Cours de mathématiques – Option Mathématiques Expertes de Terminale Générale

Table des matières

Chapitre 1 – Nombres complexes et algèbre

I – Ensemble des nombres complexes

a) Définitions et premières propriétés

Propriétés admises : Il existe un ensemble, noté $\mathbb{C}$ des *nombres complexes* qui possède les propriétés suivantes :

- **$\mathbb{C}$ contient l'ensemble $\mathbb{R}$ des réels (on note $\mathbb{R}\subset\mathbb{C}$)**
- **Les quatre opérations des nombres réels se prolongent aux nombres complexes et les règles de calculs sont les mêmes.**
- **Il existe un nombre complexe noté i tel que $i^2=-1$.**
- **Tout nombre complexe z s'écrit *de manière unique* $z=x+iy$ avec $x\in\mathbb{R}$ et $y\in\mathbb{R}$.**

Définitions : L'écriture $z=x+iy$ avec $x\in\mathbb{R}$ et $y\in\mathbb{R}$ est appelée *forme algébrique* du nombre complexe z . x est la *partie réelle* de z , notée $\Re(z)$, et y est la *partie imaginaire* de z , notée $\Im(z)$. $z\in\mathbb{R}\Leftrightarrow\Im(z)=0$ et z est un *imaginaire pur* $\Leftrightarrow\Re(z)=0$.

Exemples : Pour $z=7-6i$, on a $\Re(z)=7$ et $\Im(z)=-6$. i est un imaginaire pur.

Propriété : Deux nombres complexes sont égaux si et seulement si ils ont même partie réelle et même partie imaginaire. C'est une conséquence de l'unicité de cette forme.

b) Calculs dans l'ensemble des nombres complexes

D'après les propriétés de $\mathbb{C}$, on calcule comme dans $\mathbb{R}$, en tenant compte du fait que $i^2=-1$.
En particulier, les identités remarquables se prolongent à $\mathbb{C}$.

Exemples :

- $11+2i-(1+i)=\mathbf{10+i}$
- $(5+2i)(6-3i)=30-15i+12i-6i^2=30-3i-6\times(-1)=\mathbf{36-3i}$
- $(4-i\sqrt{3})^2=4^2-2\times4\times i\sqrt{3}+(i\sqrt{3})^2=16-8i\sqrt{3}+i^2\times3=16-8i\sqrt{3}+(-1)\times3=\mathbf{13-8i\sqrt{3}}$
- $i^{37}=i^{36}\times i^1=i^{2\times18}\times i=(i^2)^{18}\times i=(-1)^{18}\times i=1\times i=\mathbf{i}$

Propriété (4ème identité remarquable) : Pour tous complexes a et b, on a $(a+ib)(a-ib)=a^2+b^2$. Cette identité s'utilise généralement avec a et b réels.

Preuve : $(a+ib)(a-ib)=a^2-(ib)^2=a^2-i^2b^2=a^2-(-1)b^2=a^2+b^2$.

Exemple : Dans $\mathbb{C}$, $4a^2+49$ peut se factoriser ainsi : $4a^2+49=(2a)^2+7^2=(2a+7i)(2a-7i)$.

II – Conjugué d'un nombre complexe

a) Conjugaison

Définition : Soit z un nombre complexe de forme algébrique $x+iy$ avec $x\in\mathbb{R}$ et $y\in\mathbb{R}$. Le conjugué de z, noté $\overline{z}$, est le nombre complexe $x-iy$.

Exemples : $\overline{2-5i}=2+5i$; $\overline{(1-\sqrt{5})i}=(-1+\sqrt{5})i$.

b) Propriétés

$\overline{\overline{z}}=z$	$z+\overline{z}=2\Re(z)$	$z-\overline{z}=2i\Im(z)$
$z\in\mathbb{R}\Leftrightarrow\overline{z}=z$	z est un imaginaire pur $\Leftrightarrow\overline{z}=-z$	$z\overline{z}=(\Re(z))^2+(\Im(z))^2$ (4ème identité remarquable)

Preuves : Il suffit de remplacer z par sa forme algébrique $x+iy$ avec $x\in\mathbb{R}$ et $y\in\mathbb{R}$.

c) Division

L'inverse d'un nombre complexe $z\neq0$ est le nombre complexe Z tel que $z\times Z=1$.

On le note $\frac{1}{z}$. Pour tous nombres complexes z et $z'\neq0$, on définit le quotient $\frac{z}{z'}=z\times\frac{1}{z'}$; pour déterminer sa forme algébrique, **on multiplie numérateur et dénominateur par $\overline{z'}$**.

Exemple : On cherche la forme algébrique de $z=\frac{4-2i}{3+i}$.

$z=\frac{(4-2i)(3-i)}{(3+i)(3-i)}=\frac{12-4i-6i+2i^2}{3^2+1^2}=\frac{12-4i-6i-2}{10}=\frac{10-10i}{10}=1-i$ *donc* $\Re(z)=1$ *et* $\Im(z)=-1$.

d) Conjugaison et opérations

Propriétés : Pour tous nombres complexes z et z' et tout entier naturel $n \geqslant 1$, on a :

$\overline{z+z'}=\overline{z}+\overline{z'}$	$\overline{z\,z'}=\overline{z}\,\overline{z'}$	$\overline{z^n}=\overline{z}^n$	$\overline{\left(\frac{1}{z}\right)}=\frac{1}{\overline{z}}$ avec $z \neq 0$	$\overline{\left(\frac{z}{z'}\right)}=\frac{\overline{z}}{\overline{z'}}$ avec $z' \neq 0$

Preuve des deux premières propriétés : Soient x, y, x' et y' des nombres réels tels que $z=x+iy$ et $z'=x'+iy'$.

$\overline{z+z'}=\overline{x+iy+x'+iy'}=\overline{x+x'+i(y+y)}=x+x'-i(y+y')=x-iy+x'-iy'=\overline{z}+\overline{z'}$.

$zz'=(x+iy)(x'+iy')=xx'+ixy'+iyx'+i^2yy'=xx'-yy'+i(xy'+yx')$ donc

$\overline{zz'}=xx'-yy'-i(xy'+yx')$. De plus, on a :

$\overline{z}\,\overline{z'}=(x-iy)(x'-iy')=xx'-ixy'-iyx'+i^2yy'=xx'-yy'-i(xy'+yx')$ donc $\overline{zz'}=\overline{z}\,\overline{z'}$.

Chapitre 2 – Divisibilité

<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* : $\mathbb{Z}=\{...;-4;-3;-2;-1;0;1;2;3;4;...\}$

<u>Notation :</u> Pour tous réels a et b avec $a\leqslant b$ on note $[\![a;b]\!]$ l'ensemble des *entiers relatifs* compris au sens large entre a et b. On a donc $[\![a;b]\!]=\mathbb{Z}\cap[a;b]$.

<u>Exemple :</u> $[\![-3;\sqrt{2}]\!]=\{-3;-2;-1;0;1\}$.

I – Divisibilité des entiers relatifs

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 $\{-|b|;...;-1;1;...;|b|\}=[\![-b;b]\!]\setminus\{0\}$. b a donc au plus $2|b|$ diviseurs.

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

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

Dans cette partie, 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 $a|c$, alors il existe $k'\in\mathbb{Z}$ tel que $c=k'a$.
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 d'un entier relatif par un entier naturel non nul

<u>Théorème et définition :</u> Soient $a\in\mathbb{Z}$ et $b\in\mathbb{N}$ avec $b\neq 0$.
Il existe un <u>unique</u> couple (q,r) d'entiers relatifs 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>Exemples :</u> La division euclidienne de 27 par 4 donne $27=4\times 6+3$. Celle de -27 par 4 donne $-27=4\times(-7)+1$.

<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>Preuve du théorème :</u>

- *Existence de q et r :*
  - 1er cas : a est un multiple de b . Alors il existe un entier relatif q tel $a=bq$.
  - 2d cas : a n'est pas un multiple de b . Il existe des multiples de b inférieurs strictement à a et d'autres supérieurs strictement à a .
    On peut donc écrire $bq<a<b(q+1)$ où $b(q+1)$ est le plus petit multiple de b supérieur strictement à a .
    Finalement, pour tout $a\in\mathbb{Z}$, il existe un entier relatif q tel que $bq<a<b(q+1)$.
    En posant $r=a-bq$, on obtient $a=bq+r$ et $0<r<b$.

- *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 seul multiple de b strictement compris entre $-b$ et b est 0, donc $r'-r=0$, soit $r'=r$. Par (1), on en déduit que $q'=q$. Donc le couple (q,r) est unique.

III – Congruences dans l'ensemble des entiers relatifs

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 $a\equiv b(\mathit{mod}\, c)$ ou $a\equiv b[c]$ ou $a\equiv b[\mathit{mod}\, c]$.

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

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 $c|a-b$ et comme $c|c(q-q')$, alors par combinaison linéaire, $c|r-r'$. 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 $\Leftrightarrow a\equiv r[c]$ et $0\leqslant r<c$.

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

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

- **$a+a'\equiv b+b'[c]$, $a-a'\equiv b-b'[c]$ et $aa'\equiv bb'[c]$.**
- **$a^n\equiv b^n[c]$ pour tout $n\in\mathbb{N}^*$.**

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

- $a+a'=b+b'+(k+k')c$ avec $k+k'$ entier, donc $a+a'\equiv b+b'[c]$.
- $aa'=bb'+(bk'+b'k+kk'c)c$ avec $bk'+b'k+kk'c$ entier, donc $aa'\equiv bb'[c]$.
- 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 $2^5\equiv 32\equiv 0[4]$ 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 3 – Équations polynomiales dans l'ensemble des nombres complexes

I – Équations du second degré dans l'ensemble des nombres complexes

a) Racines carrées d'un nombre réel dans l'ensemble des nombres complexes

Définition : **a désigne un nombre réel. Les solutions dans $\mathbb{C}$ de l'équation $z^2=a$ sont appelées racines carrées de a dans $\mathbb{C}$.**

Propriété : **Tout nombre réel non nul admet deux racines carrées dans $\mathbb{C}$.**

- **Si $a>0$, ce sont les nombres réels $\sqrt{a}$ et $-\sqrt{a}$.**
- **Si $a<0$, ce sont les nombres imaginaires purs $i\sqrt{-a}$ et $-i\sqrt{-a}$.**

Preuve :

- Si $a>0$, $z^2=a\Leftrightarrow(z-\sqrt{a})(z+\sqrt{a})=0$. En résolvant l'équation-produit, on a la conclusion.
- Si $a<0$, $z^2=a\Leftrightarrow z^2-i^2(-a)=0\Leftrightarrow(z-i\sqrt{-a})(z+i\sqrt{-a})=0$. En résolvant l'équation-produit, on a la conclusion.

