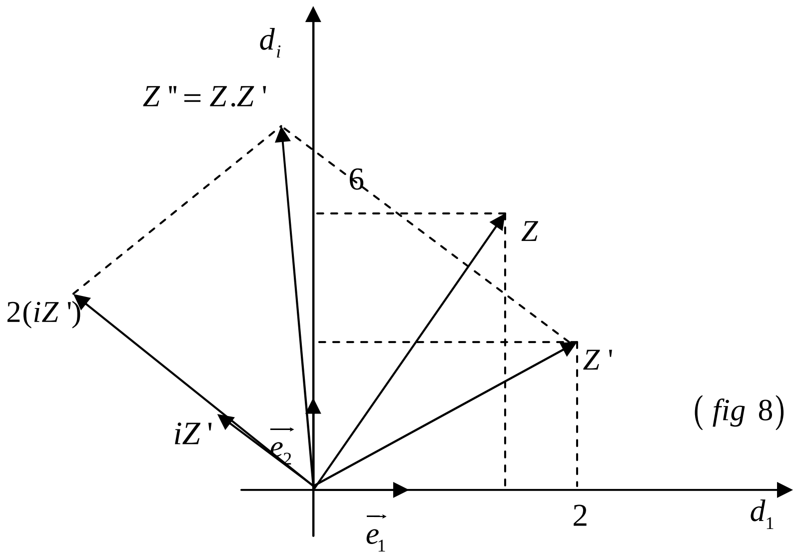
Représentation du point image de $Z'' = Z.Z'$ dans le plan complexe.



$\left(fig\ 7\right)$

Cas pratique

Représentation dans le plan complexe le point image de $Z'' = Z.Z'$ sachant que $Z = 1 + 2i$ et $Z' = 2 + 2i$. $P_Z = \left(1,2\right)$; $P_{Z'} = \left(2,2\right)$ et $P_{Z''} = \left(-2,6\right)$.



$\left(fig\ 8\right)$

4. Groupe multiplicatif des nombres complexes de module égal a 1

Soit U, un sous-ensemble de $\mathbb{C}^*$ formé de nombres complexes de module égal à 1 ie $U = \left\{Z \in \mathbb{C} \mid |Z| = 1\right\}$. On constate que $U \neq \varnothing$ car $\exists 1 \in \mathbb{C}$ tel que $|1| = 1$ donc $1 \in U$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

a) Théorème

$(\mathrm{U},.)$ est un sous-groupe de $(\mathbb{C}^*,.)$.

Montrons d'abord que la loi (.) définie dans U comme restriction de la multiplication (.) de $\mathbb{C}$, est une loi de composition interne dans U ou $\forall \mathrm{Z}, \mathrm{Z}' \in \mathrm{U}$, on a : $\mathrm{Z.Z}' \in \mathrm{U}$.

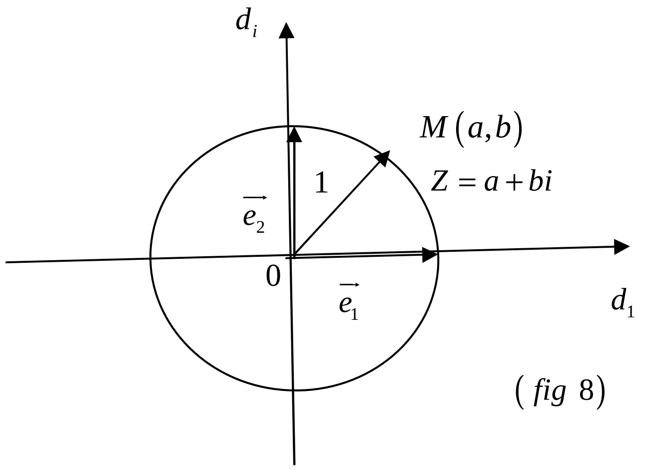
En effet, $\mathrm{Z}, \mathrm{Z}' \in \mathrm{U} \Rightarrow |\mathrm{Z}| = |\mathrm{Z}'| = 1$, appliquons P_1 de V.2.6. (2) pour avoir : $|Z.Z'| = |Z|.|Z'| = 1.1 = 1$ et $\mathrm{Z.Z}' \in \mathrm{U}$.
De plus, $\forall \mathrm{Z} \in \mathrm{U}, \mathrm{Z}^{-1} \in \mathrm{U}$.

En effet, $\mathrm{Z} \in \mathrm{U} \Rightarrow |\mathrm{Z}| = 1$ or Z^{-1} est l'inverse de Z dans $\mathbb{C}^*$ entraîne que $Z.Z^{-1} = 1$, soit $|Z.Z^{-1}| = |Z|.|Z^{-1}| = 1$, donc $|Z^{-1}| = \dfrac{1}{|Z|} = \dfrac{1}{1} = 1$ et $\mathrm{Z}^{-1} \in \mathrm{U}$ car $|Z^{-1}| = 1$.

b) Représentation de U dans le plan complexe $\mathbb{C}$

Dans le plan complexe $\mathbb{C}$, l'image de U est un cercle centré à l'origine des axes des coordonnées et de rayon égal à 1 nommé <u>cercle-unité</u>. Dans le plan Euclidien orienté par la donnée d'un repère orthonormé $\left(O, \vec{e_1}, \vec{e_2}\right)$, l'image de U est un cercle trigonométrique d'équation $x^2 + y^2 = 1$.

En effet, soit $\mathrm{Z} = \mathrm{x} + \mathrm{yi} \in \mathrm{U}$, alors $|Z| = 1$; or $|Z| = \sqrt{x^2 + y^2}$, donc $|Z| = 1$ si $\sqrt{x^2 + y^2} = 1$, soit $x^2 + y^2 = 1$.
Ainsi, si $M(a,b)$ est un point quelconque d'un tel cercle, alors on a : $a^2 + b^2 = 1$. Comme à $M(a,b) \in E_2$, on associe le nombre complexe $Z = a + bi$, on obtient alors que $\mathrm{Z} = \mathrm{a} + \mathrm{bi} \in \mathrm{U}$ (fig 8).



$(fig\ 8)$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

c) Propriété caractéristique des nombres complexes de module 1

Un nombre complexe a pour module 1 si et seulement si son conjugué est son inverse.

En effet, soit□ $\in$ U, alors $|Z| = 1$ ou $Z.\overline{Z} = 1$ entraînant que $\overline{Z} = \frac{1}{Z}$ avec $Z \neq 0$ car $|Z| = 1$.

d) Théorème

$(\mathrm{U},.)$ est un groupe isomorphe au groupe $(R,.)$ avec

$R = \{r_\partial : □ \to □ : r_\partial$ est une rotation de □, associé à $\partial \in \mu\}$.

En effet, définissons une application τ de la manière suivante :

$\tau : (\mu,.) \to (R,.)$

$\partial \to \tau(\partial) = r_\partial : □ \to □$

$Z \mapsto r_\partial(Z) = \partial.Z$

et montrons que τ est un isomorphisme des groupes abéliens ou

- τ est bijective, ce qui est évident de part la définition de τ.
- $\forall \partial, \lambda \in \mu, \tau(\partial.\lambda) = \tau(\partial) o \tau(\lambda)$

  En effet, la loi (o) étant interne dans□ , on a :

  $\tau(\partial.\lambda) = r_{\partial.\lambda} = r_\partial o r_\lambda = \tau(\partial) o \tau(\lambda)$.

D. *FORME TRIGONOMETRIQUE D'UN NOMBRE COMPLEXE*

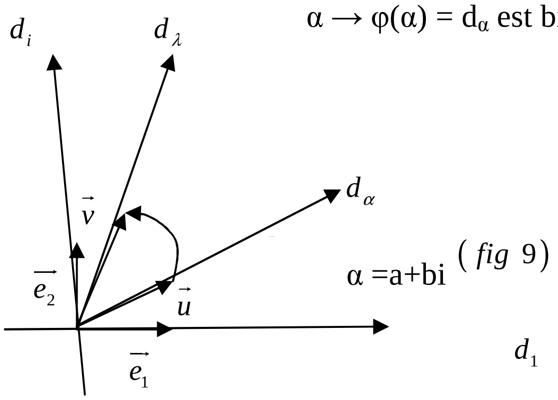
1. Introduction

Considérer α = $a + bi \in$ U, un nombre complexe de module égal à 1 dont B est le point image dans le plan complexe □ et $\vec{u}$ un vecteur unitaire de $\mathcal{V}_2$ tel que $[\vec{u}] = \alpha$, alors la demi-droite vectorielle engendrée par $\vec{u}$ est notée par d_α ie $d_\alpha = \{\lambda\vec{u} : \lambda \in □_+\}$.

Ainsi, $d_1 = \{\lambda\overrightarrow{e_1} : \lambda \in □\}$ et $d_i = \{\lambda\overrightarrow{e_2} : \lambda \in □\}$ seront appelées respectivement axe des réels et axe des imaginaires.

Si $D = \{d_\partial : \partial \in \mu\}$, alors l'application $\varphi : \mathrm{U} \to \mathrm{D}$

$\alpha \to \varphi(\alpha) = d_\alpha$ est bijective



$(fig\ 9)$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

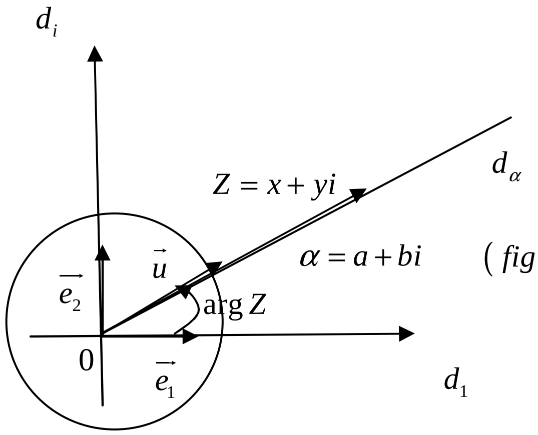
Définition 1 : On appelle angle orienté tout couple ordonné de deux demi-droites vectorielles d_α et d_λ avec $\alpha, \lambda \in U$. On le note par $\left(\widehat{d_\alpha, d_\lambda}\right)$. (fig 6).

Définition 2 : On appelle radian, l'unité d'angle telle que la mesure de l'angle plat soit π .

2. Module et argument d'un nombre complexe

Soit $Z = x + yi$, un nombre complexe non nul dont le point image dans le plan complexe $\mathbb{C}$ est P des coordonnées x et y dans la base canonique $\{\vec{e_1}, \vec{e_2}\}$ de $\mathcal{V}_2$. Alors le segment $\overline{OP}$ détermine un vecteur unitaire $\vec{u} = \overrightarrow{OB}$ de la demi-droite vectorielle d_α avec B point où le segment $\overline{OP}$ rencontre le centre trigonométrique (c).

La distance entre les points O et P, notée $d(O,P) = |0 - Z| = \sqrt{x^2 + y^2}$. Nous disons que, dans l'ensemble $\mathbb{C}$, $d(O,M) = \sqrt{x^2 + y^2}$ est le module du nombre complexe $Z = x + yi$ ou la longueur du vecteur $\overrightarrow{OP}$. On le note par ρ . D'où $\rho = d(O,P) = |0 - Z| = \sqrt{x^2 + y^2}$.



$(fig\ 10)$

a) Définition

Soit $Z = x + yi \in \mathbb{C}^*$, on appelle argument de Z, noté $(\arg Z)$ la mesure en radian de l'angle $\left(\widehat{d_1, d_\alpha}\right)$ où d_1 est la demi-droite vectorielle engendrée par le vecteur $\vec{e_1}$ et d_∂ est la demi-droite vectorielle passant par le point P(x,y) et engendrée par le vecteur unitaire $\vec{u} = \overrightarrow{OB}$, avec B(a,b) point image de nombre complexe $\alpha = a + bi \in U$.

On a alors pour $Z \in \mathbb{C}^*$, $\arg Z =$ mesure de $\left(\widehat{d_1, d_\alpha}\right)$.

On note $\arg Z \equiv a (\text{mod } 2\pi)$ ou $\arg Z = a + 2k\pi$,avec $k \in \mathbb{Z}$.

3. Expression trigonométrique d'un Nombre Complexe

Puisque $\vec{u}$ est un vecteur unitaire de la demi-droite vectorielle d_α passant par le point P(x,y) et $\rho = \sqrt{x^2 + y^2}$, la longueur du vecteur $\overrightarrow{OP}$, alors on a : $\overrightarrow{OP} = \rho.\vec{\mu}$. (s).

Or $\vec{u} = (\cos\theta)\vec{e_1} + (\sin\theta)\vec{e_2}$ avec $\arg Z = \theta(\text{mod } 2\pi)$, donc, la rélation (s) devient :

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

$\overrightarrow{OP} = \rho.\vec{u} = \rho\left(\cos\theta\overrightarrow{e_1} + \sin\theta\overrightarrow{e_2}\right)$

$= (\rho\cos\theta)\overrightarrow{e_1} + (\rho\sin\theta)\overrightarrow{e_2}$

Soit $\overrightarrow{OP} = (\rho\cos\theta)\overrightarrow{e_1} + (\rho\sin\theta)\overrightarrow{e_2}$, (s')

D'autre part $\left\{\overrightarrow{e_1}, \overrightarrow{e_2}\right\}$ étant une base de $\mathcal{V}_2$ et $\overrightarrow{OP} \in V_2$, alors le vecteur $\overrightarrow{OP}$ est une combinaison de la famille $\left\{\overrightarrow{e_1}, \overrightarrow{e_2}\right\}$, ie $\overrightarrow{OP} = x\overrightarrow{e_1} + y\overrightarrow{e_2}$ (s'') avec $x, y \in \mathbb{R}$.

(s') et (s'') $\Rightarrow x\overrightarrow{e_1} + y\overrightarrow{e_2} = (\rho\cos\theta)\overrightarrow{e_1} + (\sin\theta)\overrightarrow{e_2} \Leftrightarrow x = \rho\cos\theta$ et $y = \rho\sin\theta$ et Z devient ainsi : $Z = x + yi = (\rho\cos\theta) + i(\rho\sin\theta) = \rho(\cos\theta + i\sin\theta)$.

D'où $Z = |Z|\left(\cos(\arg Z) + i\sin(\arg Z)\right)$.

Réciproquement :

Tout couple (ρ, θ) où $\rho \in \mathbb{R}_+^*$ et $\theta \in \mathbb{R}$ représentent un nombre complexe $Z = \rho(\cos\theta + i\sin\theta) = |Z|\left(\cos(\arg Z) + i\sin(\arg Z)\right)$. Ainsi, le nombre complexe $Z = \rho(\cos\theta + i\sin\theta)$ sera représenté par le symbole $[\rho, \theta] = \left[|Z|, \arg Z\right]$ qu'on nomme forme trigonométrique de $Z = x + yi$.

Si $Z = 0$, ce qui n'est pas valable, bien que $|Z| = 0$, mais son argument n'est pas défini.

4. Egalité de deux nombres complexes écrits sous forme trigonométrique

Soient $Z = [\rho, \theta]$ et $Z' = [\rho', \theta']$ deux nombres complexes, alors

$$Z = Z' \Leftrightarrow \begin{cases} \rho = \rho' \\ \theta = \theta' (\bmod 2\pi) \end{cases}$$

5. Forme algébrique et Forme trigonométrique d'un nombre complexe

- La forme algébrique $Z = x + yi$ est liée à la forme trigonométrique $Z = \left[|Z|, \arg Z\right]$ par : $Z = |Z|\left(\cos(\arg Z) + i\sin(\arg Z)\right)$. Ce qui équivaut à $x = |Z|\cos(\arg Z)$ et $y = |Z|\sin(\arg Z)$.

  Soit par exemple $Z = \left[2, \dfrac{\pi}{3}\right]$, un nombre complexe écrit sous forme trigonométrique, déterminons la forme algébrique de Z. Comme $|Z| = 2$ et $\arg Z = \dfrac{\pi}{3}(\bmod 2\pi)$,

  alors $Z = |Z|\left[\cos(\arg Z) + i\sin(\arg Z)\right] = 2\left(\cos\dfrac{\pi}{3} + i\sin\dfrac{\pi}{3}\right) = 2\left(\dfrac{1}{2} + i\dfrac{\sqrt{3}}{2}\right) = 1 + i\sqrt{3}$.

  D'où, $Z = 1 + i\sqrt{3}$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

- Réciproquement, supposons donnée la forme algébrique d'un nombre complexe non nul $Z = x + yi$, avec $x, y \in \mathbb{R}^*$ et déterminons la forme trigonométrique de Z, ie écrire Z sous la forme $[\rho, \theta]$.

  Il est facile de déterminer $\rho = |Z| = \sqrt{x^2 + y^2}$, alors pour déterminer $\arg Z$, utilisons le système d'équations ci-dessous

$$\begin{cases} \cos\theta = \dfrac{x}{|Z|} \\ \sin\theta = \dfrac{y}{|Z|} \end{cases} \Leftrightarrow tg\theta = \frac{y}{x} \Leftrightarrow \theta \equiv arctg\left(\frac{y}{x}\right) \quad (\mathrm{mod}\, 2\pi)$$

  D'où $Z = \left[|Z|, arctg\left(\dfrac{y}{x}\right)\right]$ est la forme trigonométrique de Z. Par exemple, écrire $Z = 1 + i \in \mathbb{C}$ sous la forme $[\rho, \theta]$. On sait d'après ce qui précède, puisque $x = 1$ et $y = 1$, que $\rho = |Z| = \sqrt{2}$ et $arctg\left(\dfrac{y}{x}\right) = arctg(1) = \dfrac{\pi}{4} + 2k\pi, k \in \mathbb{Z}$.

  D'où $Z + \left[|Z|, arctg\left(\dfrac{y}{x}\right)\right] = \left[\sqrt{2}, \dfrac{\pi}{4}\right]$.

Remarque

- Soit $Z = a$, avec $a \in \mathbb{R}^*$.

  Si $a \in \mathbb{R}^*_+$, alors $|Z| = a$ et $\arg Z \equiv 0 (\mathrm{mod}\, 2\pi)$, ie $\arg Z = 2k\pi$, avec $k \in \mathbb{Z}$.

  D'où $Z = [a, 2k\pi], k \in \mathbb{Z}$.

  Si $a \in \mathbb{R}^*_-$, alors $|Z| = -a$ et $\arg Z = \pi (\mathrm{mod}\, 2\pi)$.

  D'où, $Z = [-a, \pi]$.

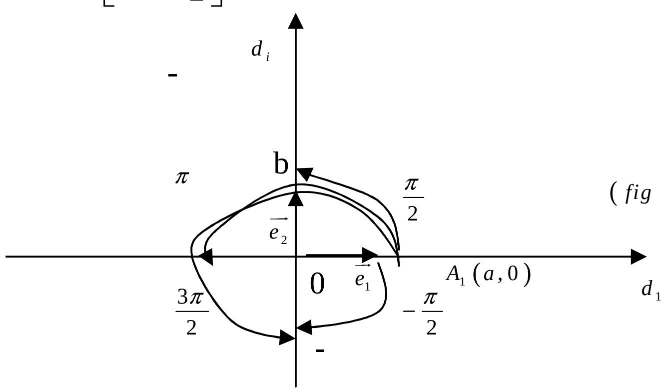
- Soit $Z = bi$, avec $b \in \mathbb{R}^K$.

  Si $b \in \mathbb{R}^*_+$, alors $|Z| = b$ et $\arg Z \equiv \dfrac{\pi}{2} (\mathrm{mod}\, 2\pi)$.

  D'où, $Z = \left[b, \dfrac{\pi}{2}\right]$.

  Si $b \in \mathbb{R}^*_-$, alors $|Z| = -b$ et $\arg Z = \dfrac{3\pi}{2} (\mathrm{mod}\, 2\pi)$ ou $\arg Z = -\dfrac{\pi}{2} (\mathrm{mod}\, 2\pi)$.

  D'où, $Z = \left[-b, \dfrac{3\pi}{2}\right]$ ou $Z = \left[-b, -\dfrac{\pi}{2}\right]$.



$(fig\ 11)$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

6. Multiplication des nombres complexes écrits sous forme trigonométrique

(1) Théorème

Soient $Z = \left[|Z|, \arg Z\right]$ et $Z' = \left[|Z'|, \arg Z'\right]$ deux nombres complexes, alors $Z.Z' = \left[|Z|, \arg Z\right].\left[|Z'|, \arg Z'\right] = \left[|Z|.|Z'|, \arg Z + \arg Z'\right]$.
Preuve aux exercices.

Ce théorème s'énonce comme suit :
Le produit de deux nombres complexes a pour module le produit des modules et pour argument la somme des arguments.

Plus généralement, si $Z_k = \left[|Z_k|, \arg Z_k\right]$, avec $k \in \{1, 2, ..., n\}$ n nombres complexes, alors le produit de ces n nombres complexes Z_k est noté par :
avec $\prod_{k=1}^{n} Z_k = \left[\prod_{k=1}^{n} |Z_k|, \sum_{k=1}^{n} \arg Z_k\right]$ où $\prod_{k=1}^{n} Z_k = Z_1.Z_2.....Z_n$, $\prod_{k=1}^{n} |Z_k| = |Z_1|.|Z_2|.....|Z_n|$ et $\sum_{k=1}^{n} \arg Z_k = \arg Z_1 + \arg Z_2 + ... + \arg Z_n$.
Preuve par récurrence sur $k \in \{1, 2, ..., n\}$.

7. Puissance d'un nombre complexe

a) Théorème

Soit $Z = \left[|Z|, \arg Z\right]$ un nombre complexe, alors
$\forall n \in \mathbb{N}^*, Z^n = \left[|Z|, \arg Z\right]^n = \left[|Z|^n, n \arg Z\right]$.
La preuve s'appuie sur le théorème 7.1.

b) Exemple

Calculer $(1+i)^n$, avec $n \in \mathbb{N}^*$.
On sait que $1+i = \left[\sqrt{2}, \frac{\pi}{4}\right]$ car $\arg(1+i) \equiv \frac{\pi}{4} (\bmod 2\pi)$, alors, d'après 8.1. ci-dessus, on a :
$(1+i)^n = \left[\sqrt{2}, \frac{\pi}{4}\right]^n = \left[\left(\sqrt{2}\right)^n, n\frac{\pi}{4}\right]$.
D'où $(1+i)^n = \left[\left(\sqrt{2}\right)^n, n\frac{\pi}{4}\right]$.

c) Formule de Abraham Moivre

Supposons que $Z \in U$, ie $|Z| = 1$ ou $Z = [1, \theta]$ avec $\arg Z = \theta (\bmod 2\pi)$, alors d'après 8.1 ci-dessus, on a : $Z^n = [1, \theta]^n = [1, n\theta]$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

D'où $\forall Z = \cos\theta + i\sin\theta \in U \subset \mathbb{C}^*$, on a :
$\left(\cos\theta + i\sin\theta\right)^n = \left(\cos n\theta + i\sin n\theta\right)$, (r)

Ce qu'on appelle Formule de ABRAHAM MOIVRE.

- Cette formule permet par exemple de calculer $\cos n\theta$, $\sin n\theta$ et ou $tgn\theta$ en fonction de $\cos\theta$, $\sin\theta$ et ou $tg\theta$, en explicitant le 1er membre de (r) d'après la formule du Binôme de Newton et en utilisant l'égalité définie dans $\mathbb{C}$.
  Soit à calculer par exemple $\cos 3\theta$, $\sin 3\theta$ en fonction de $\cos\theta$ et ou $\sin\theta$.
  D'après la formule de Moivre ci-dessus,
  On a : $\left(\cos\theta + i\sin\theta\right)^3 = \cos 3\theta + i\sin 3\theta$. (1°)
  Or d'après la formule du Binôme de Newton,ona
  $\left(\cos\theta + i\sin\theta\right)^3 = \left(\cos^3\theta - 3\cos\theta.\sin^2\theta\right) + i\left(3\cos^2.\sin\theta - \sin^3\theta\right)$, (2°), donc
  $$\cos 3\theta + i\sin 3\theta \overset{(1°)}{=} \left(\cos\theta + i\sin\theta\right)^3 \overset{(2°)}{=} \left(\cos^3\theta - 3\cos\theta.\sin^2\theta\right) + i\left(3\cos^2.\sin\theta - \sin^3\theta\right)$$
  $$\Leftrightarrow \begin{cases} \cos 3\theta = \cos^3\theta - 3\cos\theta.\sin^2\theta = 4\cos^3\theta - 3\cos\theta, \text{ car } \sin^2\theta = 1 - \cos^2\theta \\ \sin 3\theta = 3\cos^2\theta.\sin\theta - \sin^3\theta = 3\sin\theta - 4\sin^3\theta, \text{ car } \cos^2\theta = 1 - \sin^2\theta \end{cases}$$

  Montrer aussi que : $tg3\theta = \dfrac{3tg\theta - tg^3\theta}{1 - 3tg^2\theta}$.
  Exercices, calculer $\cos 2\theta$ et $\sin 4\theta$ en fonction de $\cos\theta$ et ou $\sin\theta$.

- Noter que, la formule de Moivre reste valable, $\forall m \in \mathbb{Z}$ et $\forall \theta \in \mathbb{R}$, ie
  $\left(\cos\theta + i\sin\theta\right)^m = \cos\left(m\theta\right) + i\sin\left(m\theta\right)$, (r').
  En effet, pour $m \in \mathbb{Z}_+ = \mathbb{N}$, la formule (r') reste vraie et pour $m \in \mathbb{Z}_-$, poser $m = -n$ avec $n \in \mathbb{N}$, pour avoir
  $$\left(\cos\theta + i\sin\theta\right)^m = \left(\cos\theta + i\sin\theta\right)^{-n} = \frac{1}{\left(\cos\theta + i\sin\theta\right)^n} \overset{(1°)}{=} \frac{1}{\cos n\theta + i\sin n\theta}$$
  $$= \cos n\theta - i\sin n\theta = \cos\left(-n\theta\right) + i\sin\left(-n\theta\right) = \cos\left(m\theta\right) + i\sin\left(m\theta\right)$$
  D'où $\left(\cos\theta + i\sin\theta\right)^m = \cos\left(m\theta\right) + i\sin\left(m\theta\right)$, reste valable pour tout $m \in \mathbb{Z}$.

8. Quotient de deux nombres complexes

a) L'inverse d'un nombre complexe non nul

Soit $Z = \left[\rho, \theta\right]$, un nombre complexe non nul, avec $\arg Z \equiv \theta\left(\mathrm{mod}\, 2\pi\right)$ et $\rho = \left|Z\right|$, alors Z^{-1} existe dans $\mathbb{C}^*$, puisque $Z \neq 0$.
Poser $Z^{-1} = \left[\rho', \theta'\right]$ avec $\arg Z^{-1} \equiv \theta'\left(\mathrm{mod}\, 2\pi\right)$ et $\rho' = \left|Z^{-1}\right|$, pour avoir $Z.Z^{-1} = 1$ ie $\left[\rho, \theta\right].\left[\rho', \theta'\right] = \left[1, 0\right]$ ou

$$\left[\rho.\rho', \theta + \theta'\right] = \left[1, 0\right] \Leftrightarrow \begin{cases} \rho.\rho' = 1 \\ \theta + \theta' \equiv 0\left(\mathrm{mod}\, 2\pi\right) \end{cases} \Leftrightarrow \begin{cases} \rho' = \dfrac{1}{\rho} \text{ car } \rho \neq 0 \\ \theta' = -\theta + 2k\pi, \text{ avec } k \in \mathbb{Z} \end{cases}$$

Par suite : $Z^{-1}=[\rho',\theta']=\left[\frac{1}{\rho},-\theta\right]$.

D'où $\forall\rho\in\mathbb{R}_+^*,\forall\theta\in\mathbb{R},[\rho,\theta]^{-1}=\left[\frac{1}{\rho},-\theta\right]$.

b) Théorème

Le quotient de deux nombres complexes non nuls a pour module le quotient des modules et pour argument l'excès de l'argument du numérateur sur l'argument du dénominateur.

i.e. si $Z=[\rho,\theta]\in\mathbb{C}^*$ et $Z'=[\rho',\theta']\in\mathbb{C}^*$, alors $\frac{Z}{Z'}=\frac{[\rho,\theta]}{[\rho',\theta']}=\left[\frac{\rho}{\rho'},\theta-\theta'\right]$.

En effet, $\frac{Z}{Z'}=Z.(Z')^{-1}=[\rho,\theta].\left[\frac{1}{\rho'},-\theta\right]=\left[\rho.\frac{1}{\rho'},\theta+(-\theta')\right]=\left[\frac{\rho}{\rho'},\theta-\theta'\right]$

Par exemple, pour $Z=\left[3,\frac{\pi}{3}\right]$ et $Z'=\left[\sqrt{2},\frac{\pi}{4}\right]$, on a :

$$\frac{Z}{Z'}=\frac{\left[3,\frac{\pi}{3}\right]}{\left[\sqrt{2},\frac{\pi}{4}\right]}=\left[\frac{3}{\sqrt{2}},\frac{\pi}{3}-\frac{\pi}{4}\right]=\left[\frac{3\sqrt{2}}{2},\frac{\pi}{12}\right].$$

9. Equation binôme

a) Définition

Soit $t\in\mathbb{C}$ et $n\in\mathbb{N}^*$, s'il existe $Z\in\mathbb{C}$ tel que $Z^n=t$, (b), alors Z est racine n^e du nombre complexe (t) et $Z^n-t=0$ est nommé équation binôme.

b) Existence des solutions de l'équation (b)

Prendre $t=\left[|t|,\arg t\right]$ et si $Z=\left[|Z|,\arg Z\right]$ est une solution de (b), ou une racine n^e de t, on a alors, d'après V.4.2.(8.1) et V.4.2.(4), que :

$$\left[|Z|,\arg Z\right]^n=\left[|t|,\arg t\right]\Leftrightarrow\left[|Z|^n,n.\arg Z\right]=\left[|t|,\arg t\right]$$

$$\Leftrightarrow\begin{cases}|Z|^n=|t|\\ n\arg Z=\arg t\pmod{2\pi}\end{cases}$$

$$\Leftrightarrow\begin{cases}|Z|=|t|^{\frac{1}{n}}\\ n.\arg Z=\arg t+2k\pi,\ \text{avec } k\in\mathbb{Z}\end{cases}$$

$$\Leftrightarrow\begin{cases}|Z|=\sqrt[n]{|t|}\\ \arg Z=\frac{\arg t}{n}+\frac{2k\pi}{n},k\in\{0,1,\dots,(n-1)\}\end{cases}$$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Ainsi, $Z_k = \left[\sqrt[n]{|t|}, \dfrac{\arg t + 2k\pi}{n}\right] = \sqrt[n]{|t|}\left[\cos\left(\dfrac{\arg t + 2k\pi}{n}\right) + i\sin\left(\dfrac{\arg t + 2k\pi}{n}\right)\right]$ avec $k \in \{0,1,\dots,(n-1)\}$, d'où le théorème ci-dessous.

c) Théorème

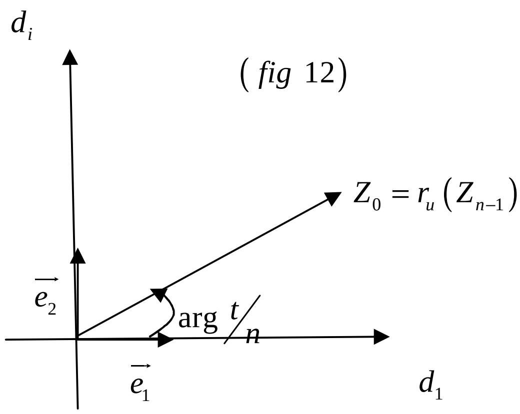
Pour $Z \in \mathbb{C}^*, t \in \mathbb{C}^*$ et $n \in \mathbb{N}^*$, l'ensemble (V_n) des n solutions de l'équation binôme $Z^n - t = 0$ est :

$$V_n = \left\{ Z_k = \left[\sqrt[n]{|t|}, \frac{\arg t + 2k\pi}{n}\right]; k \in [0, n-1] \subset \mathbb{N} \right\}$$

d) Remarque

On constate que toutes les n racines n^e de (t) ont le même module ie $|Z_k| = |Z_{k+1}| = \sqrt[n]{|t|}$ et si $\arg Z_k \equiv \theta (\operatorname{mod} 2\pi)$, alors $\arg Z_{k+1} \equiv \left(\theta + \dfrac{2\pi}{n}\right)(\operatorname{mod} 2\pi)$. Ce qui signifie que les arguments de n racines n^e de (t) sont les n termes d'une progression arithmétique dont le premier terme est argt et la raison est $\dfrac{2\pi}{n}$.

