Cours de mathématiques – Terminale scientifique (enseignement de spécialité)

Chapitre 0 – Raisonnements

I – Le raisonnement par l'absurde

Principe : Le raisonnement par l'absurde consiste à démontrer qu'une proposition est vraie en supposant qu'elle est fausse, puis, en utilisant des raisonnements corrects, à aboutir à une absurdité logique.
Comme les raisonnements sont rigoureux, la seule erreur est l'hypothèse de départ.

Exemple historique : Démontrons par l'absurde que $\sqrt{2}\notin\mathbb{Q}$ *– c'est-à-dire que* $\sqrt{2}$ *ne peut pas s'écrire sous forme d'une fraction de nombres entiers.*
Supposons que $\sqrt{2}\in\mathbb{Q}$ **.**
Il existe donc $p\in\mathbb{N}^*$ *et* $q\in\mathbb{N}^*$ *tels que* $\sqrt{2}=\frac{p}{q}$ *est irréductible.*
On a alors $2=\frac{p^2}{q^2}\Rightarrow 2q^2=p^2$ *(1)*
On en déduit que p *est un nombre pair (s'il était impair,* p^2 *serait impair...) donc il existe* $p'\in\mathbb{N}$ *tel que* $p=2p'$ *.*
On a donc $p^2=4p'^2$ *. En remplaçant dans (1), on obtient* $2q^2=4p'^2\Rightarrow q^2=2p'^2$ *(2)*
On en déduit là-encore que q *est pair, il existe donc* $q'\in\mathbb{N}$ *tel que* $q=2q'$ *.*
On en déduit que $\sqrt{2}=\frac{p}{q}=\frac{2p'}{2q'}=\frac{p'}{q'}$ *. Finalement on peut simplifier la fraction par 2, ce qui est absurde puisque* $\frac{p}{q}$ *est irréductible.*
Conclusion : L'hypothèse $\sqrt{2}\in\mathbb{Q}$ *est absurde, donc* $\sqrt{2}\notin\mathbb{Q}$ *.*

Exercice 1 : Sur une île, il y a deux types d'habitants.
Les menteurs qui mentent toujours et les honnêtes qui disent toujours la vérité.
Un homme dit : « Je suis un menteur »
Démontrer par l'absurde que cet homme n'est pas un habitant de l'île.

Exercice 2 : Démontrer par l'absurde la proposition suivante :
Pour tous réels $a>0$ et $b>0$, on a $\sqrt{a+b}<\sqrt{a}+\sqrt{b}$.

II – Le raisonnement par récurrence

Principe : Le raisonnement par récurrence s'utilise pour démontrer une propriété vraie pour tout entier $n \geqslant n_0$ avec $n_0 \in \mathbb{N}$ – c'est-à-dire que la propriété est vraie à partir du rang $n_0 \in \mathbb{N}$.
Il comporte deux étapes :

- *Initialisation :* On démontrer que la propriété est vraie au premier rang n_0.
- *Hérédité :* On démontre que si la propriété est vraie au rang n, alors elle est vraie au rang suivant $n+1$.

Cela permet de vérifier que la propriété est vraie pour tout $n \geqslant n_0$:

- Elle est vraie pour n_0 grâce à l'initialisation.
- Comme elle est vraie pour n_0, l'hérédité assure qu'elle est vraie au rang suivant n_0+1.
- Comme elle est vraie pour n_0+1, l'hérédité assure qu'elle est vraie au rang suivant n_0+2.
- Et ainsi de suite...

Illustration : Ce type de démonstration peut être illustré par une suite de dominos : on fait tomber un domino – l'initialisation – et comme la chute d'un domino entraine la chute du domino suivant – l'hérédité – alors tous les dominos seront tombés à la fin.

Exemple : On a vu en classe de première que pour tout $n \in \mathbb{N}$, $0+1+2+\ldots+n=\dfrac{n(n+1)}{2}$, *ce qui se note* $\sum_{k=0}^{n} k=\dfrac{n(n+1)}{2}$. *Démontrons cette propriété par récurrence.*

Soit $P(n)$ *la propriété* $\sum_{k=0}^{n} k=\dfrac{n(n+1)}{2}$.

- *Initialisation : Montrons* $P(0)$ *:*
  On a $\sum_{k=0}^{0} k=0$, *et* $\dfrac{0(0+1)}{2}=0$ *donc* $P(0)$ *est vraie.*
- *Hérédité : Supposons que* $P(n)$ *soit vraie :* $0+1+2+\ldots+n=\dfrac{n(n+1)}{2}$ *(1).*
  Montrons que $P(n+1)$ *est alors vraie également.*
  Pour obtenir la somme souhaitée, on ajoute $n+1$ *à chaque membre de (1) :*
  $0+1+2+\ldots+n+(n+1)=\dfrac{n(n+1)}{2}+n+1 \Leftrightarrow \sum_{k=0}^{n+1} k=\dfrac{n(n+1)}{2}+\dfrac{2(n+1)}{2} \Leftrightarrow \sum_{k=0}^{n+1} k=\dfrac{(n+1)(n+2)}{2}$
  $P(n+1)$ *est donc vraie.*
- *Conclusion : Pour tout* $n \in \mathbb{N}$, $\sum_{k=0}^{n} k=\dfrac{n(n+1)}{2}$.

Exercice 3 : Démontrer par récurrence que pour tout $n \in \mathbb{N}$, $\sum_{k=0}^{n} k^2=\dfrac{n(n+1)(2n+1)}{6}$.

Exercice 4 :
Définition : Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$. On dit que a *divise* b (ou que b est un *multiple* de a) s'il existe $k \in \mathbb{Z}$ tel que $b=ka$.
a) Démontrer par récurrence que pour tout $n \in \mathbb{N}$, 6 divise 7^n-1.
b) Démontrer par récurrence que pour tout $n \in \mathbb{N}$, 3 divise n^3-n.

Chapitre 1 – Divisibilité dans $\mathbb{Z}$

<u>Définitions :</u> On note $\mathbb{N}$ l'ensemble des *entiers naturels* : $\mathbb{N}=\{0;1;2;3;4;...\}$
On note $\mathbb{Z}$ l'ensemble des *entiers relatifs* : $\mathbb{Z}=\{...;-4;-3;-2;-1;0;1;2;3;4;...\}$

I – Divisibilité dans $\mathbb{Z}$

a) Multiples et diviseurs d'un nombre entier relatif

<u>Définition :</u> Soient $a\in\mathbb{Z}$ et $b\in\mathbb{Z}$. On dit que a *divise* b (ou que b est un *multiple* de a) s'il existe $k\in\mathbb{Z}$ tel que $b=ka$. On note $a|b$, et $a\nmid b$ dans le cas contraire.

<u>Remarques :</u>

- Pour tout $a\in\mathbb{Z}$, $0\times a=0$ donc tout entier relatif a divise 0.
- Tout entier relatif non nul b possède un nombre fini de diviseurs : en effet, ses diviseurs sont en valeur absolue inférieurs ou égaux à $|b|$, les diviseurs appartiennent à $\{-|b|;...;-1;1;...;|b|\}$. b a donc au plus $2|b|$ diviseurs.

<u>Exemple :</u> L'ensemble des diviseurs dans $\mathbb{Z}$ de 24 sont :
$\{-24;-12;-8;-6;-4;-3;-2;-1;1;2;3;4;6;8;12;24\}$.

<u>Exercice 1 :</u> Écrire un algorithme qui donne les diviseurs dans $\mathbb{N}$ d'un entier naturel.
Sur Texas Instruments, on pourra utiliser les instructions « **partDéc** » et « **partEnt** » qui se trouvent dans **math - NUM**.
Sur Casio, on pourra utiliser l'instruction « **Frac** » qui se trouve dans **OPTN - NUM**.
Ces instructions donnent la partie décimale et la partie entière d'un nombre.

b) Propriétés de la division dans l'ensemble des entiers relatifs

a, b et c sont trois entiers relatifs non nuls.

<u>Propriété :</u> Si $a|b$ et $a|c$, alors pour tout $u\in\mathbb{Z}$ et $v\in\mathbb{Z}$, $a|ub+vc$.

<u>Preuve :</u> Si $a|b$, alors il existe $k\in\mathbb{Z}$ tel que $b=ka$.
Si $a|b$, alors il existe $k'\in\mathbb{Z}$ tel que $b=k'a$.
On en déduit que $ub+vc=uka+vk'a=a(uk+vk')$ donc $a|ub+vc$ puisque $uk+vk'\in\mathbb{Z}$.

<u>Exercice résolu :</u> Soit $n\in\mathbb{Z}$ tel que $n|n+8$. Déterminons les valeurs possibles de n.

- $n|n$ et $n|n+8$ donc $n|n+8-n\Rightarrow n|8$.
- Réciproquement, si $n|8$, comme $n|n$, alors $n|n+8$.

Conclusion : $n|n+8\Leftrightarrow n|8$. Les valeurs possibles pour n sont donc $-8;-4;-2;-1;1;2;4;8$.

<u>Propriété (transitivité) :</u> Si $a|b$ et $b|c$ alors $a|c$.

<u>Preuve :</u> Si $a|b$, alors il existe $k\in\mathbb{Z}$ tel que $b=ka$. Si $b|c$, alors il existe $k'\in\mathbb{Z}$ tel que $c=k'b$. On a donc $c=k'ka$ donc $a|c$ puisque $kk'\in\mathbb{Z}$.

II – Division euclidienne

<u>Théorème et définition :</u> Soient $a\in\mathbb{N}$ et $b\in\mathbb{N}$ avec $b\neq 0$.
Il existe un <u>unique</u> couple (q,r) d'entiers naturels tels que $a=bq+r$ avec $0\leqslant r<b$.
On dit que a est le *dividende*, b le *diviseur*, q le *quotient* et r le *reste* dans la division euclidienne de a par b .