Exemples : *Les racines carrées dans $\mathbb{C}$:*

- *de 7 sont $\sqrt{7}$ et $-\sqrt{7}$.*
- *de -7 sont $i\sqrt{7}$ et $-i\sqrt{7}$.*

b) Racines complexes d'un polynôme du second degré à coefficients réels

Propriété : Soit $P(z)=az^2+bz+c$ un polynôme du second degré avec $a\in\mathbb{R}^*$, $b\in\mathbb{R}$ et $c\in\mathbb{R}$ de discriminant $\Delta=b^2-4ac$. Alors, dans $\mathbb{C}$, $P(z)$ admet :

- **Si $\Delta=0$, une unique racine réelle : $z_0=-\dfrac{b}{2a}$.**
- **Si $\Delta>0$, deux racines réelles : $z_1=\dfrac{-b+\sqrt{\Delta}}{2a}$ et $z_2=\dfrac{-b-\sqrt{\Delta}}{2a}$.**
- **Si $\Delta<0$, deux racines complexes conjuguées $z_1=\dfrac{-b+i\sqrt{-\Delta}}{2a}$ et $z_2=\dfrac{-b-i\sqrt{-\Delta}}{2a}$.**

Preuve : On part de la forme canonique $P(z)=a\left(z+\frac{b}{2a}\right)^2-\frac{\Delta}{4a}$ et on factorise par a :

$P(z)=a\left[\left(z+\frac{b}{2a}\right)^2-\frac{\Delta}{4a^2}\right]$. Chercher les racines revient donc à résoudre dans $\mathbb{C}$ $\left(z+\frac{b}{2a}\right)^2=\frac{\Delta}{4a^2}$.

- Si $\Delta=0$, $\left(z+\frac{b}{2a}\right)^2=0\Leftrightarrow z+\frac{b}{2a}=0\Leftrightarrow \boldsymbol{z=-\frac{b}{2a}}$.
- Si $\Delta>0$, $\left(z+\frac{b}{2a}\right)^2=\frac{\Delta}{4a^2}\Leftrightarrow z+\frac{b}{2a}=\frac{\sqrt{\Delta}}{2a}$ ou $z+\frac{b}{2a}=-\frac{\sqrt{\Delta}}{2a}\Leftrightarrow \boldsymbol{z=\frac{-b+\sqrt{\Delta}}{2a}}$ **ou** $\boldsymbol{z=\frac{-b-\sqrt{\Delta}}{2a}}$.
- Si $\Delta<0$, $\left(z+\frac{b}{2a}\right)^2=\frac{\Delta}{4a^2}\Leftrightarrow z+\frac{b}{2a}=\frac{i\sqrt{-\Delta}}{2a}$ ou $z+\frac{b}{2a}=-\frac{i\sqrt{-\Delta}}{2a}\Leftrightarrow \boldsymbol{z=\frac{-b+i\sqrt{-\Delta}}{2a}}$ **ou** $\boldsymbol{z=\frac{-b-i\sqrt{-\Delta}}{2a}}$.

Remarque : En remarquant que $\Delta=0$ peut être vu comme un cas particulier des deux autres cas, on a alors $z_1=z_2=z_0$, et $P(z)=a(z-z_1)(z-z_2)$.

II – Polynômes

Dans cette partie, n est un entier naturel non nul et on adoptera la convention algébrique $0^0=1$.

Définition : Un polynôme non nul P à coefficients réels de la variable complexe z est défini par une expression de la forme $P(z)=a_nz^n+a_{n-1}z^{n-1}+\ldots+a_2z^2+a_1z+a_0$ avec pour tout $k\in[\![0;n]\!]$ $a_k\in\mathbb{R}$ tels que $a_n\neq0$. L'entier naturel n est le degré du polynôme.

Remarque : On peut étendre cette définition et considérer les polynômes à coefficients complexes de la variable complexe z. Les résultats qui suivent sont énoncés dans ce cadre.

Définition : $z_0\in\mathbb{C}$ est une racine d'un polynôme P si et seulement si $P(z_0)=0$.

Exemple: P défini sur $\mathbb{C}$ par $P=2z^3+z^2+41z-21$ est un polynôme de degré 3 à coefficients réels. $\frac{1}{2}$ est une racine de P car $P\left(\frac{1}{2}\right)=0$.

Propriété : **Soit P un polynôme *à coefficients réels*. Alors, si $z_0 \in \mathbb{C}$ est une racine de P, alors nécessairement $\overline{z_0}$ est une racine de P.**

Preuve : Soit $P(z)=a_n z^n+a_{n-1}z^{n-1}+\ldots+a_2 z^2+a_1 z+a_0=\sum_{k=0}^{n} a_k z^k$ un polynôme tel que pour tout $k\in[\![0;n]\!]$ $a_k\in\mathbb{R}$. On a donc pour tout $k\in[\![0;n]\!]$ $\overline{a_k}=a_k$. Soit $z_0\in\mathbb{C}$ une racine de P. On a donc $P(z_0)=0$. On a alors $P(\overline{z_0})=\sum_{k=0}^{n} a_k \overline{z_0}^k=\sum_{k=0}^{n} \overline{a_k}\,\overline{z_0^k}=\sum_{k=0}^{n} \overline{a_k z_0^k}=\overline{\sum_{k=0}^{n} a_k z_0^k}=\overline{0}=0$ donc $\overline{z_0}$ est une racine de P.

Propriété : **Pour tous $a\in\mathbb{C}$ et $z\in\mathbb{C}$, $z^n-a^n=(z-a)(z^{n-1}+az^{n-2}+a^2z^{n-3}+\ldots+a^{n-2}z+a^{n-1})$, ce qui se note $z^n-a^n=(z-a)\sum_{k=1}^{n} a^{k-1}z^{n-k}$.**

Exemple : *Pour tout $z\in\mathbb{C}$, on a $z^5-32=z^5-2^5=(z-2)(z^4+2z^3+4z^2+8z+16)$.*

Preuve : On développe $R(z)=(z-a)(z^{n-1}+az^{n-2}+a^2z^{n-3}+\ldots+a^{n-2}z+a^{n-1})$:

$R(z)=z^n+az^{n-1}+a^2z^{n-2}+\ldots+a^{n-2}z^2+a^{n-1}z-az^{n-1}-a^2z^{n-2}-a^3z^{n-3}-\ldots-a^{n-1}z-a^n$.

En simplifiant, il reste $R(z)=z^n-a^n$.

Théorème : **Soit $a\in\mathbb{C}$. Si P est un polynôme à coefficients réels de la variable complexe de degré $n\geqslant 1$ dont a est une racine, alors on peut factoriser $P(z)$ par $(z-a)$, c'est-à-dire qu'il existe un polynôme Q de degré $n-1$ tel que pour tout $z\in\mathbb{C}$ on ait $P(z)=(z-a)Q(z)$.**

Exemple : *On considère le polynôme $P(z)=z^3+z^2+z+1$. $P(i)=0$ donc il existe un polynôme Q de degré 2 tel que pour tout $z\in\mathbb{C}$, $P(z)=(z-i)Q(z)$.*

Mieux, comme P est à coefficients réels et que i en est une racine, on en déduit que $\overline{i}=-i$ en est également une racine.

On en déduit que P peut se factoriser par $(z-i)(z+i)=z^2+1$ et donc qu'il existe un polynôme de degré 1 $R(z)$ tel que $P(z)=(z^2+1)R(z)$.

Preuve : P étant un polynôme à coefficients réels de la variable complexe de degré n, il existe des réels a_0 ; a_1 ; … a_n avec $a_n \neq 0$ tels que pour tout $z \in \mathbb{C}$, $P(z) = \sum_{k=0}^{n} a_k z^k$.

a est une racine de P donc $P(a) = 0 \Leftrightarrow P(z) = P(z) - P(a) = \sum_{k=0}^{n} a_k z^k - \sum_{k=0}^{n} a_k a^k = \sum_{k=0}^{n} a_k (z^k - a^k)$.

En utilisant la propriété précédente, on a :

$$P(z) = \sum_{k=0}^{n} a_k (z-a)(z^{k-1} + a z^{k-2} + \ldots + a^{k-2} z + a^{k-1}) = (z-a) \sum_{k=0}^{n} a_k (z^{k-1} + a z^{k-2} + \ldots + a^{k-2} z + a^{k-1}).$$

On pose $Q(z) = \sum_{k=0}^{n} a_k (z^{k-1} + a z^{k-2} + \ldots + a^{k-2} z + a^{k-1})$. Comme $a_n \neq 0$, Q est de degré $n-1$ et on a le résultat souhaité.

Théorème : Un polynôme de degré $n \geqslant 1$ admet au plus n racines.

Preuve par récurrence : Soient $n \in \mathbb{N}^*$ et $HR(n)$ l'hypothèse le polynôme P de degré n a au plus n racines.

Initialisation : Pour $n = 1$, le polynôme est défini par $P(z) = az + b$ avec $a \in \mathbb{C}^*$, $b \in \mathbb{C}$.

Il admet exactement une racine, $z = -\frac{b}{a}$ donc $HR(1)$ est vraie.

Hérédité : On suppose que pour un entier $k \geqslant 1$, $HR(k)$ est vraie, c'est-à-dire que tout polynôme de degré k admet au plus k racines. On considère un polynôme P de degré $k+1$.

- Si P n'admet pas de racine, alors $HR(k+1)$ est vraie puisque $0 \leqslant k+1$.
- Sinon, soit $a \in \mathbb{C}$ une racine de P. D'après le théorème précédent, il existe un polynôme Q tel que, pour tout $z \in \mathbb{C}$, $P(z) = (z-a)Q(z)$. Q est de degré k.
  Alors, d'après $HR(k)$, Q a au plus k racines. Par conséquent, P qui admet éventuellement la racine supplémentaire a (qui peut être déjà racine de Q) admet au plus $k+1$ racines. Donc $HR(k+1)$ est vraie.

Conclusion : Tout polynôme de degré $n \geqslant 1$ admet au plus n racines.

Chapitre 4 – PGCD et applications

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

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 : Pour tout $k\in\mathbb{Z}$:
- Si d divise a et b, alors d divise a et $a-kb$, 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 : *Avec les notations précédentes, on a :*
$D(63;75)=D(63;75-63)=D(63;12)=D(63-5\times 12;12)=D(3;12)=\{-3;-1;1;3\}$.

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	×	q	+	r
240	=	36	×	6	+	24
36	=	24	×	1	+	12
24	=	12	×	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 $r\neq 0$, 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 $r_0\neq 0$, on remplace a par b et b par r_0 : $b=r_0q_1+r_1$ avec $0\leqslant r_1<r_0$.
- Si $r_1\neq 0$, 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 $r_2\neq 0$, 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 $r_k\neq 0$ 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).