Et si, $u = \left[1, \dfrac{2\pi}{n}\right]$, ie $\arg u = \dfrac{2\pi}{n}(\operatorname{mod} 2\pi)$ et pour $k \in [0, n-1] \subset \mathbb{N}$, Z_k un point complexe dans le plan complexe $\mathbb{C}$, alors $r_u(Z_k) = Z_{k+1}$, d'où, dans le plan complexe $\mathbb{C}$, les n points complexes $Z_k = \left[\sqrt[n]{|t|}, \dfrac{\arg t + 2k\pi}{n}\right]$ avec $k \in [0, n-1] \subset \mathbb{N}$ sont les sommets d'un polygone régulier inscrit dans un cercle centré à l'origine des axes et de rayon $\sqrt[n]{|t|}$.



$(fig\ 12)$

Exemple, soit à résoudre dans $\mathbb{C}$ l'équation binôme $Z^3 - \left(1 + i\sqrt{3}\right) = 0$.

Poser $t = 1 + i\sqrt{3} = \left[2, \dfrac{\pi}{3}\right]$ car $|t| = 2$ et $\arg t \equiv \dfrac{\pi}{3}(\operatorname{mod} 2\pi)$, pour avoir $Z^3 = \left[2, \dfrac{\pi}{3}\right]$. Et, en appliquant V.5.(3), pour n=3, on obtient :

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

$$V_3 = \left\{ Z_k = \left[\sqrt[3]{2}, \frac{\frac{\pi}{3} + 2k\pi}{3} \right], k \in [0,2] \subset \mathbb{N} \right\}$$
$$= \left\{ Z_k = \left[\sqrt[3]{2}, \frac{\pi}{9} + \frac{2k\pi}{3} \right], k \in [0,2] \subset \mathbb{N} \right\}$$
$$= \left\{ Z_0 = \left[\sqrt[3]{2}, \frac{\pi}{9} \right]; Z_1 = \left[\sqrt[3]{2}, \frac{3\pi}{7} \right]; Z_2 = \left[\sqrt[3]{2}, \frac{13\pi}{9} \right] \right\}$$

Dans le plan complexe $\mathbb{C}$, les trois racines cubiques de t sont les points, sommets d'un triangle équilatéral, inscrit dans un cercle centré à l'origine des axes des coordonnées et de rayon $\sqrt[3]{2}$.

10. Cas particulier

a) Si t = 1, alors l'équation binôme (b) devient $Z^n - 1 = 0$ **et tout** $\alpha \in \mathbb{C}^*$ **tel que** $\alpha^n = 1$ **est dit racine n^e de l'unité. Un tel nombre complexe est élément de U car** $|\alpha| = 1$**.**

Comme $\arg t \equiv 0 \pmod{2\pi}$, si μ_n est l'ensemble des racines n^e de l'unité, alors

$$\mu_n = \left\{ \omega_k = \left[\sqrt[n]{|t|}, \frac{\arg t + 2k\pi}{n} \right], k \in [0, n-1] \subset \mathbb{N} \right\}$$
$$= \left\{ \omega_k = \left[1, \frac{2k\pi}{n} \right], k \in [0, n-1] \subset \mathbb{N} \right\}$$
$$= \left\{ \omega_k = \cos\left(\frac{2k\pi}{n} \right) + i \sin\left(\frac{2k\pi}{n} \right) : k \in [0, n-1] \subset \mathbb{N} \right\}$$

On constate que, pour tout n∈ IN^*, $\omega_0 = 1$ est une racine n^e de l'unité. Et, si $k = 1$,

alors $\omega_1 = \left[1, \frac{2\pi}{n} \right] = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$ est appelée racine fondamentale de l'équation binôme $Z^n = 1$.

D'après la formule d'Abraham Moivre, on a : $\forall k \in [1, n-1] : \omega_1^k = \omega_k$ (r1)

- ***Théorème***

$(\mathrm{U_n}, .)$ Est un groupe abélien isomorphe à $\left(\mathbb{Z}/n\mathbb{Z}, \dot{+} \right)$.

Preuve

Définir une application f de la manière suivante :

$$f : (\mu_n, .) \to \left(\mathbb{Z}/n\mathbb{Z}, \dot{+} \right)$$
$$\omega_k \mapsto f(\omega_k) = \dot{k}$$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Cette application f est trivialement bijective, et de plus $\forall \omega_k, \omega_l \in \mu_n$,

On a : $f(\omega_k.\omega_l) = f(\omega_k) \dot{+} f(\omega_l)$ ie f est un isomorphisme des groupes.

En effet, d'après la relation (r1) ci dessus,

$$f(\omega_k.\omega_l) = f(\omega_1^k.\omega_1^l) = f(\omega_1^{k+l}) = f(\omega_{k+l}) = \dot{k} \dot{+} l = \dot{k} \dot{+} \dot{l} = f(\omega_k) \dot{+} f(\omega_l)$$

D'où $f : (U_n, .) \to (\mathbb{Z}/n\mathbb{Z}, \dot{+})$ étant un isomorphisme et $(\mathbb{Z}/n\mathbb{Z}, \dot{+})$ un groupe abélien, alors $(\mu_n, .)$ est aussi un groupe abélien, dit groupe cyclique, puisque engendré par les puissances d'un seul élément $\omega_1 = \left[1, \frac{2\pi}{n}\right]$.

- ***Théorème***

Les racines d'un nombre complexe non nul t s'obtiennent par la multiplication de l'une quelconque d'entre elles par les racines n^e de l'unité.

Preuve

Soit Z_k, une racine n^e t de l'unité, alors $(Z_k)^n = t$, (k$_1$).

Si Z est une racine n^e de t, choisie, alors $(Z)^n = t$,

(k$_1$) et (k$_2$) $\Rightarrow \frac{(Z_k)^n}{Z^n} = \frac{t}{t}$ ou $\left(\frac{Z_k}{Z}\right)^n = 1$ entraînant que $\frac{Z_k}{Z}$ est une racine n^e de l'unité, ie $\frac{Z_k}{Z} \in U_n$.

Donc, $\exists \omega_k \in U_n$ tel que $\frac{Z_k}{Z} = \omega_k$, soit $Z_k = Z.\omega_k$, avec $k \in \{0,1,...,n-1\}$.

Ainsi, pour $Z \in V_n$,on obtient une application f définie de la manière suivante, $k \in [0, n-1] \subset \mathbb{N}$.

$$f : U_n \to V_n$$
$$\omega_k \mapsto f(\omega_k) = Z_k = Z.\omega_k$$

Cette application est bijective. D'où le théorème.

- ***Exemple***

Déterminer les racines cubiques de l'unité ou résoudre l'équation binôme $Z^3 = 1$ dans $\mathbb{C}$.

On sait que $\omega_k = \left[1, \frac{2\pi}{n}\right]$, avec $k \in \{0,1,2\}$ sont les trois racines cubiques de l'unité. On a,

pour $k = 0$, $k = 1$ et $k = 2$, $\omega_0 = 1, \omega_1 = \left[1, \frac{2\pi}{3}\right]$ et $\omega_2 = \left[1, \frac{4\pi}{3}\right]$.

On constate que $\omega_2 = \overline{\omega_1}$ et $1 + \omega_1 + \omega_1^2 = 0$.

b) Prendre n = 2 dans l'équation binôme $Z^n = t$ (b) pour avoir $Z^2 = t$ (c$_1$). Ainsi tout nombre complexe

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

non nul α tel que $\alpha^2 = t$ est nommé racine carré de (t).

(1) t écrit sous forme trigonométrique, ie $t = \left[|t|, \arg t\right]$

- Si $t = \left[|t|, \arg t\right]$, alors les deux racines carrées de (c_1) sont données par

$$V_2 = \left\{ Z_k = \left[\sqrt{|t|}, \frac{\arg t + 2k\pi}{2}\right], k \in [0,1] \subset \mathbb{Z} \right\}$$

$$= \left\{ Z_k = \left[\sqrt{|t|}, \frac{\arg t}{2} + k\pi\right], k \in [0,1] \subset \mathbb{Z} \right\}$$

$$= \left\{ Z_0 = \left[\sqrt{|t|}, \frac{\arg t}{2}\right]; Z_1 = \left[\sqrt{|t|}, \frac{\arg t}{2} + \pi\right] \right\}$$

D'où les deux racines carrées de l'équation binôme $Z^2 = t$ sont $Z_0 = \left[\sqrt{|t|}, \frac{\arg t}{2}\right]$ et

$Z_1 = \left[\sqrt{|t|}, \frac{\arg t}{2} + \pi\right] = -Z_0$.

- Remarque
  i. L'équation $Z^2 = 0$ a une racine carrée qui est égale à 0.
  ii. Les deux racines carrées d'un nombre complexe non nul t sont deux nombres complexes opposés.

Par exemple, les deux racines carrées de $t = 1 + i\sqrt{3} = \left[2, \frac{\pi}{3}\right]$ sont : $Z_k = \left[\sqrt{|t|}, \frac{\arg t}{2} + k\pi\right]$

avec $k = \{0,1\}$ ou $Z_0 = \left[\sqrt{2}, \frac{\pi}{6}\right]$ et $Z_1 = \left[\sqrt{2}, \frac{7\pi}{6}\right]$.

(2) t écrit sous forme algébrique

Soit $t = a + bi \in \mathbb{C}^*$, si $Z = x + yi$ est une racine carrée de t, alors $Z^2 = t$,

$$\mathbf{Z}^2 = t \Leftrightarrow (x+yi)^2 = a + bi \Leftrightarrow (x^2 - y^2 + 2xyi) = a + bi \Leftrightarrow \begin{cases} x^2 - y^2 = a \\ 2xy = b \end{cases}$$

ie

$$\Leftrightarrow \begin{cases} x^2 - y^2 = a \\ xy = \frac{b}{2} \end{cases} \Leftrightarrow \begin{cases} x^2 - y^2 = a \\ x^2 y^2 = \frac{b^2}{4} \\ xyb \succ 0 \end{cases} \Leftrightarrow \begin{cases} x^2 - y^2 = a \\ x^2(-y^2) = -\frac{b^2}{4} \\ xyb \succ 0 \end{cases}$$

On constate que x^2 et $(-y^2)$ sont deux racines réelles de l'équation du second degré en v à coefficients et inconnus réels : $v^2 - av - \frac{b^2}{4} = 0$ (e). Cette équation (e) a une racine positive (x^2) et une racine négative $(-y^2)$ qui sont :

$x^2 = \dfrac{\sqrt{a^2+b^2}+a}{2}$ ou $x = \varepsilon\sqrt{\dfrac{\sqrt{a^2+b^2}+a}{2}}$, avec $\varepsilon^2 = 1$

et $y^2 = \dfrac{\sqrt{a^2+b^2}-b}{2}$ ou $y = \varepsilon'\sqrt{\dfrac{\sqrt{a^2+b^2}-a}{2}}$, avec $(\varepsilon')^2 = 1$

Comme $x.y$ a le même signe que b, car $2xy = b$, alors les deux racines carrées de $t = a+bi \in \mathbb{C}^*$ sont données par :

$$Z_{1,2} = \varepsilon\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}} + \varepsilon' i\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}} \text{ , avec } \begin{cases} \varepsilon = \varepsilon' \text{ si } b \succ 0 \text{ ou} \\ \varepsilon = -\varepsilon' \text{ si } b \prec 0 \end{cases}$$

On constate que ces deux racines de t sont opposées ie $Z_1 = -Z_2$.

Exemple

Déterminer les racines carrées de $t = 1+i\sqrt{3}$.

Comme $a = 1$ et $b = \sqrt{3}$, avec $b \succ 0$, alors les deux racines carrées de t sont

$$Z_{1,2} = \varepsilon\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}} + \varepsilon' i\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}} \text{ , avec } \varepsilon = \varepsilon'.$$

Ainsi, $Z_1 = \sqrt{\dfrac{\sqrt{1+3}+1}{2}} + i\sqrt{\dfrac{\sqrt{1+3}-1}{2}} = \sqrt{\dfrac{3}{2}} + \dfrac{i}{\sqrt{2}} = \dfrac{\sqrt{6}}{2} + \dfrac{i\sqrt{2}}{2}$

Et $Z_2 = -Z_1 = -\dfrac{\sqrt{6}}{2} - \dfrac{i\sqrt{2}}{2}$.

D'où $Z_1 = \dfrac{\sqrt{6}}{2} + \dfrac{i\sqrt{2}}{2}$ et $Z_2 = -\dfrac{\sqrt{6}}{2} - \dfrac{i\sqrt{2}}{2}$.

Comme $Z_0 = \left[\sqrt{2}, \dfrac{\pi}{6}\right]$ d'après l'exemple sur V.5.(5.2.1), ie $Z_0 = \sqrt{2}\cos\dfrac{\pi}{6} + i\sqrt{2}\sin\dfrac{\pi}{6}$ et

$Z_1 = \dfrac{\sqrt{6}}{2} + \dfrac{i\sqrt{2}}{2}$, alors on a :

$$\sqrt{2}\cos\frac{\pi}{6} + i\sqrt{2}\sin\frac{\pi}{6} = \frac{\sqrt{6}}{2} + \frac{i\sqrt{2}}{2} \text{ ssi } \begin{cases} \sqrt{2}\cos\dfrac{\pi}{6} = \dfrac{\sqrt{6}}{2} \\ \sqrt{2}\sin\dfrac{\pi}{6} = \dfrac{\sqrt{2}}{2} \end{cases} \text{ ssi } \begin{cases} \cos\dfrac{\pi}{6} = \dfrac{\sqrt{3}}{2} \\ \sin\dfrac{\pi}{6} = \dfrac{1}{2} \end{cases}$$

(3) Equation du second degré à coefficient complexes

Soit $ax^2+bx+c = 0$, avec $a \neq 0$, une équation du second degré en x, à coefficients complexes, on a : $ax^2+bx+c = 0 \Leftrightarrow a\left(x^2+\dfrac{b}{a}x+\dfrac{c}{a}\right) = 0 \Leftrightarrow x^2+\dfrac{b}{a}x+\dfrac{c}{a} = 0$ car $a \neq 0$.

Par ailleurs, $x^2+\dfrac{b}{a}x+\dfrac{c}{a} = \left(x+\dfrac{b}{2a}\right)^2 - \dfrac{b^2}{4a^2} + \dfrac{c}{a} = \left(x+\dfrac{b}{2a}\right)^2 - \dfrac{b^2-4ac}{4a^2}$

Puisque $x^2+\dfrac{b}{a}x+\dfrac{c}{a} = 0$, alors $\left(x+\dfrac{b}{2a}\right)^2 - \dfrac{b^2-4ac}{4a^2} = 0$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Deux cas sont possibles :

1er cas : Les coefficients a,b,c sont des réels

i. $\Delta = b^2 - 4ac \succ 0$, alors $x_{1,2} = \dfrac{-b+\varepsilon\sqrt{b^2-4ac}}{2a}$, avec $\varepsilon^2 = 1$

ii. $\Delta = b^2 - 4ac \prec 0$, alors $x_{1,2} = \dfrac{-b+\varepsilon' i\sqrt{4ac-b^2}}{2a}$, avec $(\varepsilon')^2 = 1$

iii. $\Delta = b^2 - 4ac = 0$, alors $x = \dfrac{-b}{2a}$.

2er cas : Les coefficients a,b ou c sont complexes et $\Delta = b^2 - 4ac$ un nombre complexe

Soit δ, un nombre complexe tel que $\delta^2 = b^2 - 4ac$, ie δ est une racine carrée de $(b^2-4ac) \in \mathbb{C}$, alors $x_{1,2} = \dfrac{-b+\varepsilon\delta}{2a}$ avec $\varepsilon^2 = 1$.

Mais, si $b^2 - 4ac = 0$, alors $x = \dfrac{-b}{2a}$.

Exemple

Soit à résoudre l'équation : $x^2 + 3ix - 3 + i = 0$ dans $\mathbb{C}$.

Solution

Calculons $\Delta = b^2 - 4ac$ sachant que $a = 1$, $b = 3i$ et $c = -3 + i$?

On a : $\Delta = (3i)^2 - 4(-3+i) = 3 - 4i$, ie $\Delta = 3 - 4i \in \mathbb{C}$.

Soit $\delta \in \mathbb{C}$ tel que $\delta^2 = 3 - 4i$, alors

$$\delta_1 = \varepsilon\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}} + \varepsilon' i\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}} \text{, avec } \varepsilon = -\varepsilon'$$

$$= \sqrt{\frac{\sqrt{9+16}+3}{2}} - i\sqrt{\frac{\sqrt{9+16^2}-3}{2}}$$

$$= 2 - i$$

Comme $\delta_1 = 2 - i$, alors les deux solutions de $x^2 + 3ix - 3 + i = 0$ sont donc :

$$x_{1,2} = \frac{-3i+\varepsilon\delta}{2a} = \begin{cases} x_1 = \dfrac{-3i+(2-i)}{2a} = 1-2i \\ x_2 = \dfrac{-3i-(2-i)}{2a} = -1-i \end{cases} \quad \text{avec} \quad \varepsilon^2 = 1$$

D'où $S = \{x_1 = 1-2i, x_2 = -1-i\}$.

E. FORME EXPONENTIELLE D'UN NOMBRE COMPLEXE

1) ***On pose, pour tout*** $\theta \in \mathbb{R} : e^{i\theta} = \cos\theta + i\sin\theta$.

Ainsi, $\forall k \in \mathbb{Z}$, on a :

- $e^{2ik\pi} = 1$
- $e^{i\pi} = -1$
- $e^{i(\theta+2\pi)} = e^{i\theta}$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

- $e^{i(\theta+\pi)} = -e^{i\theta}$

2) *Propriétés*

$\forall \theta, \theta' \in \mathbb{R}$ et $\forall n \in \mathbb{Z}$,on a :

i. $e^{i\theta} = e^{i\theta'} \Leftrightarrow \theta = \theta' + 2kz; \forall z \in \mathbb{Z}$

ii. $\left(e^{i\theta}\right).\left(e^{i\theta'}\right) = e^{i(\theta+\theta')}$

iii. $\left(e^{i\theta}\right)^n = e^{in\theta}$

iv. $\left(e^{i\theta}\right)^{-1} = e^{-i\theta} = \cos\theta - i\sin\theta$

3) *Soit* $Z \in \mathbb{C}^*$ ***, ie*** $Z = \left[|Z|, \arg Z\right] = |Z|\left[\cos(\arg Z) + i\sin(\arg Z)\right] = |Z|.e^{i\arg Z}$,

car $e^{i\arg Z} = \cos(\arg Z) + i\sin(\arg Z)$.

D'où $Z = |Z|.e^{i\arg Z}$ est la forme exponentielle de Z.

4) *Exemples :*

a. Ecrire $Z = 1 + i\sqrt{3}$ sous forme exponentielle dans $\mathbb{C}$.

On sait que $Z = \left[|Z|, \arg Z\right] = \left[2, \frac{\pi}{3}\right]$ est la forme trigonométrique de Z,

alors $Z = 2.e^{i\pi/3}$ est la forme exponentielle de Z.

b. Résoudre dans $\mathbb{C}$ l'équation $e^Z = 1 + i\sqrt{3}$.

Solution :

On sait, d'après ce qui précède que, $1 + i\sqrt{3} = 2.e^{i\pi/3}$, alors pour $Z = x + iy$,on a, puisque $e^Z = 1 + i\sqrt{3}$ que ;

$$e^{x+iy} = 2.e^{i\pi/3} \Leftrightarrow e^x.e^{iy} = 2.e^{i\pi/3} \Leftrightarrow \begin{cases} e^x = 2 \\ y = \frac{\pi}{3} + 2k\pi, k \in \mathbb{Z} \end{cases} \Leftrightarrow \begin{cases} x = \ln 2 \\ y = \frac{\pi}{3} + 2k\pi, k \in \mathbb{Z} \end{cases}$$

D'où, si S est l'ensemble des solutions de $e^Z = 1 + i\sqrt{3}$, on a alors

$$S = \left\{x + yi : x, y \in \mathbb{R}\right\} = \left\{Z_k = \ln 2 + i\left(\frac{\pi}{3} + 2k\pi\right) : k \in \mathbb{Z}\right\}.$$

c. Résoudre dans $\mathbb{C} / \{-1\}$, l'équation : $(Z-1)^n - (Z+1)^n = 0, n \in \mathbb{N}^*$.

Solution :

Puisque $Z \neq -1$, on a : $\left(\frac{Z-1}{Z+1}\right)^n = e^{2ki\pi}$, car $e^{2ki\pi} = 1$, d'après ce qui a précédé. Ainsi,

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

$$\left(\frac{Z-1}{Z+1}\right)^n = e^{2ki\pi} \Leftrightarrow \frac{z-1}{z+1} = e^{\frac{2k\pi}{n}}$$

$$\Leftrightarrow \frac{Z-1}{Z+1} = e^{\frac{2ki\pi}{n}}$$

$$\Leftrightarrow Z-1 = (Z+1)e^{\frac{2ik\pi}{n}}$$

$$\Leftrightarrow Z\left(1-e^{\frac{2ik\pi}{n}}\right) = 1+e^{\frac{2ik\pi}{n}}$$

$$\Leftrightarrow Z = \frac{1+e^{\frac{2ik\pi}{n}}}{1-e^{\frac{2ik\pi}{n}}}, \text{ avec } k \neq 0$$

Soit $Z = \frac{1+e^{\frac{2ik\pi}{n}}}{1-e^{\frac{2ik\pi}{n}}}$. Diviser chaque terme du second membre de la relation par $e^{\frac{2ik\pi}{n}}$ pour avoir :

$$Z = \frac{e^{-\frac{ik\pi}{n}} + e^{\frac{ik\pi}{n}}}{e^{-\frac{ik\pi}{n}} - e^{\frac{ik\pi}{n}}} = \frac{2\cos\frac{k\pi}{n}}{-2i\sin\frac{k\pi}{n}} = \frac{\cos\frac{k\pi}{n}}{\sin\frac{k\pi}{n}}i = \left(\cot g\,\frac{k\pi}{n}\right)i$$

Avec $k \in \{1, 2, \ldots, (n-1)\}$ et $n \in \mathbb{N}^*$.

D'où $S = \left\{ Z_k = \left(\cot g\,\frac{k\pi}{n}\right)i : k \in [1, n-1] \subset \mathbb{N} \right\}$ est l'ensemble des solutions de l'équation $(Z-1)^n - (Z+1)^n = 0$.

Cas particulier, résoudre aux exercices l'équation $(Z-1)^3 - (Z+1)^3 = 0$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

CHAPITRE V.
LE POLYNOME A UNE INDETRMINEE

A. DEFINITION ET OPERATIONS

1. Définition

Soit A un anneau commutatif unitaire dont les éléments neutres sont 0 et 1 (A peut être $\mathbf{Z}, \mathbf{Z}/n\mathbf{Z}$, □ , □ , □). On appelle polynôme à une indéterminée à coefficients dans un anneau, toute suite $P = (a_0, a_1, a_2, ..., a_n, ...)$ d'éléments de A, tous nuls à partir d'un certain rang. Les éléments $a_0, a_1, a_2, ..., a_n$ sont appelés coefficients de P. ainsi un polynôme à une indéterminée, à coefficients dans A est une application de □ dans A dont seul un nombre fini des valeurs reste non nul. Il en résulte la définition de l'égalité de deux polynômes.

Soient $P = (a_0, a_1, a_2, ..., a_n, ...)$
$Q = (b_0, b_1, b_2, ..., b_n, ...)$

Alors $P = Q \Leftrightarrow a_k = b_k, \forall k \in [0, n] \subset$ □

D'autre part, P = 0 ie. $(a_0, a_1, a_2, ..., a_n, ...) = 0 \Leftrightarrow \forall k \in [0, n] \subset$ □ , on a $a_k = 0$

2. Opérations

Soit $\wp$, l'ensemble des polynômes à une indéterminée, à coefficients dans A. Dans $\wp$, on définit les opérations internes suivantes :

$P = (a_0, a_1, a_2, ..., a_n, ...) \in \wp$

$Q = (b_0, b_1, b_2, ..., b_n, ...) \in \wp$

a) *L'addition :* $P + Q = (a_0 + b_0, a_1 + b_1, ..., a_k + b_k, ...)$

b) *La multiplication :* $P.Q = (c_0, c_1, ..., c_k, ...)$
   Avec
$$\begin{aligned} c_k &= a_0 b_k + a_1 b_{k-1} + ... + a_k b_0 \\ &= \sum_{i+j=k} a_i b_j = \sum_{i=0} a_i b_{k-1} \end{aligned}$$
   C'est-à-dire $c_0 = a_0 b_0$; $c_1 = a_0 b_1 + a_1 b_0$; $c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$

Exemple :

$A = IR$ et $\begin{cases} P = (2, 4, -1, 2, ...) \\ Q = (-1, -2, 5, ...) \end{cases}$, deux polynômes.

Alors $P + Q = (1, 2, 4, 2, ...)$ et $P.Q = (-2, -8, 3, 20, -9, 10, 0, ...)$

Proposition : $(\wp, +, .)$ est un anneau commutatif unitaire.

Preuve :

1. $(\wp,+)$ est groupe commutatif dont l'élément neutre est le polynôme zéro $0=(0,0,0,...,0,...)$ et l'opposé du polynôme $P=(a_0,a_1,a_2,...,a_n,...)$ étant le polynôme $-P=(-a_0,-a_1,-a_2,...,-a_n,...)$. (+) étant commutative et associative.
2. $(\wp,.)$ est un monoïde commutatif car :
   (.) est commutative
   (.) est associative

Comme A est unitaire, alors il existe un polynôme unité $1=(1,0,0,...,0,...)$ tel que $\forall P\in\wp$, $1.P=P.1=P$.
$1=(1,0,0,...,0,...)$ est l'élément neutre de (.) dans $\wp$.
En plus, la multiplication (.) est distributive par rapport à (+) dans $\wp$ i.e. $\forall(i,j)\in\mathbb{N}^2 : a_i,b_i,c_j\in A$.

On a : $a_i\left(b_j+c_j\right)=a_ib_j+a_ic_j \Leftrightarrow \sum a_i\left(b_j+c_j\right)=\sum a_ib_j+\sum a_ic_j$

N.B : Soit $\wp_0=\left\{P=(\alpha,0,...,0,...):\alpha\in A\right\}$.
$\wp_0\subset\wp$ et de plus $\wp_0\neq\varnothing$ car $\exists\alpha=0\in A$ tel que $P=(0,0,...,0,...)\in\wp_0$

Ainsi, l'application
$\psi : A\to\wp_0$
$\alpha\mapsto\psi(\alpha)=(\alpha,0,...,0,...)$ *est un isomorphisme pour les opérateurs* $(+)$ *et* $(.)$ *définies en* (a) *et* (b).
Donc $\wp_0$ est un sous – anneau de $\wp$, d'où le théorème suivant :

Théorème :

Soit A un anneau commutatif unitaire. L'ensemble $\wp$ des polynômes à une indéterminée à coefficients dans A, muni de (+) et de (.) définies en (a) et (b) a une structure d'anneau commutatif et unitaire dont le sous – anneau $\wp_0$ décrit par les éléments de la forme $(\alpha,0,...,0,...)$ avec $\alpha\in A$ est isomorphe à A. cet isomorphisme nous permet d'identifier tout élément $a\in A$ a un polynôme $(a,0,...,0,...)$.

Ainsi les polynômes $(0,0,...,0,...)$ et $(1,0,...,0,...)$ seront désormais notés respectivement par 0 et 1. Par suite de cet isomorphisme, A est un sous – anneau de $\wp$ et tout $a\in A$ est dit polynôme constant.

c) *La multiplication d'un polynôme à une indéterminée à coefficient dans K par un scalaire avec K un corps commutatif*

1°. *Soit* $P=(a_0,a_1,a_2,...,a_n,...)\in\wp$ *et* $\alpha\in K$, alors :

$\alpha.P=(\alpha,0,0,...).(a_1,a_2,...,a_n,...)=(\alpha a_1,\alpha a_2,\alpha a_3,...,\alpha a_n,...)$ $i.e.\alpha P=\alpha(a_1,a_2,...,a_n)=(\alpha a_1,\alpha a_2,...,\alpha a_n,...$

Ceci permet de définir la multiplication externe dans ℘ à scalaires dans K.

On a :

$K\times\wp\to\wp$

$(\alpha,P)\mapsto\alpha P=(\alpha a_1,\alpha a_2,...,\alpha a_n,...)$

On vérifie trivialement que : $\forall\alpha,\beta\in K$, $\forall P,Q\in\wp$: on a :

- $(\alpha+\beta).P=\alpha P+\beta P$
- $\alpha(P+Q)=\alpha P+\alpha Q$
- $\alpha(\beta.P)=(\alpha.\beta)P$
- $1.P=P$

Conclusion :

$(\wp,+,.)$ où (.) est la multiplication externe en $\wp$, vérifie les propriétés i, ii, iii et iv, a une structure d'espace vectoriel sur le corps commutatif K.

2°. *Conséquence de la structure d'espace vectoriel*

Soit (e_k), $k\in[0,n]\subset\mathbb{N}$, une famille de polynômes dont un seul coefficient est non nul et est égal à 1. Un tel polynôme est défini comme suit :

$e_k=(\delta_{k,0},\delta_{k,1},\delta_{k,2},...,\delta_{k,i},...)$

où $\delta_{k,i}=\begin{cases}1 \text{ si } k=i\\ 0 \text{ si } k\neq i\end{cases}$, *formule de Kronecker.*

On a par exemple pour $k=0;k=1;...;k=n$:

$e_0=(1,0,...,0,...)$

$e_1=(0,1,...,0,...)$

$\vdots$

$e_n=(0,0,...,0,1,0,...)$, on constate que dans ce polynôme 1 se trouve à la (n+1)ième place dans la suite.