<u>Remarques :</u>

- Le mot « diviseur » n'a pas le même sens ici que dans la partie I.
- Il y a de multiples écritures de a sous la forme $bq+r$: par exemple, pour $a=103$ et $b=13$, on a $103=13\times 7+12=13\times 6+25=13\times 5+38$, *etc.*
  Mais seule la première égalité est la relation de division euclidienne, car $0\leqslant 12<13$.
- Lorsqu'on réalise une division « à la main », on réalise une division euclidienne.

<u>Interprétation graphique :</u> On encadre a par deux multiples consécutifs de b .

Cette interprétation permet de comprendre comment on étend la division euclidienne à $\mathbb{Z}$:
Soient $a\in\mathbb{Z}$, $b\in\mathbb{Z}$ avec $b\neq 0$, il existe un unique couple (q,r) tel que $a=bq+r$ avec $0\leqslant r<|b|$.

<u>Propriété admise pour la preuve du théorème :</u> On admettra le résultat suivant :
Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

<u>Exemples et contre-exemples :</u>

- *0 est le plus petit élément de $\mathbb{N}$.*
- *$\mathbb{Z}$ n'a pas de plus petit élément.*
- *Dans $\mathbb{R}$, la propriété est fausse : l'intervalle $]-3;8]$ n'a pas de plus petit élément.*

<u>Preuve du théorème :</u>

- Existence de q et r :
  1er cas : Si $0\leqslant a<b$, le couple $(q,r)=(0,a)$ convient.
  2d cas : Si $b\leqslant a$, alors $1\leqslant b\leqslant a$ car b est non nul.
  Soit M l'ensemble des multiples de b strictement supérieurs à a .
  L'entier $2b\times a$ appartient à M car $b\geqslant 1$ donc $2b\times a\geqslant 2a>a$.
  Donc M est une partie non vide de $\mathbb{N}$ et d'après la propriété précédente, il possède un plus petit élément, c'est-à-dire un multiple de b strictement supérieur à a tel que le multiple précédent soit inférieur ou égal à a . Soit qb ce multiple précédent.
  Il existe donc un entier relatif q tel que $qb\leqslant a<(q+1)b$.

Comme $b \leqslant a$, on a $b \leqslant a < (q+1)b$ donc $0 < q$ car $b \neq 0$ et donc q est un entier naturel.
Posons alors $r = a - bq$. Comme a, b et q sont des entiers, r est un entier également.
De $qb \leqslant a$, on en déduit que $r \geqslant 0$, donc r est un entier naturel.
De $(q+1)b > a$, on en déduit que $r < b$.
Dans les deux cas, on a trouvé un couple (q, r) tel que $a = bq + r$ avec $0 \leqslant r < b$.

- Unicité du couple (q, r) :
  Supposons qu'il existe deux couples (q, r) et (q', r') tels que :
  $a = bq + r = bq' + r'$ (1) avec $0 \leqslant r < b$ et $0 \leqslant r' < b'$ (2).
  De (1), on déduit que $b(q - q') = r' - r$ avec $q' - q$ entier, donc $r' - r$ est un multiple de b. De (2), on déduit que $-b < r' - r < b$. Le seule multiple de b strictement compris entre $-b$ et b est 0, donc $r' - r = 0$, soir $r' = r$. Par (1), on en déduit que $q' = q$. Donc (q, r) est unique.

Exercice 2 : Écrire à la calculatrice un programme qui effectue la division euclidienne de deux entiers.

III – Congruences dans $\mathbb{Z}$

Propriété et définition : Soit c un entier naturel non nul. Deux entiers relatifs a et b ont même reste dans la division euclidienne par c si et seulement si $a - b$ est un multiple de c. Si c'est le cas, on dit que a et b sont congrus modulo c (ou que a est congru à b modulo c). On note $a \equiv b\,(c)$ ou $a \equiv b\,(mod\ c)$ ou $a \equiv b\,[c]$ ou $a \equiv b\,[mod\ c]$.

Exemples : Si on s'intéresse aux congruences modulo 4, on a :
$5 \equiv 1\,(mod\ 4)$, $6 \equiv 2\,(mod\ 4)$, $7 \equiv 3\,(mod\ 4)$, $8 \equiv 0\,(mod\ 4)$, $9 \equiv 1\,(mod\ 4)$, …

Preuve de la propriété : On écrit les relations de division euclidienne par c : $a = cq + r$, $0 \leqslant r < c$ et $b = cq + r'$, $0 \leqslant r' < c$.

- Supposons que $r = r'$, alors $a - b = c(q - q')$ avec $q - q'$ entier, donc $a - b$ est un multiple de c.
- Réciproquement, si $a - b$ est multiple de c, alors $c \mid a - b$ et comme $c \mid c(q - q')$, alors par combinaison linéaire, $c \mid r - r'$. Comme $-c < r - r' < c$, il faut que $r - r' = 0$, soit $r = r'$.

Exercice résolu : Démontrons que $214 \equiv 25\,(9)$.
$214 - 25 = 189 = 9 \times 21$ donc $214 \equiv 25\,(9)$.

Remarques : Soient a un entier relatif et c un entier naturel non nul.

- a est un multiple de c si et seulement si $a \equiv 0\,[c]$.
- Les nombres congrus à a modulo c sont les nombres de la forme $a + kc$ avec $k \in \mathbb{Z}$.
- r est le reste de la division euclidienne de a par c si et seulement si on a $a \equiv r\,(mod\ c)$ et $0 \leqslant r < c$.

Propriété (transitivité) : Soient a, a' et a'' des entiers relatifs et c un entier naturel non nul.
Si $a \equiv a'\,(mod\ c)$ et $a' \equiv a''\,(mod\ c)$, alors $a \equiv a''\,(mod\ c)$.

Propriétés (congruences et opérations) : Soient a , b , a' , b' des entiers relatifs et c un entier naturel non nul. Si $a\equiv b\,(mod\,c)$ et $a'\equiv b'\,(mod\,c)$, alors :

- $a+a'\equiv b+b'\,(mod\,c)$ **et** $a-a'\equiv b-b'\,(mod\,c)$
- $a\,a'\equiv b\,b'\,(mod\,c)$
- $a^n\equiv b^n\,(mod\,c)$ **pour tout** $n\in\mathbb{N}^*$ **.**

Preuve : Par hypothèse, il existe $k\in\mathbb{Z}$ et $k'\in\mathbb{Z}$ tels que $a=b+k\,c$ et $a'=b'+k'\,c$.

- $a+a'=b+b'+(k+k')c$ avec $k+k'$ entier, donc $a+a'\equiv b+b'\,(c)$.
- $a\,a'=b\,b'+(b\,k'+b'\,k+k\,k'\,c)c$ avec $b\,k'+b'\,k+k\,k'\,c$ entier, donc $a\,a'\equiv b\,b'\,(c)$.
- Pour la dernière relation, c'est une récurrence sur la relation précédente.

Remarques : Les règles opératoires sont les mêmes qu'avec une égalité classique, cependant :

- Il n'y a pas de division, ou de « simplification » : $22\equiv 18\,(4)$ mais 11 et 9 ne sont pas congrus modulo 4.
- Pas de propriété hasardeuse avec les puissances : $5\equiv 1\,(4)$, mais $2^5\equiv 64\equiv 0\,(4)$ et $2^1\equiv 2\,(4)$ donc 2^5 et 2^1 ne sont pas congrus modulo 4.

Exercice résolu : Cherchons le reste de la division euclidienne de 2^{342} par 5.
$2^2=4$, $2^3=8$ et $2^4=16$ donc $2^2\equiv 4\,(5)$, $2^3\equiv 3\,(5)$ et $2^4\equiv 1\,(5)$.
$342=4\times 85+2$ donc $2^{342}\equiv 2^{4\times 85+2}\equiv (2^4)^{85}\times 2^2\,(5)$ donc $2^{342}\equiv 1^{85}\times 4\,(5)$ soit $2^{342}\equiv 4\,(5)$.
Comme $0\leqslant 4<5$, 2^{342} a pour reste 4 dans la division euclidienne par 5.

Chapitre 2 – Théorèmes de Bézout et de Gauss

I – PGCD de deux entiers relatifs

a) Définition et propriétés de réduction

Exemple : Les diviseurs de 12 sont 1 ; 2 ; 3 ; 4 ; 6 ; 12 et leurs opposés.
Les diviseurs de – 9 sont 1 ; 3 ; 9 et leurs opposés.
Les diviseurs communs à – 9 et 12 sont donc 1 ; 3 et leurs opposés (– 1 et – 3).

Remarques :
- Pour tout $a\in\mathbb{Z}$, les diviseurs communs à 0 et a sont les diviseurs de a.
- Pour tout $a\in\mathbb{Z}$, les diviseurs communs à 1 et a sont – 1 et 1.

Propriété et définition : Soient a et b deux entiers relatifs non tous les deux nuls.
L'ensemble des diviseurs communs à a et b admet un plus grand élément ; on l'appelle Plus Grand Commun Diviseur de a et b et on le note $PGCD(a;b)$.

Exemples : $PGCD(-9;12)=3$; $PGCD(-1;45)=1$; $PGCD(0;-457)=457$; $PGCD(100;75)=25$.

Preuve : Supposons que $a\neq 0$. L'ensemble des diviseurs communs de a et b est non vide puisqu'il contient 1 et – 1. Cet ensemble est fini car il ne contient que des entiers compris entre $-a$ et a. Donc il admet un plus grand élément qui est le plus grand des diviseurs communs à a et b.