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.** $d=PGCD(a;b)\Leftrightarrow\begin{cases}a=da'\\b=db'\end{cases}$ **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

<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 $v_0=-q_0$ qui sont des entiers.
De $b=r_0q_1+r_1$, on obtient $r_1=b-q_1r_0=b-(au_0+bv_0)q_1=au_1+bv_1$ 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 $\mathbf{33}=165-(231-165)\times2=165-2\times231+165\times2=\mathbf{165\times3+231\times(-2)}$.
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 $n\in\mathbb{Z}$, $n\times(-1)+(n+1)\times1=1$.*

III – Théorème de Gauss

<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 $75=3\times25$, 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 d'après le théorème de Bézout des entiers relatifs u et v 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, $5\times4=20$ 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 5 – Nombres premiers

I – Nombres premiers

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

Exemples :

- *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.*

Remarques :

- 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.

Théorème :

- **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 $\sqrt{n}$.**

Preuve : 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 $p^2\leqslant pq\Rightarrow p^2\leqslant n\Rightarrow p\leqslant\sqrt{n}$.

Propriété (test de primalité) : 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.

Preuve : Si n 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.

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 $800 = 8 \times 4 \times 25 = 2^5 \times 5^2$ où 2 et 5 sont des nombres premiers.

a) Existence et unicité d'une décomposition

Théorème : Tout entier $n \geqslant 2$ se décompose en un produit de nombres premiers. Cette décomposition est unique à l'ordre des facteurs près.
On peut donc écrire $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ 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 $n \geqslant 2$ un entier. On sait d'après le premier théorème du I qu'il admet un diviseur premier p_1 . On a donc $n = p_1 n_1$ 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 $n = p_1 p_2 n_2$ 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 $n = p_1 p_2 \ldots p_m$ 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 apparaît avec l'exposant $\alpha \geqslant 1$ dans une décomposition, et l'exposant $\beta \geqslant 0$ dans une autre ($\beta = 0$ si le facteur n'apparaît 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.

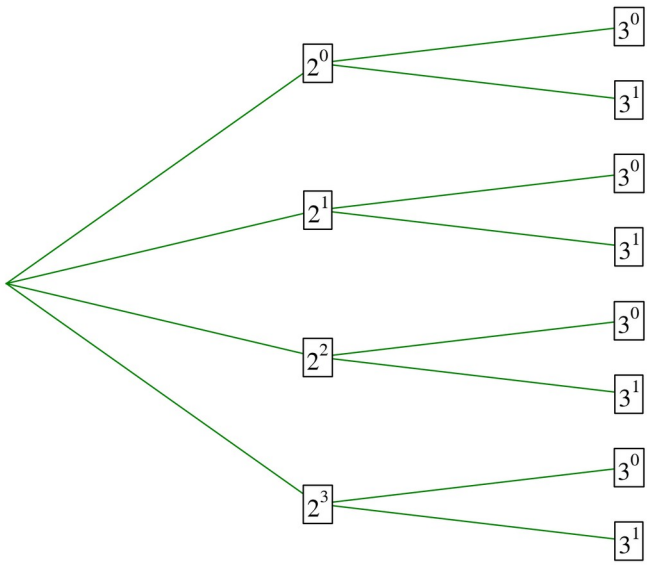
Remarque : On peut noter $n = \prod_{i=1}^{k} p_i^{\alpha_i}$.

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 dans $\mathbb{N}$ 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 déduit de la conséquence 1 que 31500 possède $3 \times 3 \times 4 \times 2 = 72$ *diviseurs dans* $\mathbb{N}$ *, et 2733750 en possède* $2 \times 8 \times 5 = 80$.
On déduit de la conséquence 2 que $PGCD(31500 ; 2733750) = 2 \times 3^2 \times 5^3 = 2250$.

III – Petit théorème de Fermat

Petit théorème de Fermat : Soit p un nombre premier et a un entier naturel non divisible par p . Alors $a^{p-1}-1$ est divisible par p , c'est-à-dire que $a^{p-1} \equiv 1 [p]$.

Preuve : (1) p n'apparaît pas la décomposition en facteurs premiers de 1, 2, …., $p-1$.

Donc p n'apparaît pas dans la décomposition en facteurs premiers de $\prod_{k=1}^{p-1} k = (p-1)!$. On en déduit que p et $(p-1)!$ sont premiers entre eux.

(2) Si $k \in [\![1 ; p-1]\!]$, alors le reste r_k de la division euclidienne de ka par p est non nul ; en effet, si p divisait ka , comme p et k sont premiers entre eux, d'après le théorème de Gauss, p diviserait a . Or ceci est impossible car par hypothèse a n'est pas divisible par p .

(3) Si $k' \in [\![1 ; p-1]\!]$ est distinct de k (par exemple $k < k'$), alors les restes r_k et $r_{k'}$ sont distincts. En effet, si $r_k = r_{k'}$, alors p diviserait $k'a - ka = a(k'-k)$. Comme $k'-k \in [\![1 ; p-1]\!]$ cela signifierait que $r_{k'-k}$ serait nul, ce qui contredit le point (2).

(4) Ainsi, les $p-1$ restes r_1 , r_2 , …, r_{p-1} sont tous distincts et appartiennent à $[\![1 ; p-1]\!]$. On en déduit que $\{r_1 ; r_2 ; \dots ; r_{p-1}\}$ est une permutation de $[\![1 ; p-1]\!]$, donc $\prod_{k=1}^{p-1} r_k = (p-1)!$.

On en déduit que $\prod_{k=1}^{p-1} (ka) \equiv \prod_{k=1}^{p-1} r_k [p] \Leftrightarrow (p-1)! a^{p-1} \equiv (p-1)! [p]$. Donc $p \mid \left((p-1)!(a^{p-1}-1)\right)$. Or p et $(p-1)!$ sont premiers entre eux donc d'après le théorème de Gauss, p divise $a^{p-1}-1$.

Conséquence : si p est premier et $a \in \mathbb{N}$, alors $a^p \equiv a [p]$.

Preuve : Si a est divisible par p , alors $a(a^{p-1}-1) = a^p - a$ est également divisible par p donc $a^p \equiv a [p]$. Sinon, d'après le petit théorème de Fermat, $a^{p-1} \equiv 1 [p] \Rightarrow a^p \equiv a [p]$.

Chapitre 6 – Nombres complexes, géométrie et formule du binôme

Dans ce chapitre, le plan est muni d'un repère orthonormé $(O;\vec{u},\vec{v})$ *direct*, c'est-à-dire que $(\vec{u};\vec{v})=\frac{\pi}{2}+2k\pi$ avec $k\in\mathbb{Z}$. On appelle ce plan le *plan complexe*.

I – Géométrie et nombres complexes

a) Affixe d'un point ou d'un vecteur

Définitions : À tout nombre complexe z de forme algébrique $x+iy$ (avec $x\in\mathbb{R}$ et $y\in\mathbb{R}$) on associe le point $M(x;y)$ du plan complexe. On dit que M est le *point image* de z et que $\overrightarrow{OM}$ est le *vecteur image* de z ; on dit que z est l'*affixe* du point M et du vecteur $\overrightarrow{OM}$.

Remarques:

- Tout point M est l'unique point image d'un complexe z, et réciproquement tout complexe z est l'unique affixe d'un point M.
- Pour indiquer que z est l'affixe de M, on note $M(z)$.
- Les nombres réels sont les affixes des points de l'axe des abscisses, appelé *axe des réels*.
- Les nombres imaginaires purs sont les affixes des points de l'axe des ordonnées appelé *axe des imaginaires purs*.

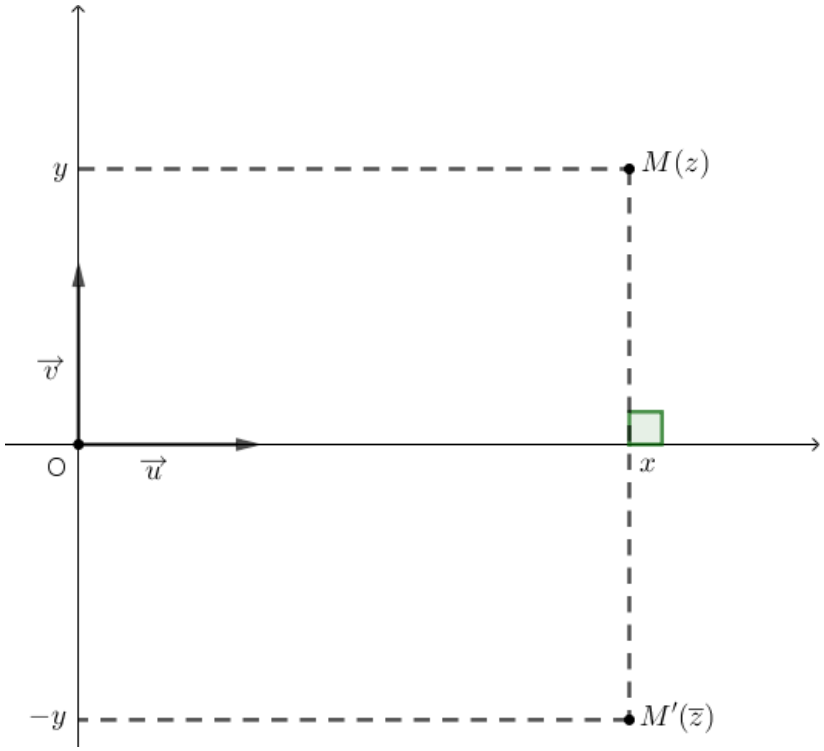
Propriétés :

- **Deux vecteurs sont égaux si et seulement si leurs affixes sont égales.**
- **Si $\vec{u}$ et $\vec{v}$ ont pour affixes respectives z et z', alors pour tout $\lambda\in\mathbb{R}$ l'affixe du vecteur $\vec{u}+\lambda\vec{v}$ est $z+\lambda z'$.**
- **Pour tous points A et B d'affixes respectives z_A et z_B, l'affixe de $\overrightarrow{AB}$ est z_B-z_A.**
- **Pour tous points A et B d'affixes respectives z_A et z_B, l'affixe de I, milieu de $[AB]$, est $z_I=\frac{z_A+z_B}{2}$.**

Remarque : Ces résultats se prouvent comme en classe de seconde, à l'aide de la relation de Chasles notamment.

<u>Interprétation géométrique du conjugué :</u> Pour tout $z\in\mathbb{C}$, les points $M(z)$ et $M'(\overline{z})$ sont symétriques l'un de l'autre par rapport à l'axe des abscisses.