Alors, la famille $B=(e_k)_{k\in[0,n]\subset\mathbb{N}}$ est une base de $\wp$ car B est une famille libre et génératrice :

- B est une famille libre car : $\forall i\in\mathbb{N}$, $a_i\in K$ et $\sum_{i=0}^{n}a_ie_i=0\Rightarrow a_1=0,\forall 1\in IN$.

  $En\,effet, a_0e_0+a_1e_1+...+a_np_n=0\Leftrightarrow a_0(1,0,...)+...+a_n(0,0,...,0,...)$

  $\Leftrightarrow(a_0,0,...)+(0,a_1,0,...)+...+(0,0,...,a_n,0,...)=(0,0,...,0,...)$.

  $\Leftrightarrow a_0=a_1=a_2=...=a_n=0$
- B est génératrice car tout polynôme $P\in\wp$ peut s'exprimer d'une manière unique comme combinaison des éléments de β .

  En effet, soit $P=(a_0,a_1,a_2,...,a_n,...)$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

$$
\begin{aligned}
Alors, P &= (a_0,\dots,0,\dots)+(0,a_1,\dots,0,\dots)+\dots+(0,0,\dots,a_n,\dots)\\
&= a_0(1,\dots,0,\dots)+a_1(0,1,\dots,0,\dots)+\dots+a_n(0,0,\dots,1,\dots)\\
&= a_0e_0+a_1e_1+\dots+a_ne_n\\
&= \sum_{i=0}^{n} a_ie_i
\end{aligned}
$$

D'où $P=\sum_{i=0}^{n} a_ie_i$ (i)

En désignant par X le polynôme $e_1=(0,1,\dots,0,\dots)$ i.e. $X=(0,1,0,\dots,0,\dots)$, alors $X^2=(0,1,0,\dots,0,\dots).(0,1,0,\dots,0,\dots)=(0,0,1,\dots,0,\dots)=e_2$.

On montre par récurrence que $k\in \mathbb{N}^*, X^k=e_k$. Il suffit donc de poser $e_0=X^0=(1,0,0,\dots,\dots)=1$, pour obtenir la base $B=(e_k)_{k\in[0,n]\subset\mathbb{N}}$ sous la forme canonique $\{X^0=1, X, X^2, X^3,\dots,X^n\}$ et le polynôme $P=\sum_{i=0}^{n} a_ie_i$ devient $P=\sum_{i=0}^{n} a_iX^i$.

i.e.

$\mathrm{P}=\sum_{i=0}^{n}\mathrm{a_iX^i}=\mathrm{a_0X^i+a_1X+a_2X^2+\dots+a_nX^n}$ est un polynôme à une indéter min ée et à coefficient dans K

Théorème : En désignant par $\mathrm{X}=(0,1,0,\dots,\dots)$

On a :

1. $\forall n\in N: a_k\in K, k\in[0,n]\subset N$, la relation
   $\mathrm{a_0+a_1X+a_2X^2+\dots+a_nX^n=0\Rightarrow a_n=0;\forall n\in N}$

2. Le polynôme $P\in\wp$ s'écrit d'une manière unique sous la forme :
   $$\mathrm{P}=\sum_{i=0}^{n}\mathrm{a_iX^i}=\mathrm{a_0+a_1X+a_2X^2+\dots+a_nX^n}=\sum_{i=0}^{n}\mathrm{a_iX^i}$$
   Où les éléments $a_0,\dots,a_n\in K$ et vérifient $a_n\neq 0,\forall n\in N$.

D'où l'ensemble $\wp$ est engendré par sa partie $\mathrm{K}\cup\{\mathrm{X}\}$ que nous noterons $\mathrm{K}[\mathrm{X}]$. Et $\mathrm{K}[\mathrm{X}]$ est l'ensemble des polynômes à une indéterminée (X) et à coefficient dans K.

i.e. $\mathrm{K}[\mathrm{X}]=\left\{\mathrm{P}=\sum_{k=0}^{n}\mathrm{a_kX^k;a_k\in K,\forall k\in[0,n]\subset N}\right\}$

D'où, $\forall P\in[K]$, P est un polynôme en x à coefficient dans K.

i.e. $\mathrm{P=a_0+a_1X+a_2X^2+\dots+a_nX^n}$ ou $P=a_nx^n+a_{n-1}x^{n-1}+\dots+a_1x+a_0$

On dit respectivement que P est ordonnée suivant les puissances croissantes ou décroissantes de x.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

B. DEGRE D'UN POLYNOME

1. Définition :

Soit $P = (a_0, a_1, ..., a_n, ...) \in \wp$.

On appelle degré de P que l'on note degP ou d°P, le plus grand naturel n tel que $a_n \neq 0$.

Exemple :

$d^\circ(2,3,0,4,...) = 3 \text{ car } a_3 = 4 \neq 0.$

2. Remarques

a. Le polynôme zéro $0 = (0,0,...,0)$ n'a pas de degré.

$P = (a,0,0,...,0,...)$

b. Le polynôme constant non nul est de degré 0.

c. Le polynôme $a_k X^k$ s'appelle monôme de degré k si : $(a_k \neq 0)$. Ainsi, le degré d'un polynôme apparaît comme celui d'un monôme de plus haut degré le composant.

d. Si d°P = n, alors $a_n X^n$ est dit monôme dominant du polynôme et $a_n \equiv$ coefficient dominant.

e. Si d°P = m et $a_n = 1$: P est dit polynôme unitaire ou polynôme normalisé.

Corollaire

Soit $P = a_n X^n + ... + a_1 X + a_0$ est un polynôme de degré n $(a_n \neq 0)$ alors $a_n^{-1} P$ est un polynôme normalisé ou unitaire.

3. Propriétés

Soient P, Q deux polynômes non nuls, à coefficients dans K.

1. Si $d^\circ P \neq d^\circ Q$ et $P + Q \neq 0$ alors $d^\circ(P+Q) = \sup\{d^\circ P, d^\circ Q\}$.
2. Si $d^\circ P = d^\circ Q$ et $P + Q \neq 0$ alors $d^\circ(P+Q) \leq \sup\{d^\circ P, d^\circ Q\}$.
3. $d^\circ(P.Q) = d^\circ P + d^\circ Q$.

N.B : Si $P, Q \in A[X]$, A un anneau commutatif unitaire, avec $P.Q \neq 0$, alors $d^\circ(P.Q) = d^\circ P + d^\circ Q$.

Théorème :

Soit A, un anneau intègre et unitaire, il en est de même de l'anneau $A[X]$ et de plus, si $P, Q \in A[X]$ sont tels que $P \neq 0$ et $Q \neq 0$.

Alors $d^\circ(P.Q) = d^\circ P + d^\circ Q$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

C. FONCTION POLYNÔME

Soit $P = a_0 + a_1X + a_2X^2 + ... + a_nX^n \in A[X]$

A, un anneau commutatif unitaire. On appelle fonction polynôme associée au polynôme P, l'application :

$\overline{P} : A \to A$

$x \to \overline{P}(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$

Où $\overline{P}(x)$ est obtenu en substituant l'élément $x \in A$ à l'indéterminée X de $A[X]$.

Si on peut écrire : $\forall P \in A[X] : P = P(X)$, alors $\overline{P}(x) = P(x)$.

Exemple :

$P(X) = 2 - 3X^2 + 4X^3 - 6X^4 \in IR[X]$, alors

$\overline{P} : \square \to \square$

$x \to \overline{P}(x) = P(x)$

$ie.\overline{P}(x) = 2 - 3x^2 + 4x^3 - 6x^4$, appelée fonction pôlynome associé au pôlynome P

Si x = 2, alors

$$\begin{aligned}\overline{P}(2) &= 2 - 3.2^2 + 4.2^3 - 6.2^4 \\ &= -74\end{aligned}$$

D. DIVISION EUCLIDIENNE DANS $K[X]$

1. Théorème et définition

K étant un corps commutatif : $f, g \in K[X]$, avec $g \neq 0$, il existe un couple unique des polynômes q et r tels que :

$f = q.g + r$ avec $r = 0$ où $d°r < d°g$. (i)

L'opération qui nous permet de passer de couple (f, g) $avec, g \neq 0$ au couple unique (q, r) vérifiant (i) s'appelle la division euclidienne des polynômes ou la division des polynômes f par g, avec g et f ordonnés suivant les puissances décroissantes de X. Les polynômes q et r sont appelés respectivement quotient et reste de la division euclidienne de f par g.

Démonstration

Soient $f = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0, avec\, a_n \neq 0$ et

$g = b_mX^m + b_{m-1}X^{m-1} + ... + b_1X + b_0, b_m \neq 0$

Etablissons l'existence de q et r et ensuite montrons leur unicité :

1. Si $d°f < d°g$,alors $q = 0$ et $r = f$.
2. Si $d°f \geq d°g$, il existe un monôme $q_1 = \frac{a_n}{b_m}X^{n-m}$ tel que :

   $f - gq_1 = r. On\, constate\, que\, d°r_1 < d°f$ (a).

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Dans $f - gq_1$, le terme de degré n disparaît et par suite, si $r_1 = 0$ ou $d°r_1 \prec d°g$, alors l'existence de q et de r est établie i.e. $q = q_1$ et $r = r_1$. Si $d°r_1 \geq d°g$, il existe le monôme q_2 avec $\mathrm{q_2 = \dfrac{monôme\, dominant\, de\, r_1}{b_m X^m}}$ tel que : $r_1 - gq_2 = r_2$ (b), avec $d°r_2 < d°g$

Si $d°r_2 \geq d°g$, on recommence l'opération car si $r_2 = 0$ où $d°r_2 \prec d°g$, alors l'existence de q et de r est établie. i.e. $\mathrm{q = q_1 + q_2}$ et $\mathrm{r = r_2}$

Supposons que, pour ce procédé rappelé, on ait trouvé le reste r_n tel que : $r_{n-1} - gq_n = r_n$, avec $d°r_n \prec d°r_{n-1}$, on obtient ainsi une suite des restes partielles $r_n, n \in [1, k']$; $k' \leq n$ donc $d°(r_n)$ décroît lorsque n croît i.e. $d°r_n \prec d°r_{n-1} \prec ... \prec d°r_2 \prec d°r_1 \prec d°r_0$.

Donc cet ensemble de degrés de $(r_n), \forall n$ admet un plus petit élément. Soit (r_p) le reste dont le degré est celui du plus petit élément.
Alors, $r_p = r_{p-1} - gq_p$ (β) avec $d°r_p \prec d°r_{p-1}$.

Je confirme que $d°r_p \prec d°g$. Sinon, i.e. $d°r_p \geq d°g$; il existerait q_{p+1} et r_{p+1} tels que : $r_{p+1} = r_p - gq_{p+1}$ avec $d°r_{p+1} \prec d°r_p$, ce qui n'est pas le cas, car r_p est l'élément de la suite (r_n) de plus petit degré, et cela contredirait notre hypothèse.

Donc, $d°r_p \prec d°g$.
En additionnant membre à membre les relations (a), (b), (α) et (β), on a :
$f - gq_1 + r_1 - fq_2 + ...r_{n-1} - gq_n + r_{p-1} - gq_p = r_1 + r_2 + ... + r_n + r_p$
$f - g\left(q_1 + q_2 + ...q_n + q_p\right) = r_p$
Posons $q = q_1 + q_2 + ...q_n + q_p$ et $r = r_p$ Pour avoir la relation (i).

Montrons leur unicité :
Supposons qu'il existe $(q.r)$ et $(q'.r')$ tels que :
$f - gq = r$ (i) avec $r = 0$ où $d°r \prec d°g$.
$f - gq' = r'$ (ii) avec $r' = 0$ où $d°r' \prec d°g$.

Par la différence (ii) - (i), on a : $f - g\left(q - q'\right) = r - r'$.
Comme $g \neq 0$, si $q - q' \neq 0$, on déduit que, d'une part $d°\left(r' - r\right) = d°\left(r' + (-r)\right) \prec d°g$.
D'autre part, $d°\left[g\left(q - q'\right)\right] = d°g + d°\left(q - q'\right) \geq d°g$, donc $d°\left[g\left(q - q'\right)\right] \geq d°g$.
Or $g\left(q - q'\right) = r' - r$, donc $d°\left(r' - r\right) \geq d°g$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

D'où on a la forme

$$\left.\begin{array}{l} d^\circ(r'-r) < d^\circ g \\ d^\circ(r'-r) \geq d^\circ g \end{array}\right\| \text{ ce qui est impossible.}$$

Donc q – q' = 0, i.e. q = q' et r = r'.

Exemple : Effectuer la division de $f(X) = 3X^5 - 6X^4 + 5X + 3$ par $g(X) = X^3 - 4X + 2$.

En effet, en divisant f par g, on trouve $q_1 = \dfrac{3X^5}{X^3} = 3X^2$ et

$r_1 = f - g.q_1 = 3X^5 - 6X^4 + 5X + 3 - 3X^5 + 12X^3 - 6X^2 = 6X^4 - 6X^2 + 5X + 3$

$d^\circ r_1 < d^\circ f$. Comme $d^\circ r_1 \geq d^\circ g$, alors diviser r1 par g.

Cela implique qu'il existe $q_2 = \dfrac{-6X^4}{X^3} = -6X$ et

$$\begin{aligned} r_2 &= r_1 - gq_2 \\ &= -6X^4 + 12X^3 - 6X^2 + 5X + 3 + 6X^4 - 24X^2 + 12X \\ &= 12X^4 - 30X^2 + 17X + 3. \end{aligned}$$

Il suit que $r_2 = 12X^3 - 30X^2 + 17X + 3. d^\circ r_2 < d^\circ r_1$.

Comme $d^\circ r_2 = d^\circ g$, alors diviser r_2 par g. Pour cela, il existe $q_3 = \dfrac{\text{monôme dominant de } r_2}{\text{monôme dominant de } g} = \dfrac{12X^3}{X^3} = 12$

$$\begin{aligned} \text{et } r_3 = r_2 - gq_3 &= 12X^3 - 30X^2 + 17X + 3 - 12X^3 + 48X - 24 \\ &= -30X^2 + 65X - 21 \end{aligned}$$

D'où $q = q_1 + q_2 + q_3 = 3X^2 - 6X + 12$ et $r_3 = -30X^2 + 65X - 21$

Disposition pratique

$$\begin{array}{rl|l} & f = 3X^5 - 6X^4 + 0X^3 + 0X^2 + 5X + 3 & X^3 - 4X + 2 = g \\ \hline -gq_1 & -3X^5 \quad + 12X^3 - 6X^2 & \underbrace{3X^2}_{q_1} - \underbrace{6X}_{q_2} + \underbrace{12}_{q_3} \\ r_1 = f - gf_1 = & -6X^4 + 12X^3 - 6X^2 + 5X + 3 & \\ -gq_2 = & 6X^4 \quad - 24X^2 + 12X & \\ r_2 = r_1 - gq_2 = & 12X^3 - 30X^2 + 17X + 3 & \\ -gq_3 = & -12X^3 \quad + 48X - 24 & \\ r_3 = & -30X^2 + 65X - 21 & \end{array}$$

Définition :

Soient $h, g \in K[X], g \neq 0$, nous dirons que f est divisible par g, s'il existe un et un seul polynôme $q \in K[X]$ tel que $f = g.q$ i.e. $r = 0$.

Exemple :

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

$P(X)=X^4-16\in \square[X]$.

$P(X)$ est divisible par X^2-4 car $\exists \mathrm{q}=\mathrm{X}^2+4\in \mathrm{IR}[\mathrm{X}]$ tel que :

$X^4-16=(X^2-4)(X^2+4)$. où i.e. $r=0$ et $q(X)=X^2+4$.

2. Divisibilité dans $K[X]$

On sait que : $\forall p\in K[X]$, avec $P=P(X)$. L'application : $\begin{aligned}&\overline{P}:K\to K\\ &x\to \overline{P}(x)=P(x)\end{aligned}$

est une fonction polynomiale associée au polynôme P.

Si $P(X)=a_0+a_1X+a_2X^2+...+a_nX^n$, alors $\overline{P}(x)=a_0+a_1x+a_2x^2+...+a_nx^n=\beta\in K$.

et β s'appelle valeur numérique du polynôme pour l'élément $\alpha\in K$.

Théorèmes :

Soit $P(X)=a_0+a_1X+a_2X^2+...+a_nX^n\in K$ et $a\in K$.

1. Le reste de la division euclidienne de $P(X)$ par $X-a$ est $P(a)$.
2. Le polynôme $P(X)$ est divisible par $X-a$ ssi $P(a)=0$.
3. le quotient de la division de $P(X)$ par $X-a$ est de degré m – 1 si $d°P=m$ et ce quotient et le reste s'obtiennent par la méthode des coefficients indéterminés.

Preuve

1. Diviser $P(X)$ par $X-a\Rightarrow$ le reste est de degré 0, i.e. le reste est une constante, alors $P(X)=(X-a)q(X)+r; r\in K$. Pour $X=a\in K, P(a)=r$.
2. Supposer que $r=0$, i.e. $P(a)=0$, alors $(X-a)$ divise $P(X)$.
3. Soit $P(X)=a_nX^n+a_{n-1}X^{n-1}+...+a_1X+a_0$, (i) $a_n\neq 0$, divisons $P(X)$ par $X-a$.

Pour cela, *Posons* $q=q_{n-1}X^{n-1}+q_{n-2}X^{n-2}+...+q_0, avec\, q_{n-1}\neq 0$

Alors,

$$\begin{aligned}P(X)&=(X-a)q+r\\ &=(X-a)\left(q_{n-1}X^{n-1}+q_{n-2}X^{n-2}+...+q_1X+q_0\right)+r\\ &=q_{n-1}X^n+(q_{n-2}-aq_{n-1})X^{n-1}+...+(q_1-aq_2)X^2+(q_0-aq_1)X+r-aq_0 \qquad \text{(iii)}\end{aligned}$$

Par identification (i) et (ii), on a :

$$\begin{cases}a_n=q_{n-1}\Rightarrow a_{n-1}=a_n\\ a_{n-1}=q_{n-2}-aq_{n-1}\Rightarrow q_{n-2}=a_{n-2}-aq_{n-1}\\ ...\\ a_1=q_0-aq_1\Rightarrow q_0=a_1-aq_1\\ a_0=r-aq_0\Rightarrow r=a_0-aq_0\end{cases}$$

En pratique les calculs sont disposés de la manière suivante :

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Exemple : Divisons le polynôme $P(X) = X^3 + 4X^2 - 5X + 6$ par le polynôme $X - 2$.
On sait que r = p(2) = 8 + 16 – 10 + 6 = 20.
Comme :
$d^\circ P = 3$, alors $d^\circ q(X) = 3 - 1 = 2$. Posons $q(X) = aX^2 + bX + c$ pour avoir $P(X) = (X-2)(aX^2 + bX + c)$.
Par identification, on obtient, $a = 1; b = 6;$ et $c = 7$.
D'où $q(X) = X^2 + 6X + 7$ et $r = 20$.

Théorème

Tout polynôme $P \in K[X]$ divisible par $X - a$ et par $X - b$ est, si $a \neq b$, divisible par $(X-a)(X-b)$ et réciproquement. On montre par récurrence sur $n \in \mathbb{N}^*$ que :
Tout polynôme P à coefficients dans un corps commutatif K, divisible séparablement par $(X-a_1), (X-a_2), ..., (X-a_n)$ avec $a_1, a_2, ..., a_n$ distincts deux à deux, est divisible par le produit $(X-a_1)(X-a_2)...(X-a_n)$ et réciproquement.

Preuve (exercice)

Exemple :
Soit $P(X) = X^3 - 3X^2 + 2 \in \mathbb{R}[X]$.

$P(X)$ est divisible par $X - 1$ et $X - 2$. Alors le polynôme $P(X)$ est divisible par $(X-1)(X-2)$.

Définition 1 :

Soit $P \in K[X]$, i.e. $P = P[X]$ et $a \in K$. On dit que a est une racine du polynôme P ssi $P[a] = 0$. On dit encore que a est un zéro de P.

Exemple :
Soit $P(X) = X^2 + 1 \in \mathbb{C}[X]$. Alors a = i est une racine de ce polynôme car $P[i] = 0$.

Corollaire :
Un polynôme $P(X)$ est divisible par $X - a$ ssi a est une racine de $P(X)$.

Exemple :
Soit $P(X) = X^2 - 2 \in \mathbb{R}[X]$. $a = \sqrt{2}$ est une racine de ce polynôme. Alors $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$.ce qui prouve que X²–2 est divisible par X² $-\sqrt{2}$.

Définition 2 :

On appelle ordre de multiplicité d'une racine $a \in K$ du polynôme $P \in K[X]$, le plus grand nombre naturel k tel que le polynôme P soit divisible par $(X-a)^k$.
Si $k = 1$, on dit que a est une racine simple de P.
Si $k > 1$, on dit que est une racine multiple d'ordre k du polynôme $P \in K[X]$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

D'où, si $a \in K$ est une racine multiple d'ordre k du polynôme P, alors $\exists P(X) \in K[X]$ tel que : $P(X) = (X-a)^k .Q(X)$, avec $Q(a) \neq 0$; si non ; i.e. $Q(a) = 0$.
Alors $Q(X)$ sera divisible par $X - a$. Ce qui supposerait l'existence d'un polynôme $Q_1(X)$ tel que : $Q(X) = (X-a)^k .Q_1(X)$.

Ce qui entraînerait que $P(X) = (X-a)^{k'} .Q_1(X)$ avec $k' \succ k$. Ce qui contredirai l'hypothèse selon laquelle a est une racine multiple d'ordre.

Théorème :

Soit $P(X) = a_0 + a_1 X + a_2 X^2 + ... + a_n X^n$, un polynôme à coefficients dans un corps commutatif K, de caractéristique nulle. Alors les trois propositions suivantes sont équivalentes : $(a \in K)$

1. a est une racine multiple d'ordre k du polynôme P.
2. a est une racine de P, et une racine multi^le d'ordre $(k-1)$ du polynôme $P'(X)$, où $P'(X)$ est la dérivée du polynôme $P(X)$ par rapport à l'indéterminé X
3. $P(a) = P'(a) = ... = P^{(k-1)}(a) = 0$ avec $P^{(k)}(a) \neq 0$.
   $P^{(k)}(X)$ est la dérivée d'ordre k du polynôme de $P(X)$.
   Preuve (exercice)

***Exemple* :**

a) Soit $P(X) = X^3 - 3X^2 - 3X - 1 \in \mathbb{R}[X]$; montrons que 1 est une racine multiple d'ordre 3 de P. Pour cela, calculons $P(1)$, $P'(1)$, $P''(1)$, $P'''(1)$.

Comme $P(X) = X^3 - 3X^2 - 3X - 1 \, alors \, P(1) = 0$

Alors

$$P'(X) = 3X^2 - 6X + 3 \, alors \, P'(1) = 0$$
$$P''(X) = 6X - 6 \, alors \, P''(1) = 0$$
$$P'''(X) = 6 \Rightarrow P'''(1) = 6 \neq 0$$

Donc 1 une racine triple de P.

b) Soit P(x) =X^{3} ⁻ 2X² + 3aX + b $\in$ IR[X].Déterminons a et b dans IR pour que ce polynôme soit divisible par (X ⁻ 2)².

Réponse :

P est divisible par (X ⁻ 2)² si et seulement si P(2) = P'(2) =0 et P''(2) $\neq$ 0.
P(X) = X^{3} ⁻ 2X² + 3aX + b $\Rightarrow$ P(2) = 8 ⁻ 8 + 6a + b = 6a + b
P(X) = 3X² ⁻ 4X + 3a $\Rightarrow$P'(2) = 12 ⁻ 8 + 3a = 4 + 3a

$$\begin{array}{l} P(2) = 0 \Leftrightarrow \\ P'(2) = 0 \Leftrightarrow \end{array} \begin{cases} 6a + b = 0 \\ 4 + 3a = 0 \end{cases} \Leftrightarrow \begin{cases} b = -6a = -6(-\dfrac{4}{3}) = 8 \\ a = -\dfrac{4}{3} \end{cases}$$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

E. POLYNÔMES IRREDUCTIBLES DE L'ANNEAU $K[x]$

1. Définition

Un polynôme $P \in K[X]$ est dit irréductible ou premier sur K, lorsqu'il ne peut être décomposé en un produit des polynômes des degrés inférieurs appartenant à $K[X]$. Dans le cas contraire, on dit que P est un polynôme réductible ou décomposable et on peut alors écrire : $P = P_1.P_2 : P_1, P_2 \in K[X]$, avec $d°P_1$ ou $d°P_2 \prec d°P$.

Noter que (P_1 et P_2 ne peuvent pas être des constantes, car tout polynôme non nul constant est diviseur trivial de tout polynôme $P \in K[X]$).

Remarque :

Le caractère réductible ou irréductible d'un polynôme P dépend essentiellement de corps de base choisie.

Exemples :

a) Tout polynôme de degré 1 est irréductible quelques soit le corps K.
b) Le polynôme nul est réductible, donc un polynôme irréductible est non nul.

c) $P(X) = X^2 + \alpha X + \beta$ est un polynôme :
   - irréductible dans $IR(X)$ à condition que $\alpha^2 - 4\beta \prec 0$
   - réductible dans $C(X)$ car $X^2 + \alpha X + \beta = (X - z_1)(X - z_2)$ avec z_1, z_2 solutions de l'équation $X^2 + \alpha + \beta = 0$

d) $P(X) = X^2 - 7$, est un polynôme :
   - réductible dans $IR(X)$ et $C(X)$ car $X^2 - 7 = \left(X - \sqrt{7}\right).\left(X + \sqrt{7}\right)$
   - irréductible dans $Q(X)$.

e) $P(X) = X^3 - 64$ est réductible dans $Q(X), IR(X)$ et $C(X)$.

   Dans $IR(X)$ et $Q[X]$, $X^3 - 64 = (X - 4)\left(X^2 + 4X + 16\right)$

   Dans $C[X]$, $X^3 - 64 = (X - 4)(X - z_1)(X - z_2)$ avec z_1, z_2 racines du polynôme $X^2 + 4X + 16$

2. Théorème

Théorème fondamental

Tout polynôme $P \in K[X]$, de degré non nul admet au moins un facteur irréductible et peut s'écrire d'une manière unique (à l'ordre près de ses facteurs) sous la forme :

$P(X) = \alpha (h_1)^a \cdot (h_2)^b \cdot .... \cdot (h_i)^q$ où $\alpha \in K^*$;

h1, h2,…, hi sont des polynômes unitaires irréductibles deux à deux distincts et *a, b,…, q* sont des entiers strictement positifs dont la somme est égale au degré de *P*.

Cette décomposition s'appelle ***la factorisation canonique*** du polynôme $P \in K[X]$.
Preuve (exercice)

Exemple :
Factoriser le Polynôme :

$$P(X) = 3X^3 - 9X + 6$$

$$\begin{aligned} On\,a\, P(X) &= 3X^3 - 9X + 6 = 3(X^3 - 3X + 2) \\ &= 3(X-1)(X^2 + X - 2) \\ &= 3(X-1)(X-1)(X-2) \\ &= 3(X-1)^2(X-2) \end{aligned}$$

Soit à factoriser l polynôme P(X) ci-dessous :
$P(X) = a_n X^n + \ldots\ldots\ldots\ldots + a_1 X + a_0 \cdot (a_n \leq 0)$

N.B. Si le Polynôme *P(x)* admet des racines entières, alors ces racines sont à prendre parmi les diviseurs du terme indépendants a_0.

Si P(X) admet les racines rationnelles alors $r = \frac{d}{s}$

Où *d est un* diviseur du terme indépendant a_0
s est un diviseur du coefficient déterminant (a_n)

3. Polynômes irréductibles de $IR(X)$ et de $C(X)$

a) Corps algébriquement clos.

Soit K un corps commutatif tel que tout polynôme $P \in K[X]$, de degré non nul admet au moins une racine a_1 dans *K*.

i.e. $P(X) = (X - a_1) P_1(X)$ avec $d°P_1(X)=d°P(X)-1$.

Alors on montre par récurrence sur $0 \prec m = d°P(X)$

que $P(X) = (X - a_1)(X - a_2)\ldots\ldots(X - a_n) P_n(X)$ avec $d°P_n(X)=0$.

Donc $P_n(X)=a_n$ = Coefficient dominant de *P*.

Comme tout polynôme de degré 1 est irréductible, il résulte que dans un tel corps, les seuls polynômes irréductibles sont les polynômes du premier degré en *x*.

D'où le théorème suivant :

b) Théorème et définition :

Pour un corps commutatif K, les propriétés suivantes sont équivalentes :

(i) Tout polynôme $P \in K[X]$, de degré non nul, admet au moins une racine dans K.

(ii) Tout polynôme $P \in K[X]$, de degré $n \succ 0$, admet n racines : $a_1, a_2, \ldots, a_n$ dans K.

(iii) Les seuls polynômes irréductibles dans $K[X]$ sont les polynômes du premier degré.

Tout corps commutatif K tel que l'une des propriétés suivantes soit vérifiées est appelé ***: corps algébriquement clos.***

Ainsi, les corps Q et IR ne sont pas algébriquement clos car :

$\exists P_1(X) = X^2 - 3 \in \mathbb{Q}[X]$ tel que $I_1(X)$ n'a pas de racines dans Q.

$\exists P_2(X) = X^2 + 1 \in \mathbb{R}[X]$ tel que $I_2(X)$ n'a pas de racines dans IR.

(1) Cas du corps C.

Théorème fondamental d'algèbre dit théorème d'Alembert-Gauss.
Le corps commutatif C est un corps algébriquement *clos*.
La démonstration de ce théorème recourt non seulement aux propriétés algébriques de Q, mais aussi aux propriétés topologiques découlant de celle de IR.

La conséquence de ce théorème et la définition de corps algébriquement clos montrent que :

$$\forall P \in C[X] \text{ ; avec } P = a_0 + a_1 X + \ldots\ldots + a_n X^n \quad (a_n \neq 0)$$

$$P = a_n (X - a_1)(X - a_2)\ldots\ldots\ldots(X - a_n)$$

Avec $a_1, \ldots, a_n$ des nombres complexes distincts ou non.

Exemple :

$$P(X) = X^3 - 8 \in C[X] = (X-2)(X^2 + 2X + 4) = (X-2)\left(X + 1 - i\sqrt{3}\right)\left(X + 1 + i\sqrt{3}\right)$$

(2) Cas De corps des réels (IR)

(a) Propriétés fondamentale des Polynômes à coefficients dans IR.

Si P est un polynôme à coefficients dans IR, de degré non nul, admet $z = a + bi \in C$ pour racine, elle admet aussi $\overline{z} = a - bi \in C$, pour racine ($\overline{z} \equiv$ conjugué de z).

(b) Conséquence.

Tout polynôme $P(X) \in IR[X]$, de degré non nul n admet n racines qui sont soit réelles, soit complexes conjuguées deux à deux.

Corollaire :

Les polynômes irréductibles de $IR[X]$ sont des polynômes du degré 1 et les polynômes de la forme $aX^2 + bX + c \quad (b \neq 0 \neq a)$ avec $b^2 - 4ac \prec 0$.