Remarques : Soient a et b deux entiers relatifs non tous les deux nuls.
- $PGCD(a;b)\in\mathbb{N}$.
- $PGCD(a;b)=PGCD(b;a)=PGCD(|a|;|b|)$; on se ramène en général au cas où a et b sont positifs.
- $PGCD(1;b)=1$ et $PGCD(0;b)=|b|$ (avec ici $b\neq 0$).

Définition : a et b sont premiers entre eux si et seulement si $PGCD(a;b)=1$.

Exemple : $PGCD(47;15)=1$ *donc 47 et 15 sont premiers entre eux.*

Propriété : Soit $D(a;b)$ l'ensemble des diviseurs communs à deux entiers relatifs a et b.
Alors $D(a;b)=D(a-k\times b;b)$ pour tout $k\in\mathbb{Z}$.

Preuve :
- Si d divise a et b, alors d divise a et $a-kb$ pour tout $k\in\mathbb{Z}$, donc d divise $a-kb$ et b.
- Si d divise $a-kb$ et b, alors d divise $(a-kb)+kb$ c'est-à-dire a, donc d divise a et b.
  Conclusion : $D(a;b)=D(a-kb;b)$ pour tout $k\in\mathbb{Z}$.

Exemple : $D(63;75)=D(63;75-63)=D(63;12)=D(63-5\times12;12)=D(3;12)=\{-3;-1;1;3\}$

Propriété de réduction du PGCD : Soient a et b deux entiers relatifs non tous les deux nuls.

- **$PGCD(a;b)=PGCD(a-kb;b)$ pour tout $k\in\mathbb{Z}$.**
- **Si $0<b\leqslant a$, $PGCD(a;b)=PGCD(r;b)$ où r est le reste de la division euclidienne de a par b.**
- **Si b est un diviseur positif de a, $PGCD(a;b)=b$.**

Preuve :

- C'est une conséquence immédiate de la propriété précédente.
- Si $0<b\leqslant a$, on applique l'égalité précédente avec $k=q$, quotient de la division euclidienne de a par b.
- Si $b|a$ avec $b>0$, $r=0$ donc $PGCD(a;b)=PGCD(0;b)=b$.

b) L'algorithme d'Euclide

Cet algorithme permet de déterminer le PGCD de deux entiers naturels non tous les deux nuls, en utilisant la relation :
Si $0<b\leqslant a$, $PGCD(a;b)=PGCD(r;b)$ où r est le reste de la division euclidienne de a par b.

Exemple : Cherchons $PGCD(240;36)$.

a	$=$	b	$\times$	q	$+$	r
240	$=$	36	$\times$	6	$+$	24
36	$=$	24	$\times$	1	$+$	12
24	$=$	12	$\times$	2	$+$	0

On déduit de ces relations que :
$PGCD(240;36)=PGCD(24;36)=PGCD(12;24)=PGCD(12;0)=12$.

Propriété (algorithme d'Euclide) :
Soient a et b deux entiers tels que $0<b\leqslant a$.
L'algorithme suivant permet de calculer en un nombre fini d'étapes $PGCD(a;b)$.

- **Calculer le reste r de la division euclidienne de a par b.**
- **Tant que $r\neq0$, remplacer a par b et b par r.**
- **Calculer le reste r de la division euclidienne de a par b.**
- **Fin Tant que.**
- **Retourner b.**

Preuve : Écrivons les divisions successives : $a=bq_0+r_0$ avec $0\leqslant r_0<b$.

- Si $r_0=0$, on s'arrête à cette première étape.
- Si $r_0\neq0$, on remplace a par b et b par r_0 : $b=r_0q_1+r_1$ avec $0\leqslant r_1<r_0$.
- Si $r_1\neq0$, on remplace b par r_0 et r_0 par r_1 : $r_0=r_1q_2+r_2$ avec $0\leqslant r_2<r_1$.
- Si $r_2\neq0$, on remplace r_0 par r_1 et r_1 par r_2 : $r_1=r_2q_3+r_3$ avec $0\leqslant r_3<r_2$.

On construit ainsi une liste strictement décroissante r_0, r_1, r_2, … Or il n'y a qu'un nombre fini d'entiers entre r_0 et 0. Cette liste est donc finie donc il existe $k\in\mathbb{N}$ tel que $r_k\neq0$ et $r_{k+1}=0$.
Comme $r_{k+1}=0$, l'algorithme s'arrête. Il comporte bien un nombre fini d'étapes.
On a donc $PGCD(a;b)=PGCD(r_k;r_{k+1})=PGCD(r_k;0)=r_k$ (dernier reste non nul).

Exercice : Écrire à la calculatrice un programme déterminant le PGCD de deux entiers naturels avec l'algorithme d'Euclide.

Propriété : Soient a et b deux entiers relatifs non tous les deux nuls.
Les diviseurs communs à a et b sont les diviseurs de leur PGCD.

Exemple : Déterminons les diviseurs communs à – 12 458 et 3 272.
Cherchons $PGCD(12458;3272)$:

- $12458=3272\times3+2642$
- $3272=2642\times1+630$
- $2642=630\times4+122$
- $630=122\times5+20$
- $122=20\times6+2$
- $20=2\times10+0$

On a donc $PGCD(-12458;3272)=2$ donc les diviseurs communs à – 12 458 et 3 272 sont : – 2 ; – 1 ; 1 ; 2.

Preuve : Deux nombres entiers opposés ayant les mêmes diviseurs, on peut supposer $0\leqslant b\leqslant a$.

- Si $b=0$, alors $a\neq0$. $D(a,b)=D(a)$ et $PGCD(a;b)=a$ donc la propriété est vraie.
- Si $b\neq0$ et $b|a$, $D(a;b)=D(b)$ avec $b=PGCD(a;b)$ donc la propriété est encore vraie.
- Si $b\neq0$ et $b\nmid a$, avec les notations de la preuve de l'algorithme d'Euclide et la propriété on a : $D(a;b)=D(r_0;b)=D(r_0;r_1)=\ldots=D(r_k;r_{k+1})=D(r_k;0)=D(r_k)$ avec $r_k=PGCD(a;b)$.

c) Autres propriétés du PGCD de deux entiers

Propriété d'homogénéité : Soient a et b deux entiers relatifs non tous les deux nuls.
Pour tout $\lambda\in\mathbb{N}^*$, $PGCD(\lambda a;\lambda b)=\lambda PGCD(a;b)$.

Preuve : Si a ou b est nul, ou si $a|b$, le résultat est trivial.
Sinon, on suppose $0<b<a$. La recherche de $PGCD(\lambda a;\lambda b)$ à l'aide de l'algorithme d'Euclide conduit à écrire des égalités qui sont celles de la recherche de $PGCD(a;b)$ multipliées par λ.
Pour le dernier reste non nul, on aura donc $PGCD(\lambda a;\lambda b)=\lambda PGCD(a;b)$.

Exemple : $PGCD(150;100)=50$ $PGCD(3;2)=50\times1=50$.

Propriété caractéristique : Soient a et b deux entiers relatifs non tous les deux nuls et d un entier naturel. $d=PGCD(a;b)\Leftrightarrow\begin{cases}a=da'\\b=ba'\end{cases}$ avec a' et b' premiers entre eux.

Preuve : Si $d=PGCD(a;b)$, il existe a' et b' tels que $a=da'$ et $b=db'$.
Alors, $PGCD(a;b)=PGCD(da';db')=d\,PGCD(a';b')$ par homogénéité, puisque $d\in\mathbb{N}^*$.
Comme $PGCD(a;b)=d$, on en déduit que $PGCD(a';b')=1$ et donc que a' et b' sont premiers entre eux.
Réciproquement, si $a=da'$ et $b=db'$ avec a' et b' premiers entre eux et $d\in\mathbb{N}$, alors $d\neq0$ car a et b sont non tous les deux nuls, donc par homogénéité,
$PGCD(a;b)=d\,PGCD(a';b')=d\times1=d$.

Exemple : *$90=9\times10$ et $40=4\times10$ avec 9 et 4 premiers entre eux donc* $PGCD(90;40)=10$.

II – Théorème de Bézout et théorème de Gauss

<u>Propriétés :</u> Soient a et b deux entiers relatifs non tous les deux nuls et $d=PGCD(a;b)$.
1. Il existe u et v entiers relatifs tels que $au+bv=d$: c'est la relation de Bézout.
2. L'ensemble des entiers $au+bv$ (avec $u\in\mathbb{Z}$, $v\in\mathbb{Z}$) est l'ensemble des multiples de d.

<u>Remarque :</u> Il n'y a pas unicité du couple $(u;v)$ tel que $au+bv=d$.

<u>Preuve :</u>
1. On utilise les notations de la démonstration de l'algorithme d'Euclide.
De $a=bq_0+r_0$ on obtient $r_0=a-bq_0=au_0+bv_0$ avec $u_0=1$ et $v_0=-q$ qui sont des entiers.
De $b=r_0q_1+r_1$, on obtient $r_1=b-q_1r_1=b-(au_0+bv_0)q_1=au_1+bv_1$ avec $u_1=-u_0q_1$ et $v_1=1-v_0q_1$ entiers.
Pas-à-pas, on exprime chaque reste comme combinaison linéaire entière de a et b jusqu'à r_k, c'est-à-dire d.
2. Soit $n=au+bv$ avec u et v appartenant à $\mathbb{Z}$. Comme d divise a et b, d divise n. Toute combinaison linéaire de a et b est un multiple de d.
Réciproquement, si n est un multiple de d, il existe $k\in\mathbb{Z}$ tel que $n=kd$. Or, il existe u et v entiers tels que $d=au+bv$ donc $n=(ku)a+(kv)b$. Il existe donc deux entiers u' et v' tels que $n=au'+bv'$. Tout multiple de d est une combinaison linéaire entière de a et b.