En effet, si $z=x+iy$ avec $x\in\mathbb{R}$ et $y\in\mathbb{R}$, alors $\overline{z}=x-iy$ donc M et M' ont la même abscisse et des ordonnées opposées.



<u>b) Module d'un nombre complexe</u>

<u>Définition :</u> Soit $z\in\mathbb{C}$ de forme algébrique $x+iy$ avec $x\in\mathbb{R}$ et $y\in\mathbb{R}$.

Le *module* de z est le nombre réel positif noté $|z|$ défini par $|z|=\sqrt{x^2+y^2}$.

<u>Interprétation géométrique du module :</u> Dans le plan complexe, si M a pour affixe z, alors $|z|=OM$.

<u>Remarques :</u>

- Si $x\in\mathbb{R}$, alors le module de x est la valeur absolue de x.
- $|z|=0\Leftrightarrow OM=0\Leftrightarrow M=O\Leftrightarrow z=0$.

<u>Propriétés :</u> Pour tout $z\in\mathbb{C}$,

(1) $\lvert -z\rvert=\lvert z\rvert$	**(2)** $\lvert\overline{z}\rvert=\lvert z\rvert$	**(3)** $z\,\overline{z}=\lvert z\rvert^2$

<u>Preuves :</u> (1) et (2) découlent de la définition, et (3) de la quatrième identité remarquable.

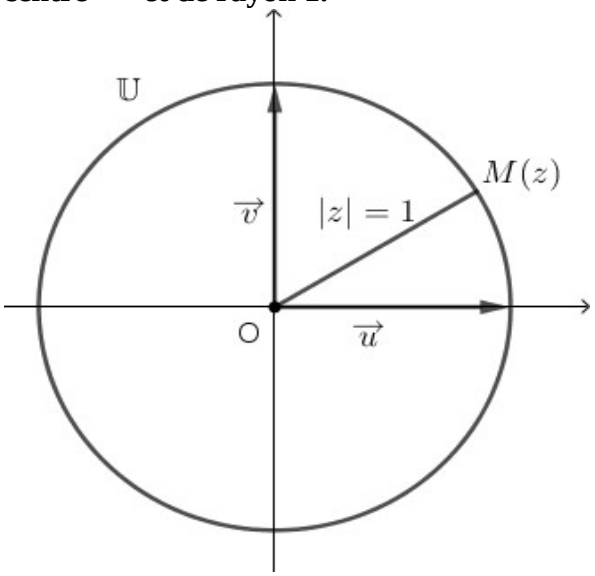
Propriétés : **Pour tous complexes z , z' et tout entier naturel non nul n , on a :**

(1) $\lvert zz'\rvert=\lvert z\rvert\lvert z'\rvert$	**(2)** $\lvert z^n\rvert=\lvert z\rvert^n$	**(3)** $\left\lvert\frac{1}{z'}\right\rvert=\frac{1}{\lvert z'\rvert}$ **si** $z'\neq 0$	**(4)** $\left\lvert\frac{z}{z'}\right\rvert=\frac{\lvert z\rvert}{\lvert z'\rvert}$ **si** $z'\neq 0$

Preuves :

- (1) $\lvert zz'\rvert^2=zz'\times\overline{zz'}=zz'\bar{z}\,\overline{z'}=z\bar{z}z'\overline{z'}=\lvert z\rvert^2\lvert z'\rvert^2=(\lvert z\rvert\lvert z'\rvert)^2$. Or $\lvert zz'\rvert$ et $\lvert z\rvert\lvert z'\rvert$ sont des réels positifs, donc on en déduit que $\lvert zz'\rvert=\lvert z\rvert\lvert z'\rvert$.
- (2) se démontre par récurrence en utilisant (1).
- (3) et (4) se démontrent en utilisant (1) et le fait que pour tout $z'\neq 0$, $z'\times\frac{1}{z'}=1$.

Définition : **On note IU l'ensemble des nombres complexes de module 1. Il s'agit dans le plan complexe du cercle de centre O et de rayon 1.**



Propriétés : **Pour tous complexes z et z' de l'ensemble IU , on a :**

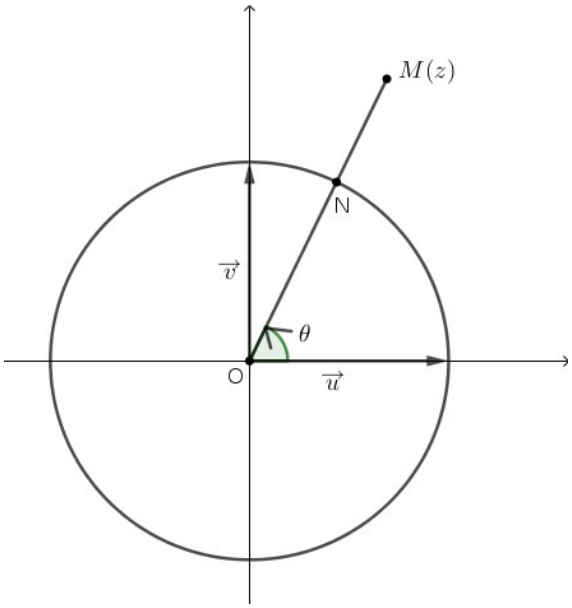
(1) $zz'\in IU$	**(2)** $\frac{1}{z'}\in IU$	**(3)** $\frac{z}{z'}\in IU$

Preuves : Comme $z\in IU$ et $z'\in UI$, on a $\lvert z\rvert=\lvert z'\rvert=1$. ce qui entraîne :

- $\lvert zz'\rvert=\lvert z\rvert\lvert z'\rvert=1\times 1=1$ donc $zz'\in UI$; on a donc (1).
- $\left\lvert\frac{1}{z'}\right\rvert=\frac{\lvert 1\rvert}{\lvert z'\rvert}=\frac{1}{1}=1$ donc $\frac{1}{z'}\in UI$; on a donc (2).
- En appliquant (1) à z et $\frac{1}{z'}$ (qui appartient à UI d'après (2)) on obtient (3).

c) Arguments d'un nombre complexe

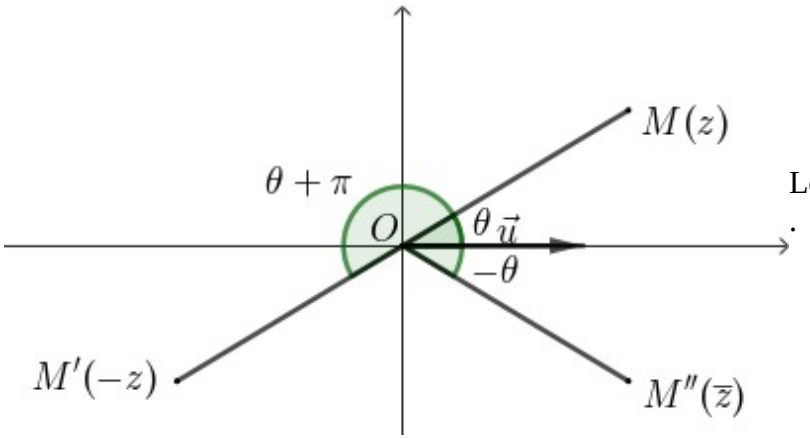
Définition : Soit z un nombre complexe non nul de point image M dans le plan complexe, et N est le point du cercle trigonométrique tel que $\overrightarrow{ON}=\frac{1}{OM}\overrightarrow{OM}$. On appelle *argument* de z et on note $\arg(z)$ tout nombre réel θ dont N est l'image sur le cercle trigonométrique.



Remarques : Un nombre complexe non nul a une infinité d'arguments : si θ est l'un d'eux, les autres s'écrivent $\theta+k2\pi$ avec $k\in\mathbb{Z}$. On note $\arg(z)=\theta$ ou $\arg(z)=\theta[2\pi]$ ce qui se lit : « modulo 2π ». On dit aussi qu'une mesure de l'angle orienté $(\vec{u};\overrightarrow{OM})$ est θ.

Propriétés : Pour tout complexe non nul z :

$\arg(-z)=\arg(z)+\pi[2\pi]$	$\arg(\overline{z})=-\arg(z)[2\pi]$
$z\in\mathbb{R}\Leftrightarrow\arg(z)=0[\pi]$	z est un imaginaire pur $\Leftrightarrow\arg(z)=\frac{\pi}{2}[\pi]$



Les angles sont mesurés depuis $(O;\vec{u})$.

II – Formes trigonométrique et exponentielle d'un complexe non nul

a) Forme trigonométrique d'un complexe non nul

Soit $z\in\mathbb{C}^*$ dont θ est un argument. On considère le point M image de z et N le point tel que $\overrightarrow{ON}=\frac{1}{|z|}\overrightarrow{OM}$. N appartient donc au cercle trigonométrique et est l'image de θ, donc N a pour coordonnées cartésiennes $(\cos(\theta);\sin(\theta))$ et l'affixe de N est $z_N=\cos(\theta)+i\sin(\theta)$.

Comme $\overrightarrow{OM}=|z|\overrightarrow{ON}$, on en déduit que $z=|z|(\cos(\theta)+i\sin(\theta))$.

Définition : Soit $z\in\mathbb{C}^*$. L'écriture $z=|z|(\cos(\theta)+i\sin(\theta))$ où $\arg(z)=\theta[2\pi]$ est appelée une *forme trigonométrique* de z.

Propriétés :

- **Deux nombres complexes non nuls sont égaux si et seulement si ils ont *même module* et *même argument modulo* 2π.**
- **Si $z=r(\cos(\alpha)+i\sin(\alpha))$ avec $r>0$, alors $|z|=r$ et $\arg(z)=\alpha[2\pi]$.**
- **Si $z=r(\cos(\alpha)+i\sin(\alpha))$ avec $r<0$, alors $|z|=-r$ et $\arg(z)=\alpha+\pi[2\pi]$.**

b) Relation fonctionnelle

La fonction f définie sur $\mathbb{R}$ par $f(\theta)=\cos(\theta)+i\sin(\theta)$ est dérivable sur $\mathbb{R}$ comme somme de fonctions dérivables sur $\mathbb{R}$. Pour tout $\theta\in\mathbb{R}$, $f'(\theta)=\cos'(\theta)+i\sin'(\theta)\Leftrightarrow$

$f'(\theta)=-\sin(\theta)+i\cos(\theta)=i^2\sin(\theta)+i\cos(\theta)=i(i\sin(\theta)+\cos(\theta))=if(\theta)\Leftrightarrow \boldsymbol{f'(\theta)=if(\theta)}$.

f est donc solution de l'équation différentielle $y'=iy$, donc pour tout $\theta\in\mathbb{R}$ on a : $f(\theta)=ke^{i\theta}$ avec $k\in\mathbb{C}$.