Ainsi tout polynôme $P \in IR[X]$, de degré $m \succ 0$, et de coefficient dominant a_m peut s'écrire d'une manière unique à l'ordre près de ses facteurs sous la forme :

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

$P(X)=a_n.P_1^{\alpha^1}.P_2^{\alpha^2}..........P_h^{\alpha^h}.S_1^{\beta^1}.S_2^{\beta^2}........S_k^{\beta^k}$ où $P_i\left(1\le i\le h\right)$ et $P_j\left(1\le j\le k\right)$ sont des polynômes irréductibles respectivement du premier et du second degré et $\alpha_1,\alpha_2,.......,\alpha_h,\beta_1,\beta_2,.......,\beta_k$ sont des entiers strictement positifs vérifiant :

$$\left(\alpha_1+\alpha_2+......+\alpha_h\right)+2\left(\beta_1+\beta_2+......+\beta_k\right)=m$$

Exemple :

Factoriser $f(X)=X^4+X^3+4X^2-15X+9$ dans $\mathbb{R}[X]$

$$=(X-1)\left(X^3+2X^2+6X-9\right)$$
$$=(X-1)(X-1)\left(X^2+3X+9\right)$$
$$=(X-1)^2\left(X^2+3X+9\right)$$

P_1=X-1 ;S_1=X^2+3X+9 ; $\alpha_1=2$ et $\beta_1=1$. D'ou $d°P=\alpha_1+2\beta_1=2+2=4$

F. DERNIER DIVISEUR COMMUN (D.D.C.) ET PREMIER MULTIPLE COMMUN (P.M.C.)

Des polynômes de $K[X]$, K corps commutatif

1. Définition :

Soient $f,g\in K[X]$, deux polynômes non nuls. Alors le dernier diviseur commun des polynômes *f* et *g*, noté : *d.d.c.(f,g)* est le polynôme ***unitaire***, du degré maximum, diviseur

Commun des polynômes *f* et *g*. Si ce polynôme existe, il est unique.

2. Méthode de recherche de d.d.c. (f,g) $f\neq 0\neq g$.

a) Factorisation des polynômes.

Exemple :

d.d.c.(f,g), avec

$$f(X)=X^4+X^3+4X^2-15X+9$$
$$g(X)=X^2-4X+3$$

Factorisons les polynômes *f(X)* et *g(X)*.

$$f(X)=(X-1)^2\left(X^2+3X+9\right)$$
Et $g(X)=(X-1)(X-3)$

D'où *d.d.c.(f,g)*= $X-1$

Théorème

Soient $f,g\in K[X]$, avec $f\neq 0\neq g$.

Alors il existe deux polynômes *q* et *r* respectivement quotient et reste de la division euclidienne de *f* par *g*.

Ainsi, les diviseurs communs aux polynômes *f* et *g* sont aussi les diviseurs communs aux polynômes *q* et *r*.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

En effet, puisque $g \neq 0$, effectuons la division euclidienne de f par q,g par r, r par r_1… etc. et on va s’ arrêter lorsqu’on aura trouvé un reste nul.

$$
\begin{array}{ll}
f = g \cdot q + r & \left(d^\circ r \prec d^\circ g\right) \\
g = r \cdot q_1 + r_1 & \left(d^\circ r_1 \prec d^\circ r\right) \\
r = r_1 \cdot q_2 + r_2 & \left(d^\circ r_2 \prec d^\circ r_1\right) \\
r_1 = r_2 \cdot q_3 + r_3 & \left(d^\circ r_3 \prec d^\circ r_2\right) \\
r_{n-2} = r_{n-1} \cdot q_n + r_n & \left(d^\circ r_n \prec d^\circ r_{n-1}\right) \\
r_{n-1} = r_n \cdot q_{n+1} \quad \text{avec} & r_{n+1} = 0
\end{array}
$$

Donc $r_{n+1} = 0$, le dernier reste non nul. r_n est le dernier diviseur commun de *f* et *g*. Alors normalisé ou unitarisé.

Exemple :
Chercher le *d.d.c.(f,g),*

$$
\text{avec} \quad
\begin{array}{l}
f\left(X\right) = X^4 + X^3 - 3X^2 - 4X - 1 \\
g\left(X\right) = X^3 + X^2 - X - 1
\end{array}
$$

Divisons f et g,g par r ; r par r_1

f par g ;

$$
\begin{array}{r|l}
f = X^4 + X^3 - 3X^2 - 4X - 1 & X^3 + X^2 - X - 1 = g \\
\hline
-X^4 - X^3 \qquad\qquad\qquad & X \\
\hline
r = -3X^2 - 4X - 1 &
\end{array}
$$

g par r ;

$$
\begin{array}{r|l}
g = X^3 + X^2 - X - 1 & -3X^2 - 4X - 1 = r \\
\hline
-X^3 - \frac{4}{3}X^2 - \frac{x}{3} & -\frac{X}{3} + \frac{1}{9} \\
\hline
-\frac{X^2}{3} - \frac{4}{3}X - 1 & \\
\frac{X^2}{3} + \frac{4}{9}X + \frac{1}{9} & \\
\hline
\mathbf{r_1} = -\frac{8}{9}X - \frac{8}{9} &
\end{array}
$$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

r par r₁ ;

$$
\begin{array}{l|l}
r = -3X^2 - 4X - 1 & -\frac{8}{9}X - \frac{8}{9} \\ \cline{2-2}
\quad 3X^2 + 3X & \frac{27}{8}X + \frac{9}{8} \\ \cline{1-1}
\qquad -X - 1 & \\
\qquad\ X + 1 & \\ \cline{1-1}
\qquad r_2 = 0 &
\end{array}
$$

Comme $r_2 = 0$, alors

$r_1 = -\frac{8}{9}X - \frac{8}{9}$, alors unitaire est le ddc(f, g).ie, $\text{ddc}(f,g) = |r_1| = -\frac{9}{8}r_1 = X + 1$

3. Théorème :

Le premier multiple commun $f, g \in (K[X])$ est le quotient de leur produit par leur dernier diviseur commun.

Preuve :

Soit $M \in K[X]$, le $p.m.c(f, g)$, $\exists D \in K[X]$ tel que $M = \frac{f \cdot g}{D}$

i.e. $f.g = D.M$

(i) Montrons que D est un diviseur commun aux polynômes *f* et *g*.

M étant un multiple de f et g, alors $\exists P_1, P_2 \in K[X]$ tels que $M = P_1.f = P_2.g$

(i) devient $\begin{cases} f.g = D.P_1.f \\ f.g = D.P_2.g \end{cases} \Rightarrow \begin{cases} g = D.P_1 \\ f = D.P_2 \end{cases}$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

CHAPITRE VI
CALCUL MATRICIEL ET APPLICATIONS LINEAIRES

A. GENERALITES

1. Définition :

Soit K, un corps commutatif, on appelle matrice de type (m, n) ; m, n $\in$ IN*, un tableau rectangulaire ou carré à m colonnes et n lignes formé des éléments de K.
Si I et J sont deux parties finies non vides de IN, avec #I= m et #J = n, m, n $\in$ IN*, alors l'élément situé à l'intersection de la i^{ieme} colonne et j^{ieme} ligne est généralement désigné par la notation telle que a_i^j ou a_{ij}. L'indice inférieur (i) indique la colonne d'un élément dans la notation a_i^j et la ligne dans la notation a_{ij}. Tandis que, l'indice supérieur (j) indique la ligne d'un élément dans la notation a_i^j et la colonne dans la notation a_{ij}.
L'objet mathématique ainsi obtenu sera noté soit par une lettre majuscule, par exemple : A et on écrit :

A= $\left(a_i^j\right)_{i=1,\ldots,m}^{j=1,\ldots,n}$ ou $A=\left(a_{ij}\right)i=1,\ldots m$ et $j=1,\ldots,n$ soit en utilisant un tableau d'éléments de K, lesquels éléments sont mis entre parenthèses.

$$A=\begin{pmatrix} a_1^1 & a_2^1\ldots a_i^1\ldots a_m^1 \\ a_1^2 & a_2^2\ldots a_i^2 \quad a_m^2 \\ \vdots & \vdots \quad \vdots \quad \vdots \\ a_1^j & a_2^j\ldots a_i^j \quad a_m^j \\ \vdots & \vdots \quad \vdots \quad \vdots \\ a_1^n\ldots & a_2^n\ldots a_i^n\ldots a_m^n \end{pmatrix} \quad \text{ou} \quad A=\begin{pmatrix} a_{11}\ldots a_{12}\ldots a_{1n} \\ a_{21}\ldots a_{22} \quad a_{2n} \\ \vdots \quad \vdots \quad \vdots \\ a_{m1}^j\ldots a_{m2} \; a_{mn} \end{pmatrix}$$

Notez que dans notre cours, on va opter pour la notation (a_i^j).
On appelle hauteur d'une matrice A le nombre (n) de ses lignes et on appelle longueur de A le nombre (m) de ses colonnes.
Si m $\prec$ n ou m $\succ$ n, alors A est dite matrice rectangulaire de type (m, n). On note par m_k (m, n) l'ensemble des matrices de type (m, n) et à coefficient dans K.

$\Rightarrow \mathrm{m}_k$(m, n) $=\left\{A=(a_i^j):(i,j)\in I\times J; a_i^j\in K\right\}$

Si m= n, alors A est dite matrice carrée d'ordre n. On note par m_n(K) l'ensemble des matrices carrées d'ordre n, à coefficient dans K.
Si n=1, c.à.d. $A=(a_i^j)_{i=1,\ldots,m}=(a_1^1\ a_2^1\ \ldots a_m^1)$ est dite matrice uniligne

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Si m=1, c.à.d. $A = \left(a_i^j\right)^{j=1,\dots,n} = \begin{pmatrix} a_1^1 \\ a_1^2 \\ \vdots \\ a_1^n \end{pmatrix}$ est dite matrice unicolonne.

Exemples :

$$A = \begin{pmatrix} 2 & 3 & 4 & 7 \\ 0 & 5 & 6 & -3 \\ 5 & -6 & 10 & 1 \end{pmatrix}$$ est une matrice de type (4, 3)

Pour cette matrice : $a_4^2 = -3$; $a_1^2 = 0$; $a_3^2 = 6$

$B = \begin{pmatrix} 3 & 6 \\ 7 & 8 \end{pmatrix}$ Matrice carrée d'ordre 2

$C = \begin{pmatrix} 1 & 3 & 4 & 5 \end{pmatrix}$ Matrice uniligne de type (4,1)

$D = \begin{pmatrix} -7 \end{pmatrix}$ Matrice carrée d'ordre 1

2. Egalite de deux matrices

a) Définition :

Deux matrices A et B sont égales, ce qu'on écrit A=B ssi :

i) A et B sont de même type

ii) les éléments correspondants des matrices A et B sont égaux

si $A = \left(a_i^j\right)$ et $B = \left(b_i^j\right)$ $\forall (i, j) \in I \times J$

Alors A=B ssi $a_i^j = b_i^j; \forall (i, j) \in I \times J$

b) Exemples :

1) Soient A = $\begin{pmatrix} a_1^1 & a_2^1 \\ a_1^2 & a_2^2 \\ a_1^3 & a_2^3 \end{pmatrix}$ et B = $\begin{pmatrix} b_1^1 & b_2^1 \\ b_1^2 & b_2^2 \\ b_1^3 & b_2^3 \end{pmatrix}$ deux matrice de type (2,3) chacune,

Alors A = B $\Leftrightarrow \begin{cases} a_1^1 = b_1^1 & a_2^1 = b_2^1 \\ a_1^2 = b_1^2 & a_2^2 = b_2^2 \\ a_1^3 = b_1^3 & a_2^3 = b_2^3 \end{cases}$

2) Soient A = $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ et B = $\begin{pmatrix} 1 & a \\ 3 & b \end{pmatrix}$ deux matrice d'ordre deux.

Alors A = B $\Leftrightarrow$ a = 2 et b = 4

Par contre pour A = $\begin{pmatrix} 3 & 6 & 7 \\ 10 & 9 & 4 \end{pmatrix}$ et B = $\begin{pmatrix} 3 & 6 & 7 \\ 10 & 9 & -4 \end{pmatrix}$. On a : A $\neq$ B car 4 $\neq$ -4

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

3. Transposition d'une matrice

a) Définition :

Soit A= $\left(a_i^j\right)$ (i, j) ∈ I x J; une matrice de type (m, n). La transposée de A est la matrice notée $\overset{t}{A}$ ou At ou encore Ậ qui admet comme colonnes successives les lignes successives de A.

Si $A = \left(a_i^j\right)$ (i, j)∈ I x J est une matrice de type (m, n), alors

$A^t = (a_j^i)\ (j,i) \in J \times I$ est une matrice de type (n,m)

b) Exemples :

1) Soit A = $\begin{pmatrix} a_1^1 & a_1^2 & a_3^1 \\ a_1^2 & a_2^2 & a_3^2 \end{pmatrix}$ alors $A^t = \begin{pmatrix} a_1^1 & a_1^2 \\ a_1^2 & a_2^2 \\ a_3^1 & a_3^2 \end{pmatrix}$

2) $\begin{pmatrix} 1 & 3 \\ -10 & 5 \\ 6 & 7 \end{pmatrix}^t = \begin{pmatrix} 1 & -10 & 6 \\ 3 & 5 & 7 \end{pmatrix}$ et ${}^t\begin{pmatrix} 4 & 6 \\ 8 & 9 \end{pmatrix} = \begin{pmatrix} 4 & 8 \\ 6 & 9 \end{pmatrix}$

3) $\begin{pmatrix} a & b & c \end{pmatrix}^t = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$

T.P. : Transposez les matrices suivantes :

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{pmatrix};\ B = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{pmatrix};\ C = \begin{pmatrix} 10 & -6 & 1 \\ 7 & 8 & 2 \\ 9 & -10 & 3 \\ 0 & 3 & 5 \end{pmatrix};\ D = (a)$$

c) Propriétés

$\forall A \in m_n(K)\,\text{on a} : \left(A^t\right)^t = A$

4. Remarques

a) Matrice Nulle

Une matrice est nulle si tous ses éléments sont nuls

Soit $A = (a_i^j)\ (i,\ j) \in I \times J;\text{alors } A = 0 \Leftrightarrow a_i^j = 0\ \forall\,(i, j) \in I \times J$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Par exemple les matrices $0=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$; $0=\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$ sont nulles, l'une d'ordre 2 et l'autre de type (5,2).

b) Matrice Opposée

Soit $A=(a_i^j)$ une matrice, alors la matrice $(-A)=(-a_i^j)$ $(i, j) \in I \times J$ est dite matrice opposée de A.

Exemple :

a) soit $A=\begin{pmatrix} a_1^1 & a_2^1 & a_3^1 \\ a_1^2 & a_2^2 & a_3^2 \end{pmatrix}$ alors $(-A)=\begin{pmatrix} -a_1^1 & -a_2^1 & -a_3^1 \\ -a_1^2 & -a_2^2 & -a_3^2 \end{pmatrix}$

b) soit $B=\begin{pmatrix} -6 & 7 \\ 8 & -9 \end{pmatrix}$ alors $(-B)=\begin{pmatrix} 6 & -7 \\ -8 & 9 \end{pmatrix}$

5. Matrices carrées

a) Éléments diagonaux

Soit A=$(a_i^j)_{i=j=1,\ldots,n}$ une matrice carrée d'ordre n. alors les éléments de la forme $a_i^i; \forall i=1,\ldots,n$ sont dits éléments diagonaux de A. ils forment ce qu'on appelle la diagonale principale da A.

Par exemple :

$$A=\begin{pmatrix} a_1^1 & a_2^1 \\ a_1^2 & a_2^2 \end{pmatrix}$$ une matrice carrée d'ordre 2, les éléments diagonaux de A sont a_1^1 et a_2^2

b) Matrice diagonale

Soit $A=(a_i^j)_{j=i=1,\ldots,n}$ une matrice carrée d'ordre n. A est dite matrice diagonale, si tout élément n'appartenant pas à la diagonale principale est nul ou encore A est dite matrice diagonale si $\forall i, j,\ i \neq j \Rightarrow a_i^j = 0.$ on la note par diag $\left(a_1^1, a_1^2, \ldots, a_n^n\right)$

$$\text{On a, diag}\left(a_1^1\ a_2^2 \ldots a_n^n\right)=\begin{pmatrix} a_1^1 & 0 & \cdots & 0 \\ 0 & a_2^2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & a_n^n \end{pmatrix}$$

$$\operatorname{diag}(1,3,0)=\begin{pmatrix}1 & 0 & 0\\ 0 & 3 & 0\\ 0 & 0 & 0\end{pmatrix}$$ est une matrice diagonale d'ordre 3

N.B. : Toute matrice diagonale dont tous les éléments diagonaux sont égaux entre - eux est dite ***matrice scalaire,*** si $a_1^1 = a_2^2 = \ldots\ldots = a_n^n = a$,

$$\text{alors, } \operatorname{diag}(a,a,a,\ldots,a)=\begin{pmatrix}a & 0\cdots 0\\ 0 & a\cdots 0\\ \vdots & \vdots \quad \vdots\\ 0 & 0\cdots a\end{pmatrix}$$ est une matrice scalaire

Définition : Toute matrice scalaire dont les éléments diagonaux sont tous égaux à 1 est dite matrice unité d'ordre n. on la note par I_n.

Ainsi : $I_n = \begin{pmatrix}1 & 0\cdots 0\\ 0 & 1\cdots 0\\ \vdots & \vdots \quad \vdots\\ 0 & 0\cdots 1\end{pmatrix}$

Par exemple $I_2 = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ et $I_3 = \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$, matrices unités d'ordre respectifs 2 et 3.

c) Matrice triangulaire

Soit $A = \left(a_i^j\right)_{i=j=1,\ldots,n}$ une matrice carrée d'ordre n. A est dite matrice triangulaire :

Supérieure, si tout élément se trouvant en dessous de la diagonale principale est nul ie A est dite matrice triangulaire supérieure si i<j$\Rightarrow a_i^j = 0$

Inférieure, si tout élément se trouvant au dessus de la diagonale principale est nul ie A est dite matrice triangulaire inférieure si i > j$\Rightarrow a_i^j = 0$

Pour une matrice carrée A d'ordre 3.

Soit :

$$A = \begin{pmatrix}a_1^1 & a_2^1 & a_3^1\\ a_1^2 & a_2^2 & a_3^2\\ a_1^3 & a_2^3 & a_3^3\end{pmatrix}$$

Alors

$$\operatorname{tsup}(A) = \begin{pmatrix}a_1^1 & a_2^1 & a_3^1\\ 0 & a_2^2 & a_3^2\\ 0 & 0 & a_3^3\end{pmatrix}$$ est une matrice la triangulaire Supérieure.

$$\operatorname{tinf}(A) = \begin{pmatrix}a_1^1 & 0 & 0\\ a_1^2 & a_2^2 & 0\\ a_1^3 & a_2^3 & a_3^3\end{pmatrix}$$ est la matrice triangulaire inférieure.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

On note par $\tau_n(K)$ l'ensemble des matrices triangulaires (supérieure ou inférieure) d'ordre n à coefficient dans K. et par $Diag(a_1^1, a_2^2, a_3^3, ..., a_n^n)$ l'ensemble des matrices diagonales d'ordre n.

6. Matrice Symétrique et Matrice Antisymétrique

Soit A = $((a_i^j)_{i=j=1,2,...,n}$ une matrice carré d'ordre n

A est dite matrice symétrique si elle est égale à sa transposée. i.e. A est symétrique si $t_A = A$

Exemple :

La matrice A = $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{pmatrix}$ est symétrique car ${}^tA = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{pmatrix} = A$

Par contre, la matrice B = $\begin{pmatrix} 2 & -3 \\ 3 & 6 \end{pmatrix}$ n'est pas symétrique car ${}^tB = \begin{pmatrix} 2 & 3 \\ -3 & 6 \end{pmatrix} \neq B$

Soit $A = (a_i^j)_{i=j=1,...,n}$ une matrice carrée d'ordre n, A est dite antisymétrique si la transposée de A est égale à la matrice opposée de A.

C'est-à-dire A est antisymétrique si $A^t = (-A)$.

Exemple :

Soit $A = \begin{pmatrix} 0 & -3 \\ 3 & 0 \end{pmatrix}$,alors A est antisymétrique car

$A^t = (-A)$, En effet $A^t = \begin{pmatrix} 0 & 3 \\ -3 & 0 \end{pmatrix}$ et $-A = \begin{pmatrix} 0 & 3 \\ -3 & 0 \end{pmatrix}$

On a donc : $A^t = (-A)$

Soit $B = \begin{pmatrix} 0 & 1 & -2 \\ -1 & 0 & 5 \\ 2 & -5 & 0 \end{pmatrix}$, alors B est antisymétrique car $B^t = \begin{pmatrix} 0 & -1 & 2 \\ 1 & 0 & -5 \\ -2 & 5 & 0 \end{pmatrix} = (-B)$.

T.P. : Les matrices suivantes sont – elles antisymétriques ?

$A = \begin{pmatrix} 0 & -6 \\ 6 & 1 \end{pmatrix}$ $\quad B = \begin{pmatrix} 0 & 5 & 6 \\ -5 & 0 & -8 \\ -6 & 8 & 0 \end{pmatrix}$ $\quad C = \begin{pmatrix} 0 & 5 & -6 \\ -5 & 0 & -8 \\ 6 & 8 & 1 \end{pmatrix}$

B. OPERATIONS MATRICIELLES

1. Addition des matrices

a) Définition :

Soient $A = (a_i^j)$ et $B = (b_i^j)_{i=1,...,m}^{j=1,...,n}$ deux matrices de type (m, n)

La somme de ces deux matrices s'obtient en additionnant les éléments correspondants de ces deux matrices. C'est-à-dire $A+B=\left(a_i^j+b_i^j\right)_{i=1,\dots,m}^{j=1,\dots,n}$

b) Exemples :

$$A=\begin{pmatrix} a_1^1 & a_2^1 & a_3^1 \\ a_1^2 & a_2^2 & a_3^2 \end{pmatrix} \quad \text{et} \quad B=\begin{pmatrix} b_1^1 & b_2^1 & b_3^1 \\ b_1^2 & b_2^2 & b_3^2 \end{pmatrix}$$

$$A+B=\begin{pmatrix} a_1^1+b_1^1 & a_2^1+b_2^1 & a_3^1+b_3^1 \\ a_1^2+b_1^2 & a_2^2+b_2^2 & a_3^2+b_3^2 \end{pmatrix}$$

b) Soient $A=\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}$ et $B=\begin{pmatrix} 6 & -5 \\ 10 & 1 \\ 0 & 3 \end{pmatrix}$ alors $A+B=\begin{pmatrix} 7 & -3 \\ 13 & 5 \\ 5 & 9 \end{pmatrix}$

c) Soient $A=\begin{pmatrix} 1/2 & -3 \\ 4 & 3/4 \end{pmatrix}$ et $B=\begin{pmatrix} 2/3 & 1/5 \\ -2/3 & -4 \end{pmatrix}$ alors

$$A+B=\begin{pmatrix} 7/6 & -14/5 \\ 10/3 & -13/4 \end{pmatrix}$$

c) Propriétés :

P₁. La somme des matrices est commutative et associative c'est-à-dire
$\forall\ A=(a_i^j); B=(b_i^j)\ , C=(c_i^j)_{i=1,\dots,m}^{j=1,\dots,n}$ 3 matrices de type (m, n), on a :
A+B=B$\neq$A
(A+B)+C=A+ (B+C)
En effet : i) A+B=$(a_i^j)+(b_i^j)=(a_i^j+b_i^j)=(b_i^j+a_i^j)=(b_i^j)+(a_i^j)=B+A$
ii) $(A+B)+C=[(a_i^j)+(b_i^j)]+(c_i^j)$
$= (a_i^j)+[(b_i^j)+(c_i^j)]=A+(B+C)$

P₂. La matrice nulle (o) est l'élément neutre de l'addition dans $m_k(m,n)$ car $\forall A\in m_k(m,n)$ on a : $A+0=A$

P3. $\forall A\in m_k(m,n)$ avec $A=(a_i^j)_{i=1,..,m}^{j=1,..,n}$ alors $(-A)=(-a_i^j)_{i=1,\dots,m}^{j=1,\dots,n}$ est dit matrice opposé de A.
Et on a : A+(-A)= $(a_i^j)+(-a_i^j)=(a_i^j-a_i^j)=0$
P₃. $\forall$ A,B$\in$ m_k (m,n) on a : $(A + B)^t = A^t + B^t$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Conclusion :
P_1, P_2, $P_3 \Rightarrow [m_k(m,n);+]$ est un groupe abélien en particulier $[m_n(K);+]$ est aussi un groupe abélien.

d) Conséquence de la structure du groupe $[m_k(m,n);+]$

$\forall A,B \in m_k(m,n) \exists!\ X \in m_k(m,n)$ tel que X+B=A en effet

$B \in m_k(m,n) \overset{P_3}{\Longrightarrow} (-B) \in m_k(m,n)$. De

$X + B = A, \text{on a}: (X+B)+(-B) = A+(-B)$

$$\Leftrightarrow X+(B-B) = A+(-B) \Leftrightarrow X+O = A-B \Leftrightarrow X = A-B$$

D'où $A - B = A + (-B)$ i. e. Retrancher une matrice revient à ajouter son opposé.

Exemple :

$$\text{Soient } A = \begin{pmatrix} 2 & 3 \\ 4 & -6 \\ -5 & 7 \end{pmatrix} \text{ et } B = \begin{pmatrix} -3 & 7 \\ 10 & -11 \\ -2 & 4 \end{pmatrix} \text{ alors, } A - B = \begin{pmatrix} 2 & 3 \\ 4 & -6 \\ -5 & 7 \end{pmatrix} - \begin{pmatrix} -3 & 7 \\ 10 & -11 \\ -2 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 2 & 3 \\ 4 & -6 \\ -5 & 7 \end{pmatrix} + \begin{pmatrix} 3 & -7 \\ -10 & 11 \\ 2 & -4 \end{pmatrix}$$

$$= \begin{pmatrix} 5 & -4 \\ -6 & 5 \\ -3 & 3 \end{pmatrix}$$

e) Remarques

R_1. La somme de deux matrices diagonales est une matrice diagonale
R_2. La somme de deux matrices triangulaires inférieures est une matrice triangulaire inférieure .
R_3. La somme de deux matrices triangulaires supérieures est une matrice triangulaire supérieure.

D'où $[\text{Diag}(a_1^1, a_2^2, \ldots, a_n^n), +]$ est un groupe abélien et $[\tau_n(k);+]$ est un groupe abélien.

f) Théorème

Toute matrice carrée A d'ordre n à coefficient dans K peut se décomposer en une somme d'une matrice symétrique (S) et d'une matrice anti – symétrique (T).
Cette décomposition est unique si K est un corps de caractéristique nulle.
En effet ; $\forall A \in m_k(K)$; $\exists S$, T avec S matrice symétrique et T matrice anti – symétrique tel que A = S + T.
Comme A = S + T, alors $A^t = (S+T)^t = S^t + T^t = S - T$. i.e. $A^t = S - T$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

D'où on a : $\begin{cases} S+T=A \\ S-T=A^t \end{cases} \Leftrightarrow \begin{cases} S=\dfrac{A+A^t}{2} \\ T=\dfrac{A-A^t}{2} \end{cases}$

Exercice :

Décomposer les matrices suivantes en une somme de deux matrices S et T :

a) $A=\begin{pmatrix} 3 & 4 \\ 5 & 6 \end{pmatrix}$ b) $A=\begin{pmatrix} 10 & 11 \\ 7 & 8 \end{pmatrix}$ c) $A=\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$

Solution :

a) A = S + T où $S=\dfrac{A+A^t}{2}$ et $T=\dfrac{A-A^t}{2}$

$$A^t=\begin{pmatrix} 3 & 5 \\ 4 & 6 \end{pmatrix} \Rightarrow S=\frac{1}{2}\begin{pmatrix} 6 & 9 \\ 9 & 12 \end{pmatrix} \text{ et } T=\frac{1}{2}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$\text{D'où } A=\frac{1}{2}\begin{pmatrix} 6 & 9 \\ 9 & 12 \end{pmatrix}+\frac{1}{2}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}=\begin{pmatrix} 3 & \frac{9}{2} \\ \frac{9}{2} & 6 \end{pmatrix}+\begin{pmatrix} 0 & -\frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix}$$

Vérifier au TP que $S^t = S$ et $T^t = -T$.

b) et c) à faire comme exercices.

2. MULTIPLICATION D'UNE MATRICE PAR UN SCALAIRE

a) Définition

La multiplication d'une matrice par un scalaire revient à multiplier chaque élément de la matrice par ce scalaire, c à d : si $A=\left(a_i^j\right)_{i=1\ldots m}^{j=1\ldots n}$ et $\alpha \in K$, alors $\alpha \cdot A=\alpha\left(a_i^j\right)_{i=1\ldots m}^{j=1\ldots n}=\left(\alpha a_i^j\right)_{i=1\ldots m}^{j=1\ldots n}$.

b) Exemples

1) Soient $A=\begin{pmatrix} a_1^1 & a_2^1 & a_3^1 \\ a_1^2 & a_2^2 & a_3^2 \end{pmatrix}$ et $\alpha \in K$, alors $\alpha \cdot A=\begin{pmatrix} \alpha a_1^1 & \alpha a_2^1 & \alpha a_3^1 \\ \alpha a_1^2 & \alpha a_2^2 & \alpha a_3^2 \end{pmatrix}$.

2) $3\begin{pmatrix} 1 & 3 \\ -5 & 6 \end{pmatrix}=\begin{pmatrix} 3 & 9 \\ -15 & 18 \end{pmatrix}$ c) $\dfrac{1}{2}\begin{pmatrix} 6 & 9 \\ 9 & 12 \end{pmatrix}=\begin{pmatrix} 3 & \frac{9}{2} \\ \frac{9}{2} & 6 \end{pmatrix}$

c) Propriétés

$\forall A,B \in m_K(m,n)$ et $\forall \alpha,\beta \in K$

$P_1 : \alpha(A+B)=\alpha A+\alpha B$

$P_2 : (\alpha+\beta)A=\alpha A+\beta A$

$P_3 : \alpha(\beta \cdot A)=(\alpha \cdot \beta)A$

$P_4 : 1 \cdot A = A$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

d) Conclusion

P_1, P_2, P_3, P_4 munissent le groupe additif $[m_K(m, n), +]$ d'une structure d'un espace vectoriel sur K de dimension m × n.
En particulier (m_n (K), + .) est un espace vectoriel sur K de dimension n^2.

(τ_n (K), +, ·) est un sous-espace vectoriel de (m_n (K), +, ·) de dimension $\frac{n(n+1)}{2}$.

Exemple :

a) Soit $m_2(IR) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in IR \right\}$

$\Rightarrow$ (m_2 ®, +, ·) est un espace vectoriel de dimension 4, c'est-à-dire n² = 2² = 4, cherchons une base de cet espace vectoriel.

$$\text{On sait que}: \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & d \end{pmatrix}$$

$$= a\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + b\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + c\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + d\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$= aM_1 + bM_2 + cM_3 + dM_4$$

Avec $M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$; $M_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$; $M_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$; $M_4 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

$\Rightarrow$ $\{M_1, M_2, M_3, M_4\}$ est une base de m_2 ®.