<u>Exemple :</u> Pour $a=231$, et $b=165$, on a :
- $231=165+66$
- $165=66\times2+33$
- $66=33\times2+0$

Donc $PGCD(231;165)=33$. En utilisant les relations précédentes, on a :
- $33=165-66\times2$
- $66=231-165$

Donc $\mathbf{33=165-(231-165)\times2=165-2\times231+165\times2=165\times3+231\times(-2)}$.
On remarque que l'on a aussi : $\mathbf{165\times17+231\times(-12)=33}$.

<u>Théorème de Bézout :</u> Soient a et b deux entiers relatifs.
a et b sont premiers entre eux si et seulement si il existe deux entiers relatifs u et v tels que $au+bv=1$.

<u>Preuve :</u> Si a et b sont premiers entre eux, $d=1$ et d'après la proposition précédente, il existe $u\in\mathbb{Z}$ et $v\in\mathbb{Z}$ tels que $au+bv=1$.
Réciproquement, s'il existe $u\in\mathbb{Z}$ et $v\in\mathbb{Z}$ tels que $au+bv=1$, alors un diviseur commun à a et b divise 1, donc c'est soit 1 soit – 1 donc $PGCD(a;b)=1$.

<u>Exemples :</u>
- *$a=4$ et $b=-9$ sont premiers entre eux car $4\times(-2)+9\times1=1$.*
- *Deux entiers consécutifs sont toujours premiers entre eux, car pour $n\in\mathbb{Z}$, $n\times(-1)+(n+1)\times1=1$.*

<u>Théorème de Gauss :</u> Soient a , b et c trois entiers relatifs non nuls.
Si a divise bc et si a est premier avec b , alors a divise c .

<u>Exemple :</u> 5 divise $75=3\times 25$, 5 et 3 sont premiers entre eux donc 5 divise 25.

<u>Contre-exemple :</u> Pour $a=12$, $b=6$ et $c=10$, a n'est premier ni avec b , ni avec c .
a divise $bc=60$, mais a ne divise ni b ni c .
L'hypothèse a premier avec b est donc capitale.

<u>Preuve :</u> a divise bc donc il existe $k\in\mathbb{Z}$ tel que $bc=ka$. Comme a et b sont premiers entre eux, il existe u et v entiers relatifs tels que $au+bv=1$.
En multipliant par c cette relation, on obtient : $acu+bcv=c$, soit $acu+kav=c$ soit $a(cu+kv)=c$. Comme $cu+kv\in\mathbb{Z}$, a divise c .

<u>Corollaire du théorème de Gauss :</u> Si deux nombres premiers entre eux a et b divisent un entier c , alors ab divise c .

<u>Exemple :</u> 5 divise 100, 4 divise 100. Comme 5 et 4 sont premiers entre eux, $5\times 4=20$ divise 100.

<u>Preuve :</u> $a|c$ donc il existe $k\in\mathbb{Z}$ tel que $c=ka$. Comme b est premier avec a et que $b|ka$, alors d'après le théorème de Gauss il existe $l\in\mathbb{Z}$ tel que $k=lb$. On a donc $c=lba$, donc $ab|c$.

Chapitre 3 – Nombres premiers

I – Nombres premiers

<u>Définition :</u> Un nombre entier naturel est premier si et seulement s'il possède exactement deux diviseurs positifs : 1 et lui-même.

<u>Exemples :</u>
- *2 est premier car ses seuls diviseurs positifs sont 1 et 2.*
- *0 n'est pas premier car il possède une infinité de diviseurs positifs.*
- *1 n'est pas premier car il a un seul diviseur positif : 1.*

<u>Exercice 1 :</u> Dresser la liste des nombres premiers inférieurs à 50.

<u>Remarques :</u>
- Un entier supérieur à 2 qui n'est pas premier est dit composé.
- Si p est un nombre premier et n un entier, ou bien p divise n, ou bien p et n sont premiers entre eux, puisqu'ils n'ont que 1 comme diviseur positif commun.

<u>Théorème :</u>
- **Tout entier naturel supérieur ou égal à 2 admet un diviseur premier.**
- **Tout entier naturel n non premier supérieur à 2 admet un diviseur premier p inférieur ou égal à $\sqrt{n}$.**

<u>Preuve :</u> Soit $n\in\mathbb{N}$, $n\geqslant 2$. Si n est premier, il admet un diviseur premier : lui-même.
Si n n'est pas premier, il admet un diviseur positif autre que lui-même et 1.
On considère alors E, ensemble des diviseurs positif (autres que n et 1) de n.
D'après la remarque précédente, E n'est pas vide. Il admet donc un plus petit élément, que l'on note p.
Supposons que p ne soit pas premier. Il existerait un diviseur positif d de p. d serait aussi diviseur de n. Donc d serait un élément de E, ce qui contredit le fait que p soit le plus petit élément de E. C'est absurde. Donc p est premier.
p est premier et divise n donc il existe $q\in\mathbb{N}$ tel que $n=pq$ avec $1<q<n$.
Donc q est un diviseur de n (autre que n et 1) donc $q\in E$ et $p\leqslant q$ puisque p est le plus petit élément de E.
On a donc $p^2\leqslant pq\Rightarrow p^2\leqslant n\Rightarrow p\leqslant\sqrt{n}$.

<u>Propriété (test de primalité) :</u> Soit n un entier naturel supérieur ou égal à 2. Si n n'est divisible par aucun des nombres premiers inférieurs ou égaux à $\sqrt{n}$, alors n est premier.

<u>Preuve :</u> Si n n'est n'est pas premier, il admet un diviseur premier inférieur ou égal à $\sqrt{n}$.
Le test de primalité est la contraposée de cette proposition.

Exemples :

- *Déterminons si 4559 est premier :* $\sqrt{4559} \approx 67{,}52$.
  On teste la divisibilité de 4559 par les nombres premiers inférieurs ou égaux à 67.
  On remarque que $4559 = 47 \times 97$ *donc 4559 n'est pas premier.*
- *Déterminons si 4561 est premier :* $\sqrt{4561} \approx 67{,}54$.
  On teste la divisibilité de 4561 par les nombres premiers inférieurs ou égaux à 67.
  Aucune division ne fonctionne, donc 4561 est premier.

Exercice 2 : Écrire un programme à la calculatrice qui détermine si un entier est premier ou non.

Théorème : Il existe une infinité de nombres premiers.

Preuve par l'absurde : Supposons que l'ensemble des nombres premiers est fini.
Il n'existerait qu'un nombre n de nombres premiers : p_1 , p_2 , p_3 , …, p_n .
Considérons le nombre $N = p_1 \times p_2 \times p_3 \times \ldots \times p_n + 1$, ce qui se note $N = \prod_{i=1}^{n} p_i + 1$.
Comme $N = p_1 (p_2 \times p_3 \times \ldots \times p_n) + 1$: 1 est le reste de la division euclidienne de N par p_1 , donc N n'est pas divisible par p_1 .
De même, en effectuant les divisions euclidiennes par les autres nombres premiers p_2 , …, p_n , on détermine que N n'est divisible par aucun nombre premier.
Donc N serait premier. Donc N serait l'un des nombres p_1 , …, p_n , ce qui est faux. C'est absurde.
Conclusion : l'ensemble des nombres premiers est infini.

II – Décomposition en facteurs premiers

Exemple : *On peut écrire* $800=8\times4\times25=2^5\times5^2$ *où 2 et 5 sont des nombres premiers.*

a) Existence et unicité d'une décomposition

Théorème : Tout entier $n\geqslant2$ **se décompose en un produit de nombres premiers. Cette décomposition est unique à l'ordre des facteurs près.**
On peut donc écrire $n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$ **où** p_1 **,** p_2 **, …,** p_k **sont des nombres premiers deux à deux distincts et** α_1 **,** α_2 **, …,** α_k **sont des entiers naturels non nuls.**

Preuve :

- Existence : Soit $n\geqslant2$ un entier. On sait d'après le premier théorème du I qu'il admet un diviseur premier p_1. On a donc $n=p_1n_1$ avec $1\leqslant n_1<n$.
  Si $n_1=1$, alors $n=p_1$ et la propriété est démontrée.
  Sinon, alors n_1 possède un diviseur premier p_2 et on a donc $n=p_1p_2n_2$ où $1\leqslant n_2<n_1$.
  On continue ainsi tant que le quotient n_i est supérieur à 1.
  On forme ainsi une liste d'entiers n_1, n_2,… strictement décroissante et minorée par 1.
  Elle est donc finie, c'est-à-dire qu'à partir d'un certain rang m on a $n_m=1$ et donc $n=p_1p_2\dots p_m$ où les p_i sont des nombres premiers non nécessairement distincts.
  En regroupant les facteurs égaux on a la factorisation voulue.

- Unicité : On suppose qu'un certain nombre premier p apparait avec l'exposant $\alpha\geqslant1$ dans une décomposition, et l'exposant $\beta\geqslant0$ dans une autre ($\beta=0$ si le facteur l'apparait pas dans cette décomposition).
  On a alors $n=p^\alpha a=p^\beta b$, où a et b sont des produits de nombres premiers distincts de p.
  Si $\alpha>\beta$, $p^{\alpha-\beta}a=b$, donc p divise b, ce qui contredit le fait que p ne fait pas partie des facteurs de b.
  Si $\alpha<\beta$, $a=p^{\beta-\alpha}b$, ce qui contredit le fait que p ne fait pas partie des facteurs de a.
  Donc $\alpha=\beta$. Ce qui garantit l'unicité de la factorisation.