Comme $f(0)=\cos(0)+i\sin(0)=1$ et $ke^{i\times 0}=ke^0=k$, on en déduit que $k=1$.

On a donc, pour tout $\theta\in\mathbb{R}$, $f(\theta)=e^{i\theta}$.

Notation : Pour tout $\theta\in\mathbb{R}$, on peut noter $\cos(\theta)+i\sin(\theta)=e^{i\theta}$. Cette notation est due à Euler en 1748. Ainsi, $e^{i\theta}$ désigne le nombre complexe de module 1 dont un argument est θ.

Exemples :

$e^{i2\pi}=1$	$e^{i\pi}=-1$	$e^{i\frac{\pi}{2}}=i$	$e^{i\frac{\pi}{3}}=\frac{1}{2}+i\frac{\sqrt{3}}{2}$

c) Forme exponentielle

Tout nombre complexe $z \neq 0$ admet une forme trigonométrique $z = |z|(\cos(\theta) + i\sin(\theta))$ avec $\theta = \arg(z)[2\pi]$. On peut donc écrire $z = |z|e^{i\theta}$.

Définition : Une *forme exponentielle* d'un nombre complexe $z \neq 0$ dont un argument est θ, est l'écriture $z = |z|e^{i\theta}$.

Exemple : Le nombre complexe $z = -2e^{i\frac{\pi}{6}}$ n'est pas une forme exponentielle car $-2 < 0$.

Pour déterminer la forme exponentielle, on peut utiliser le fait que $e^{i\pi} = -1$.

On a donc $z = 2e^{i\pi}e^{i\frac{\pi}{6}} = 2e^{i\left(\pi + \frac{\pi}{6}\right)} = 2e^{i\frac{7\pi}{6}}$.

d) Propriétés de la forme exponentielle

Propriétés : Pour tous réels θ et θ' et tout entier naturel n, on a :

- $\left|e^{i\theta}\right| = 1$ **et** $\arg\left(e^{i\theta}\right) = \theta[2\pi]$
- $e^{i\theta} = e^{i\theta'} \Leftrightarrow \theta = \theta'[2\pi]$
- **Formule de Moivre :** $\left(e^{i\theta}\right)^n = e^{in\theta}$
- $e^{i\theta} \times e^{i\theta'} = e^{i(\theta+\theta')}$ **et** $\dfrac{e^{i\theta}}{e^{i\theta'}} = e^{i(\theta-\theta')}$
- $\dfrac{1}{e^{i\theta}} = e^{i(-\theta)} = \overline{e^{i\theta}}$

Remarques :

- Ces propriétés traduisent les propriétés de l'argument.
- La formule de Moivre peut s'écrire $\left(\cos(\theta) + i\sin(\theta)\right)^n = \cos(n\theta) + i\sin(n\theta)$.

Propriétés (formules d'Euler) : Pour tout réel θ, $\cos(\theta) = \dfrac{e^{i\theta} + e^{-i\theta}}{2}$ et $\sin(\theta) = \dfrac{e^{i\theta} - e^{-i\theta}}{2i}$.

Preuve : $e^{i\theta} = \cos(\theta) + i\sin(\theta)$ et $e^{-i\theta} = \cos(-\theta) + i\sin(-\theta) = \cos(\theta) - i\sin(\theta)$.

Ainsi, $e^{i\theta} + e^{-i\theta} = 2\cos(\theta) \Leftrightarrow \dfrac{e^{i\theta} + e^{-i\theta}}{2} = \cos(\theta)$ et $e^{i\theta} - e^{-i\theta} = 2i\sin(\theta) \Leftrightarrow \dfrac{e^{i\theta} - e^{-i\theta}}{2i} = \sin(\theta)$.

e) Formules d'addition et de duplication, propriétés de l'argument

Théorème (formules d'addition) : Pour tous réels a et b, on a :

(1) $\cos(a+b)=\cos(a)\cos(b)-\sin(a)\sin(b)$	**(2)** $\cos(a-b)=\cos(a)\cos(b)+\sin(a)\sin(b)$
(3) $\sin(a+b)=\sin(a)\cos(b)+\sin(b)\cos(a)$	**(4)** $\sin(a-b)=\sin(a)\cos(b)-\sin(b)\cos(a)$

Preuves : On part de la relation fonctionnelle $e^{ia}e^{ib}=e^{i(a+b)}$. On a donc avec les formes trigonométriques : $(\cos(a)+i\sin(a))(\cos(b)+i\sin(b))=(\cos(a+b)+i\sin(a+b))\Leftrightarrow$
$\cos(a)\cos(b)+i\cos(a)\sin(b)+i\sin(a)\cos(b)+i^2\sin(a)\sin(b)=(\cos(a+b)+i\sin(a+b))\Leftrightarrow$
$\cos(a)\cos(b)-\sin(a)\sin(b)+i(\cos(a)\sin(b)+\sin(a)\cos(b))=(\cos(a+b)+i\sin(a+b))$.
En égalisant les parties réelles, on obtient (1) et en égalisant les parties imaginaires on obtient (3). En remplaçant b par $-b$ dans (1) et (3) et en utilisant la parité de la fonction cosinus et l'imparité de la fonction sinus, on obtient (2) et (4). On peut également utilisation la relation fonctionnelle $e^{ia}e^{-ib}=e^{i(a-b)}$.

Conséquence (formules de duplication) : Pour tout réel a, on a :

$\cos(2a)=\cos^2(a)-\sin^2(a)$	$\cos(2a)=2\cos^2(a)-1$
$\cos(2a)=1-2\sin^2(a)$	$\sin(2a)=2\sin(a)\cos(a)$

Preuve : il suffit de prendre $b=a$ dans les relations (1) et (3), et d'utiliser le fait que $\cos^2(a)+\sin^2(a)=1$.

Propriétés : Pour tous complexes non nuls z et z' et tout entier naturel n, on a :

(1) $\arg(zz')=\arg(z)+\arg(z')[2\pi]$	**(2)** $\arg(z^n)=n\arg(z)[2\pi]$
(3) $\arg\left(\frac{1}{z'}\right)=-\arg(z')[2\pi]$	**(4)** $\arg\left(\frac{z}{z'}\right)=\arg(z)-\arg(z')[2\pi]$

Preuves : En posant $z=|z|(\cos(\theta)+i\sin(\theta))$ et $z'=|z'|(\cos(\theta')+i\sin(\theta'))$, on a donc :

- $zz'=|z||z'|(\cos(\theta)+i\sin(\theta))(\cos(\theta')+i\sin(\theta'))\Leftrightarrow$
  $zz'=|zz'|(\cos(\theta)\cos(\theta')-\sin(\theta)\sin(\theta')+i(\sin(\theta)\cos(\theta')+\sin(\theta')\cos(\theta)))$. En utilisant les formules d'addition on a : $zz'=|zz'|(\cos(\theta+\theta')+i\sin(\theta+\theta'))$. Donc $\arg(zz')=\arg(z)+\arg(z')[2\pi]$ ce qui fournit (1).
- Avec une récurrence immédiate, (1) permet d'obtenir (2).
- $\arg\left(z'\times\frac{1}{z'}\right)=\arg(1)=0$ et $\arg\left(z'\times\frac{1}{z'}\right)=\arg(z')+\arg\left(\frac{1}{z'}\right)$ fournissent (3).
- (1) et (3) fournissent (4).

III – Racines *n*-ièmes de l'unité

<u>Définition :</u> Une racine *n*-ième de l'unité est une solution dans $\mathbb{C}$ de l'équation $z^n=1$.

<u>Exemple :</u> i *est une racine quatrième de l'unité, puisque* $i^4=1$.

<u>Propriété :</u> Les racines *n*-ièmes de l'unité s'écrivent $e^{i\frac{2k\pi}{n}}$ avec $k\in[\![0;n-1]\!]$.

<u>Preuve :</u> On pose $z=re^{i\theta}$ avec $r>0$ et $\theta\in\mathbb{R}$. On a donc :

$$z^n=1\Leftrightarrow r^n e^{in\theta}=1\Leftrightarrow\begin{cases}r^n=1\\ n\theta=0\,[2\pi]\end{cases}\Leftrightarrow\begin{cases}r=1\\ \theta=\dfrac{k2\pi}{n}\text{ avec }k\in\mathbb{Z}\end{cases}$$

Or, tout entier relatif k peut s'écrire $k=nq+s$ avec s, q dans $\mathbb{Z}$ tels que $0\leqslant s<n$.

Ainsi, $\dfrac{k2\pi}{n}=q\times 2\pi+\dfrac{s2\pi}{n}$, soit $\dfrac{k2\pi}{n}=\dfrac{s2\pi}{n}\,[2\pi]$.

L'équation $z^n=1$ possède donc n solutions : les nombres complexes $e^{i\frac{2s\pi}{n}}$ avec $s\in[\![0;n-1]\!]$.

IV – Formule du binôme de Newton dans l'ensemble des nombres complexes

<u>a) Les coefficients binomiaux</u>

<u>Définition :</u> Soient k et n deux entiers naturels tels que $k\leqslant n$. Le nombre de combinaisons de k éléments parmi n est noté $\binom{n}{k}$.

<u>Remarque :</u> L'ordre des éléments n'intervient pas. $\binom{n}{k}$ est notamment le nombre de chemins comportant k succès pour n réalisations indépendantes de la même épreuve de Bernoulli.

<u>Propriétés :</u> On peut démontrer que, pour tous entiers n et k tels que $k\leqslant n$, on a :

$\binom{n}{0}=1$	$\binom{n}{1}=n$	$\binom{n}{k}=\binom{n}{n-k}$	Si $0\leqslant k\leqslant n-1$ on a $\binom{n}{k}+\binom{n}{k+1}=\binom{n+1}{k+1}$

<u>Conséquence :</u> Pour tout entier n on a $\binom{n}{n}=1$ et $\binom{n}{n-1}=n$.

<u>b) Le triangle de Pascal</u>

Le triangle de Pascal est un tableau qui donne les valeurs des coefficients binomiaux $\binom{n}{k}$.