Soit $A = \begin{pmatrix} 3 & 0 \\ 0 & 5 \end{pmatrix}$ = $3M_1 + 0M_2 + 0M_3 + 5M_4$, c'est-à-dire A s'écrit comme combinaison linéaire de la base ci haute.

b) L'ensemble $\tau_2(IR) = \left\{ A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in IR \right\}$ est un sous-espace vectoriel de m_2 (IR) de dimension $\frac{n(n+1)}{2} = \frac{2(2+1)}{2} = 3$. Ainsi pour toute matrice $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$,

$$\text{On a A}; \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & c \end{pmatrix}$$

$$= a\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + b\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + c\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$= aM_1 + bM_2 + cM_4$$

$\Rightarrow$ La famille $\{M_1, M_2, M_3\}$ est une base de $\tau_2(IR)$.

TP : Montrer que (m_3 ®, +, ·) est un espace vectoriel de dimension n² = 3² = 9 et (τ_3 ( ), +, ·) est un sous-espace vectoriel de dimension $\frac{n(n+1)}{2} = \frac{3(3+1)}{2} = 6$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

3. MULTIPLICATION DES MATRICES

a) Définition

Soient $A=\left(a_i^j\right)_{i=1\ldots m}^{j=1\ldots n}$ et $B=\left(b_k^i\right)_{k=1\ldots p}^{i=1\ldots m}$ deux matrices des types respectifs (m, n) et (p, m).

Le produit des matrices A et B est la matrice $P=\left(p_k^j\right)_{k=1\ldots p}^{j=1\ldots n}$ c à d A · B = P où l'élément p_k^j se trouvant à l'intersection de la j^{ème} ligne de A et de la k^{ème} colonne de B, s'obtient en multipliant la j^{ème} ligne de A par la k^{ème} colonne de B. Un tel produit est dit ***ligne colonne***, en abrégé ***LICO***.

Ainsi $p_k^j=\sum_{i=1}^{m} a_i^j\cdot b_k^i = a_1^j\cdot b_k^1 + a_2^j b_k^2 \ldots + a_i^j\cdot b_k^i + \ldots + a_m^j\cdot b_k^m$.

Noter que l'élément p_1^1 de la matrice produit s'obtiendra en multipliant la 1ère ligne de A par la 1ère colonne de B.

b) Remarques

R$_1$. Si A est une matrice de type (m, n) et B une matrice de type (p, q), alors (A · B) n'est possible que si m = q. Dans ce cas, A · B est une matrice de type (p, n).
R$_2$. La multiplication des matrices est toujours possible si celles-ci sont carrées d'un seul et même ordre.
R$_3$. La multiplication des matrices n'est pas commutative. Mais s'il peut exister deux matrices A et B telle que A · B = B · A, on dit alors que A et B sont *commutables ou permutable*

c) Exemples

Multiplions les matrices suivantes :

a) $\begin{pmatrix} a_1^1 & a_2^1 & a_3^1 \\ a_1^2 & a_2^2 & a_3^2 \end{pmatrix}\cdot\begin{pmatrix} b_1^1 & b_2^1 \\ b_1^2 & b_2^2 \\ b_1^3 & b_2^3 \end{pmatrix}=\begin{pmatrix} a_1^1b_1^1+a_2^1b_1^2+a_3^1b_1^3 & a_1^1b_2^1+a_2^1b_2^2+a_3^1b_2^3 \\ a_1^2b_1^1+a_2^2b_1^2+a_3^2b_1^3 & a_1^2b_2^1+a_2^2b_2^2+a_3^2b_2^3 \end{pmatrix}$

b) $\begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix}\cdot\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}=\begin{pmatrix} 4 & 8 & 12 \\ 5 & 10 & 15 \\ 6 & 12 & 18 \end{pmatrix}$

c) $\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \end{pmatrix}.\begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}=\begin{pmatrix} 1+4+9 & 4+10+18 \\ 0+4+3 & 0+10+12 \end{pmatrix}=\begin{pmatrix} 14 & 32 \\ 7 & 22 \end{pmatrix}$

Exercices

1) Calculer X = A² – 4A + 6I$_n$ si : a) A = $\begin{pmatrix} 2 & 5 \\ 3 & 4 \end{pmatrix}$ et b) A = $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$

2) Calculer si possible : a) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ -1 & 0 & 4 & 3 \end{pmatrix}\cdot\begin{pmatrix} 2 & 5 & 0 \\ -3 & 6 & 1 \\ 1 & 7 & 2 \\ -4 & 2 & -1 \end{pmatrix}$; b) $\begin{pmatrix} 6 \\ 7 \\ 8 \\ 10 \end{pmatrix}\cdot\begin{pmatrix} a & b & c & d \end{pmatrix}$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

d) Propriétés

P_1. La multiplication n'est pas commutative et associative dans m_n (K),
P_2. La matrice unité d'ordre n notée I_n est l'élément neutre de la multiplication dans m_n (K), c'est-à-dire : $\forall$ A$\in$ m_n (K), on a : $A \cdot I_n = I_n \cdot A = A$
P_3. La multiplication est distributive par rapport à l'addition dans m_n (K) c'est-à-dire :
$\forall$ A, B, C $\in$ m_n (K), on a : $(A + B) \cdot C = A \cdot B + A \cdot C$.
$P_4 : {}^t(A)(B) = {}^tB.{}^tA$

e) Conclusion

(m_n (K), +, ·) est un anneau unitaire non commutatif.
NB : Soit A une matrice carrée d'ordre n à coefficients dans K.
S'il existe une matrice B $\in$ m_n (K) telle que $A \cdot B = B \cdot A = I_n$, alors A est dite matrice inversible et B est la matrice inverse de A. On note alors dans ce cas que $B = A^{-1}$.

Exemple :

Inversez la matrice $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ si possible.

Soit $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ matrice inverse de A, si elle existe, alors $A \cdot B = B \cdot A = I_2$.

On a : $A \cdot B = I_2 \Leftrightarrow \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$$\Leftrightarrow \begin{pmatrix} a+2c & b+2d \\ 3a+4c & 3b+4d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\Leftrightarrow \begin{cases} a+2c=1 \\ 3a+4c=0 \end{cases} \quad \text{et} \quad \begin{cases} b+2d=0 \\ 3b+4d=1 \end{cases}$$

$$\Leftrightarrow \begin{cases} a=-2 \\ c=\dfrac{3}{2} \end{cases} \quad \text{et} \quad \begin{cases} b=1 \\ d=-\dfrac{1}{2} \end{cases}$$

Donc, $B = \begin{pmatrix} -2 & 1 \\ \dfrac{3}{2} & -\dfrac{1}{2} \end{pmatrix}$

Vérifions que $B \cdot A = I_2$: $\begin{pmatrix} -2 & 1 \\ \dfrac{3}{2} & -\dfrac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$\Rightarrow$ B est la matrice inverse de A.

TP : Inversez les matrices suivantes : a) $A = \begin{pmatrix} 3 & 4 \\ 5 & 6 \end{pmatrix}$ b) $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

C. MATRICE ECHELONNEE

1. Définition 1

Soit $A = \left(a_i^j\right)_{i=1\ldots m}^{j=1\ldots n}$ une matrice de type (m, n) à coefficients dans K.
A est dite matrice échelonnée si ses lignes satisfont aux conditions suivantes :

1° Toute ligne nulle n'est suivie que des lignes nulles.
2° L'indice colonne de tout premier terme non nul d'une ligne non nulle est inférieur à l'indice colonne de tout premier terme non nul de la ligne suivante.

C'est-à-dire A est une matrice échelonnée si le nombre de zéros précédant chaque premier élément non nul d'une ligne augmente de ligne en ligne jusqu'à ce qu'il n'y ait que des lignes nulles. Ainsi chaque premier élément non nul d'une ligne non nulle d'une matrice échelonnée est appelé ***élément distingué*** ou ***élément remarquable***.

$$\begin{pmatrix} a_1^1 & a_2^1 & \ldots & a_m^1 \\ a_1^2 & a_2^2 & \ldots & a_m^2 \\ \ldots & \ldots & \ldots & \ldots \\ a_1^n & a_2^n & \ldots & a_m^n \end{pmatrix} \Rightarrow \begin{pmatrix} a_1^1 & a_2^1 & \cdots & a_m^1 \\ 0 & a_2^2 & \cdots & a_m^2 \\ \cdots & \cdots & a_r^r & a_m^r \\ 0 & 0 & 0 & a_m^n \end{pmatrix}$$ est une matrice échelonnée.

Exemples

a) $\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ 0 & b_2 & b_3 & b_4 \\ 0 & 0 & c_3 & c_4 \\ 0 & 0 & 0 & d_4 \end{pmatrix}$: a_1, b_2, c_3 et d_4 sont les éléments distingués ou remarquables.

b) $\begin{pmatrix} 1 & 2 & 0 & 0 & 3 \\ 0 & 0 & 5 & 6 & 7 \\ 0 & 0 & 0 & 7 & 5 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$ c) $\begin{pmatrix} 5 & 1 & 4 \\ 0 & 3 & 6 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ sont des matrices échelonnées.

2. Définition 2

Une matrice échelonnée est dite matrice échelonnée et réduite par les lignes si :
1° les éléments remarquables sont les seuls éléments non nuls de leurs colonnes respectives.
2° chacun étant égal à 1.

Exemple :

$$\begin{pmatrix} 1 & 2 & 5 & 8 & 3 \\ 0 & 0 & 5 & 6 & 7 \\ 0 & 0 & 0 & 7 & 5 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$: Matrice échelonnée réduite.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

3. Opérations élémentaires sur les lignes (réduction d'une matrice à la forme échelonnée)

θ_1. On peut inter changer la i[ème] ligne et la j[ème] ligne : $L_i \leftrightarrow L_j$.

Soit par exemple le matrice $\begin{pmatrix} 0 & 3 & 5 & 6 \\ 1 & 5 & 8 & 9 \\ 4 & 6 & 10 & 2 \end{pmatrix} \begin{array}{l} L_1 \\ L_2 \\ L_3 \end{array} \sim L_1 \leftrightarrow L_2 \begin{pmatrix} 1 & 5 & 8 & 9 \\ 0 & 3 & 5 & 6 \\ 4 & 6 & 10 & 2 \end{pmatrix}$ ou

$$\sim L_1 \leftrightarrow L_3 \begin{pmatrix} 4 & 6 & 10 & 2 \\ 1 & 5 & 8 & 9 \\ 0 & 3 & 5 & 6 \end{pmatrix}$$

θ_2. On peut remplacer L_i par $\alpha L_j + L_i$ avec $\alpha \in K^*$ ie $L_i \leftrightarrow \propto L_j + L_i$ Noter que le premier nombre non nul de L_j est 1

$$\begin{pmatrix} 1 & 5 & 8 & 9 \\ 0 & 3 & 5 & 6 \\ 4 & 6 & 10 & 2 \end{pmatrix} \begin{array}{l} L_1 \\ L_2 \\ L_3 - 4L_1 + L_3 \end{array} \sim \begin{pmatrix} 1 & 5 & 8 & 9 \\ 0 & 3 & 5 & 6 \\ 0 & -14 & -22 & -34 \end{pmatrix}$$

ici, on a transformé 4 en 0 sur la 3[ème] ligne.

θ_3. On peut remplacer L_i par $\alpha L_j + \beta L_i$ avec $\alpha, \beta \in K^*$ i.e. $L_1 \leftrightarrow \alpha L_j + \beta L_i$
Noter dans ce cas que le premier nombre non nul de la ligne de référence (L_j) est un nombre différent de 1

Exemple :

$$\begin{pmatrix} 1 & 5 & 8 & 9 \\ 0 & 3 & 5 & 6 \\ 0 & -14 & -22 & -34 \end{pmatrix} \begin{array}{l} L_1 \\ L_2' \\ L_3 \leftrightarrow 14L_2 + 3L_3' \end{array} \sim \begin{pmatrix} 1 & 5 & 8 & 9 \\ 0 & 3 & 5 & 6 \\ 0 & 0 & 4 & 18 \end{pmatrix}$$

θ_4. On peut remplacer la 1[ère] ligne par αL_i i.e. $L_i \leftrightarrow \alpha L_i$ avec $\alpha \in K^*$

Exemple

$$\begin{pmatrix} 1 & 0 & 0 & 9 \\ 0 & 3 & 0 & 6 \\ 0 & 0 & 28 & -18 \end{pmatrix} \begin{array}{l} \\ L_2 \Leftrightarrow \tfrac{1}{3} L_2 \\ L_3 \Leftrightarrow \tfrac{1}{28} L_3 \end{array} \sim \begin{pmatrix} 1 & 0 & 0 & 9 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & -\tfrac{9}{14} \end{pmatrix}$$

Exemples
Résoudre les matrices suivantes à la forme échelonnée.

$$a)\ A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \quad b)\ A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \\ 3 & 6 & 11 & 13 \\ 4 & 9 & 9 & 14 \end{pmatrix} \quad c)\ A = \begin{pmatrix} 2 & 1 & -1 & 4 & 5 \\ 3 & 4 & 6 & -3 & 2 \\ -5 & 6 & 7 & 10 & 11 \end{pmatrix}$$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Solution

$$a)\ A=\begin{pmatrix}1&2&3\\4&5&6\\7&8&9\end{pmatrix}\begin{matrix}L_1\\L_2\leftrightarrow -4L_1+L_2\\L_3\leftrightarrow -7L_1+L_3\end{matrix}\sim\begin{pmatrix}1&2&3\\0&-3&-6\\0&-6&-12\end{pmatrix}\begin{matrix}L_1\\L'_2\\L'_3\leftrightarrow -2L'_2+L_3\end{matrix}\sim\begin{pmatrix}1&2&3\\0&-3&-6\\0&0&0\end{pmatrix}$$

$$b)\ A=\begin{pmatrix}1&2&3&4\\2&4&9&10\\3&6&11&13\\4&9&9&14\end{pmatrix}\begin{matrix}L_1\\L_2\leftrightarrow -2L_1+L_2\\L_3\leftrightarrow -3L_1+L_3\\L_4\leftrightarrow -4L_1+L_4\end{matrix}\sim\begin{pmatrix}1&2&3&4\\0&0&3&4\\0&0&2&1\\0&1&-3&-2\end{pmatrix}\begin{matrix}L_1\\L'_2\\L'_3\\L'_4\end{matrix}\underset{L_2\leftrightarrow L_4'}{\sim}\begin{pmatrix}1&2&3&4\\0&1&-3&-2\\0&0&2&1\\0&0&3&4\end{pmatrix}\begin{matrix}L_1\\L_2\\L_3\\L'_4\leftrightarrow -3L_3+2L_4\end{matrix}$$

$$\sim\begin{pmatrix}1&2&3&4\\0&1&-3&-2\\0&0&2&1\\0&0&0&5\end{pmatrix}$$

D. MATRICE ET APPLICATIONN LINEAIRE

1. Rappel sur l'application linéaire

a) Définition 1

Soient E, F deux espaces vectoriels de dimensions finies sur K et $f : E \to F$ une application. Alors f est dite application linéaire si :

1° $\forall\ u, v \in E : f(u + v) = f(u) + f(v)$

2° $\forall\ \alpha \in K, \forall\ u \in E : f(\alpha u) = \alpha f(u)$

b) Définition 2 :

$f : E \to F$ est dite application linéaire si : $\forall\ \alpha, \beta \in K, \forall\ u, v \in E : f(\alpha u + \beta v) = \alpha f(u) + \beta f(v)$.

Noter que si $f : E \to F$ est une application linéaire, alors $f(0_E) = 0_F$ et $f(1_E) = 1_F = 1$.

Exemples :

L'homothétie (h) de rapport k de R^3 dans R^3 définie comme suit :

$h : R^3 \to R^3$

$(x, y, z) \to h(x, y, z) = (kx, ky, kz)$ est une application linéaire.

En effet :

1° $\forall\ u = (x, y, z), v = (x', y', z') \in R^3$:

$h(u + v) = h[(x, y, z) + (x', y', z')]$

$= h(x + x', y + y', z + z')$

$= [k(x + x'), k(y + y'), k(z + z')]$

$= (kx + kx', ky + ky', kz + kz')$

$= (kx, ky, kz) + (kx', ky', kz')$

$= h(u) + h(v)$ (1ère condition).

2° $\forall\ \alpha \in R, \forall\ u = (x, y, z) \in R^3$:

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

$h(\alpha u) = h[\alpha(x, y, z)]$
$= h(\alpha x, \alpha y, \alpha z)$
$= (k\alpha x, k\alpha y, k\alpha z)$
$= (\alpha(kx), \alpha(ky), \alpha(kz))$
$= \alpha(kx, ky, kz)$
$= \alpha h(u)$ (2ème condition).

La symétrie (S) par rapport à l'origine des axes de coordonnées définie ci – dessous est une application linéaire i.e.:
$s : IR^2 \rightarrow IR^2$
$(x, y) \rightarrow s(x, y) = (-x, -y)$

3° La projection (p) de R^3 sur R^2 définie comme suit est une application linéaire :
$p : \quad R^3 \rightarrow R^2$
$(x, y, z) \rightarrow p(x, y, z) = (x, y)$.

4° $f : IR^3 \rightarrow IR$
$(x, y, z) \rightarrow f(x, y, z) = (2x - y + z \,;\, -x + 2y - 3z)$ est une application linéaire.

Par contre $f : IR \rightarrow IR$
$x \rightarrow f(x) = 2x + 3$ n'est pas linéaire.

2. Définition :

Soient E, F deux K espace et f ; $E \rightarrow F$, une application linéaire.
Déf$_1$: on appelle noyau de f noté Kerf l'ensemble des éléments de E qui ont pour image le zéro de F, càd $\text{Kerf} = \{u \in F : f(u) = 0_F\} \subset E$.

Déf$_2$: on appelle image de f notée Imf l'ensemble des éléments de F qui ont au moins un antécédant dans E .i.e. $\text{Imf} = \{f(u) : u \in E\} \subset F$.

Exemples :
Soit $p : IR^3 \rightarrow IR^2$
$(x, y, z) \rightarrow p(x, y, z) = (x, y)$ une application linéaire.
Cherchons Kerp
On a : $\text{Kerp} = \{(x, y, z) \in IR^3 : p(x, y, z) = (0,0)\}$
$= \{(x, y, z) \in IR^3 : (x, y) = (0,0)\}$
$= \{(x, y, z) \in IR^3 : x = 0 \text{ et } y = 0$
$= \{(0, 0, z) : z \in IR\}$
Cherchons aux exercices Kerh, Kerj et Kerf des exemples a, b et c ci – dessus.

3. Remarque :

Soient E, F deux K – espaces notons par $\mathcal{L}(E, F)$ l'ensemble des applications linéaires de E vers F et montrons aux exercices que $[\mathcal{L}(E,F), + , \bullet)$ est un K espace

4. Théorème (Matrice et application linéaire)

Soient E et F deux espaces vectoriels des dimensions finies sur le corps commutatif K (dimE = m et dimF = n) se donner une application linéaire f entre E et F revient a se donner une matrice A de type (m, n) et à coefficient dans un corps commutatif K et réciproquement c à d : l'application $\delta : \mathcal{L}(E, F) \to m_k(m, n)$

$f \to \delta(f) = A$ est un isomorphisme d'espaces vectoriels,

Si B = $\{e_1, e_2, e_3, \ldots, e_m\}$ est une base de E et B' = $\{u_1, u_2, u_3, \ldots, u_n\}$ une base de F. Alors d'après le théorème ci – dessus, à $f \in \mathcal{L}(E, F)$, on va associer une matrice

$A = \left(a_i^j\right)_{i=1,\ldots m}^{j=1,\ldots n}$ tell que $\boxed{f(e_i) = \sum_{j=1}^{n} a_i^j u_j}$

En effet, $\forall$ i = 1, …m, on a : $e_i \in E$ et comme

Parc que f : E $\to$ F est une application, alors $f(e_i) \in F$

$f(e_i) \in F$ et B' = $\{u_1, u_2, \ldots, u_n\}$ une base de F

alors $f(e_i) = a_i^1 u_1 + a_i^2 u_2 + \ldots + a_i^n u_n$

Ainsi, $f(e_i) = a_1^1 u_1 + a_1^2 u_2 + \ldots + a_1^n u_n$

$f(e_2) = a_2^1 u_1 + a_2^2 u_2 + \ldots + a_2^n u_n$

$\vdots$

$f(e_m) = a_m^1 u_1 + a_m^2 u_2 + \ldots + a_m^n u_n$

La transposé de matrice des coefficients de (u_j) est dite matrice représentative de f par rapport aux base B et B', on la note par : m(f, B, B')

$$D'ou\ \ A = m(f, B, B') = \begin{pmatrix} a_1^1 & a_2^1 \ldots\ldots a_m^1 \\ a_1^2 & a_2^2 \ldots\ldots a_m^2 \\ \vdots & \vdots \quad\quad \vdots \\ a_1^n & a_2^n \ldots\ldots a_m^n \end{pmatrix}$$

En résumé, si on donne f : E $\to$ F

U $\to$ f(u) = v et on voudra la représenter matriciellement.

Quatre étape sont à suivre :

1°) Choisir des bases de E et F par exemple, prendre

B = $\{e_1, e_2, \ldots, e_n\}$ base de E

B' = $\{u_1, u_2, \ldots, u_n\}$ base de F.

2°) chercher les images de vecteurs de base B de Epar f

3°) exprimer chaque image du vecteur de base B de E par rapport à la base de F.

.

4°) Transposer de la matrice des coefficients des $(u_j)_{j=1,\ldots,n}$

Exemple :

a) Représentez matriciellement les applications linéaires ci-dessous par rapport aux bases canoniques des espaces donnés.

a_1) f : IR² $\to$ IR²

(x,y) $\to$ f(x,y) = (2x – y, 3x + 4y) une application linéaire

Solution :

1° On sait que la base canonique de IR^2 est :B = $\{e_1 = (1,0); e_2 = (0,1)\}$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

2° Chercher les images des vecteurs e_1 et e_2 par f

On a : ▪ $f(e_1)=f(1,0)=(2.1-0\ ;3-1+4.0)=(2,3)$

▪$f(e_2)=f(0,1)=(2.0-1\ ;3.0+4.1)=(-1,4)$

D'où $F(e_1)=(2,3)$ et $f(e_2)=(-1,4)$.

3° Exprimons ces images dans la base B de IR²

On a $(2,3)=2e_1+3e_2$ et $(-1,4)=-1e_1+4e_2$ car B est la base canonique de IR²

D'ou $\begin{cases} f(e_1)=2e_1+3e_2 \\ f(e_2)=-e_1+4e_2 \end{cases}$ et $m(f,B,B')=\begin{pmatrix} 2 & -1 \\ 3 & 4 \end{pmatrix}$

$a_2)$ $g : IR^3 \to IR^3$

$(x, y, z) \mapsto f(x, y, z) = (x + y\ ; y + z\ ; x + z)$ une application linéaire aux exercices.

$a_3)$ $h : IR^3 \to IR^2$

$(x, y, z) \mapsto f(x, y, z) = (x + y\ ; 25x - y + 3z)$ une application linéaire aux execices.

$a_4)$ $f : IR^3 \to IR^2$

$(x, y, z) \mapsto f(x, y, z) = (2x + y - 3z\ ; x - 2y)$ une application linéaire aux exercices.

b) Représentez l'application linéaire g de l'exemple a_4 ci – dessus par rapport aux bases :

$B_1 = \{e_1 = (1, 1, 0)\ ; e_2 = (1, -1, 1)\ ; e_3 = (0, 0, 1)\}$ de IR^3 et

$B_2 = \{u_1 = (1\ ,2)\ ; u_2 = (1, 2)\}$ de IR²

Réponses

On a : $f(e_1) = f(1, 1, 0) = (3, 1)$ et $(3, -1) = a.u_1 + b.u_2$

$f(e_2) = f(1, -1, 1) = (-2, 3)$ et $(-2, 3) = a.u_1 + b.u_2$

$f(e_3) = f(0, 0, 1) = (-3, 0)$ et $(-3\ , 0) = a.u_1 + b.u_2$

Déterminons les scalaires a et b

En effet, $a.n_1 + b.n_2 = (3, -1) \Leftrightarrow a(1, 2) + b(2, 1) = (3, 1)$

$$\Leftrightarrow \begin{cases} a+2b=3 \\ 2a+b=-1 \end{cases} \Leftrightarrow a = \frac{-5}{3} \text{ et } b = \frac{7}{3}$$

$$\Leftrightarrow \begin{cases} a+2b=-2 \\ 2b+b=3 \end{cases} \Leftrightarrow a = \frac{8}{3} \text{ et } b = \frac{-7}{3}$$

$$\Leftrightarrow \begin{cases} a+2b=-3 \\ 2a+b=0 \end{cases} \Leftrightarrow a = 1 \text{ et } b = -2$$

$$\text{D'où } \begin{cases} f(e_1)=(3,-1)=-\frac{5}{3}u_1+\frac{7}{5}u_2 \\ f(e_2)=(-2,3)=\frac{8}{3}u_1-\frac{7}{3}u_2 \\ f(e_3)=(-3,0)=u_1-2u_2 \end{cases} \quad \text{Et } m(f,B_1,B_2) = \begin{pmatrix} -\frac{5}{3} & \frac{8}{3} & 1 \\ \frac{7}{3} & -\frac{7}{3} & -2 \end{pmatrix}$$

Exercices :

Idem, mais avec les bases

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

$B_3 = \{e_1 = (0,1,1); e_2 = (1,1,-1), e_3 = (1,0,1) \}$ de IR^3

$B'_3 = \{u_1 = (3,1); u_2 = (3,1) \}$ de IR^2

Réciproquement

Soient E, F deux K – espace de dimensions réciproques m et n et f : E $\to$ F une application linéaire représentée canoniquement par la matrice

$A = (\left(a_i^j\right)_{i=1,\dots,m}^{j=1,\dots,n}$

Si X$\in$ E, déterminer alors f(x) = ?

Schématiquement, on a la situation suivante

$E \xrightarrow[A=\left(a_j^i\right)]{f} F$

$\underset{1\le i\le m}{\left(e_i\right)}\ \underset{1\le j\le m}{\left(u_j\right)}$

$X \to f(x) = ?$

Comme X$\in$E et (e_i) une base de E alors $X = \sum_{i=1}^{m} x_i e_i$

$\Rightarrow X = (x_1 , x_2, \dots, x_n)$

X$\in$E et f : E $\to$ F, une application implique que f(X)$\in$F, c à d $\exists$Y$\in$F tel que f(X) = Y

Y$\in$F et (u_j) une base de F$\Rightarrow\exists y^1, y^2, \dots, y^n \in$ K tel que $Y = \sum_{j=1}^{n} y' u_j$,i.e. $Y = (y^1, y^2,\dots,y^h)$

$f(X) = Y \Leftrightarrow A.X^t = Y^t$.. D'où $f(x_1 , x_2 , \dots, x_n) = (y^1, y^2, \dots,y^n)$

Exemple :

Soient f : $IR^3 \to IR^2$ une application linéaire représentée canoniquement par

$A = \begin{pmatrix} 2 & 1 & -3 \\ 1 & -2 & 0 \end{pmatrix}$

Déterminer f(x), sachant que X = (x, y, z) $\in IR^3$

Solution

En effet, x = (x, y, z) $\in IR^3$ et f : $IR^3 \to IR^2$ une application linéaire implique qu'il existe $Y = (y^1, y^2) \in IR^2$ tel que f(x) = Y

Ainsi $f(X) = y \Leftrightarrow AX^t = Y^t$

$$\Leftrightarrow \begin{pmatrix} 2 & 1 & -3 \\ 1 & -2 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} y^1 \\ y^2 \end{pmatrix} \Leftrightarrow \begin{pmatrix} 2x + y - 3x \\ x - 2y \end{pmatrix} = \begin{pmatrix} y^1 \\ y^2 \end{pmatrix}$$

$$\Leftrightarrow \begin{cases} y^1 = 2x + y - 3z \\ y^2 = x - 2y \end{cases}$$

D'où $f(X) = Y \Leftrightarrow f(x, y, z) = (y^1, y^2) = (2x + y - 3z , x - 2y)$.

Finalement f(x, y, z) = (2x + y – 3y, x – 2y)

Exercices

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Soit f : $IR^3 \rightarrow IR^2$ une application linéaire déterminé par A = $\begin{pmatrix} 3 & 5 \\ 4 & 6 \end{pmatrix}$ par rapport à la base canonique de IR²
Déterminer f(X) = ? avec X = (x, y) $\in$ IR²

Solution
X = (x, y)$\in$ IR² $\Rightarrow \exists$ y = $(y^1, y^2) \in$ IR² tel que f(x) = Y
f(x) = Y $\Leftrightarrow$ A . $X^t = Y^t$

$$\Leftrightarrow \begin{pmatrix} 3 & 5 \\ 4 & 6 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y^1 \\ y^2 \end{pmatrix} \Rightarrow \begin{pmatrix} 3x+5y \\ 4x+6y \end{pmatrix} = \begin{pmatrix} y^1 \\ y^2 \end{pmatrix}$$

$$\Leftrightarrow \begin{cases} y_1 = 3x+5y \\ y_2 = 4x+6y \end{cases}$$

f(x, y) = (y_1, y_2) et $y_1 = 3x + 5y$ et $y_2 = 4x + 6y$, donc f(x, y) = (3x + 5y ; 4x + 6y)

E. DETERMINANT

1. Généralites

a) Définition :

Soit A une matrice carrée d'ordre 2 à coefficient dans un corps commutatif K.