Remarque : On peut noter $n=\prod_{i=1}^{k}p_i^{\alpha_i}$.

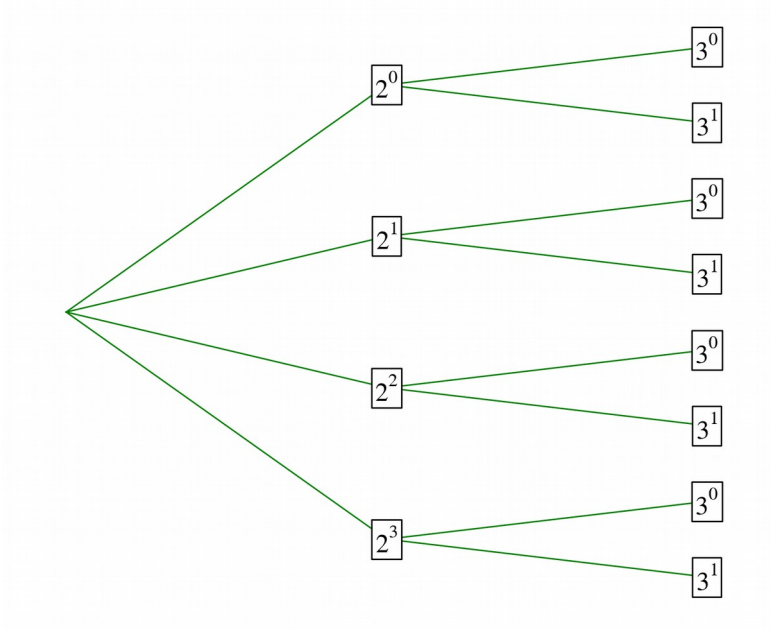
Exercice 3 : Écrire un programme à la calculatrice qui donne la décomposition en facteurs premiers d'un entier.

b) Diviseurs d'un entier naturel supérieur ou égal à 2

Propriété : Si $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ est la décomposition en facteurs premiers d'un entier naturel n, les diviseurs de n sont de la forme $p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ où $0 \leqslant \beta_1 \leqslant \alpha_1$, …, $0 \leqslant \beta_k \leqslant \alpha_k$.

Preuve : Les nombres entiers de la forme $p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ où $0 \leqslant \beta_1 \leqslant \alpha_1$, …, $0 \leqslant \beta_k \leqslant \alpha_k$ sont des diviseurs de n. En effet, on peut écrire $n = (p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}) \times p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \dots p_k^{\alpha_k - \beta_k}$ où les exposants $\alpha_i - \beta_i$ sont positifs ou nuls.
Réciproquement, soit d un diviseur de n. Si p^β divise d (avec p premier), alors p^β divise n. L'unicité de la décomposition en facteurs premiers de n implique que le nombre p^β doit figurer dans cette décomposition, et donc que p est l'un des p_i et que $0 \leqslant \beta \leqslant \alpha_i$.
d est donc de la forme souhaitée.

Exemple : *$24 = 2^3 \times 3$ donc 24 a pour diviseurs les entiers $2^\alpha \times 3^\beta$ où $0 \leqslant \alpha \leqslant 3$ (donc $\alpha = 0$, 1, 2 ou 3) et $0 \leqslant \beta \leqslant 1$ (donc $\beta = 0$ ou 1).On peut donc lister tous les diviseurs de 24 :*



- $2^0 \times 3^0 = 1$
- $2^0 \times 3^1 = 3$
- $2^1 \times 3^0 = 2$
- $2^1 \times 3^1 = 6$
- $2^2 \times 3^0 = 4$
- $2^2 \times 3^1 = 12$
- $2^3 \times 3^0 = 8$
- $2^3 \times 3^1 = 24$

Conséquence 1 : Si $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ est la décomposition en facteurs premiers d'un entier naturel n, le nombre de diviseurs de n est $(1+\alpha_1)(1+\alpha_2)\dots(1+\alpha_k) = \prod_{i=1}^{k} (1+\alpha_i)$.

Preuve : Un diviseur de n est de la forme $p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ où $0 \leqslant \beta_1 \leqslant \alpha_1$, …, $0 \leqslant \beta_k \leqslant \alpha_k$.
Pour chaque p_i avec $1 \leqslant i \leqslant k$, l'exposant peut prendre $1+\alpha_i$ valeurs possibles.
Le nombre total de diviseurs est alors $(1+\alpha_1)(1+\alpha_2)\dots(1+\alpha_k)$, puisque l'unicité de la décomposition en produit de facteurs premiers assure que ces diviseurs sont tous différents.

Conséquence 2 : Soient a et b deux entiers naturels supérieurs ou égaux à 2.
Le PGCD de a et b est égal au produit des facteurs premiers communs aux décompositions de a et b, chacun d'eux étant affecté du plus petit exposant avec lequel il figure dans a et b.

Exemple : *$31500 = 2^2 \times 3^2 \times 5^3 \times 7$ et $2733750 = 2 \times 3^7 \times 5^4$.*
On a donc $PGCD(31500 ; 2733750) = 2 \times 3^2 \times 5^3 = 2250$.

Chapitre 4 – Matrices

I – Nature d'une matrice et vocabulaire

a) Définitions

Définition : Soient m et n deux entiers naturels non nuls.
Une matrice de dimension $m\times n$ est un tableau rectangulaire formé de m lignes et n colonnes de nombres réels.

Remarque : Quand on parle de dimension (ou taille, ou format) $m\times n$, on ne calcule pas le produit !

Exemple : $\begin{pmatrix} 2 & 2 & 3,5 \\ 0 & -1 & \frac{8}{3} \end{pmatrix}$ *est une matrice de 2 lignes et 3 colonnes, donc de taille* 2×3 .

Définitions :

- **Une *matrice ligne* est une matrice formée d'une seule ligne.**
- **Une *matrice colonne* est une matrice formée d'une seule colonne.**
- **Une *matrice carrée* d'ordre n est une matrice $n\times n$.**

Exemples : $\begin{pmatrix} 2 & 6 & 1 \end{pmatrix}$ *est une matrice ligne,* $\begin{pmatrix} 5 \\ 1 \\ \frac{1}{5} \end{pmatrix}$ *est une matrice colonne,* $\begin{pmatrix} 1 & 2 & 3 & 5 \\ 7 & -5 & 0 & 0 \\ 4 & 7 & 8 & 6 \\ 2 & 0 & 0 & 1 \end{pmatrix}$

est une matrice carrée d'ordre 4.

b) Écriture générale d'une matrice

Une matrice A de taille $m\times n$ (avec $m\in\mathbb{N}^*$ et $n\in\mathbb{N}^*$) peut s'écrire sous cette forme :

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m-1,1} & a_{m-1,2} & \cdots & a_{m-1,n} \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix}.$$

Les nombres a_{ij} (notés parfois $a_{i,j}$ pour éviter les ambigüités) avec $\begin{cases} 1\leqslant i\leqslant m \\ 1\leqslant j\leqslant n \end{cases}$ s'appellent les *coefficients* de la matrice A . On peut alors noter $A=(a_{ij})_{1\leqslant i\leqslant m,\,1\leqslant j\leqslant n}$.
Le coefficient a_{ij} est donc le nombre placé à la i ième ligne et la j ième colonne.

Définition : Deux matrices seront égales si et seulement si elles ont le même format et ont les mêmes coefficients aux mêmes places.

c) Matrices particulières

Définition : Dans une matrice carrée d'ordre n, les coefficients a_{11}, a_{22}, …, a_{nn} forment la *diagonale principale* de la matrice.

Définition : Une matrice carrée est *diagonale* si et seulement si ses coefficients qui ne sont pas sur la diagonale principale sont tous nuls.

Exemple : $\begin{pmatrix} 5 & 0 & 0 \\ 0 & -5 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ *est une matrice diagonale.*

Définition : La matrice unité d'ordre n (ou matrice identité d'ordre n), notée I_n, est la matrice carrée d'ordre n contenant uniquement des 1 sur sa diagonale principale et des 0 ailleurs.

Exemple : $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Définition : La matrice nulle d'ordre n, notée O_n, est la matrice carrée d'ordre n dont tous les coefficients sont nuls.

II – Opérations sur les matrices

a) Addition et multiplication par un réel

Définition : Si $A=(a_{ij})$ et $B=(b_{ij})$ sont deux matrices de même taille $m \times n$, leur somme $A+B$ est définie par $A+B=(a_{ij}+b_{ij})_{1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n}$.
On ne peut donc ajouter que des matrices de même taille, et pour cela on ajoute les coefficients situés à la même place.

Exemple : $\begin{pmatrix} 2 & 4 \\ -1 & 10 \end{pmatrix} + \begin{pmatrix} 3 & -4 \\ 6 & 5 \end{pmatrix} = \begin{pmatrix} 2+3 & 4-4 \\ -1+6 & 10+5 \end{pmatrix} = \begin{pmatrix} 5 & 0 \\ 5 & 15 \end{pmatrix}$.

Définition : Soit $A=(a_{ij})_{1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n}$ une matrice et $\lambda \in \mathbb{R}$. La matrice λA est la matrice $(\lambda a_{ij})_{1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n}$. Multiplier une matrice par un réel revient à multiplier tous les coefficients par ce réel.