Comme $0\leqslant k\leqslant n$, il a la forme d'un triangle. Il peut bien sûr être prolongé pour $n=4$, $n=5$, … et pour $k=4$, $k=5$, …

	$k=0$	$k=1$	$k=2$	$k=3$
$n=0$	$\binom{0}{0}$			
$n=1$	$\binom{1}{0}$	$\binom{1}{1}$		
$n=2$	$\binom{2}{0}$	$\binom{2}{1}$	$\binom{2}{2}$	
$n=3$	$\binom{3}{0}$	$\binom{3}{1}$	$\binom{3}{2}$	$\binom{3}{3}$

Les remarques et propriétés précédentes permettent de calculer les coefficients :

- Pour $n\in\mathbb{N}$, $\binom{n}{0}=1$ donc dans la colonne « $k=0$ » toutes les valeurs valent 1.
- Pour $n\in\mathbb{N}$, $\binom{n}{n}=1$ donc dans la diagonale $\binom{0}{0}$, $\binom{1}{1}$, … toutes les valeurs valent 1.
- Pour $0\leqslant k\leqslant n-1$, $\binom{n}{k}+\binom{n}{k+1}=\binom{n+1}{k+1}$ donc la valeur de la case $\binom{n+1}{k+1}$ s'obtient en ajoutant la case du dessus $\binom{n}{k+1}$ avec la case à côté de cette dernière $\binom{n}{k}$.
- Pour $n\in\mathbb{N}$ et $k\in\mathbb{N}$ avec $k\leqslant n$, $\binom{n}{k}=\binom{n}{n-k}$ donc chaque ligne peut se lire dans les deux sens.

On obtient donc :

	$k=0$	$k=1$	$k=2$	$k=3$
$n=0$	1			
$n=1$	1	1		
$n=2$	1	2	1	
$n=3$	1	3	3	1

c) La formule du binôme de Newton

Propriété : Pour tous $a\in\mathbb{C}$ et $b\in\mathbb{C}$, et pour tout $n\in\mathbb{N}^*$ on a :

$$(a+b)^n=a^n+\binom{n}{1}a^{n-1}b+\binom{n}{2}a^{n-2}b^2+\binom{n}{3}a^{n-3}b^3+\ldots+\binom{n}{n-1}a^1b^{n-1}+b^n .$$

Ceci se note de manière condensée : $(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$ lorsque a et b sont non nuls.

Exemple : *Soit $z\in\mathbb{C}$. On a alors :*

$$(z-1)^4=z^4+\binom{4}{1}z^3\times(-1)^1+\binom{4}{2}z^2\times(-1)^2+\binom{4}{3}z^1\times(-1)^3+(-1)^4=z^4-4z^3+6z^2-4z+1 .$$

Preuve par récurrence : Soient $a\in\mathbb{C}$, $b\in\mathbb{C}$, et $n\in\mathbb{N}^*$.

Soit $P(n)$ l'hypothèse $(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$.

Initialisation : $(a+b)^1=a+b$ et $a^1+b^1=a+b$ donc $P(1)$ est vraie.

Hérédité : On suppose que pour un entier naturel $h\geqslant 1$ $P(h)$ est vraie :

$(a+b)^h=\sum_{k=0}^{h}\binom{h}{k}a^{h-k}b^k$. On multiplie chaque membre par $(a+b)$:

$$(a+b)(a+b)^h=(a+b)\left(\sum_{k=0}^{h}\binom{h}{k}a^{h-k}b^k\right)\Leftrightarrow$$

$$(a+b)^{h+1}=a^{h+1}+a\sum_{k=1}^{h}\binom{h}{k}a^{h-k}b^k+b\sum_{k=0}^{h-1}\binom{h}{k}a^{h-k}b^k+b^{h+1}\Leftrightarrow a^{h+1}+\sum_{k=1}^{h}\binom{h}{k}a^{h-k+1}b^k+\sum_{k=0}^{h-1}\binom{h}{k}a^{h-k}b^{k+1}+b^{h+1}$$

On pose $t=h-1$ dans la première somme et $t=h$ dans la seconde :

$$(a+b)^{h+1}=a^{h+1}+\sum_{t=0}^{h-1}\binom{h}{t+1}a^{h-t}b^{t+1}+\sum_{t=0}^{h-1}\binom{h}{t}a^{h-t}b^{t+1}+b^{h+1}\Leftrightarrow$$

$$(a+b)^{h+1}=a^{h+1}+\sum_{t=0}^{h-1}\left[\binom{h}{t+1}+\binom{h}{t}\right]a^{h-t}b^{t+1}+b^{h+1}$$. Or, comme $0\leqslant t\leqslant h-1$, $\binom{h}{t+1}+\binom{h}{t}=\binom{h+1}{t+1}$ donc

$$(a+b)^{h+1}=a^{h+1}+\sum_{t=0}^{h-1}\binom{h+1}{t+1}a^{h-t}b^{t+1}+b^{h+1}$$. On pose $k=t+1$:

$$(a+b)^{h+1}=a^{h+1}+\sum_{k=1}^{h}\binom{h+1}{k}a^{h+1-k}b^k+b^{h+1}$$ donc $P(h+1)$ est vraie.

Conclusion : Pour tout $n\in\mathbb{N}$, $(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$.

Chapitre 7 – Calcul matriciel et applications

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 complexes.

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 ambiguïtés) 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 complexe

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 $\lambda \in \mathbb{C}$. La matrice λA est la matrice $(\lambda a_{ij})_{1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n}$. Multiplier une matrice par un complexe revient à multiplier tous les coefficients par ce complexe.

Remarques :

- On a de façon évidente $A+B=B+A$.
- Les règles de priorité sont les mêmes qu'avec les complexes : $2A+3B$ désigne la matrice $(2A)+(3B)$.
- Pour tous complexes λ et μ, on a $\lambda(\mu A)=(\lambda\mu)A$ 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 $A\times B=\begin{pmatrix}a_{11} & a_{12} & \dots & a_{1n}\end{pmatrix}\times\begin{pmatrix}b_{11}\\ b_{21}\\ \dots\\ b_{n1}\end{pmatrix}=a_{11}\times b_{11}+a_{12}\times b_{21}+\dots+a_{1n}\times b_{n1}$.

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

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

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 complexe 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).

Exemple : *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 nul).

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 $A^0=I_n$.

Exemple : *Soit* $A=\begin{pmatrix}1 & 4\\ 0 & 1\end{pmatrix}$. *On a donc* $A^2=A\times A=\begin{pmatrix}1 & 8\\ 0 & 1\end{pmatrix}$, $A^3=A^2\times A=\begin{pmatrix}1 & 12\\ 0 & 1\end{pmatrix}$, $A^4=A^2\times A^2=\begin{pmatrix}1 & 16\\ 0 & 1\end{pmatrix}$.

On peut démontrer par récurrence que pour tout $n\in\mathbb{N}$, $A^n=\begin{pmatrix}1 & 4n\\ 0 & 1\end{pmatrix}$.

III – Matrices inversibles et application aux systèmes linéaires

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 $(B'A)B=I_nB=B$. 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 complexe $ad-bc$ est appelé déterminant de la matrice A, est noté $det(A)$ ou Δ. On note aussi, pour le calcul, $det(A)=\begin{vmatrix}a & b\\ c & d\end{vmatrix}$.

Exemple : *Pour* $\begin{pmatrix}3 & 1\\ 4 & 2\end{pmatrix}$, *on a* $\Delta=\begin{vmatrix}3 & 1\\ 4 & 2\end{vmatrix}=3\times2-1\times4=2$.

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

- **Si $\Delta\neq0$, 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 $\Delta\neq0$, $\frac{1}{\Delta}$ 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.

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

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

c) Application aux systèmes linéaires

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

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.

Théorème : Un système linéaire à n inconnues x_1, x_2, …, x_n :
$\begin{cases}a_{11}x_1+a_{12}x_2+\ldots+a_{1,n}x_n=y_1\\ a_{21}x_1+a_{22}x_2+\ldots+a_{2,n}x_n=y_2\\ \qquad\ldots\\ a_{n,1}x_1+a_{n,2}x_2+\ldots+a_{n,n}x_n=y_n\end{cases}$ **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 : $X=A^{-1}Y$.

Preuve : 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.

IV – Matrices et transformations du plan

Le plan est muni d'un repère orthonormé direct $(0;\vec{i},\vec{j})$.

a, b, c et d sont quatre nombres **réels**.

<u>Définition :</u> Une *translation* de vecteur $\vec{t}\begin{pmatrix}a\\b\end{pmatrix}$, qui à tout point $M(x;y)$ du plan associe son point image $M'(x';y')$ tel que $\overrightarrow{MM'}=\vec{t}$ se définit matriciellement comme la somme des matrices colonnes $\begin{pmatrix}x'\\y'\end{pmatrix}=\begin{pmatrix}x\\y\end{pmatrix}+\begin{pmatrix}a\\b\end{pmatrix}$.

<u>Propriété admise :</u> Pour les transformations géométriques planes suivantes, on définit la *matrice de transformation* $T=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ qui, à tout point $M(x;y)$ du plan, associe son point image $M'(x';y')$ tel que $\begin{pmatrix}x'\\y'\end{pmatrix}=T\times\begin{pmatrix}x\\y\end{pmatrix}$:

- **pour une symétrie axiale par rapport à l'axe des abscisses, $T=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$;**
- **pour une symétrie axiale par rapport à l'axe des ordonnées, $T=\begin{pmatrix}-1&0\\0&1\end{pmatrix}$;**
- **pour une rotation de centre O et d'angle θ, $T=\begin{pmatrix}\cos(\theta)&-\sin(\theta)\\\sin(\theta)&\cos(\theta)\end{pmatrix}$;**
- **pour une homothétie de centre O et de rapport $k\in\mathbb{R}$, $T=k\,I_2$.**

<u>Exemple :</u> La matrice associée à la rotation de centre O et d'angle $\frac{\pi}{3}$ est $\begin{pmatrix}\frac{1}{2}&-\frac{\sqrt{3}}{2}\\\frac{\sqrt{3}}{2}&\frac{1}{2}\end{pmatrix}$.

V – Graphes

a) Définitions

Définitions : Un *graphe* est une représentation composée de *sommets* (des points) reliés par des *arêtes* (segments).

Un *graphe orienté* est un graphe dont les arêtes sont munies d'un sens de parcours.

L'*ordre* d'un graphe est le nombre de sommets de ce graphe.

Le *degré* d'un sommet est le nombre d'arêtes incidentes à ce sommet, sans tenir compte de leur éventuel sens de parcours.

Deux *sommets* sont adjacents lorsqu'ils sont reliés par au moins une arête.

Un *graphe* est complet lorsque tous ses sommets sont deux-à-deux adjacents.