C.à.d. A = $\begin{pmatrix} a_1^1 & \ldots\ldots & a_n^1 \\ \vdots & & \vdots \\ a_1^n & \ldots\ldots & a_n^n \end{pmatrix}$

Alors le déterminant de A noté dét(A) ou $|A|$ est un scalaire appartenant à K et défini comme suit :

$$|A| = \begin{vmatrix} a_1^1 & a_2^1 \ldots\ldots a_n^1 \\ a_1^2 & a_2^2 \ldots\ldots a_n^2 \\ \vdots & \vdots \qquad \vdots \\ a_1^n & a_2^n \ldots\ldots a_n^n \end{vmatrix} = \sum_{S \in \delta_n} \varepsilon(s) a_{\rho_1}^1 a_{\rho_2}^2 \ldots a_{\rho_n}^n$$

Où * δ_n est l'ensemble des permutations de n éléments de E avec E = {1, 2, 3, …, n}
* ε (s) est la signature de la permutation (s) avec S = $(\rho_1, \rho_2, \ldots, \rho_n)$ une permutation de E ie ; ε (s) = $(-1)^{I(s)}$
* I(S) est le nombre d'inversions. ie. Le nombre de couples (ρ_i, ρ_j) Tel que i < j $\Rightarrow \rho_i \succ \rho_j$
* $a_{\rho_1}^1 . a_{\rho_2}^2 \ldots a_{\rho_n}^n$ étant un produit de n facteurs dont chacun appartient à une ligne et une seule de A et une colonne et une seule de A.
Cette sommation s'étend aux n! termes

Exemple
a) Pour E = {1,2}, on a $\delta_2 = \{S_1 = (1,2); S_2 = (2,1)\}$
$\Rightarrow I(S_1) = 0$ et $\varepsilon(S_1) = 1$; I(S2) $= 1, ie (2,1) et I(S_2) = -1$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

b) Pour E={1,2,3} ; on a : $\delta_3 = \{S_1 = 123; S_2 = 132; S_3 = (213); S_4 = (231), S_5 = (312); S_6 = (321)\}$

Nombre d'inversions = 0 1 1 2 2 3

Pour la permutation $S_5 = (3, 1, 2)$ par exemple, on a les couples (3, 1) et (3, 2).
Pour $S_6 = (3, 2, 1)$ on a les couples (3, 2) ; (3, 1) et (2, 1). D'où $I(S_5) = 2$ et $I(S_6) = 3$

b) Calcul de déterminant

Déterminant d'ordre 1

$$\left|a_1^1\right| = a_1^1 \qquad \text{Exemple : } |4| = 4 \; ; \; |-4| = -4$$

Déterminant d'ordre 2

On a : $$\begin{vmatrix} a_1^1 & a_2^1 \\ a_1^2 & a_2^2 \end{vmatrix} = \sum_{s\in\delta_2} \varepsilon(s) a^1_{\rho_1} a^2_{\rho_2} \quad \text{Avec} \quad \delta_2 = \left\{S_1 = (1,2); S_2 = (2,1)\right\}$$

$$= \varepsilon(S_1) a_1^1 a_2^2 + \varepsilon(S_2) a_2^1 a_1^2 = a_1^1 a_2^2 - a_2^1 a_1^2 \text{ car } \varepsilon(S_1) = 1 \text{ et } \varepsilon(S_2) = -1$$

Exemple : $\begin{vmatrix} 3 & 7 \\ 4 & 8 \end{vmatrix} = 3.8 - 4.7 = 24 - 28 = -4$ et $\begin{vmatrix} 5 & -6 \\ 4 & 3 \end{vmatrix}$ =5.3-(-6).4=15+24=39

Déterminant d'ordre 3

$$\begin{vmatrix} a_1^1 & a_2^1 & a_3^1 \\ a_1^2 & a_2^2 & a_3^2 \\ a_1^3 & a_2^3 & a_3^3 \end{vmatrix} = \sum_{s\in\delta_2} \varepsilon(s) a^1_{\rho_1} a^2_{\rho_2} a^3_{\rho_3}$$

$$\text{avec } \delta_3 = \left\{ S_1 = \underset{1}{123}; S_2 = \underset{-1}{132}; S_3 = \underset{-1}{213}; S_4 = 231; S_5 = 312; \underset{1}{S_6} = \underset{-1}{321} \right\}$$

$$\sum_{S\in\delta_3} \varepsilon(s) a^1_{\rho_1} a^2_{\rho_2} a^3_{\rho 3} \qquad avec \delta_3 = \{S_1 = 123; S_2 = 132; S_3 = 213; S_4 = 231; S_5 = 312; S_6 = 321\}$$

$$= \varepsilon(s_1)\, a^1_{\rho_1} a^2_{\rho_2} a^3_{\rho_3} + \varepsilon(s_2)\, a^1_{\rho_1} a^2_{\rho_2} a^3_{\rho_3} + \varepsilon(s_3)\, a^1_{\rho_1} a^2_{\rho_2} a^3_{\rho_3} + \varepsilon(s_4)\, a^1_{\rho_1} a^2_{\rho_2} a^3_{\rho_3}$$
$$+ \varepsilon(s_5)\, a^1_{\rho_1} a^2_{\rho_2} a^3_{\rho_3} + \varepsilon(s_6)\, a^1_{\rho_1} a^2_{\rho_2} a^3_{\rho_3}$$
$$= a_1^1 a_2^2 a_3^3 - a_1^1 a_3^2 a_2^3 - a_2^1 a_1^2 a_3^3 + a_2^1 a_3^2 a_1^3 + a_3^1 a_1^2 a_2^3 - a_3^1 a_2^2 a_1^3$$
$$= (a_1^1 a_2^2 a_3^3 + a_2^1 a_3^2 a_1^3 + a_3^1 a_1^2 a_2^3) - (a_1^1 a_3^2 a_2^3 + a_2^1 a_1^2 a_3^3 + a_3^1 a_2^2 a_1^3)$$

Ceci est matérialisé par le schéma ci-dessous dit règle de Sarrüs

1ère forme de la règle de Sarrüs (R.S.)

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

$$\left|\begin{array}{ccc:cc} a_1^1 & a_2^1 & a_3^1 & a_1^1 & a_2^1 \\ a_1^2 & a_2^2 & a_3^2 & a_1^2 & a_2^2 \\ a_1^3 & a_2^3 & a_3^3 & a_1^3 & a_2^3 \end{array}\right| = (a_1^1a_2^2a_3^3 + a_2^1a_3^2a_1^3 + a_3^1a_1^2a_2^3) - a_3^1a_2^2a_1^3 - a_1^1a_3^2a_2^3 - a_2^1a_2^2a_3^3$$

Exemple :

Soit A = $\begin{pmatrix} -2 & 5 & -1 \\ 1 & 6 & 4 \\ 4 & 0 & -3 \end{pmatrix}$; calculer |A|

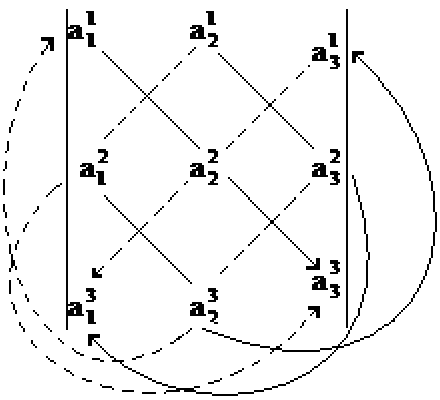
On a : |A| = $\left|\begin{array}{ccc:cc} -2 & 5 & -1 & -2 & 5 \\ 1 & 6 & 4 & 1 & 6 \\ 4 & 0 & -3 & 4 & 0 \end{array}\right|$ = 36 + 80 + 0 – (-24 +0 -15) = 116 + 39 = 155

2^e forme de la règle de Sarrüs

$$\begin{array}{|ccc|} a_1^1 & a_2^1 & a_3^1 \\ a_1^2 & a_2^2 & a_3^2 \\ a_1^3 & a_2^3 & a_3^3 \\ \hline a_1^1 & a_2^1 & a_3^1 \\ a_1^2 & a_2^2 & a_3^2 \end{array} = a_1^1a_2^2a_3^3 + a_2^1a_3^2a_1^3 + a_1^2a_2^3a_3^1 - a_1^3a_2^2a_3^1 - a_3^2a_2^3a_1^1 - a_1^2a_2^1a_3^3$$

Exemple : $\begin{array}{|ccc|} \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \mathbf{4} & \mathbf{5} & \mathbf{6} \\ \mathbf{1} & \mathbf{0} & \mathbf{-2} \\ \hline \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \mathbf{4} & \mathbf{5} & \mathbf{6} \end{array}$ = -20+0+12 -15-0+16 = 3

3^e forme de la règle de Sarrüs



Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

2. Propriétés

P$_1$. Le déterminant d'une matrice triangulaire ou diagonale est égal au produit des éléments diagonaux

Exemple : $\begin{vmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{vmatrix} = a.d.f \;;\; \begin{vmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{vmatrix} = a.b.c$

P$_2$. Une matrice A et sa transposée (A^t) ont le même déterminant c a d $|\mathbf{A}| = |\mathbf{A^t}|$

Exemple : $A = \begin{pmatrix} 3 & 5 \\ 6 & 4 \end{pmatrix} \Rightarrow A^t = \begin{pmatrix} 3 & 6 \\ 5 & 4 \end{pmatrix}$

On a $|A| = \begin{vmatrix} 3 & 5 \\ 6 & 4 \end{vmatrix} = -18$ et $|A^t| = \begin{vmatrix} 3 & 6 \\ 5 & 4 \end{vmatrix} = -18$

P$_3$. Un déterminant est fonction linéaire de chacunes de ses colonnes ou de ses lignes.

Ie. $|A| = \begin{array}{c} \begin{vmatrix} a_1^1 & a_2^1 \cdots & a_n^1 \\ a_1^2 & a_2^2 \cdots & a_n^2 \\ \vdots & \vdots & \vdots \\ a_1^n & a_2^n \cdots & a_n^n \end{vmatrix} \begin{matrix} L_1 \\ L_2 \\ \vdots \\ L_n \end{matrix} \\ \begin{matrix} C_1 & C_2 & \cdots\cdots & C_n \end{matrix} \end{array} = \det(C_1, C_2, \ldots, C_n) = \det(L_1, L_2, \ldots, L_n)$

Conséquences :

C$_1$. Toute permutation de deux rangées d'indice différents transforme le det(A) en – det(A) càd : $\det(C_1, C_2, \ldots, C_n) = -\det(C_2, C_1, \ldots, C_n)$ ou $\det(L_1, L_2, \ldots L_n) = -\det(L_2, L_1, \ldots, L_n)$

Exemple : $\begin{vmatrix} 1 & 3 \\ 5 & 8 \end{vmatrix} = -7 \Rightarrow \begin{vmatrix} 3 & 1 \\ 8 & 5 \end{vmatrix} = -\begin{vmatrix} 1 & 3 \\ 5 & 8 \end{vmatrix} = -(-7) = 7$

C$_2$. Un déterminant est nul si une rangée est nulle ou deux rangées parallèles d'indices différents sont identiques ou proportionnelles i.e. $C_i = \alpha\, C_j$ ou $L_j = \beta\, L_i$

Exemple : $\begin{vmatrix} 0 & 5 & 1 \\ 0 & 6 & 2 \\ 0 & 7 & 3 \end{vmatrix} = 0 \;;\; \begin{vmatrix} 1 & 2 & 3 \\ 2 & 5 & 6 \\ 3 & 1 & 9 \end{vmatrix} = 0$ car $C_3 = 3\, C_1$

$\begin{vmatrix} 1 & 2 & 5 \\ 1 & 2 & 5 \\ 1 & 4 & 6 \end{vmatrix} = 0$ car L_1 et L_2 sont identiques

P$_4$. $\forall \lambda \in K^*$; $\lambda\det(C_1, C_2, \ldots, C_n) = \det(\lambda C_1, C_2, \ldots, C_n) = \det(C_1, C_2, \ldots, \lambda C_i, \ldots, C_n)$
i.e. Multiplier un déterminant par un scalaire revient à multiplier ce scalaire soit par une colonne soit par une ligne.

P_5. $\det(C_1, C_2, \dots, C_i + C_j, \dots, C_n) = \det(C_1, C_2, \dots, C_i, \dots, C_n) + \det(C_1, C_2, \dots, C_j, \dots, C_n)$

P_6. La valeur d'un déterminant ne change pas si on ajoute à une rangée la combinaison linéaire des autres rangées.

Càd, $\det(C_1, C_2, \dots, C_n) = \det(C_1 + \sum_{j=2}^{n} \alpha_j C_j , C_2, \dots, C_n)$

$= \det(C_1 + \alpha_2 C_2 + \alpha_3 C_3 + \dots + \alpha_n C_n , C_2, \dots, C_n)$

Exemples

a) $\begin{vmatrix} 3 & 5 \\ 7 & 8 \end{vmatrix} = -11 \Rightarrow (-3) \begin{vmatrix} 3 & 5 \\ 7 & 8 \end{vmatrix} = -3\,(-11) = 33$

D'après P_4, on a : $(-3) \begin{vmatrix} 3 & 5 \\ 7 & 8 \end{vmatrix} = \begin{vmatrix} (-3)3 & (-3)5 \\ 7 & 8 \end{vmatrix} = \begin{vmatrix} -9 & -15 \\ 7 & 8 \end{vmatrix} = -72 + 105 = 33$

b) $\begin{vmatrix} 1+3 & 6 \\ 2+4 & 5 \end{vmatrix} = \begin{vmatrix} 1 & 6 \\ 2 & 5 \end{vmatrix} + \begin{vmatrix} 3 & 6 \\ 4 & 5 \end{vmatrix} = -7 -9 = -16$, (d'après P_5)

Vérification :

$\begin{vmatrix} 1+3 & 6 \\ 2+4 & 5 \end{vmatrix} = \begin{vmatrix} 4 & 6 \\ 6 & 5 \end{vmatrix} = 20 - 36 = -16$

c) Montrons que $\det(C_1,C_2,C_3) = \det(C_1+\lambda C_2 ,C_2 , C_3)$.

En effet, $\det(C_1+\lambda C_2 ,C_2 , C_3) = \det(C_1 ,C_2 , C_3) + \det(\lambda C_2 ,C_2 , C_3)$, en vertu de P_5
$= \det(C_1,C_2 , C_3)$ car $\det(\lambda C_2,C_2 , C_3) = 0$ parcque $C_1 = \lambda C_2$

Tout comme : $\det(C_1,C_2 , C_3) = \det(C_1, C_2+\alpha C_1+bC_3 , C_3)$

En effet, $\det(C_1, C_2+\alpha C_1+bC_3 , C_3) = \det (C_1,C_2,C_3) + \det (C_1,\alpha C_1,C_3) + \det (C_1, bC_3,C_3)$
$= \det (C_1,C_2,C_3)$.

a) Par exemple, calculons $\begin{vmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{vmatrix} = ?$

On a $\begin{vmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{vmatrix} = \begin{vmatrix} 1+2+3 & 2 & 3 \\ 2+3+4 & 3 & 4 \\ 3+4+5 & 4 & 5 \end{vmatrix} = \begin{vmatrix} 6 & 2 & 3 \\ 9 & 3 & 4 \\ 12 & 4 & 5 \end{vmatrix} = 3 \begin{vmatrix} 2 & 2 & 3 \\ 3 & 3 & 4 \\ 4 & 4 & 5 \end{vmatrix} = 3.0 = 0$ car $C_1 = C_2$

b) Montrer sans calculer que $\begin{vmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{vmatrix} = 0$

En effet, $\begin{vmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{vmatrix} = \begin{vmatrix} 1 & 2-2.1 & 3-3.1 \\ 2 & 3-2.2 & 4-3.2 \\ 3 & 4-2.3 & 5-3.3 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ 2 & -1 & -2 \\ 3 & -2 & -4 \end{vmatrix} = 0$ car $C_2=2C_1$

$C_1 ; C_2-2C_1 ; C_3-3C_1$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

3. Déterminant d'un produit de deux matrices

a) Introduction

Soient A et B deux matrices carrées d'ordre n à coefficient dans un corps commutatif K, alors A.B est aussi une matrice carrée d'ordre n et on a :

1°) det (A.B) = det (A.det(B)
2°) $\det(\lambda.A) = \lambda^n.\det(A)\ \forall\ \lambda \in K$
3°) $\det(A+B) \neq \det(A) + \det(B)$

Exemple : Si $A=2I_n$ et $B=3I_n$ i.e

$$A = \begin{pmatrix} 2 & 0\cdots & 0 \\ 0 & 2\cdots & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0\cdots & 2 \end{pmatrix} \text{ et } B = \begin{pmatrix} 3 & 0\cdots & 0 \\ 0 & 3\cdots & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0\cdots & 3 \end{pmatrix}$$

Alors,$A.B = (2\ I_n) . (3I_n) = 6\,I_n^2 = 6\ I_n$
$\mathrm{Det}(A) = 2^n$ et $\det(B) = 3^n \Rightarrow \det(A.B) = 6^n$
Vérifions si det(A.B) = det(A) . det(B)

On a : $\mathrm{Det}(A) . \det(B) = 2^n . 3^n = (2 .3)^n = 6^n = \det(A.B)$
$\mathrm{Det}(\lambda.A) = \lambda^n \det(A) = \lambda^n.2^n = (2\lambda)^n$
$\mathrm{Det}(A) + \det(B) \neq \det (A+B)$ *Vérifier aux exercices*.

b) Consequence du théorème ci-dessus

Supposons que la matrice carrée A d'ordre n à coefficients dans un corps commutatif K est inversible c a d la matrice inverse A^{-1} existe. Avec A^{-1} matrice carrée d'ordre n, alors :
$\mathbf{A.A^{-1} = I_n = A^{-1}.A}$
$\Rightarrow \det(A.A^{-1}) = \det(I_n) = \det(A^{-1}.A)$ si et seulement si $\det(A).\det(A^{-1}) = 1 = \det(A^{-1}) . \det(A)$ ceci prouve que

Det(A) et $\det(A^{-1})$ sont inverses l'un de l'autre et comme $\det(A) \in K, \det(A^{-1}) \in A \neq 0$.
D'où le théorème ci – dessous

c) Théorème

Soit A une matrice carrée d'ordre n à coefficient dans un corps commutatifK, alors les propositions suivantes sont équivalentes :

- A est inversible,
- $\mathrm{Det}(A) \neq 0$
- $\forall\ X \in m_n(K)$ telle que : $A.X = 0$ alors $X = 0$

Définition
*Une matrice carrée A est dite régulière si $\det(A) \neq 0$.
*Une matrice carrée A est dite singulière si $\det(A) = 0$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Par exemple :

$A = \begin{pmatrix} 1 & 3 \\ 4 & 5 \end{pmatrix}$ est régulière (inversible) car det(A) $\neq$ 0.par contre la matrice $\begin{vmatrix} 1 & 2 \\ 4 & 8 \end{vmatrix}$ est singulier car det(B) = 0

4. Mineur et cofacteur

a) Définitions

Soit A(a_i^j)$_{i,j=1,..,n}$ une matrice carrée d'ordre n. En supposant la i^{ème} colonne et la j^{ième} ligne de A, sans changer l'ordre des autres rangées, on obtient une sous-matrice (M_i^j) d'ordre (n-1) de A.

Def$_1$: on appelle mineur associé à l'élément (a_i^j) de A le déterminant de la sous-matrice (M_i^j) obtenue en supprimant la i^{ème} colon e et la j^{ième} ligne de A sans chager l'ordre des autres rangées.

Def$_2$: on appelle cofacteur associé à l'élément (a_i^j) noté A_i^j le mineur associé à l'élément a_i^j et affecté de sa signature c a d A_i^j = (-1)$^{i+j}$ $|M_i^j|$

b) Théorème : (calcul d'un déterminant)

Soit $A = \begin{pmatrix} a_1^1 & a_2^1 \cdots & a_i^1 \cdots & a_n^1 \\ a_1^2 & a_2^2 \cdots & a_i^2 \cdots & a_n^2 \\ \vdots & & \vdots & \vdots \\ a_1^j & a_2^j \cdots & a_i^j \cdots & a_n^j \\ \vdots & \vdots & \vdots & \vdots \\ a_1^n & a_2^n \cdots & a_i^j \cdots & a_n^n \end{pmatrix}$ une matrice carrée d'ordre n

Alors le déterminant de A est égal à la somme des produits obtenus en multipliant les éléments d'une rangée (colonne ou ligne) par leurs cofacteurs respectifs c a d, si on veut calculer det(A) par rapport a :

j^{ième} ligne de A, on a : det(A) = $a_1^j A_1^j + a_2^j A_2^j + ... + a_i^j A_i^j + a_n^j A_n^j = \sum_{i=1}^{n} a_i^j . A_i^j$

i^{ème} colone, on a : det(A) = $a_i^1 A_i^1 + a_i^2 A_i^2 + ... + a_i^j A_i^j + ... + a_i^n A_i^n = \sum_{j=1}^{n} a_i^j . A_i^j$

Exemple :

a) Soit $A = \begin{pmatrix} 3 & 4 & 5 \\ 1 & 2 & 6 \\ 0 & 8 & 7 \end{pmatrix}$, déterminez les mineurs et les cofacteurs associés a 4,7,1 et calculer det (A) par rapport à la 3^{ième}ligne et par rapport à la 1^{ième}colonne.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Réponse

a_1) le mineur associé à 4 est $\begin{vmatrix} 1 & 6 \\ 0 & 7 \end{vmatrix}$ = 7

et le cofacteur associé à 4 est $A_2^1 = (-1)^3 \begin{vmatrix} 1 & 6 \\ 0 & 7 \end{vmatrix} = -7$

a_2) le mineur et le cofacteur associé a 7 sont respectivement

$$\left|M_3^3\right| = \begin{vmatrix} 3 & 4 \\ 1 & 2 \end{vmatrix} = 2 \qquad \text{et } A_3^3 = (-1)^6 \begin{vmatrix} 3 & 4 \\ 1 & 2 \end{vmatrix} = 2$$

a_3) le mineur et le cofacteur associé a 1 sont respectivement :

$$\left|M_1^2\right| = \begin{vmatrix} 4 & 5 \\ 8 & 7 \end{vmatrix} = 28\ 40 = -12 \text{ et } A_2^1 = (-1)^3 \begin{vmatrix} 4 & 5 \\ 8 & 7 \end{vmatrix} = 12$$

a_4) calcul de det(A) par rapport a la 3^e ligne de A

On a : det(A) = $0.\ A_1^3 + 8.\ A_2^3 + 7.\ A_3^3$

$$= 0\ .\begin{vmatrix} 4 & 5 \\ 1 & 6 \end{vmatrix} + (-8) \begin{vmatrix} 3 & 5 \\ 1 & 6 \end{vmatrix} + 7 \begin{vmatrix} 3 & 4 \\ 1 & 2 \end{vmatrix} = -90$$

a_5) calcul de det(A) par rapport à la 1ère colonne

On a : det(A)= $3.\ A_1^1 + 1.\ A_1^2 + 0\ A_1^3 .= 3 \begin{vmatrix} 2 & 6 \\ 8 & 7 \end{vmatrix} - 1 \begin{vmatrix} 4 & 5 \\ 8 & 7 \end{vmatrix} + 0 \begin{vmatrix} 4 & 5 \\ 2 & 6 \end{vmatrix} = 3(-34) + 12 + 0 = -90$

Calculons le déterminant ci-après :

$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 5 & 6 \\ 4 & 0 & 1 & 2 \\ 1 & 3 & -1 & -5 \end{vmatrix}$. En utilisant la 1ère ligne,

On a : $\begin{vmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 5 & 6 \\ 4 & 0 & 1 & 2 \\ 1 & 3 & -1 & -5 \end{vmatrix} = \begin{vmatrix} 4 & 5 & 6 \\ 0 & 1 & 2 \\ 3 & -1 & -5 \end{vmatrix} -2 \begin{vmatrix} 3 & 5 & 6 \\ 4 & 1 & 2 \\ 2 & -1 & -5 \end{vmatrix} + 3 \begin{vmatrix} 3 & 4 & 6 \\ 4 & 0 & 2 \\ 1 & 3 & -5 \end{vmatrix} - 4 \begin{vmatrix} 3 & 4 & 5 \\ 4 & 0 & 1 \\ 1 & 3 & 1 \end{vmatrix}$

ou en utilisant lap ropriété 6 ci-dessus ; on a

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 5 & 6 \\ 4 & 0 & 1 & 3 \\ 1 & 3 & -1 & -5 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 3 & -2 & 4 & -6 \\ 4 & -8 & -11 & -14 \\ 1 & 1 & -4 & -9 \end{vmatrix} = 1\ . \begin{vmatrix} -2 & -4 & -6 \\ -8 & -11 & -14 \\ 1 & -4 & -9 \end{vmatrix} = -2 \begin{vmatrix} 1 & 2 & 3 \\ -8 & -11 & -14 \\ 1 & -4 & -9 \end{vmatrix}$$

$$\left.\begin{array}{l} C_2 \approx C_2 - 2C_1 \\ C_3 \approx C_3 - 3C_1 \\ C_4 \approx C_4 - 4C_1 \end{array}\right\}$$ Opérations faites sur les colonnes. Le reste est à terminer aux exercices.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

5. Comatrice et matrice adjointe

Soit $A = (a_i^j)_{i,j=1,\dots n}$ une matrice carré d'ordre n à coefficient dans K

Def$_1$ on appelle comatrice de A, notée com(A) la matrice des coefficients de A c a d $com(A)=(A_i^j)_{i,j=1\dots n}$

Def$_2$ on appelle matrice adjointe de A notée *A la transposé de la comatrice de A c a d

$$*A = {}^t com(A) = (A_j^i)$$

Théorème:

$\forall A\in m_n(K)$, on a $\boxed{A\cdot *A = \det(A).In = (*A).A}$

Exemple :

a) soit $A=\begin{pmatrix} 3 & 5 \\ 4 & 7 \end{pmatrix}$ déterminer com(A), adj A et vérifier le théorème ci-dessus

On a: $Com(A) = \begin{pmatrix} 7 & -4 \\ 5 & 3 \end{pmatrix}$ et $*A = {}^t com(A) = \begin{pmatrix} 7 & -5 \\ -4 & 3 \end{pmatrix}$

Calculons A. *A

On a : $A .*A = \begin{pmatrix} 3 & 5 \\ 4 & 7 \end{pmatrix}\begin{pmatrix} 7 & -5 \\ -4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$; on voit que det(A) = 1

b) Soit $A = \begin{pmatrix} 2 & 1 & 3 \\ 4 & 0 & 5 \\ 3 & 2 & 1 \end{pmatrix}$,

Déterminer com(A), *A et vérifier le théorème ci-dessus.

On constate que : Dét(A) = 15

$$\text{On a : } Com(A) = \begin{pmatrix} \begin{vmatrix} 0 & 5 \\ 2 & 1 \end{vmatrix} & -\begin{vmatrix} 4 & 5 \\ 3 & 1 \end{vmatrix} & \begin{vmatrix} 4 & 0 \\ 3 & 2 \end{vmatrix} \\ -\begin{vmatrix} 1 & 3 \\ 2 & 1 \end{vmatrix} & \begin{vmatrix} 2 & 3 \\ 3 & 1 \end{vmatrix} & -\begin{vmatrix} 2 & 1 \\ 3 & 2 \end{vmatrix} \\ \begin{vmatrix} 1 & 3 \\ 0 & 5 \end{vmatrix} & -\begin{vmatrix} 2 & 3 \\ 4 & 5 \end{vmatrix} & \begin{vmatrix} 2 & 1 \\ 4 & 0 \end{vmatrix} \end{pmatrix} = \begin{pmatrix} -10 & 11 & 8 \\ 5 & -7 & -1 \\ 5 & 2 & -4 \end{pmatrix}$$

D'ou $Com(A) = \begin{pmatrix} -10 & 11 & 8 \\ 5 & -7 & -1 \\ 5 & 2 & -4 \end{pmatrix}$ entraîne que $*A = \begin{pmatrix} -10 & 5 & 5 \\ 11 & -7 & 2 \\ 8 & -1 & -4 \end{pmatrix}$

Calculons A .*A

$$\text{On a : } A .*A = \begin{pmatrix} 2 & 1 & 3 \\ 4 & 0 & 5 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} -10 & 5 & 5 \\ 11 & -7 & 2 \\ 8 & -1 & -4 \end{pmatrix} = \begin{pmatrix} 15 & 0 & 0 \\ 0 & 15 & 0 \\ 0 & 0 & 15 \end{pmatrix} = 15 . I_3 = \text{dét}(A) . I_3$$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

F. INVERSION D'UNE MATRICE

Soit A une matrice carrée d'ordre n à coefficient dans K.
Si dét(A) $\neq 0$; alors A est inversible c.à.d. A^{-1} existe. On sait par ailleurs que :
$A\,.{}^*A =$ dét(A)$.I_n = ({}^*A)\,.\,A$. En divisant chaque terme de l'égalité ci-dessus par dét(A) $\neq 0$,
On obtient :

$$\frac{A.{}^*A}{\det(A)} = I_n = \frac{{}^*A.A}{\det(A)} \Rightarrow A^{-1} = \qquad \boxed{A^{-1} = \frac{1}{\det A}.{}^*A}$$

Exemple :
Inverser les matrices suivantes :

$A = \begin{pmatrix} 3 & 5 \\ 4 & 7 \end{pmatrix}$.On sait que dét(A) = 1 et $^*A = \begin{pmatrix} 7 & -5 \\ -4 & 3 \end{pmatrix}$

Alors A^{-1} existe et on a : $A^{-1} = \dfrac{1}{\text{dét}A}$. adj$A = \begin{pmatrix} 7 & -5 \\ -4 & 3 \end{pmatrix}$.

D'où $A^{-1} = \begin{pmatrix} 7 & -5 \\ -4 & 3 \end{pmatrix}$

Soit $A = \begin{pmatrix} 2 & 1 & 3 \\ 4 & 0 & 5 \\ 3 & 2 & 1 \end{pmatrix}$ On sait que dét(A) = 15,donc A^{-1} existe .comme

$^*A = \begin{pmatrix} -10 & 5 & 5 \\ 11 & -7 & 2 \\ 8 & -1 & -4 \end{pmatrix}$, alors $A^{-1} = \dfrac{1}{\det A}.{}^*A$

$$= \frac{1}{15}\begin{pmatrix} -10 & 5 & 5 \\ 11 & -7 & 2 \\ 8 & -1 & -4 \end{pmatrix}$$

G. RANG D'UNE MATRICE

Soit $A = \left(a_i^j\right)_{\substack{j=1,\dots n \\ i=1,\dots m}}$ une matrice de type (m, n) à coefficients dans K.

Définition : On appelle rang colonnes de A, le nombre de vecteurs colonnes Linéairement indépendants.

Définition : On appelle rang lignes de A le nombre de vecteurs lignes linéairement Indépendants.

Théorème : Soit A une matrice de type (m, n), alors rang colonne de A est égal au rang ligne de A. Ainsi le rang d'une matrice A, noté rg(A) est égal au rang colonne ou rang ligne de A.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Définition : Soit A une matrice de type (m, n). Alors rang de A est égal à l'ordre maximum d'un mineur non nul de A ou le rang de A est égal au nombre de lignes non nulles d'une matrice échelonnée.

Exemples :

a) soit A = $\begin{pmatrix} 1 & 2 & 5 \\ 3 & 6 & 7 \end{pmatrix}$, determiner le rang de A. On cherche les sous-matrices carrées de A et leurs déterminant.