Remarques :

- On a de façon évidente $A+B=B+A$.
- Les règles de priorité sont les mêmes qu'avec les réels : $2A+3B$ désigne la matrice $(2A)+(3B)$.
- Pour tous réels λ et μ, on peut montrer que $\lambda(\mu A)=(\lambda\mu)A$ et $\lambda(A+B)=\lambda A+\lambda B$.
- On peut désormais définir la différence de deux matrices A et B de même taille : $A-B=A+(-1)B$.
- Pour toute matrice carrée A d'ordre n, on a $A+O_n=A$.

b) Multiplication d'une matrice ligne par une matrice colonne

Définition : Soit n un entier naturel non nul.
Soient $A=(a_{1j})$ une matrice ligne $1\times n$ et $B=(b_{n1})$ une matrice colonne $n\times 1$ (le nombre de colonnes de A est donc égal au nombre de lignes de B).

Alors $A\times B=\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n}\end{pmatrix}\times\begin{pmatrix} b_{11}\\ b_{21}\\ \dots\\ b_{n1}\end{pmatrix}=\left(a_{11}\times b_{11}+a_{12}\times b_{21}+\dots+a_{1n}\times b_{n1}\right)$ **.**

Remarque : On peut donc écrire $A\times B=(\sum_{k=1}^{n} a_{1k}b_{k1})$

Exemple : $\begin{pmatrix} 2 & -3 & 1\end{pmatrix}\times\begin{pmatrix} 4\\ 2\\ 0\end{pmatrix}=\left(2\times 4+(-3)\times 2+1\times 0\right)=(2)$.

c) Multiplication de deux matrices

Théorème : Le produit AB de deux matrices A et B existe si et seulement si le nombre de colonnes de A est égal au nombre de lignes de B .

Définition : Soient A une matrice de taille $m\times n$ et B une matrice de taille $n\times p$.
Le produit $A\times B$ ou AB est la matrice de taille $m\times p$ dont le coefficient situé à la ligne i et la colonne j est le coefficient du produit de la ligne i de A par la colonne j de B pour $1\leqslant i\leqslant m$ et $1\leqslant j\leqslant p$.

Exemples :

- *Le produit d'une matrice 2×3 par une matrice 3×3 est une matrice 2×3 :*

$$\begin{pmatrix} 1 & 2 & -2\\ 5 & 0 & 2\end{pmatrix}\times\begin{pmatrix} 1 & 2 & 0\\ -1 & -1 & 2\\ 2 & 0 & 2\end{pmatrix}=$$
$$\begin{pmatrix} 1\times 1+2\times(-1)+(-2)\times 2 & 1\times 2+2\times(-1)+(-2)\times 0 & 1\times 0+2\times 2+(-2)\times 2\\ 5\times 1+0\times(-1)+2\times 2 & 5\times 2+0\times(-1)+2\times 0 & 5\times 0+0\times 2+2\times 2\end{pmatrix}=$$
$$\begin{pmatrix} -5 & 0 & 0\\ 9 & 10 & 4\end{pmatrix}.$$

- *Le produit de deux matrices 2×2 est une matrice 2×2 : On peut* ***au brouillon*** *adopter cette présentation. De plus, on ne détaille pas le calcul des sommes :*

$$\begin{array}{cc} & \times\begin{pmatrix} \boldsymbol{0} & 3\\ \boldsymbol{4} & 2\end{pmatrix}\\ \begin{pmatrix} 1 & 2\\ \boldsymbol{3} & \boldsymbol{5}\end{pmatrix} & \begin{pmatrix} 8 & 7\\ \boldsymbol{20} & 19\end{pmatrix}\end{array}$$

(le coefficient de la deuxième ligne, première colonne du produit est le produit de la deuxième ligne de la première matrice par la première colonne de la deuxième matrice : $3\times 0+5\times 4=20$).

Propriétés admises : **Soient A, B, C des matrices carrées d'ordre $n\in\mathbb{N}^*$.**

- **Associativité : $(A\times B)\times C=A\times(B\times C)$. Ce produit se note $A\times B\times C$ ou ABC.**
- **Distributivité : $A\times(B+C)=AB+AC$ et $(A+B)\times C=AC+BC$.**
- **Produit par un réel λ : $(\lambda A)\times B=\lambda AB$ et $A\times(\lambda B)=\lambda AB$.**
- **Soit I_n la matrice unité d'ordre n alors $I_n\times A=A$ et $A\times I_n=A$.**

Remarque : La multiplication de matrices n'est pas commutative : en général, $A\times B\neq B\times A$ (le produit AB peut même exister, alors que BA n'existe pas).

Exemples : *Soient* $A=\begin{pmatrix}1 & 2\\ -2 & 3\end{pmatrix}$ *et* $B=\begin{pmatrix}2 & 2\\ -1 & 0\end{pmatrix}$.

On a $AB=\begin{pmatrix}0 & 2\\ -7 & -4\end{pmatrix}$ *mais* $BA=\begin{pmatrix}-2 & 10\\ -1 & -2\end{pmatrix}$ *donc* $AB\neq BA$.

Remarque : Soient A, B et C des matrices carrées d'ordre $n\in\mathbb{N}^*$.
Si $AB=AC$, on ne peut pas en déduire que $B=C$ (on ne peut pas « simplifier » par A).

Exemple : $\begin{pmatrix}2 & 1\\ 4 & 2\end{pmatrix}\times\begin{pmatrix}4 & -2\\ 2 & 1\end{pmatrix}=\begin{pmatrix}10 & -3\\ 20 & -6\end{pmatrix}$ *et* $\begin{pmatrix}2 & 1\\ 4 & 2\end{pmatrix}\times\begin{pmatrix}5 & -5\\ 0 & 7\end{pmatrix}=\begin{pmatrix}10 & -3\\ 20 & -6\end{pmatrix}$.

Remarque : Soient A et B deux matrices carrées d'ordre $n\in\mathbb{N}^*$.
Si $AB=O_n$, on ne peut pas en déduire que $A=O_n$ ou $B=O_n$ (on ne peut pas, comme pour les nombres, utiliser le théorème de l'équation produit nulle).

Exemple : $\begin{pmatrix}2 & 1\\ 4 & 2\end{pmatrix}\times\begin{pmatrix}1 & -3\\ -2 & 6\end{pmatrix}=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$.

d) Puissances entières positives de matrices

Définition : Soit A une matrice carrée d'ordre $n\in\mathbb{N}^*$, on notera $A^2=A\times A$, $A^3=A\times A\times A$, *etc.* Plus généralement, pour $k\in\mathbb{N}^*$, A^k sera le produit de k matrices toutes égales à A. Par convention, on posera $A^0=I_n$.

Exercice 1 : Soit $A=\begin{pmatrix}1 & 2\\ 1 & 1\end{pmatrix}$. Calculer A^0, A^1, A^2, A^3 et A^4.

III – Matrices inversibles et application aux systèmes

a) Matrices inversibles

Définition et propriété : Soit A une matrice carrée d'ordre $n \in \mathbb{N}^*$.
On dit que A est inversible si et seulement si il existe une matrice carrée d'ordre n, notée A^{-1} telle que $A \times A^{-1} = A^{-1} \times A = I_n$.
La matrice A^{-1} est nécessairement unique, et appelée matrice inverse de A.

Exemple : $\begin{pmatrix} 1 & -0,5 \\ -2 & 1,5 \end{pmatrix} \times \begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ *et* $\begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix} \times \begin{pmatrix} 1 & -0,5 \\ -2 & 1,5 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. *La matrice* $\begin{pmatrix} 1 & -0,5 \\ -2 & 1,5 \end{pmatrix}$ *est donc inversible et son inverse est* $\begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix}$.

Preuve de l'unicité : Supposons que A possède deux inverses, notés B et B'.
On a donc $AB = I_n$, $AB' = I_n$, $BA = I_n$, $B'A = I_n$. On peut donc écrire :
$B'(AB) = B'I_n = B'$. On a aussi $(B'A)B = I_n B = B$. Comme $B'(AB) = (B'A)B$, on a $B' = B$.

b) Matrices inversibles d'ordre 2

Définition : Soit A une matrice carrée d'ordre 2. On a donc $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Le réel $ad - bc$ est appelé déterminant de la matrice A, et noté $det(A)$ ou Δ.

Exemple : Pour $\begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix}$, *on a* $\Delta = 3 \times 2 - 1 \times 4 = 2$.

Théorème : Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ une matrice carrée d'ordre 2. Alors :

- **Si $\Delta \neq 0$, A est inversible ; on a $A^{-1} = \frac{1}{\Delta} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.**
- **Si $\Delta = 0$, A n'est pas inversible.**

Preuve :

- Si $\Delta \neq 0$, $\frac{1}{\Delta}$ existe. Soit $B = \frac{1}{\Delta} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. On a alors
  $AB = \frac{1}{ad - bc} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{ad - bc} \begin{pmatrix} ad - bc & 0 \\ 0 & ad - bc \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$.
  De même, on vérifie que l'on a aussi $BA = I_2$ donc B est l'inverse de A.
- Si $\Delta = 0$, démontrons par l'absurde que A n'est par inversible : on suppose que A admet une inverse A'. Soit $B = \begin{pmatrix} -c & a \\ -c & a \end{pmatrix}$.
  On a $B(AA') = BI_2 = B$ et $(BA)A' = \left(\begin{pmatrix} -c & a \\ -c & a \end{pmatrix} \times \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) \times A' = \begin{pmatrix} 0 & ad - bc \\ 0 & ad - bc \end{pmatrix} \times A' = O_2$
  car $ad - bc = 0$.

Comme $B(AA')=(BA)A'$, on en déduit que $B=O_2$ et donc $c=a=0$.

De même, soit $C=\begin{pmatrix} d & -b \\ d & -b \end{pmatrix}$.