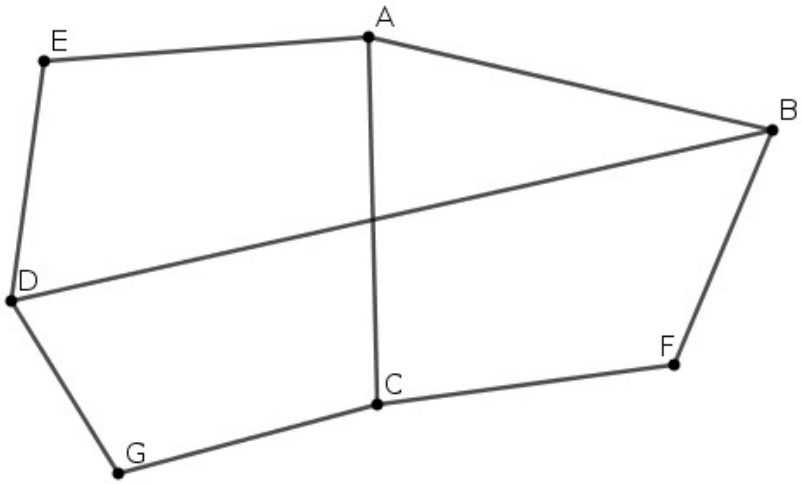
Exemple :

Le graphe ci-contre est d'ordre 7.

Il n'est pas orienté.

B *est de degré 3.*

A *et* G *ne sont pas adjacents, donc le graphe ne peut être complet.*



Théorème : Un graphe complet d'ordre n possède :

- $\boldsymbol{n(n-1)}$ **arêtes s'il est orienté ;**
- $\dfrac{\boldsymbol{n(n-1)}}{\boldsymbol{2}}$ **arêtes s'il est non orienté.**

Preuve :

- S'il est orienté, comme tous les sommets sont adjacents, une arrête est définie par un couple ordonnée $(a;b)$ de sommets. Il y a donc n possibilités pour le sommet a, et $n-1$ pour le sommet b. Le nombre d'arêtes est $n\times(n-1)$.
- S'il est non orienté, par rapport à la situation précédente, il y a deux fois moins d'arêtes, car les couples $(a;b)$ et $(b;a)$ correspondent à une même arête. Le nombre d'arêtes est donc $\dfrac{n\times(n-1)}{2}=\binom{n}{2}$.

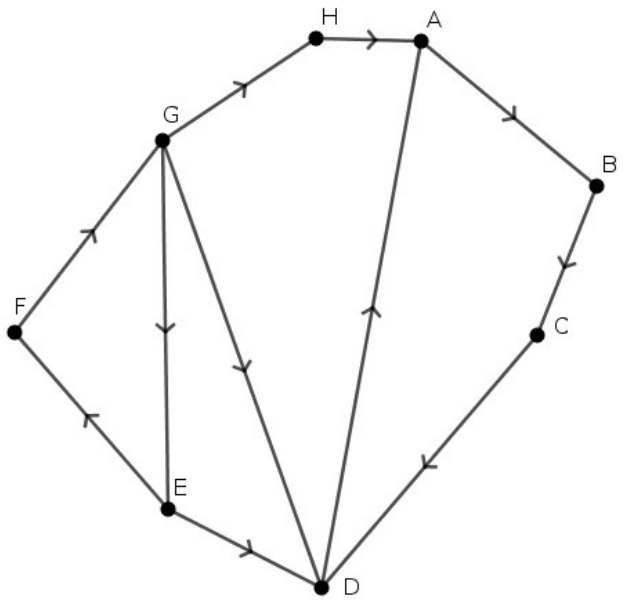
<u>Définitions :</u> Pour un graphe non orienté, une *chaîne* est une suite d'arêtes consécutives reliant deux sommets (éventuellement confondus).

La *longueur* d'une chaîne est le nombre d'arêtes la composant.

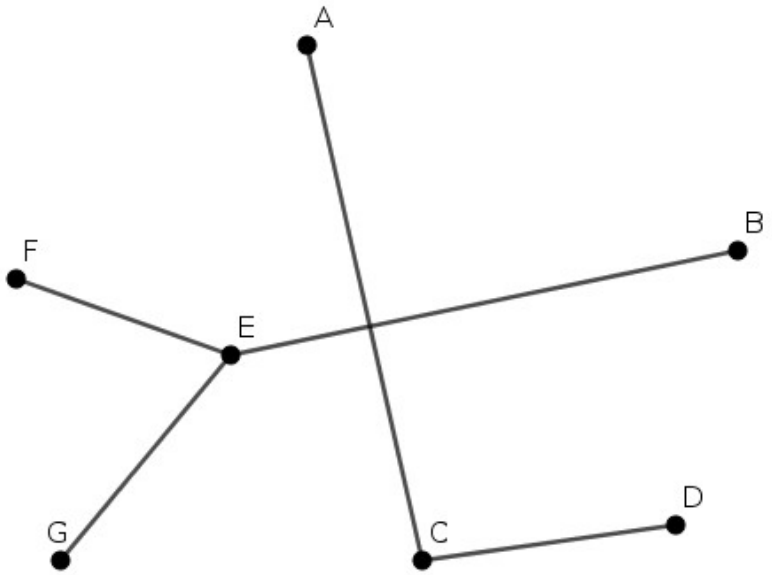
Pour un graphe orienté, un *chemin* est une suite d'arêtes consécutives reliant deux sommets (éventuellement confondus) en tenant compte du sens de parcours des arêtes.

Un graphe non orienté est *connexe* lorsque chaque couple de ses sommets peut-être relié par une chaîne.

<u>Exemple :</u> Avec le graphe orienté ci-dessous, le chemin $A-B-C-D-A$ est de longueur 4.



<u>Exemple :</u> Le graphe ci-dessous n'est pas connexe, puisque A et B ne sont pas reliés par une chaîne.



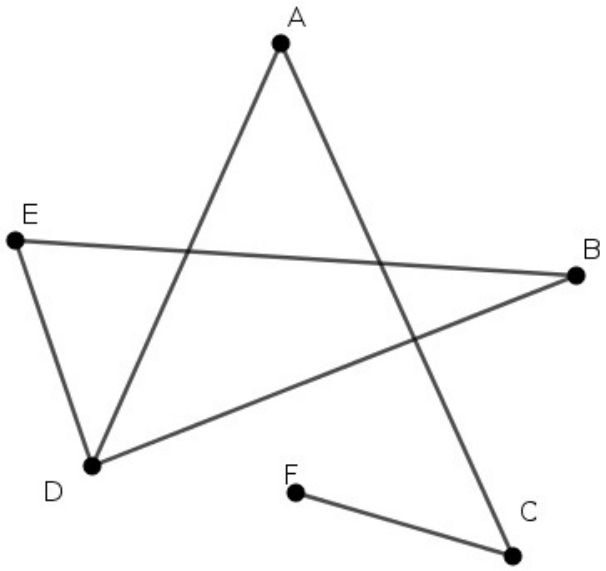
b) Calcul matriciel et graphes

Définition : Soit n un entier naturel non nul. On considère un graphe d'ordre n (éventuellement orienté) dont les sommets sont numérotés de 1 à n et rangés dans l'ordre croissant.

La *matrice d'adjacence* de ce graphe est la matricée carrée d'ordre n, notée M, dont le coefficient m_{ij} est égal au nombre d'arêtes partant du sommet i pour arriver au sommet j.

Remarques : La matrice d'un graphe non orienté est symétrique. La matrice d'un graphe comporte des zéros sur sa diagonale, les autres coefficients étant des 1 ou des 0.

Exemple : Pour le graphe ci-dessous, la matrice d'adjacence M est : $M=\begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$.



Propriété : Soient n et k deux entiers naturels non nuls et M la matrice d'adjacence d'un graphe d'ordre n (orienté ou non), dont les sommets sont numérotés de 1 à n et rangés dans l'ordre croissant. Alors, le terme de la i-ème ligne et de la j-ième colonne de la matrice M^k donne le nombre de chaînes (ou de chemins) de longueur k reliant le sommet i au sommet j.

Preuve : On démontre le résultat par récurrence sur k. Soit $P(k)$ l'hypothèse « Pour tout $i\in[\![1;n]\!]$ et pour tout $j\in[\![1;n]\!]$, le coefficient a_{ij} de la matrice M^k est le nombre de chaînes ou chemins de longueur k reliant le sommet i au sommet j ».

Initialisation : Si $k=1$, $M^k=M$ et pour tout $i\in[\![1;n]\!]$ et pour tout $j\in[\![1;n]\!]$, $m_{ij}=1$ si i est relié à j et 0 sinon. m_{ij} est alors le nombre de chemins ou chaînes de longueur 1. $P(1)$ est donc vraie.

Hérédité : On suppose que $P(k)$ est vraie pour un certain k. En notant $M^k=(a_{ij})_{,\leqslant i\leqslant n,1\leqslant j\leqslant n}$, on a donc que a_{ij} est le nombre de chaînes ou chemins de longueur k reliant i à j.

On note $M^{k+1}=(b_{ij})_{1\leqslant i\leqslant n,1\leqslant j\leqslant n}$. Comme $M^{k+1}=M^k\times M$, on a donc pour tout $i\in[\![1;n]\!]$ et pour tout $j\in[\![1;n]\!]$ $b_{ij}=\sum_{c=1}^{n}a_{ic}m_{cj}$, où a_{ic} donne le nombre de chaînes de longueur k reliant les sommets i et c, et m_{cj} donne le nombre de chaînes de longueur 1 reliant les sommets c et j.

Pour tout $c\in[\![1;n]\!]$, m_{cj} vaut 1 si les sommets c et j sont adjacents et 0 sinon.

Ainsi, $a_{ic}\times m_{cj}$ vaut a_{ic} si les sommets c et j sont adjacents et 0 sinon.

Cela correspond donc au nombre de chaînes ou chemins de longueur $k+1$ reliant le sommet i au sommet j pour lesquelles la dernière arête relie le sommet c au sommet j.

Ainsi, $b_{ij}=\sum_{c=1}^{n}a_{ic}m_{cj}$ correspond au nombre de chaînes de longueur $k+1$ reliant le sommet i au sommet j, en considérant toutes les possibilités pour l'avant-dernier sommet.

Conclusion : Pour tout k entier naturel non nul, le coefficient a_{ij} de la matrice M^k est le nombre de chaînes ou chemins de longueur k reliant le sommet i au sommet j.

Exemple : Avec l'exemple précédent, on a $M^5=\begin{pmatrix}2&7&10&17&7&0\\7&12&6&18&13&1\\10&6&0&2&6&5\\17&18&2&14&18&5\\7&13&6&18&12&1\\0&1&5&5&1&0\end{pmatrix}$. *Comme* $a_{23}=6$, *il y a 6 chaînes de longueur 5 reliant* B *à* C. *Comme* $a_{16}=0$, *il n'y a aucune chaîne de longueur 5 reliant* A *à* F.

Chapitre 8 – Suites et matrices

I – Suites de matrices colonnes

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

a) Expression du terme général

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

Théorème : La suite $(X_n)_{n\in\mathbb{N}}$ définie par $X_n = U_n - C$ vérifie $X_{n+1} = A\,X_n$ et donc pour $n \in \mathbb{N}$, $X_n = A^n X_0$, c'est-à-dire $U_n = A^n(U_0 - C) + C$.