S'il y a une sous-matrice carrée dont le déterminant est différent de zéro, alors le rang de la matrice A est égal à l'ordre de cette sous-matrice. Dans notre exemple il existe une sous-matrice $\begin{pmatrix} 1 & 5 \\ 3 & 7 \end{pmatrix}$ telle que

$$\begin{vmatrix} 1 & 5 \\ 3 & 7 \end{vmatrix} = -8 \neq 0 \Rightarrow \text{rg(A)} = 2$$

N.B. : Si toutes les sous-matrices d'ordre 2 ont pour déterminant 0, alors le rang est inférieur à 2 c.à.d le rang de A est égale à 1
On peut aussi échelonner la matrice A.

$$A = \begin{pmatrix} 1 & 2 & 5 \\ 3 & 6 & 7 \end{pmatrix} \begin{matrix} L_1 \\ L_2 \Rightarrow -3L_1 + L_2 \end{matrix} \Leftrightarrow \begin{pmatrix} 1 & 2 & 5 \\ 0 & 0 & -8 \end{pmatrix} \text{ matrice échelonnée}$$

Alors le rang de A égal au nombre de lignes non nulles d'une matrice échelonnée.
$\Rightarrow$ rg(A) = 2.

b) soit $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$ Déterminer le rang de A

On a :

$$\text{Det(A)} = \begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ 4 & -3 & -6 \\ 7 & -6 & -12 \end{vmatrix} = 0 \ \text{ D'ou rang}(A) < 3 \text{ car déterminant de A est égal à zéro}$$

On constate qu'il existe une sous-matrice $B \equiv \begin{pmatrix} 1 & 2 \\ 4 & 5 \end{pmatrix}$ tel que det(B)=-3 $\neq$0. Donc rg(A)=2.

c) Soit A = $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 7 \end{pmatrix}$ Déterminons le rang de A.

$$\text{On a : dét}(A) = \begin{vmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 7 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 & 4 \\ 2 & 1 & 1 & 5 \\ 3 & 1 & 1 & 6 \\ 4 & 1 & 1 & 7 \end{vmatrix} = 0 \qquad \begin{matrix} C_2 \leftrightarrow C_2 - C_1 \\ C_3 \leftrightarrow C_3 - C_2 \end{matrix} \quad \text{ceci entraîne que rg(A)} < 4$$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

On constate par ailleurs qu'il n'existe aucune une sous – matrice de A d'ordre 3 qui soit régulière.
Ce qui entraîne que rg(A) < 3.

Comme il existe une sous-matrice $\begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}$ telque $\begin{vmatrix} 1 & 2 \\ 2 & 3 \end{vmatrix} = 3 - 4 = -1 \neq 0$, alors rg(A)=2.

N.B. On peut aussi déterminer le rang de A en echellonant cette matrice, on a alors :

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 7 \end{pmatrix} \begin{array}{l} L_1 \\ L_2 \leftrightarrow -2L_1 + L_2 \\ L_3 \leftrightarrow -3L_1 + L_3 \\ L_4 \leftrightarrow -3L_2 + L_3 \end{array} \quad □ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & -1 & -2 & -3 \\ 0 & -2 & -4 & -6 \\ 0 & -3 & -6 & -9 \end{pmatrix} \begin{array}{l} L_1 \\ L'_2 \\ L'_3 \leftrightarrow -2L'_2 + L'_3 \\ L'_4 \leftrightarrow -3L'_2 + L'_3 \end{array}$$

$$□ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & -1 & -2 & -3 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \Rightarrow \text{rg}\, A = 2$$ car la matrice échelonné de A contient 2 lignes non nulles.

Exercice :
Chercher aux exercices le rang de A, avec :

$$A = \begin{pmatrix} 2 & 1 & 3 & 0 & 4 \\ 1 & 2 & 3 & 5 & 0 \\ 3 & 4 & 0 & 1 & 2 \end{pmatrix}$$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

CHAPITRE VII
SYSTEMES D'EQUATIONS LINEAIRES
EQUATION LINEAIRE

A. INTRODUCTION

1. Définition :

Soient E, F deux espaces vectoriels sur K de dimensions respectives m et 1 ; f ; E → F, une application linéaire, on appelle équation linéaire tout prédicat de la forme *f(x) = b (i)* ; définie sur E avec b Є F , X Є E est dit solution de (i) ,b est le terme indépendant de (i). Si S est l'ensemble des solutions de (i), alors S = f^{-1}(b) = {β Є E ; f(β) = b}

- Si S = Ø, alors f(x) = b est dite équation impossible
- Si b = 0, alors f(x) = 0 est dite équation linéaire et homogène.

Remarquons que les solutions de cette équation appartient à Kerf, ce qui implique que l'équation f(x) = 0 ne peut jamais être impossible car elle contient toujours la solution banale à savoir x = 0

2. Théorème :

Soient E, F deux espaces vectoriels sur K de dimensions respectives m et n ; f ;E → F une application linéaire.
Si x_0 est une solution particulière de l'équation linéaire f(x) = b et S l'ensemble des solutions de cette même équation, alors S = { $X = X_0 + t$: t Є Kerf }

Preuve :
X_0 solution de f(x) = b $\Rightarrow f(x_0) = b$, comme *f(x) = b* et $f(x_0) = b$, on doit avoir $f(x) = f(x_0)$
$\Leftrightarrow f(x) - f(x_0) = 0 \Leftrightarrow f(x - x_0) = 0$.
$\Leftrightarrow$ $(x - x_0)$ Є Kerf i.e.∃t Є Kerf tel que $t = x - x_0 \Leftrightarrow x = x_0 + t$ *c.q.f.d.*

3. Exemple

Soit f : $IR^n \to IR$
$(x_1,\ldots, x_n) \to f(x_1, x_2, \ldots\ldots, x_n) \equiv a_1x_1 + a_2x_2 + \ldots\ldots + a_nx_n$ une application linéaire.

Si bЄIR, alors $f(x_1, x_2, \ldots\ldots, x_n)$ = b, c à d $a_1x_1 + a_2x_2 + \ldots a_nx_n = b$ est une équation linéaire à n inconnues $x_1, x_2, x_3, \ldots, x_n$. Pour résoudre cette équation dans R^n, deux cas sont possibles.

1 °cas : Supposer que l'un au moins des coefficients des inconnues est non nul, soit a_n c à d $a_n \neq 0$, alors n $a_nx_n = b - a_1x_1 - a_2x_2 - \ldots - a_{n-1}x_{n-1}$

$\Leftrightarrow a_n\, x_n = \frac{b}{a_n} - \frac{a_1}{a_n} x_1 - \frac{a_2}{a_n} x_2 - \ldots\ldots\ldots\ldots\ldots - \frac{a_{n-1}}{a_n} x_{n-1}$, avec $x_1, x_2, \ldots\ldots, x_{n-1}$ Є R

D'où S= $\{(x_1,x_2,\ldots,x_{n-1},x_n) \in R^n : x_n=\frac{b}{a_n}-\frac{a_1}{a_n}x_1-\ldots-\frac{a_{n-1}}{a_n}x_{n-1}\}$

S=($\{x_1, x_2,\ldots\ldots, x_{n-1}, \frac{b}{a_n}-\frac{a_1}{a_n}x_1-\frac{a_2}{a_n}x_2-\ldots\ldots\ldots-\frac{a_{n-1}}{a_n}x_{n-1}\}; x_1, x_2,\ldots, x_{n-1} \in$ R)

2è cas : Supposer que tous les coefficients de inconnues sont nuls i.e $a_1 = a_2 = \ldots a_n= 0$, alors 0X= b
Si $\neq$0, alors l'équation 0X=b est impossible. Ce qui implique s = ø
si b=0, alors 0X = 0 est une équation qui admet une infinité de solutions. D'ou l'ensemble S = R^n

Exemples :

a) Soit f : $IR^3 \to IR$
(x, y, z) $\to$ f(x, y, z) = x + 2y + 3z, une application linéaire.

Si b = 2Є IR, alors f(x, y, z) = 2, càd x + 2y + 3z = 2 est une équation linéaire à 3 inconnues x, y et z.

Résolvons cette équation :
On a x + 2y + 3z = 2 (i) $\Leftrightarrow$ x = 2 − 2y − 3z : y, z Є R
D'où S = {(x, y, z) Є R^3 : x = 2 − 2y − 3z, y, z} = {(2 − 2y − 3z, y, z) : y, z Є R}.

Quelques solutions particulières de cette équation.
Si y = 0 ; z = 0 ; alors x = 2 ; d'où (2, 0, 0) est une solution de (i)
Si y = 1 ; z = 1 ; alors x = -3 ; d'où (-3, 1, 1) est une solution de (i)
Si y = 3 ; z = 1 ; alors x = -4 ; d'où (-4, 3, 0) est une solution de (i)

Si b = - 4, alors x + 2y + 3z = -4 est une équation linéaire. En la résolvant, on a :
x + 2y + 3z = -4 $\Rightarrow$ 2y = -4 – x − 3z ; x, z Є R

$$\Rightarrow y = -2 - \frac{x}{4} - \frac{3}{2}z : x, y \in R$$

D'ou S = {(x, y, z) Є R^3 : $y = -2 - \frac{x}{2} - \frac{3}{2}z : x, z$ Є R}

$$= \{ (x, -2-\frac{x}{4} - \frac{3}{2}z, z) : x, z \in IR \in R\}$$

Donner aux exercices quelques solutions particulières de cette équation.

b) 2x + y − 3z = 4 une équation linéaire à 3 inconnues x, y, z qu'il faut résoudre dans IR^3
2x + y − 3z = 4 $\Rightarrow$ y = 4 − 2x + 3z ; x, y, z Є IR
D'où S=$\{(x, y, z) \in IR\}$;y = 4 − 2x + 3z}={(x, 4 − 2x + 3z, z) : x, zЄ R}
Quelques solutions particulières (1, 5, 1) ; (2, 6, 2) ;(-2, 2, -2), etc.
• Résoudre l'équation linéaire ci-dessous sachant qu'elle admet (1, 5, 1) comme particulière.

Solution
Soit f : $R^3 \to R$
(x, y, z) $\to$ f(x, y, z) = 2x + y − 3z, une application linéaire.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

On sait que S $=\{x = x + t_0 ; t \in Kerf\}$ est l'ensemble des solutions de cette équation.

Cherchons kerf :

On a : Kerf = $\{(x, y, z) \in R^3 : f(x, y, z) = 0_R\} = \{(x, y, z) \in R^3 : 2x + y - 3z=0\}$

$=\{(x, y, z) \in IR^3 : y \equiv -2x + 3z\}$

$=\{(x, -2x + 3z, z) : x; z \in IR\}$

Comme $x_0 = (1, 5, 1)$ et $t = (x, -2x + 3z, z) \in$ Kerf avec $x, z \in R$

Alors $S = \{x = x_0 + t ; t \in kerf\}$

$= \{x = (1, 5, 1) + (x, -2x + 3z, 1 + z) : x, z \in R\}$

$= \{(1 + x, 5 - 2x + 3z, 1 + z) : x, z \in R\}$

Vérifions que

$= 2 (1+ x) + (5 - 2x + 3z) - 3 (1 + z) = 4$

$= 2(1 + x) + (5 - 2x + 3z) - 3(1 + z) = 2 + 2x + 5 - 5 - 2x + 3z - 3 + 3z$

$= 4$

B. SYSTEME D'EQUATION LINEAIRE

1. Définition

Soient E, un espace vectoriel sur K, (F_i) une famille de n espaces vectoriels sur K,et $f_i : E \to F_i$ une application linéaire. Avec i=1,…n.

Alors $\forall\, b \in F_i$, la famille $f_i(x) = b_i$ d'équations linéaires est dite système d'équations linéaire. On le note par S.

Ainsi, $S \cong f_i(x) = b_i \iff \begin{cases} f_1(x) = b_1 \\ f_2(x) = b_2 \\ \vdots \qquad \vdots \\ f_n(x) = b_n \end{cases}$

Si $b_i = 0, \forall i = 1, n$;alors $S \cong f_i(x)=0$ est dit système d' équation linéaires et homogènes.

Remarque : noter que tout système d'équations linéaires est équivalent à une équation linéaire.

2. Système de n équations linéaires à m inconnues

a) Définition et Notation

(1) Définition

Soient E, F deux espaces vectoriels sur K des bases respectives B,B' et $f : E \to F$ une application linéaire dont $A=\left(a_i^j\right)_{i\equiv1,\dots,m}^{j\equiv1,\dots,n}$ est sa matrice représentative par rapport aux bases canoniques B et B' $(\dim E \equiv m, \dim F \equiv n)$.

Alors $\forall B \in F$: l'équation linéaire f(X)= B est équivalente à un système de n équations linéaires à m inconnues.

Ie S=f(X)=B $\iff S \equiv AX = B$ avec $X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ et $B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Alors, A.X=B $\Leftrightarrow \begin{pmatrix} a_1^1 & a_2^1 ....a_m^1 \\ a_1^2 & a_2^2 ....a_m^2 \\ \vdots & \vdots \quad \vdots \\ a_1^n & a_2^n \quad a_m^n \end{pmatrix} \bullet \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix} \equiv \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$

$$\Leftrightarrow \begin{pmatrix} a_1^4 x_1 + x_2 a_2^2 + ... + a_m^1 x_m \\ a_1^2 x_1 + a_2^2 x_2 + ... + a_m^2 x_m \\ \vdots \qquad \vdots \\ a_1^m x_1 + a_2^2 x_2 + ... + a_m^n x_m \end{pmatrix} \equiv \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

$$\Leftrightarrow \begin{cases} a_1^1 x_1 + a_2^1 x_2 + ... + a_m^1 x_m = b_1 \\ a_1^2 x_1 + a_2^2 x_2 + ... + a_m^2 x_m = b_2 \\ \vdots \qquad \vdots \qquad \vdots \\ a_1^n x_1 + a_2^n x_2 + ... + a^n x_m = b_n \end{cases}$$

On obtient ainsi un système de n équations à m inconnues.

Les éléments $a_i^j \ \forall i \equiv 1,....m \ et \ \forall j \equiv 1,....n$ *sont dits coefficients des inconnues.*

$x_1, x_2, ...x_m$ *sont dits inconnues du système S et* $b_1, b_2, ...b_n$ *sont les termes indépendant de S.*

Ainsi tout m - uplès ($k_1, k_2, \ldots\ldots k_n$) vérifiant chacune de n équation du système est dit solution de S.

(2) Notation

Le système ci-dessous :

$$S \cong \begin{cases} a_1^1 x_1 + a_2^1 x_2 + ... + a_m^1 x_m = b_1 \\ a_1^2 x_1 + a_2^2 x_2 + ... + a_m^2 x_m = b_2 \\ \vdots \qquad \vdots \qquad \vdots \qquad \vdots \\ a_1^n x_1 + a_2^n x_2 + ... + a_m^n x_m = b_n \end{cases}$$

Est noté soit par : $S \equiv \sum_{i=1}^{m} a_i^j x_i = b_j \ (j = 1,...., n)$

Soit par: S $\cong$ A.X = B avec X et B matrices uni colonnes respectivement des inconnues et des termes indépendants et A matrice du système S.

ie.X $= \begin{pmatrix} x_1 \\ x_2 \\ . \\ . \\ . \\ x_m \end{pmatrix}$; B $= \begin{pmatrix} b_1 \\ b_2 \\ . \\ . \\ . \\ b_n \end{pmatrix}$ et A $= \begin{pmatrix} a_1^1 & a_2^1 & \cdot & \cdot & \cdot & a_m^1 \\ a_1^2 & a_2^2 & \cdot & \cdot & \cdot & a_m^2 \\ . & . \\ . & . \\ . & . \\ a_1^n & a_2^n & \cdot & \cdot & \cdot & a_m^n \end{pmatrix}$

Ce qui montre que le rang du système (S) est égal au rang de la matrice A, ie rg(S) = rg(A).

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

b) Théorème de CRAMER

Soient E,F deux espaces vectoriels sur K de dimension n chacun .ie dimE = dimF = n et f : E → F une application linéaire dont A est la matrice représentative par rapport aux bases spécifiques de E et F,alors les propositions suivantes sont équivalentes :

i) f est un isomorphisme d'espaces vectoriels.
ii) rg (f)=rg (A)=n
iii) dét(A)≠0
iv) $\forall B \in F, l'équation\ f(X) = B$ *admet une solution et une seule en* $X \in E$

On dit dans le cas que :

$$\Rightarrow S \cong f(X) = B \Leftrightarrow A.X = B \Leftrightarrow \left(\sum_{ii=1}^{n} a_i^j x_i = b_j \quad = 1,\ldots.n \right) \text{est un système de cramer}$$

Corollaire :

Un système $S = \sum_{ii=1}^{n} a_i^j x_i = b_j \ (j = 1,\ldots.n)$ de n équations linéaires à n inconnues est dit de cramer si le système des n équations linéaires et homogènes n'admet que la solution triviale ou banale à savoir $x_1 = x_2 = \ldots = x_n = 0$.

3. Téchniques de résolutions d'un système d'équations lineaires

a) Méthode d'éliminations successives des inconnues dite Algorithme de GAUSS

a_1 Principe :

Cette méthode consiste à mettre sous forme échelonnée le système à résoudre grâce à certaines combinaisons linéaires faites sur les lignes de manière à éliminer plusieurs inconnues.

a_2 Exemples :

Résoudre par Algorithme de Gauss les systèmes d'équations linéaires ci-dessous

a) $\begin{cases} x + 2y = 4 & L_1 \\ 3x + 7y = 5 & L_2 \to -3L_1 + L_2 \end{cases} \Leftrightarrow \begin{cases} x + 2y = 4 \ (1) \\ y = -7 \Rightarrow y = -7 \quad (2) \end{cases}$

(2) dans (1) $\Rightarrow$ x + 2(-7) = 4
$\Rightarrow$ x – 14 = 4
$\Rightarrow$ x = 18

D'où $S = \{(18, -7)\}$

b) $\begin{cases} 2x - y + 4z \ = -4 & L_1 \\ 3x + 2y - 3z = 17 & l_2 \to -3L_1 + 2L_2 \\ 5x - 3y + 8z = -10 & L_3 \to -5L_1 + 2L_3 \end{cases} \Leftrightarrow \begin{cases} 2x - y + 4z = -4 & L'_1 \\ 7y - 18z = 46 & L'_2 \\ -y - 4z = 0 & L'_3 \to L'_2 + 7L'_3 \end{cases}$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

$$\Leftrightarrow \begin{cases} 2x - y + 4z = -4 \quad (1) \\ \quad 7y - 18z = 46 \quad (2) \\ \qquad -46z = 46 \Rightarrow z = -1 \quad (3) \end{cases}$$

(3) dans (2) $\Rightarrow$ 7y - 18(-1) = 46 soit 7y = 28 entraînant que *y = 4. (5)*

(5) et (3) dans (1) $\Rightarrow$ 2x = -4+4+4 ssi 2x = 4, soit $\boxed{x = 2}$

D'où $S \equiv \{(2,4,-1)\}$.

TP. Résoudre les systèmes d'équations ci-dessous par algorithme de Gauss.

$$a)\begin{cases} x + 2y + 3z + 4t \equiv 1 \\ 2x + 3y + 4z + 5t \equiv 2 \\ 3x + 5y + 7z + 9t \equiv 4 \\ 4x + 8y + 9z + 12t \equiv 6 \end{cases} \qquad b)\begin{cases} x + y - 4z \equiv 2 \\ 3x - 2y + z \equiv 5 \\ 5x + 4y + 2z \equiv 7 \end{cases}$$

b) Méthode de déterminant

b_1 Méthode de CRAMER

Soit S $\cong \sum_{i\equiv 1}^{n} a_i^j x = b_{j_i}$ $(j \equiv 1,......,n)$ un système de Cramer, ie dét(A) $\neq 0$

Alors S admet une solution et une seule en $\{x_1, x_2, \ldots, x_n\}$ donnée par les formules suivantes ;

$x_i = \dfrac{dét(A_i)}{dét(A)}$ $avec\, i = 1, 2, ...n$ ou A_i est la matrice A dans laquelle la $i^{ème}$ colonne est remplacée par la colonne des termes indépendants.

Exemples :

Résoudre par la méthode de Cramer les systèmes d'équations linéaires ci-dessous

$$a)\begin{cases} x + 2y \equiv 4 \\ 3x + 7y \equiv 5 \end{cases} \qquad b)\begin{cases} 2x - 4y + 4z \equiv -4 \\ 3x + 2y - 3z \equiv 17 \\ 5x - 3y + 8z \equiv -10 \end{cases}$$

Solution

a) $\begin{cases} x + 2y \equiv 4 \\ 3x + 7y \equiv 5 \end{cases} \Leftrightarrow \begin{pmatrix} 1 & 2 \\ 3 & 7 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 5 \end{pmatrix}$, on pose $A = \begin{pmatrix} 1 & 2 \\ 3 & 7 \end{pmatrix}$, $X = \begin{pmatrix} x \\ y \end{pmatrix}$ et $B = \begin{pmatrix} 4 \\ 5 \end{pmatrix}$

Comme dét(A) $\equiv \begin{vmatrix} 1 & 2 \\ 3 & 7 \end{vmatrix} \equiv 1 \neq 0$, alors x $\equiv \dfrac{\begin{vmatrix} 4 & 2 \\ 5 & 7 \end{vmatrix}}{1} \equiv 18$ et y $\dfrac{\begin{vmatrix} 1 & 4 \\ 3 & 5 \end{vmatrix}}{1} \equiv -7$

D'où x = 18 et y = -7 et S = $\{(18,-7)\}$.

b) $\begin{cases} 2x - y + 4z = -4 \\ 3x + 2y - 3z = 17 \\ 5x - 3y + 8z = -10 \end{cases} \equiv \begin{pmatrix} 2 & -1 & 4 \\ 3 & 2 & -3 \\ 5 & -3 & 8 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} \equiv \begin{pmatrix} -4 \\ 17 \\ 10 \end{pmatrix}$

On pose $A=\begin{pmatrix}2 & -1 & 4\\ 3 & 2 & -3\\ 5 & 3 & 8\end{pmatrix}$; $X=\begin{pmatrix}x\\ y\\ z\end{pmatrix}$ et $B=\begin{pmatrix}-4\\ 17\\ -10\end{pmatrix}$

Calculons le déterminant de A.

$$\text{On a dét}(A)\equiv\begin{vmatrix}2 & -1 & 4\\ 3 & 2 & -3\\ 5 & -3 & 8\end{vmatrix}=\begin{vmatrix}0 & -1 & 0\\ 7 & 2 & 5\\ -1 & -3 & -4\end{vmatrix}=(-28+5)=-23$$

$$x=\frac{\det(A_1)}{\det(A)}=\frac{\begin{vmatrix}-4 & -1 & 4\\ 17 & 2 & -3\\ -10 & -3 & 8\end{vmatrix}}{-23}=\frac{\begin{vmatrix}0 & -1 & 0\\ 9 & 2 & 5\\ 2 & -3 & -4\end{vmatrix}}{-23}=\frac{(-36-10)}{-23}=-2$$ (on a remplacé la 1ère colonne de A par la colonne des termes indépendants).

$$y=\frac{\det(A_2)}{\det(A)}=\frac{\begin{vmatrix}2 & -4 & 4\\ 3 & 17 & -3\\ 5 & -10 & 8\end{vmatrix}}{-23}=\frac{\begin{vmatrix}2 & 0 & 0\\ 3 & 23 & -9\\ 5 & 0 & -2\end{vmatrix}}{-23}=\frac{2(-46)}{-23}=4$$ (on a remplacé la 2ème colonne de A par la colonne des termes indépendants).

$$z=\frac{\det(A_3)}{\det(A)}=\frac{\begin{vmatrix}2 & -1 & -4\\ 3 & 2 & 17\\ 5 & -3 & -10\end{vmatrix}}{-23}=\frac{\begin{vmatrix}0 & -1 & 0\\ 7 & 2 & 9\\ -1 & -3 & 2\end{vmatrix}}{-23}=\frac{14+9}{-23}=-1$$ (on a remplacé la 3ème colonne par la colonne des termes indépendants).

D'où S = $\{(2,4,-1)\}$.

b_2 Méthode de la matrice inverse

Soit $S\cong\sum_{i\equiv 1}^{n}a_i^j x_i=b_j \quad (j=1,\dots\dots\dots,n)$ un système de cramer, ie. dét(A) ≠ 0. Comme det(A) ≠ 0, Alors A est inversible, donc A^{-1} existe.

On sait que $S\equiv\sum_{i\equiv 1}^{n}a_i^j x_i\equiv b_j$ est équivalent à S ≅ A.X=B. Comme la matrice A^{-1} existe, alors de AX = B, on obtient : $A^{-1}(AX)\equiv A^{-1}B$

$\Leftrightarrow (A^{-1}A)X\equiv A^{-1}.B\Leftrightarrow I_nX\equiv A^{-1}.B.Soit\ X=A^{-1}.B$

De cette égalité matricielle, on tire les valeurs des inconnues $x_1, x_2, \dots, x_n$.

Exemple :

Résoudre par la méthode de la matrice inverse les systèmes d'équations linéaires suivants :

a) $\begin{cases}x+2y=4\\ 3x+7y=5\end{cases}$ $\qquad b)\begin{cases}2x-y+4z=-4\\ 3x+2y-3z=17\\ 5x-3y+8z=-10\end{cases}$

Solution :

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

a) $\begin{cases} x+2y\equiv 4 \\ 3x+7y\equiv 5 \end{cases} \Leftrightarrow \begin{pmatrix} 1 & 2 \\ 3 & 7 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}=\begin{pmatrix} 4 \\ 5 \end{pmatrix} \Leftrightarrow AX=B$ avec $A=\begin{pmatrix} 1 & 2 \\ 3 & 7 \end{pmatrix}$; $X=\begin{pmatrix} x \\ y \end{pmatrix}$ et $B=\begin{pmatrix} 4 \\ 5 \end{pmatrix}$.

Recherche de la matrice inverse de A.

Comme dét(A) $=\begin{vmatrix} 1 & 2 \\ 3 & 7 \end{vmatrix}=1\neq 0$ alors A^{-1} existe avec $A^{-1}=\dfrac{1}{\det(A)}\cdot {}^{*}A$

Com (A) $\equiv\begin{pmatrix} 7 & -3 \\ -2 & 1 \end{pmatrix}\Rightarrow {}^{*}A=\begin{pmatrix} 7 & -2 \\ -3 & 1 \end{pmatrix}$ *et* $A^{-1}=\begin{pmatrix} 7 & -2 \\ -3 & 1 \end{pmatrix}$

$AX=B \Leftrightarrow X=A^{-1}.B \Leftrightarrow \begin{pmatrix} x \\ y \end{pmatrix}=\begin{pmatrix} 7 & -2 \\ -3 & 1 \end{pmatrix}\begin{pmatrix} 4 \\ 5 \end{pmatrix}$

$\Leftrightarrow \begin{pmatrix} x \\ y \end{pmatrix}=\begin{pmatrix} 18 \\ -7 \end{pmatrix} \Leftrightarrow \begin{cases} x=18 \\ y=-7 \end{cases}$ $D'où\ S=\{(18-7)\}$

Résoudre l'exemple b) aux exercices.

Autre méthode de recherche d'une matrice inverse.

Soit $A=\left(a_i^j\right)_{i=j=1,\dots\dots,n}$ une matrice carrée d'ordre n dont dét(A) $\neq 0$ ie A inversible.

Poser $A^{-1}=\begin{pmatrix} D_1 \\ D_2 \\ \vdots \\ D_n \end{pmatrix}$ la matrice inverse de A. Pour avoir A. $A^{-1}=I_n$ *avec* $I_n=\begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix}$

$A.A^{-1}=I_n \Leftrightarrow S\cong\sum_{i\equiv 1}^{n} a_i^j D_i=e_j$; $(j=1,\ \dots,n)$, un système de n équations linéaires à n inconnues (D_i). Ce système est de Cramer car det(A) $\neq 0$. Et les solutions de S seront exprimées en fonction des $\left(e_j\right)_{j=1,\dots,n}$. D'où les lignes de A^{-1} seront constituées des coefficients de $\left(e_j\right)_{j=1,\dots,n}$

Exemple :

a) Soit $A=\begin{pmatrix} 1 & 2 \\ 3 & 7 \end{pmatrix}$ Cherchons par la méthode ci-dessus la matrice inverse de A. On sait que det(A) = 1 $\neq$ 0.

Posons $A^{-1}=\begin{pmatrix} D_1 \\ D_2 \end{pmatrix}$ *pour avoir* $:A.A^{-1}=I_2$ avec $I_2=\begin{pmatrix} e_1 \\ e_2 \end{pmatrix}$

$A.A^{-1}=I_2 \Leftrightarrow \begin{pmatrix} 1 & 2 \\ 3 & 7 \end{pmatrix}\begin{pmatrix} D_1 \\ D_2 \end{pmatrix}\equiv\begin{pmatrix} e_1 \\ e_2 \end{pmatrix} \Leftrightarrow \begin{cases} D_1+2D_2=e_1 \\ 3D_1+7D_2=e_2 \end{cases}$

En appliquant la méthode Cramer, on obtient :

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

$$D_1 = \frac{\begin{vmatrix} e_1 & 2 \\ e_2 & 7 \end{vmatrix}}{1} = 7e_1 - 2e_2 \quad et \quad D_2 = \frac{\begin{vmatrix} 1 & e_1 \\ 3 & e_2 \end{vmatrix}}{1} = -3e_1 + e_2$$

D' où $\begin{cases} D1 = 7e_1 - 2e_2 \\ D2 = -3e_1 + e_2 \end{cases}$ et la matrice $A^{-1} = \begin{pmatrix} 7 & -2 \\ -3 & 1 \end{pmatrix}$.

b) Soit A $= \begin{pmatrix} 2 & -1 & 4 \\ 3 & 2 & -3 \\ 5 & -3 & 8 \end{pmatrix}$, cherchons par la méthode de l'inverse de A.

Pour cela, poser

$$A^{-1} = \begin{pmatrix} D_1 \\ D_2 \\ D_3 \end{pmatrix} \text{ pour avoir } A.A^{-1} = I_3 \text{ ainsi } A.A^{-1} = I_3 \Leftrightarrow \begin{pmatrix} 2 & -1 & 4 \\ 3 & 2 & -4 \\ 5 & -3 & 8 \end{pmatrix}\begin{pmatrix} D_1 \\ D_2 \\ D_3 \end{pmatrix} = \begin{pmatrix} e_1 \\ e_2 \\ e_3 \end{pmatrix}$$

$$\Leftrightarrow \begin{cases} 2D_1 - D_2 + 4D_3 = e_1 \\ 3D_1 + 2D_2 - 3D_3 = e_2 \\ 5D_1 - 3D_2 + 8D_3 = e_3 \end{cases}$$

On obtient ainsi un système de trois équations à trois inconnues qui sont D_1 ; D_2 et D_3 à résoudre soit par la méthode de cramer soit par algorithme de Gauss.

c) Méthode de CHOLESKI

Soit S= $\sum_{i=1}^{n}$ $a_i x_i = b_j$ (j=1,….,n) un système de cramer

La méthode de CHOLESKI consiste à décomposer la matrice A en un produit U.V de la manière ci – dessous, avec U et V les matrices triangulaires.

$$A = U.V \text{ avec } U = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ u_1^2 & 1 & 0 & \dots & 0 \\ u_1^3 & u_2^3 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ u_1^n & u_2^n & u_3^n & \dots & 1 \end{pmatrix} \quad \text{et} \quad V = \begin{pmatrix} V_1^1 & V_2^1 & \dots & V_n^1 \\ 0 & V_2^2 & \dots & V_n^2 \\ \vdots & \vdots & & \\ 0 & 0 & \dots & V_n^n \end{pmatrix}$$

Les éléments de U et V se déterminent immédiatement en égalant successivement les éléments de ligne de A à ceux des lignes de U.V

Comme A.V = B et A = U.V, on obtient :

(U.V) X = B qui se décomposé en 2 équations

UY = B et ensuite VX = Y

On résout d'abord UY=B et ensuite VX=Y pour tirer les valeurs de X.***Exemple :***

Résoudre par la méthode de Choleski le système d'équations linéaires ci-dessous.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

a) $\begin{cases} x+2y=4 \\ 3x+7y=5 \end{cases}$ b) $\begin{cases} 2x-y+4z=-4 \\ 3x+2y-3z=17 \\ 5x-3y+8z=-10 \end{cases}$

Solution:

a) $\begin{cases} x+2y=4 \\ 3x+7y=5 \end{cases} \Leftrightarrow \begin{pmatrix} 1 & 2 \\ 3 & 7 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 4 \\ 5 \end{pmatrix} \Leftrightarrow$ A.X = B

Posons A= $\begin{pmatrix} 1 & 2 \\ 3 & 7 \end{pmatrix}$ U = $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$ et V= $\begin{pmatrix} b & c \\ 0 & d \end{pmatrix}$

Pour avoir U.V = $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \begin{pmatrix} b & c \\ 0 & d \end{pmatrix} = \begin{pmatrix} b & c \\ ab & ac+d \end{pmatrix}$

A = U.V $\Leftrightarrow \begin{pmatrix} 1 & 2 \\ 3 & 7 \end{pmatrix} = \begin{pmatrix} b & c \\ ab & ac+d \end{pmatrix}$

$$\begin{cases} b=1, c=2 \\ ab=-3, ac+d=7 \end{cases} \Leftrightarrow \begin{cases} b=1, c=2 \\ a=3, 6+d=7 \end{cases}$$

$\Leftrightarrow$ a = 3 ; b = 1 ; c = 2 et d = 1.