On a $C(AA')=CI_2=C$ et $(CA)A'=\left(\begin{pmatrix} d & -b \\ d & -b \end{pmatrix}\times\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)\times A'=\begin{pmatrix} ad-bc & 0 \\ ad-bc & 0 \end{pmatrix}\times A'=O_2$ car $ad-bc=0$.

Comme $C(AA')=(CA)A'$, on en déduit que $C=O_2$ et donc $b=d=0$.

On en déduit que $A=O_2$, ce qui est absurde puisque O_2 n'est pas inversible – son produit par n'importe quelle matrice carrée d'ordre 2 valant toujours O_2, il ne peut égaler I_2.

Donc A n'est pas inversible.

<u>Exemple :</u> Soit $A=\begin{pmatrix} 1 & 3 \\ 5 & 6 \end{pmatrix}$. $\Delta=1\times6-5\times3=-9$ *donc* A *est inversible.*

On a alors $A^{-1}=\frac{1}{-9}\begin{pmatrix} 6 & -3 \\ -5 & 1 \end{pmatrix}=\begin{pmatrix} -\frac{2}{3} & \frac{1}{3} \\ \frac{5}{9} & -\frac{1}{9} \end{pmatrix}$.

<u>c) Application aux systèmes linéaires</u>

<u>Exemple :</u> On considère le système linéaire d'inconnues x_1, x_2, x_3 *suivant :*

$\begin{cases} 2x_1-3x_2+4x_3=-1 \\ x_1+x_2-5x_3=2 \\ -4x_1+3x_2=6 \end{cases}$ *. On remarque qu'il peut s'écrire sous la forme d'un produit de matrices :*

$$\begin{pmatrix} 2 & -3 & 4 \\ 1 & 1 & -5 \\ -4 & 3 & 0 \end{pmatrix}\times\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}=\begin{pmatrix} -1 \\ 2 \\ 6 \end{pmatrix}.$$

On a alors $AX=Y$ *avec* $A=\begin{pmatrix} 2 & -3 & 4 \\ 1 & 1 & -5 \\ -4 & 3 & 0 \end{pmatrix}$, $X=\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ *et* $Y=\begin{pmatrix} -1 \\ 2 \\ 6 \end{pmatrix}$.

L'inconnue est alors la matrice colonne X.

<u>Théorème :</u> Un système linéaire à n inconnues x_1, x_2, …, x_n :

$\begin{cases} a_{11}x_1+a_{12}x_2+\ldots+a_{1,n}x_n=y_1 \\ a_{21}x_1+a_{22}x_2+\ldots+a_{2,n}x_n=y_2 \\ \ldots \\ a_{n,1}x_1+a_{n,2}x_2+\ldots+a_{n,n}x_n=y_n \end{cases}$ **peut s'écrire sous la forme $AX=Y$, où $A=(a_{ij})_{1\leqslant i\leqslant n,1\leqslant j\leqslant n}$ est une matrice carrée d'ordre n, $X=(x_i)$ et $Y=(y_i)$ sont des matrices colonnes $n\times1$.**

Si A est inversible, le système a alors une solution unique : $X=A^{-1}Y$.

<u>Preuve :</u> Si A est inversible, de $AX=Y$ on déduit $A^{-1}(AX)=A^{-1}Y$ d'où $(A^{-1}A)X=A^{-1}Y$ par associativité. On a donc $X=A^{-1}Y$.

Réciproquement, si $X=A^{-1}Y$, alors $AX=AA^{-1}Y=I_nY=Y$.

$A^{-1}Y$ est donc l'unique solution du système écrit sous forme matricielle.

Chapitre 5 – Suites de matrices

I – Puissances d'une matrice

On rappelle que pour A *matrice carrée d'ordre* $n\in\mathbb{N}^*$ *et pour* $k\in\mathbb{N}^*$, A^k *sera le produit de* k *matrices toutes égales à* A, *et que* $A^0=I_n$.

a) Cas des matrices diagonales

Propriété : Soit D une matrice diagonale. Pour tout $n\in\mathbb{N}^*$, D^n est la matrice diagonale obtenue en élevant à la puissance n tous les coefficients de D.

Exemple : Si $D=\begin{pmatrix}5 & 0\\ 0 & -1\end{pmatrix}$, *alors* $D^4=\begin{pmatrix}5^4 & 0\\ 0 & (-1)^4\end{pmatrix}=\begin{pmatrix}625 & 0\\ 0 & 1\end{pmatrix}$.

b) Cas des matrices triangulaires

Définition : Une matrice carrée est dite :

- **triangulaire supérieure (respectivement inférieure) si tous ses éléments situés en-dessous (respectivement au-dessus) de sa diagonale sont nuls ;**
- **Strictement triangulaire si elle est triangulaire avec des coefficients diagonaux nuls.**

Exemples : $\begin{pmatrix}1 & 0 & 0\\ -3 & -5 & 0\\ 5 & 0 & 2\end{pmatrix}$ *est triangulaire inférieure,* $\begin{pmatrix}0 & 2 & -6\\ 0 & 0 & 56\\ 0 & 0 & 0\end{pmatrix}$ *est strictement triangulaire supérieure.*

Propriétés : Les puissances d'une matrice triangulaire sont triangulaires de même forme. Les puissances d'une matrice strictement triangulaire d'ordre n sont nulles à partir de l'exposant n.

Preuve : On traitera le cas $n=3$, pour M matrice strictement triangulaire supérieure :
Si $M=\begin{pmatrix}0 & a & b\\ 0 & 0 & c\\ 0 & 0 & 0\end{pmatrix}$, on a $M^2=\begin{pmatrix}0 & 0 & ac\\ 0 & 0 & 0\\ 0 & 0 & 0\end{pmatrix}$, $M^3=O_3$. On en déduit que pour $n\geqslant 3$, $M^n=O_3$.

Définition : Une matrice carrée dont une puissance est nulle est dite nilpotente. Le plus petit entier k pour lequel la puissance de la matrice est nulle est appelé *indice de nilpotence*.
On déduit de la propriété précédente que si M d'ordre n est strictement triangulaire, son indice de nilpotence est inférieur ou égal à n.

Remarque : Ces propriétés permettent de calculer des puissances d'une matrice en la décomposant en somme de matrices particulières ou en effectuant des calculs par blocs.

II – Diagonalisation d'une matrice carrée d'ordre 2

Définition : Une matrice carrée A est dite diagonalisable s'il existe une matrice carrée P inversible et une matrice diagonale D telles que $A=PDP^{-1}$.

Théorème : Si $A=PDP^{-1}$, pour tout $n\in\mathbb{N}$, $A^n=PD^nP^{-1}$.

Preuve : On raisonne par récurrence sur $n\in\mathbb{N}$.
Soit $P(n)$ la propriété $A^n=PD^nP^{-1}$.

- Initialisation : Pour $n=0$, $A^0=I_2$ et $PD^0P^{-1}=PI_2P^{-1}=PP^{-1}=I_2$. $P(0)$ est vraie.
- Hérédité : On suppose $P(n)$ vraie. On a donc $A^n=PD^nP^{-1}$.
  $A^{n+1}=AA^n=PDP^{-1}PD^nP^{-1}=PDD^nP^{-1}=PD^{n+1}P^{-1}$. $P(n+1)$ est vraie.
- Conclusion : Pour $n\in\mathbb{N}$, $A^n=PD^nP^{-1}$

Propriété : Une matrice A d'ordre 2 est diagonalisable si et seulement s'il existe deux réels λ et μ (non nécessairement distincts) et deux matrices colonnes à coefficients réels non proportionnelles V et W telles que $AV=\lambda V$ et $AW=\mu W$.
Dans ce cas, λ et μ sont appelés les *valeurs propres* de la matrice A ; la matrice $P=[V\,W]$ formée par la colonne des coefficients de V en première colonne et la colonne des coefficients de W en seconde colonne est inversible et telle que $A=P\begin{pmatrix}\lambda & 0\\ 0 & \mu\end{pmatrix}P^{-1}$.

Exemple : Soient $A=\begin{pmatrix}-4 & 6\\ -1 & 1\end{pmatrix}$, $V=\begin{pmatrix}3\\ 1\end{pmatrix}$ *et* $W=\begin{pmatrix}2\\ 1\end{pmatrix}$.

On a $AV=\begin{pmatrix}-6\\ -2\end{pmatrix}=-2V$ *et* $AW=\begin{pmatrix}-2\\ -1\end{pmatrix}=-W$. *On en déduit que* A *est diagonalisable et a deux valeurs propres : – 2 et – 1.*
En posant $P=\begin{pmatrix}3 & 2\\ 1 & 1\end{pmatrix}$, *on a* $A=P\begin{pmatrix}-2 & 0\\ 0 & -1\end{pmatrix}P^{-1}$.