D'où U = $\begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}$; V = $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$

Résolvons d'abord l'équation

1°) U.Y = B $\Leftrightarrow \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 4 \\ 5 \end{pmatrix}$ avec $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$

$$\Leftrightarrow \begin{pmatrix} y_1 \\ 3y_1 + y_2 \end{pmatrix} = \begin{pmatrix} 4 \\ 5 \end{pmatrix} \Rightarrow \begin{cases} y_1 = 4 \\ 3y_1 + y_2 = 5 \Rightarrow y_2 = -7 \end{cases} \Leftrightarrow \begin{cases} y_1 = 1 \\ y_2 = -7 \end{cases}$$

Puis,

2°) V.X $= y \Leftrightarrow \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 4 \\ -7 \end{pmatrix} \Leftrightarrow \begin{cases} x+2y=4 \Rightarrow x=18 \\ y=-7 \end{cases}$ $d'où \quad S = \{(18,-7)\}$

d) Théorème de FONTENE – ROUCHE

Soit S $\equiv \sum_{i=1}^{m} a_i^j x_i = b_j \quad (j = 1, ..., n)$ un système de n équations à m inconnues et de rang r.

Si r = n, alors le système (S) admet des solutions obtenues en résolvant le système de cramer à r équations principales et en attribuant des valeurs arbitraires aux (n-r) inconnues.

r < n et l'un des déterminants principaux $\neq 0$ alors le système (S) n' a pas de solution.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

$r < n$ et tous les déterminants principaux sont nuls, alors le système (S) se réduit à r équations principales et se résoud comme au (i).

CHAPITRE VIII DIAGONALISATION D'UNE MATRICE CARREE

A. VALEUR ET VECTEUR PROPRE

Soit f un endomorphisme (endo) de E, avec E, un espace vectoriel de dimension n sur le corps commutatif K.

1. Définition (vecteur propre)

On appelle vecteur propre de f tout vecteur v de E tel qu'il existe un scalaire $\lambda \in K$ vérifiant $f(v) = \lambda v$(1)
Si v = 0, alors tout $\lambda \in K$ convient.
En effet, $f(0) = \lambda . 0 \Leftrightarrow 0 = \lambda .0$, vraie $\forall \lambda \in K$
Si $v \neq 0$, alors λ est unique.
Supposons qu'il existe $\lambda_1, \lambda_2 \in K$ tel que $f(v) = \lambda_1 V$ et $f(v) = \lambda_2 V$ et montrons que $\lambda_1 = \lambda_2$.
En effet $f(v) = \lambda_1 v$ et $f(v) = \lambda_2 v \Leftrightarrow \lambda_1 v = f(v) = \lambda_2 v$

$$\begin{aligned}
&\Leftrightarrow \lambda_1 v = \lambda_2 v \\
&\Leftrightarrow \lambda_1 v - \lambda_2 v = 0 \\
&\Leftrightarrow (\lambda_1 - \lambda_2)v = 0 \\
&\Leftrightarrow \lambda_1 - \lambda_2 = 0 \text{ car } v \neq 0 \\
&\Leftrightarrow \lambda_1 = \lambda_2
\end{aligned}$$

2. Définition (valeur propre)

On appelle valeur propre de f tout scalaire $\lambda \in K$ tel qu'il existe un vecteur non nul v de E vérifiant $f(v) = \lambda v$.
Si $\lambda \in K$ est une valeur propre de f, alors l'ensemble des vecteurs propres associés à λ constitue un sous-espace vectoriel de E. On le note par $V(\lambda)$.
c.à.d. $V(\lambda) = \{v \in E : f(v) = \lambda v\} \subset E$

Montrons aux exercices que $V(\lambda)$ est un sous-espace vectoriel de E.

3. Théorème :

Soit f un endo de E ; E un K-espace de dimension n.

A tout vecteur propre v de E correspond une valeur propre $\lambda \in K$ dite valeur propre associée à v.
A toute valeur propre $\lambda \in K$ correspond une infinité de vecteurs qui constitue un ensemble d'éléments $v \in E$ tel que $f(v) = \lambda v$. Il est noté par $V(\lambda)$ et appelé sous-espace propre associé à λ.
Preuve au T.P.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

4. Définition :

On appelle spectre de f, l'ensemble des valeurs propres de f. Noter qu'un endo f de E peut avoir au plus n valeurs propres si dim E = n.

5. Propositions (Somme directe des sous-espaces propres)

Soient $\lambda_1, \lambda_2, \ldots \lambda_k$, k valeurs propres distinctes de f, alors les sous-espaces propres $V(\lambda_1)$; $V(\lambda_2)$; … ; $V(\lambda_k)$ forment la somme directe de A, càd :

- $V(\lambda_i) \cap V(\lambda_j) = \{0\}$; $\forall$ i, j $\in$ {1, 2, …, k} avec $i \neq j$
- $V(\lambda_1) + V(\lambda_2) + \ldots + V(\lambda_k) = E$

Supposons que λ_1, λ_2 sont deux valeurs propres distinctes de f et montrons que $V(\lambda_1) \cap V(\lambda_2) = \{0\}$.
En effet, soit $V \in V(\lambda_1) \cap V(\lambda_2)$; Alors $v \in V(\lambda_1)$ et $v \in V(\lambda_2) \Leftrightarrow f(v) = \lambda_1 v$ et $f(v) = \lambda_2 v$.
Il suit que $\lambda_1 v = f(v) = \lambda_2 v \Leftrightarrow \lambda_1 v = \lambda_2 v \Leftrightarrow (\lambda_1 - \lambda_2)v = 0 \Leftrightarrow v = 0$
D'où $V(\lambda_1) \cap V(\lambda_2) = \{0\}$.

6. Corollaire :

Soient $\lambda_1, \lambda_2, \ldots \lambda_k$, k valeurs propres de f. Si $v_1, v_2, \ldots, v_k$ sont des vecteurs propres associés respectivement à ces valeurs propres, alors :
$\{v_1, v_2, \ldots, v_k\}$ est une famille linéairement indépendante (k< n)
$\{v_1, v_2, \ldots, v_k\}$ est une base de E ssi k = n c.à.d dét. $\{v_1, v_2, \ldots, v_n\} \neq 0$

7. Théorème :

Soient f un endo de E, E un K-espace de dimension n et $\lambda \in K$, alors les propositions suivantes sont équivalentes :

i) λ est une valeur propre de f
ii) $(f - \lambda\, id_E)$ n'est pas bijective avec

$$id_E : E \to E$$
$$v \mapsto id_E(v) = v, \text{ dite application identique de E}$$

Preuve :
Montrons que i) implique ii).
$\lambda \in K$, est une valeur propre de f $\Rightarrow \exists\ v \in E^*$ tel que $f(v) = \lambda v \Leftrightarrow f(v) - \lambda\, id_E(v) = 0$
$\Leftrightarrow (f - \lambda\, id_E)(v) = 0$
$\Leftrightarrow \operatorname{Ker}(f - id_E) \neq \{0\}$ car $V \neq 0$
$\Leftrightarrow f - id_E$ n'est pas injective
et par conséquent f n'est pas bijective.

8. Polynôme Caractéristiques d'un Endomorphisme

a) Théorème 1 :

Soit $A = (a_i^j)$ i = j = 1, …, n une matrice carrée d'ordre n à coefficient dans K, associée canoniquement à un endo f de K-espace E de dimension n, alors les propositions suivantes sont équivalentes :

- $\lambda \in K$ est une valeur propre
- $(A - \lambda I_n)$ n'est pas inversible
- $\text{Dét}(A - \lambda I_n) = 0$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Comme A = $\begin{pmatrix} a_1^1 & a_2^1 \dots a_n^1 \\ a_1^2 & a_2^2 \dots a_n^2 \\ \vdots & \vdots \quad \vdots \\ a_1^n & a_2^n \dots a_n^m \end{pmatrix}$

Alors A - λ I_n = $\begin{pmatrix} a_1^1 & a_2^1 \dots a_n^1 \\ a_1^2 & a_2^2 \dots a_n^2 \\ \vdots & \vdots \quad \vdots \\ a_1^n & a_2^n \dots a_n^n \end{pmatrix}$ + $\begin{pmatrix} -\lambda & 0 & \dots & 0 \\ 0 & -\lambda & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & -\lambda \end{pmatrix}$

$$= \begin{pmatrix} a_1^1 - \lambda & a_2^1 & \dots & a_n^1 \\ a_1^2 & a_2^2 - \lambda & \dots & a_n^1 \\ \vdots & \vdots & & \vdots \\ a_1^n & a_2^n & \dots & a_n^n - \lambda \end{pmatrix}.$$

D'où dét(A - λ I_n) = $\begin{vmatrix} a_1^1 - \lambda & a_2^1 & \dots & a_n^1 \\ a_1^2 & a_1^2 - \lambda & \dots & a_n^2 \\ \vdots & \vdots & & \vdots \\ a_1^n & a_2^n & \dots & a_n^n - \lambda \end{vmatrix}$

En calculant ce déterminant, on obtient un polynôme à une indéterminée (λ) et de degré n qu'on note par $P_A(\lambda)$ et qu'on appelle Polynôme Caractéristique de A.

$\Rightarrow$ $P_A(\lambda)$ = dét(A - λ I_n).

b) Théorème 2 :

Les valeurs propres de A sont les racines de son polynôme caractéristique. Il y en a n ou plus avec n l'ordre de la matrice A.

En résumé, pour chercher les valeurs et les vecteurs propres de A, on procède comme suit :

1° $P_A(\lambda)$ = dét (A - λ I_n). Poser $P_A(\lambda) = 0$ pour tirer les valeurs propres λ_1, λ_2, …, λ_n

2° Recherche des vecteurs propres associés à chacune des valeurs propres trouvées.

Pour une valeur propre λ_i , soit v $\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ vecteur propre associé à λ_1, alors (A -λ_i I_n) (v) = 0.

En calculant, on obtient un système de n équations linéaires et homogènes à n inconnues qui n'est pas de Cramer, dont l'ensemble des solutions est noté $S(\lambda_i) = V(\lambda_i)$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

9. Exemples :

Chercher les valeurs et vecteurs propres des matrices suivantes :

a) $A = \begin{pmatrix} 2 & 2 \\ 1 & 3 \end{pmatrix}$; b) $B = \begin{pmatrix} 4 & 2 \\ -1 & 1 \end{pmatrix}$; c) $A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$

Solution:

a) $A = \begin{pmatrix} 2 & 2 \\ 1 & 3 \end{pmatrix}$

$P_A(\lambda) = \begin{vmatrix} 2-\lambda & 2 \\ 1 & 3-\lambda \end{vmatrix} = (2 - \lambda)(3 - \lambda) - 2 = 6 - 3\lambda - 2\lambda + \lambda^2 - 2 = \lambda^2 - 5\lambda + 4$

Soit $P_A(\lambda) = \lambda^2 - 5\lambda + 4$, le polynôme caractéristique associé à la matrice A

Poser $P_A(\lambda) = 0$ ssi $\lambda^2 - 5\lambda + 4 = 0$ pour avoir $\lambda_1 = 1$, $\lambda_2 = 4$ comme valeurs propres de A.

Vecteurs propres associés à chacune des valeurs propres.

Pour $\lambda_1 = 1$, soit v $\begin{pmatrix} x \\ y \end{pmatrix}$ vecteur propre associé à $\lambda_1 = 1$, alors $(A - \lambda_1 I_2)(v) = 0$

Ssi $\begin{pmatrix} 2-1 & 2 \\ 1 & 3-1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \Leftrightarrow \begin{cases} x+2y=0 \\ x+2y=0 \end{cases} \Leftrightarrow x+2y = 0 \Leftrightarrow x = -2y$; $y \in IR$

D'où $S_1 = V(\lambda_1) = \{(x, y) \in IR^2 : x = -2y\}$

$= \{(-2y, y) : y \in IR\}$

$= \{y(-2, 1) : y \in IR\}$

$\Rightarrow V_1 = \begin{pmatrix} -2 \\ 1 \end{pmatrix}$ vecteur propre associé à $\lambda_1 = 1$

Pour $\lambda_2 = 4$; soit v$\begin{pmatrix} x \\ y \end{pmatrix}$ vecteur propre associé à λ_2

Alors $\begin{pmatrix} -2 & 2 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \Leftrightarrow \begin{cases} -2x+2y=0 \\ x-y=0 \end{cases} \Leftrightarrow x = y : y \in IR$

$\Rightarrow S_2 = V(\lambda_2) = \{(x, y) \in IR^2 : x=y\} = \{(y,y) : y \in IR\} = \{(1, 1) : y \in IR\}$

D'où $V_2\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ est un vecteur propre associé à $\lambda_2 = 4$

En résumé

$$\begin{cases} \lambda_1 = 1 \to V_1 = \begin{pmatrix} -2 \\ 1 \end{pmatrix} \\ \lambda_2 = 4 \to V_2 = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \end{cases}$$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

On constate que $\{V_1, V_2\}$ est une base de IR² formée des vecteurs propres car

$$\text{Dét}(V_1, V_2) = \begin{vmatrix} -2 & 1 \\ 1 & 1 \end{vmatrix} = -2 - 1 = -3 \neq 0$$

c) Soit $A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ une matrice carrée d'ordre trois.

$$\text{Alors } P_A(\lambda) = \begin{vmatrix} 2-\lambda & 1 & 1 \\ 1 & 2-\lambda & 1 \\ 1 & 1 & 2-\lambda \end{vmatrix}$$

$$= \begin{vmatrix} 2-\lambda & 1 & 0 \\ 1 & 2-\lambda & -1+\lambda \\ 1 & 1 & 1-\lambda \end{vmatrix}$$

$$= (1-\lambda) \begin{vmatrix} 2-\lambda & 1 & 0 \\ 1 & 2-\lambda & -1 \\ 1 & 1 & 1 \end{vmatrix} L_2+L_3$$

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

$$= (1-\lambda) \begin{vmatrix} 2-\lambda & 1 \\ 2 & 3-\lambda \end{vmatrix}$$

$$= (1-\lambda)[(2-\lambda)(3-\lambda) - 2] = (1-\lambda)(6 - 5\lambda + \lambda^2 - 2) = (1-\lambda)(\lambda^2 - 5\lambda + 4)$$

Soit $P_A(\lambda) = (1-\lambda)(\lambda^2 - 5\lambda + 4)$. D'où $P_A(\lambda) = 0$ ssi $\lambda_1=1$; $\lambda_2=1$; $\lambda_3=4$. Ce qui entraîne que les valeurs propres de A sont $\lambda_1=\lambda_2=1$; $\lambda_3=4$

Vecteurs propres associés à chacune des valeurs propres trouvées

Pour la valeur propre double $\lambda_1 = \lambda_2 = 1$ soit $V \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ vecteur propre associé à $\lambda_1 = \lambda_2 = 1$

Alors $(A - \lambda_1 I_3)V = 0 \Leftrightarrow \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \Leftrightarrow \begin{cases} x+y+z=0 \\ x+y+z=0 \\ x+y+z=0 \end{cases} \Rightarrow x = -y - z$;

avec $y, z \in$ IR

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

D'où $V(\lambda_1) = \{(x, y, z) \in IR : x = -y - z\}$
$= \{(-y - z ; y, z) ; y, z \in IR\}$
$= \{(-y, y, 0) + (-z, 0, z) ; y, z \in IR\}$
$= \{y(-1, 1, 0) + z(-1, 0, 1) : y, z \in \}$
$= \{y\mu_1 + z\mu_2 : y, z \in IR\}$, avec $\mu_1 = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}$ et $\mu_2 = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}$

D'où $\mu_1 = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}$ et $\mu_2 = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}$ sont les vecteurs propres associés à $\lambda_1 = \lambda_2 = 1$

Pour la valeur propre $\lambda_3 = 4$, soit $V\begin{pmatrix} x \\ y \\ z \end{pmatrix}$, un vecteur propre associé à $\lambda_3 = 4$

Alors $(A - 4I_3)V = 0 \Leftrightarrow \begin{pmatrix} -2 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & -2 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \Leftrightarrow \begin{cases} -2x + y + z = 0 \\ x - 2y + z = 0 \rightarrow L_1 + 2L_2 \\ x + y - 2z = 0 \rightarrow L_1 + 2L_3 \end{cases}$

Ssi $\begin{cases} -2x + y + z = 0 \\ -3y + 3z = 0 \\ 3y - 3z = 0 \end{cases} \Leftrightarrow \begin{cases} -2x + y + z = 0 \Rightarrow x = y \quad (1) \\ y - z = 0 \Rightarrow y = y \quad (2) \end{cases}$

(2) dans (1) $\Rightarrow -2x + 2z = 0 \Rightarrow x = z$; $z \in IR$

D'où $V(\lambda_3) = \{(x, y, z) \in IR^3 : x = z, y = z\}$
$= \{(z, z, z) ; z \in IR\}$
$= \{z(1, 1, 1) ; z \in IR\}$
$= \{z\mu_3 ; z \in IR\}$ avec $\mu_3 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$

$\Rightarrow \mu_3 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ est un vecteur propre associé à $\lambda_3 = 4$

En résumé à $\lambda_1 = \lambda_2 = 1$, on associe $\mu_1 = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}$, $\mu_2 = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}$ et à $\lambda_3 = 4$, on associe $\mu_3 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$

$\Rightarrow \{\mu_1, \mu_2, \mu_3\}$ est une base de IR^3 formée des vecteurs propre de A, car dét $(\mu_1, \mu_2, \mu_3) \neq 0$.

B. REDUCTION D'UNE MATRICE CARREE A LA FORME DIAGONALE

1. Théorème (Caractérisation des applications linéaires diagonalisables)

Soit f un endo de E, avec E un K-espace de dimension n sur le corps commutatif K. Alors les propositions suivantes sont équivalentes :

- f est diagonalisable
- E admet une base de vecteurs propres
- E admet une base dans laquelle f est réduit à la forme diagonale.
- Toute racine du polynôme caractéristique de f est réelle et de multiplicité égale à la dimension du sous-espace propre associé.

2. Corollaire :

Une matrice carrée A d'ordre n est dite diagonalisable ssi toutes les racines de son polynôme caractéristique sont réelles et simples.

3. Théorème (Matrices diagonalisables)

Soit A une matrice carrée d'ordre n, associée canoniquement à un endo f de E. D'après le théorème ci-dessus, les propositions suivantes sont équivalentes :

- A est une matrice diagonalisable
- A admet n vecteurs propres qui forment une base de E
- A est semblable à une matrice diagonale D. C.à.d il existe une matrice carrée P inversible d'ordre n telle que : $D = P^{-1}. A . P$

Toute racine du polynôme caractéristique de A est réelle et de multiplicité égale à la dimension du sous-espace propre associé.
P est dite matrice de passage de la base canonique de E à la base des vecteurs propres de E. Les colonnes de P sont les vecteurs propres correspondants aux valeurs propres. Les termes diagonaux de D sont les valeurs propres correspondant aux vecteurs propres de P

On a : $P = (V_1\ V_2 \dots V_n)$ et $D = P^{-1}. A .P = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix} = \mathit{diag}\,(\lambda_1, \lambda_2, ..., \lambda_n)$

4. Définition :

Deux matrices A et B sont semblables si elles ont les mêmes valeurs propres.

5. Exemples :

Diagonaliser si possible les matrices suivantes :

a) $A = \begin{pmatrix} 2 & 2 \\ 1 & 3 \end{pmatrix}$; b) $A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Solution :

a) A = $\begin{pmatrix} 2 & 2 \\ 1 & 3 \end{pmatrix}$, on sait que les valeurs propres de A et leurs vecteurs propres associés sont $\lambda_1 = 1$, $\lambda_2 = 4$.

A $\lambda_1 = 1$, on a associé $V_1 = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$ et à $\lambda_2 = 4$, on a aussi a associé $V_2 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

Comme A est une matrice d'ordre 2 et A admet deux vecteurs propres, alors A est diagonalisable :

$\Rightarrow P = (V_1\ V_2) = \begin{pmatrix} -2 & 1 \\ 1 & 1 \end{pmatrix}$, soit $P = \begin{pmatrix} -2 & 1 \\ 1 & 1 \end{pmatrix}$ la matrice de passage de la base canonique à la base des vecteurs propres de A

Alors, $D = P^{-1}.\ A\ .P = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} = \mathit{diag}\,(\lambda_1, \lambda_2)$.

En effet, la matrice $P = \begin{pmatrix} -2 & 1 \\ 1 & 1 \end{pmatrix}$ est inversible car det (P) = -3 $\neq$ 0.

Cherchons P^{-1}.

$\text{ComP} = \begin{pmatrix} 1 & -1 \\ -1 & -2 \end{pmatrix}$ et ${}^{*}P = \begin{pmatrix} 1 & -1 \\ -1 & -2 \end{pmatrix}$ entraînant que $P^{-1} = -\frac{1}{3}\begin{pmatrix} 1 & -1 \\ -1 & -2 \end{pmatrix} = \begin{pmatrix} -\frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{2}{3} \end{pmatrix}$

Calculons alors $D = P^{-1}.A.P$.

$$\text{On a } D = \begin{pmatrix} -\frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{2}{3} \end{pmatrix}\begin{pmatrix} 2 & 2 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} -\frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{2}{3} \end{pmatrix}\begin{pmatrix} -2 & 4 \\ 1 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}$$

D'où les matrices A et D sont semblables car elles ont les mêmes valeurs propres.

b) $A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

c) On sait d'après l'exemple c du IV. 1. 9, que $\{u_1 = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}$; $u_2 = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}$; $u_3 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$) est une base de IR^3 formée des vecteurs propres de A, alors $P = (u_1 u_2 u_3) = \begin{pmatrix} -1 & -1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ est la matrice de passage de la base canonique à la base des vecteurs propres.

Comme $\det P = \begin{vmatrix} -1 & -1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{vmatrix} = \begin{vmatrix} -1 & -1 & 1 \\ 0 & -1 & 2 \\ 0 & 1 & 1 \end{vmatrix} = 3 \neq 0$, alors P^{-1} existe et on a :

$D = P^{-1}.A.D = \mathrm{diag}(\lambda_1, \lambda_2, \lambda_3) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{pmatrix}$ à vérifier aux exercices.

Exercices.

Diagonaliser si possible les matrices ci-dessous :

a) $A = \begin{pmatrix} 4 & 2 \\ -1 & 1 \end{pmatrix}$; b) $A = \begin{pmatrix} 1 & -3 & 3 \\ 3 & -5 & 3 \\ 6 & -6 & 4 \end{pmatrix}$; c) $A = \begin{pmatrix} -15 & 1 & -9 \\ 0 & 6 & 0 \\ 4 & 1 & -3 \end{pmatrix}$

6. Remarque : (Puissance entière d'une matrice carrée d'ordre n)

Si $D = P^{-1}. A. P$, alors on peut exprimer A en fonction de P et D de la manière suivante

$$\begin{aligned} D = P^{-1}. A . P \Leftrightarrow P.D.P^{-1} &= P(P^{-1}.A .P)P^{-1} \\ &= (P.P^{-1}) . A .(P.P^{-1}) \\ &= I_n . A . I_n \\ &= A \end{aligned}$$

D'où $D = P^{-1}. A. P \Leftrightarrow \boxed{A = P. D. P^{-1}}$

Calculons alors A^n, $\forall\, n \in IN^*$

On a : $A^n = A . A . A . \dots . A$; or $A = P. D.P^{-1}$

Donc
$$\begin{aligned} A^n &= (P. D.P^{-1}) .(P.D.P^{-1}) . \dots . (P.D.P^{-1}) \\ &= P. D.P^{-1}. P.D.P^{-1}. \dots . P.D.P^{-1} \\ &= P.D(P^{-1}.P) . D.(P^{-1}.P).D. \dots .(P^{-1}.P).D.P^{-1} \\ &= P.D.I_n.D.I_n.D. \dots .I_n D P^{-1} \\ &= P.D.D.D. \dots .D.P^{-1} \\ &= P. D^n.P^{-1} \end{aligned}$$

D'où $\boxed{A^n = P.D^n.P^{-1}}$ avec $D^n = \mathrm{diag}\,(\lambda_1^n \lambda_2^n, \dots, \lambda_n^n)$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

$$= \begin{pmatrix} \lambda_1^n & 0 & \dots & 0 \\ 0 & \lambda_2^n & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & \lambda_n^n \end{pmatrix}$$

Définition :
Soit A une matrice carrée d'ordre n, on appelle Trace de A notée tr (A) la somme des valeurs propres de A ou la somme des éléments diagonaux de A.

7. Théorème de CALEY - HAMILTON

Toute matrice carrée A d'ordre n est une racine de son polynôme caractéristique.
C.à.d : Si $P_A(\lambda)$ est le polynôme caractéristique de A, alors $P_A(\lambda) = 0$

Remarque :
Si A est inversible, on peut chercher la matrice inverse à partir du théorème de *Cayley - Hamilton.*

***Exemple* :** $A = \begin{pmatrix} 2 & 2 \\ 1 & 3 \end{pmatrix}$

a) Diagonaliser A
b) Déterminer la trace (A)
c) Inverser si possible la matrice A à partir du théorème de *Cayley - Hamilton.*
d) Vérifier le théorème 7 ci – dessus.

Solution :
a) On sait que $P_A(\lambda) = \lambda^2 - 5\lambda + 4$ et les valeurs propres de A sont $\lambda_1 = 1$, $\lambda_2 = 4$.

à $\lambda_1 = 1 \;\rightarrow\; V_1 = \begin{pmatrix} -2 \\ 1 \end{pmatrix}$ et à $\lambda_2 = 4 \;\rightarrow\; V_2 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

D'où $P = (V_1\ V_2) = \begin{pmatrix} -2 & 1 \\ 1 & 1 \end{pmatrix}$ et $D = P^{-1}AP = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}$ (déjà fait)

Avec $P^{-1} = \begin{pmatrix} -\frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{2}{3} \end{pmatrix}$

b) La trace de A est égale à 1 + 4 = 2 + 3 = 5.

c) Calculons A^n.

On sait que $A^n = P.D^n.P^{-1} = \begin{pmatrix} -2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1^n & 0 \\ 0 & 4^n \end{pmatrix} \begin{pmatrix} \frac{-1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{2}{3} \end{pmatrix}$

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

$$= \begin{pmatrix} -2 & 4^n \\ 1 & 4^n \end{pmatrix} \begin{pmatrix} \frac{-1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{2}{3} \end{pmatrix}$$

$$= \begin{pmatrix} \frac{2+4^n}{3} & \frac{-2+2.4^n}{3} \\ \frac{-1+4^n}{3} & \frac{1+2.4^n}{3} \end{pmatrix}$$

D' où $A^n = \boxed{\begin{pmatrix} \frac{2+4^n}{3} & \frac{-2+2.4^n}{3} \\ \frac{-1+4^n}{3} & \frac{1+2.4^n}{3} \end{pmatrix}}$

Vérifions le théorème de Cayley Hamilton.

Comme A = $\begin{pmatrix} 2 & 2 \\ 1 & 3 \end{pmatrix}$ et $P_A(\lambda) = \lambda^2 - 5\lambda + 4$

Alors $P_A(A) = 0$ d' après le théorème de **Cayley – Hamilton**, vérifions que $P_A(A)=0$.

On a $P_A(A) = A^2 - 5A + 4I_2$.

Or $A^2 = \begin{pmatrix} 2 & 2 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 2 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 6 & 10 \\ 5 & 11 \end{pmatrix}$,

Donc $P_A(A) = \begin{pmatrix} 6 & 10 \\ 5 & 11 \end{pmatrix} + \begin{pmatrix} -10 & -10 \\ -5 & -15 \end{pmatrix} + \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Cherchons la matrice inverse de A à partir du théorème de *Cayley* - *Hamilton.*

On sait d'après le théorème de *Caley-Hamilton* que :

$P_A(A) = 0$ i.e. $A^2 - 5A + 4I_2 = 0$

Comme dét (A) = $4 \neq 0$, alors A^{-1} existe.

$\Rightarrow (A^2 - 5A + 4I_2)A^{-1} = 0A^{-1} \Leftrightarrow A - 5I_2 + 4A^{-1} = 0$

$\Rightarrow 4A^{-1} = 5I_2 - A$

$\Rightarrow A^{-1} = \frac{1}{4}[5I_2 - A]$

Soit $A^{-1} = \frac{1}{4}\left[\begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix} - \begin{pmatrix} 2 & 2 \\ 1 & 3 \end{pmatrix}\right] = \frac{1}{4}\begin{pmatrix} 3 & -2 \\ -1 & 2 \end{pmatrix}$

D'où $A^{-1} = \begin{pmatrix} \frac{3}{4} & \frac{-2}{4} \\ \frac{-1}{4} & \frac{2}{4} \end{pmatrix}$.

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Table des matières

CHAPITRE I
ELEMENTS DE LOGIQUE ET NOTION DES ENSEMBLES

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

CHAPITRE II
RELATIONS ET APPLICATIONS

CHAPITRE III
STRUCTURES ALGEBRIQUES

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

CHAPITRE IV
L'ENSEMBLE DES NOMBRES COMPLEXES

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

CHAPITRE V.
LE POLYNOME A UNE INDETRMINEE

CHAPITRE VI
CALCUL MATRICIEL ET APPLICATIONS LINEAIRES

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com

CHAPITRE VII
SYSTEMES D'EQUATIONS LINEAIRES
EQUATION LINEAIRE

CHAPITRE VIII
DIAGONALISATION D'UNE MATRICE CARREE

Print by Maison FAKAM, contact : 0994907833, 0853366628, alinabiwenyamuhanga@yahoo.com