Preuve :

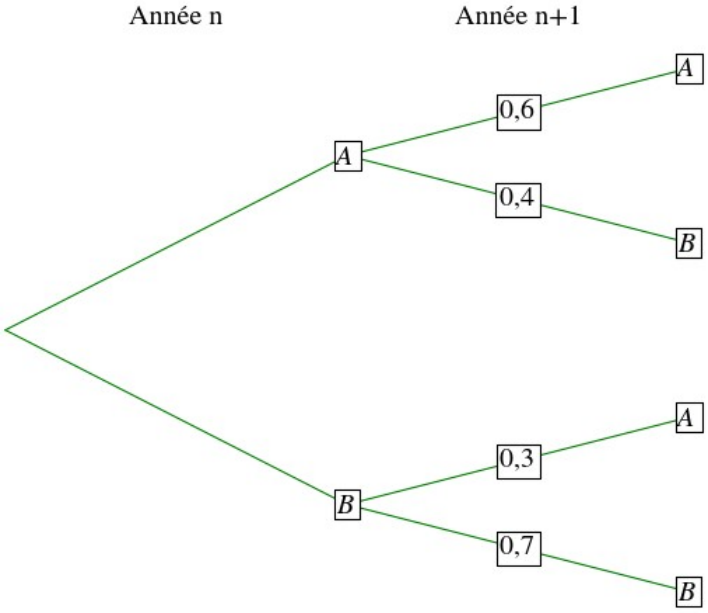
- Si A est diagonalisable, il existe λ et μ et $P=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ inversible tels que $A=P\begin{pmatrix}\lambda & 0\\ 0 & \mu\end{pmatrix}P^{-1}$. Posons $V=\begin{pmatrix}a\\ c\end{pmatrix}$ et $W=\begin{pmatrix}b\\ d\end{pmatrix}$. Comme P est inversible, son déterminant est non nul, donc $ad-bc\neq 0$, donc V et W ne sont pas proportionnels.
  Par calcul, on a $AV=\lambda V$ et $AW=\mu W$.
- Réciproquement, on suppose qu'il existe deux réels λ et μ et deux matrices colonnes à coefficients réels non proportionnelles $V=\begin{pmatrix}a\\ c\end{pmatrix}$ et $W=\begin{pmatrix}b\\ d\end{pmatrix}$ telles que $AV=\lambda V$ et $AW=\mu W$.
  On pose $D=\begin{pmatrix}\lambda & 0\\ 0 & \mu\end{pmatrix}$ et $P=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$.
  Le déterminant de P est non nul car V et W ne sont pas proportionnelles, donc P est inversible, et comme $AV=\lambda V$ et $AW=\mu W$, on a $AP=PD$ donc $A=PDP^{-1}$.

III – Exemple de marche aléatoire (chaine de Markov)

Problème : Dans un pays, deux opérateurs de téléphonie mobile A et B se partagent le marché. En 2010, A en contrôle 80 %, et B 20 %. On a observé que, chaque année :

- 60 % de la clientèle de A lui reste fidèle, tandis que 40 % passe chez B.
- 70 % de la clientèle de B lui reste fidèle, tandis que 30 % passe chez A.

Ces proportions sont stables : il n'y a pas de fuite vers des opérateurs étrangers, et pas d'abandon de consommation de produits.
On veut chercher à connaître la répartition des parts de marché au bout d'une longue période.



Modélisation : Pour tout $n \in \mathbb{N}$, soient a_n et b_n les parts de marché de A et B en $2010+n$.
L'année $2010+n+1$, les clients de A sont constitués des 60 % de clients fidèles à A de $2010+n$ et des 30 % de clients de B de $2010+n$ qui ont changé d'opérateur.
L'année $2010+n+1$, les clients de B sont constitués des 70 % de clients fidèles à B de $2010+n$ et des 40 % de clients de A de $2010+n$ qui ont changé d'opérateur.

On a donc pour tout $n \in \mathbb{N}$, $\begin{cases} \boldsymbol{a_{n+1}=0{,}6\,a_n+0{,}3\,b_n} \\ \boldsymbol{b_{n+1}=0{,}4\,a_n+0{,}7\,b_n} \end{cases}$ **avec** $\begin{cases} \boldsymbol{a_0=0{,}8} \\ \boldsymbol{b_0=0{,}2} \end{cases}$.

1) Posons, pour $n \in \mathbb{N}$, $P_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$. Le système précédent se traduit par $\boldsymbol{P_{n+1} = \begin{pmatrix} 0{,}6 & 0{,}3 \\ 0{,}4 & 0{,}7 \end{pmatrix} P_n}$.

Définition : La matrice $\begin{pmatrix} 0{,}6 & 0{,}3 \\ 0{,}4 & 0{,}7 \end{pmatrix}$ est appelée *matrice de transition* associée à la marche aléatoire.

2) Comme pour tout $n \in \mathbb{N}$ $a_n+b_n=1$, on a $\begin{cases} a_{n+1}=0{,}6\,a_n+0{,}3(1-a_n) \\ b_{n+1}=0{,}7\,b_n+0{,}4(1-b_n) \end{cases} \Leftrightarrow \begin{cases} a_{n+1}=0{,}4(1-b_n)+0{,}7\,b_n \\ b_{n+1}=0{,}3\,b_n+0{,}4 \end{cases}$.
On en déduit que pour $n \in \mathbb{N}$, $\boldsymbol{P_{n+1}=D\,P_n+E}$, avec $D = \begin{pmatrix} 0{,}3 & 0 \\ 0 & 0{,}3 \end{pmatrix}$ et $E = \begin{pmatrix} 0{,}3 \\ 0{,}4 \end{pmatrix}$.

Définition : On appelle *état stable* de la marche aléatoire toute matrice S telle que $S=D\,S+E$. En effet, si un des termes de la suite (P_n) est égal à S, tous les termes suivants seront égaux à S.

3) On résout $S=DS+E$: soit $S=\begin{pmatrix} a \\ b \end{pmatrix}$. On a donc

$$\begin{pmatrix} a \\ b \end{pmatrix}=\begin{pmatrix} 0,3 & 0 \\ 0 & 0,3 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}+\begin{pmatrix} 0,3 \\ 0,4 \end{pmatrix} \Leftrightarrow \begin{cases} a=0,3\,a+0,3 \\ b=0,3\,b+0,4 \end{cases} \Leftrightarrow \begin{cases} a=\dfrac{3}{7} \\ b=\dfrac{4}{7} \end{cases} \text{ donc } \boldsymbol{S=\begin{pmatrix} \frac{3}{7} \\ \frac{4}{7} \end{pmatrix}}.$$

4) On pose pour $n\in\mathbb{N}$, $\boldsymbol{X_n=P_n-S}$. Comme $S=DS+E$, on a :
$X_{n+1}=P_{n+1}-S=DP_n+E-(DS+E)=D(P_n-S)=DX_n \Leftrightarrow \boldsymbol{X_{n+1}=DX_n}$.
$(\boldsymbol{X_n})$ **est une suite géométrique de matrices de raison** $\boldsymbol{D}$ **et de premier terme**

$$\boldsymbol{X_0=P_0-S=\begin{pmatrix} 0,8-\frac{3}{7} \\ 0,2-\frac{4}{7} \end{pmatrix}} \text{ soit } \boldsymbol{X_0=\begin{pmatrix} \frac{13}{35} \\ -\frac{13}{35} \end{pmatrix}}.$$

On a donc pour $n\in\mathbb{N}$, $X_n=D^nX_0=\begin{pmatrix} 0,3 & 0 \\ 0 & 0,3 \end{pmatrix}^n\begin{pmatrix} \frac{13}{35} \\ -\frac{13}{35} \end{pmatrix}=\begin{pmatrix} 0,3^n & 0 \\ 0 & 0,3^n \end{pmatrix}\begin{pmatrix} \frac{13}{35} \\ -\frac{13}{35} \end{pmatrix}=\begin{pmatrix} 0,3^n\times\frac{13}{35} \\ 0,3^n\times\left(-\frac{13}{35}\right) \end{pmatrix}$.

5) On a donc comme $X_n=P_n-S$, $\boldsymbol{P_n=\begin{pmatrix} 0,3^n\times\frac{13}{35}+\frac{3}{7} \\ 0,3^n\times\left(-\frac{13}{35}\right)+\frac{4}{7} \end{pmatrix}}$.

6) Comme $-1<0,3<1$, on a $\lim\limits_{n\to+\infty} 0,3^n=0$.

On en déduit que $\lim\limits_{n\to+\infty} 0,3^n\times\frac{13}{35}+\frac{3}{7}=\frac{3}{7}$ et $\lim\limits_{n\to+\infty} 0,3^n\times\left(-\frac{13}{35}\right)+\frac{4}{7}=\frac{4}{7}$.

Donc $\boldsymbol{\lim\limits_{n\to+\infty} P_n=\begin{pmatrix} \frac{3}{7} \\ \frac{4}{7} \end{pmatrix}}$.

<u>Conclusion :</u> La part de marché de A tend à se rapprocher de $\frac{3}{7}$, celle de B tend à se rapprocher de $\frac{4}{7}$.

IV – Suites de matrices colonnes $U_{n+1}=AU_n+B$

Dans cette partie, U_n est une matrice colonne à m lignes, A une matrice carrée d'ordre m et B une matrice colonnes à m lignes, avec $m\in\mathbb{N}^*$.
On note (R) la relation $U_{n+1}=AU_n+B$.

a) Expression du terme général

Une suite constante égale à S vérifie la relation (R) si et seulement si $S=AS+B$.
Dans ce cas, en posant $X_n=U_n-S$ on a $X_{n+1}=U_{n+1}-S=AU_n+B-(AS+B)=A(U_n-S)=AX_n$.

Théorème : La suite $(X_n)_{n\in\mathbb{N}}$ définie par $X_n=U_n-S$ vérifie $X_{n+1}=AX_n$ et donc pour $n\in\mathbb{N}$, $X_n=A^nX_0$, c'est-à-dire $U_n=A^n(U_0-S)+S$.

Preuve : On utilise le fait que $(X_n)_{n\in\mathbb{N}}$ est géométrique de raison A.

b) Limite d'une suite de matrices

Une suite de matrices $(U_n)_{n\in\mathbb{N}}$ (toutes de même format) converge vers la matrice L si les coefficients de U_n convergent vers les coefficients de L correspondants.
En pratique, on exprime chaque coefficient en fonction de n, et on cherche la limite de chaque coefficient.

Remarque : Si $U_n=A^nU_0$ et si $\lim\limits_{n\to+\infty}A^n=L$, alors $\lim\limits_{n\to+\infty}U_n=LU_0$.