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 $U_n = A^n U_0$ et si $\lim\limits_{n\to+\infty} A^n = L$, alors $\lim\limits_{n\to+\infty} U_n = L U_0$.

II – 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.

Remarque : Ce résultat se démontre par récurrence.

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.

III – Diagonalisation d'une matrice carrée

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 k l'ordre de A .
Soit $P(n)$ la propriété $A^n=PD^nP^{-1}$.
- Initialisation : Pour $n=0$, $A^0=I_k$ et $PD^0P^{-1}=PI_kP^{-1}=PP^{-1}=I_k$. $P(0)$ 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 $n\in\mathbb{N}$, $A^n=PD^nP^{-1}$

IV – Chaînes de Markov

a) Vocabulaire

Définitions :

- **Un *processus* est une suite (X_n) de variables aléatoires à valeurs dans un même ensemble E appelé *ensemble des états.* Les éléments de E sont appelés *états*.**
- **Pour tout état $i \in E$ et tout $n \in \mathbb{N}$, dire que le processus est dans l'état i à l'instant n signifie que l'évènement $\{X_n = i\}$ est réalisé.**

Définition d'une chaîne de Markov : Une chaîne de Markov sur un espace d'états E est un processus (X_n) tel que :

- **Pour tout état $i \in E$, l'évènement $\{X_{n+1} = i\}$ ne dépend que de l'état dans lequel était le processus à l'instant n (« le futur ne dépend que de l'instant présent »).**
- **La probabilité de passer de l'état i à l'état j ne dépend pas de l'instant n.**

Exemple : Dans un certain pays, s'il pleut un certain jour, alors il pleut également le lendemain avec une probabilité égale à 0,7. De plus, s'il ne pleut pas un certain jour alors il pleut le lendemain avec une probabilité égale à 0,2.
On choisit au hasard une journée. X_n est la variable aléatoire qui prend la valeur 1 s'il pleut après n jours et 2 sinon.
Comme le fait qu'il pleuve une journée ne dépend que du temps de la journée précédente et que la probabilité que le temps change ou non ne dépend pas du rang de la journée, on en déduit que la suite (X_n) est une chaîne de Markov à deux états 1 et 2.

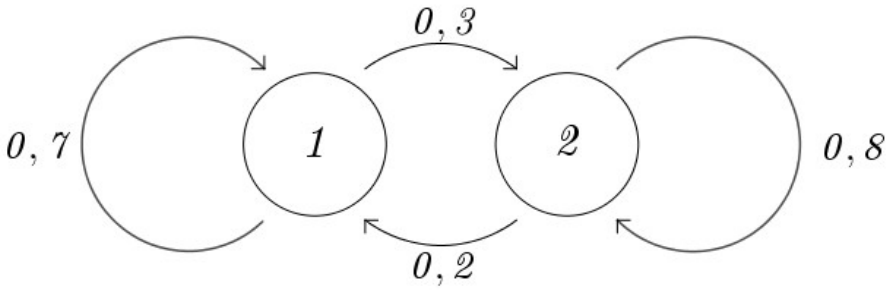
b) Graphe et matrice de transition d'une chaîne de Markov

Définitions :

- Un graphe *pondéré* est un graphe dans lequel chaque arête est affectée d'un nombre réel positif appelé *poids* de cette arête.
- Un graphe *probabiliste* est un graphe orienté pondéré par des réels appartenant à $[0;1]$ et dans lequel la somme des poids des arêtes issues de chaque sommet est égale à 1.

On associe à une chaîne de Markov le graphe dont les sommets sont les états et dont l'arrête orientée reliant l'état i à l'état j est pondérée par la probabilité de passer de l'état i à l'état j. Par construction, c'est un graphe probabiliste.

Exemple : Avec l'exemple précédent, le graphe associé est le suivant :



On associe à une chaîne de Markov dont k est le nombre d'états la matrice de transition $P=(p_{ij})_{\substack{1\leqslant i\leqslant k\\1\leqslant j\leqslant k}}$ telle que p_{ij} est la probabilité de passer de l'état i à j. On a donc $p_{ij}=P_{(X_n=i)}(X_{n+1}=j)$ pour tous $1\leqslant i\leqslant k$, $1\leqslant j\leqslant k$ et $n\in\mathbb{N}$.

Exemple : *Avec l'exemple précédent, on a* $P=\begin{pmatrix}0,7 & 0,3\\0,2 & 0,8\end{pmatrix}$.

Remarque : Les évènements $(X_n=j)$ avec $1\leqslant j\leqslant k$ formant une partition de l'univers Ω (y compris en les conditionnant par un évènement $(X_n=i)$), on en déduit que la somme des coefficients de chaque ligne de la matrice égale 1.

V – Distributions d'une chaîne de Markov

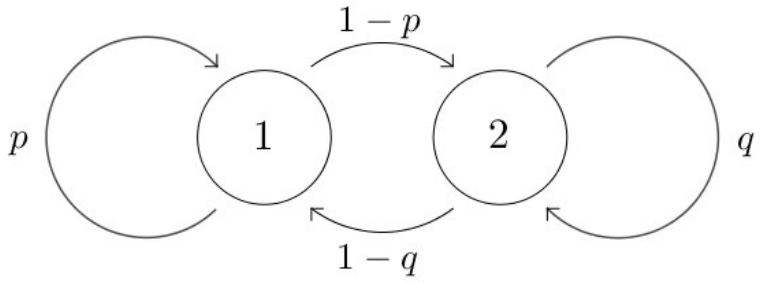
Dans ce paragraphe, (X_n) est une chaîne de Markov de matrice de transition P.

a) Distribution après plusieurs transitions

Propriété : Pour tous états i et j, et tout entier naturel $n\geqslant 1$, le coefficient en ligne i et colonne j de la matrice P^n est la probabilité de passer de l'état i à l'état j en n transitions.

Preuve par récurrence : On se place dans le cas d'une chaîne de Markov à deux états notés 1 et 2. Le cas général est analogue.

Soient p la probabilité de passer de l'état 1 à 1 et q celle de passer de 2 à 2. On a donc $0\leqslant p\leqslant 1$ et $0\leqslant q\leqslant 1$ et nécessairement, le graphe associé est le suivant :



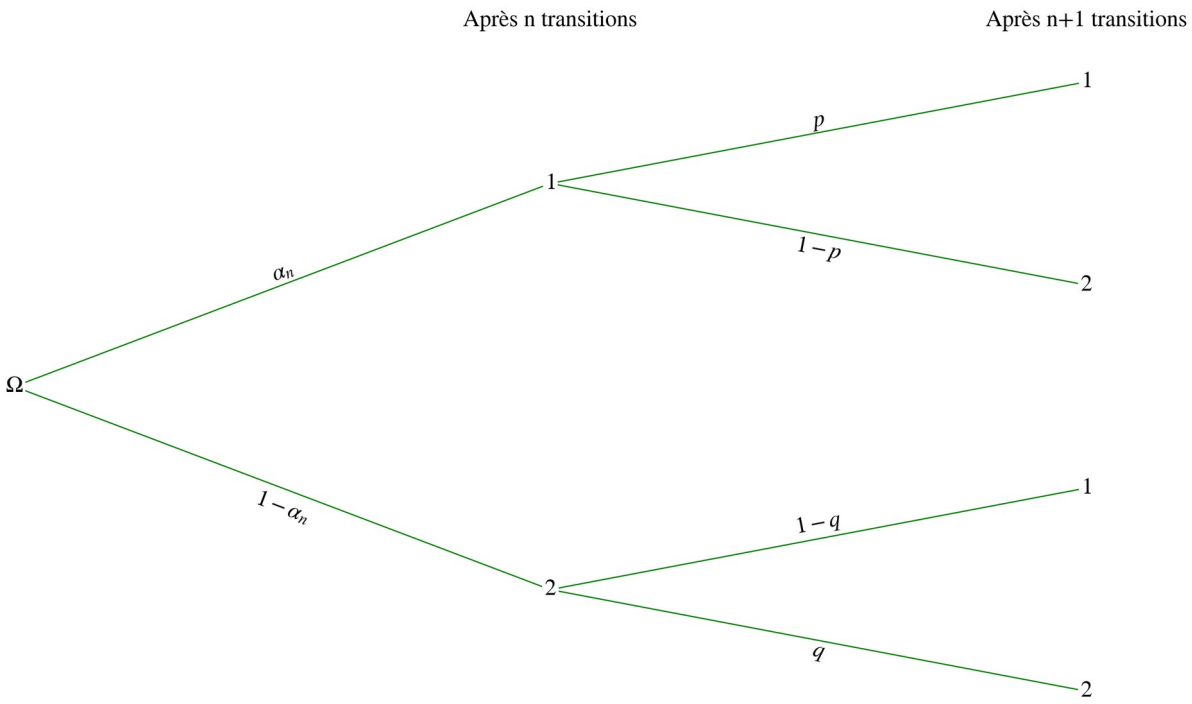
La matrice de transition associée est $P=\begin{pmatrix}p & 1-p\\1-q & q\end{pmatrix}$.

Pour tout entier $n\geqslant 1$, on note $Q(n)$ la propriété « Pour tous états i et j, le coefficient $(P^n)_{ij}$ est la probabilité de passer de l'état i à l'état j en n transitions ».

Initialisation : Par définition de la matrice P, le coefficient $(P^1)_{ij}$ est la probabilité de passer de l'état i à l'état j en une transition, donc $Q(1)$ est vraie.

Hérédité : On suppose que pour un entier $n \geqslant 1$, $Q(n)$ est vraie. On a donc $P^n = \begin{pmatrix} \alpha_n & 1-\alpha_n \\ 1-\beta_n & \beta_n \end{pmatrix} \Rightarrow$

$$P^{n+1} = P^n \times P = \begin{pmatrix} \alpha_n & 1-\alpha_n \\ 1-\beta_n & \beta_n \end{pmatrix} \times \begin{pmatrix} p & 1-p \\ 1-q & q \end{pmatrix} = \begin{pmatrix} \alpha_n p + (1-\alpha_n)(1-q) & \alpha_n(1-p) + (1-\alpha_n)q \\ (1-\beta_n)p + \beta_n(1-q) & (1-\beta_n)(1-p) + \beta_n q \end{pmatrix}.$$



Avec l'arbre ci-dessus et la formules des probabilités totales, on peut constater que pour tous états i et j, le coefficient $\left(P^{n+1}\right)_{ij}$ est la probabilité de passer de l'état i à l'état j en $n+1$ transitions, donc $Q(n+1)$ est vraie.

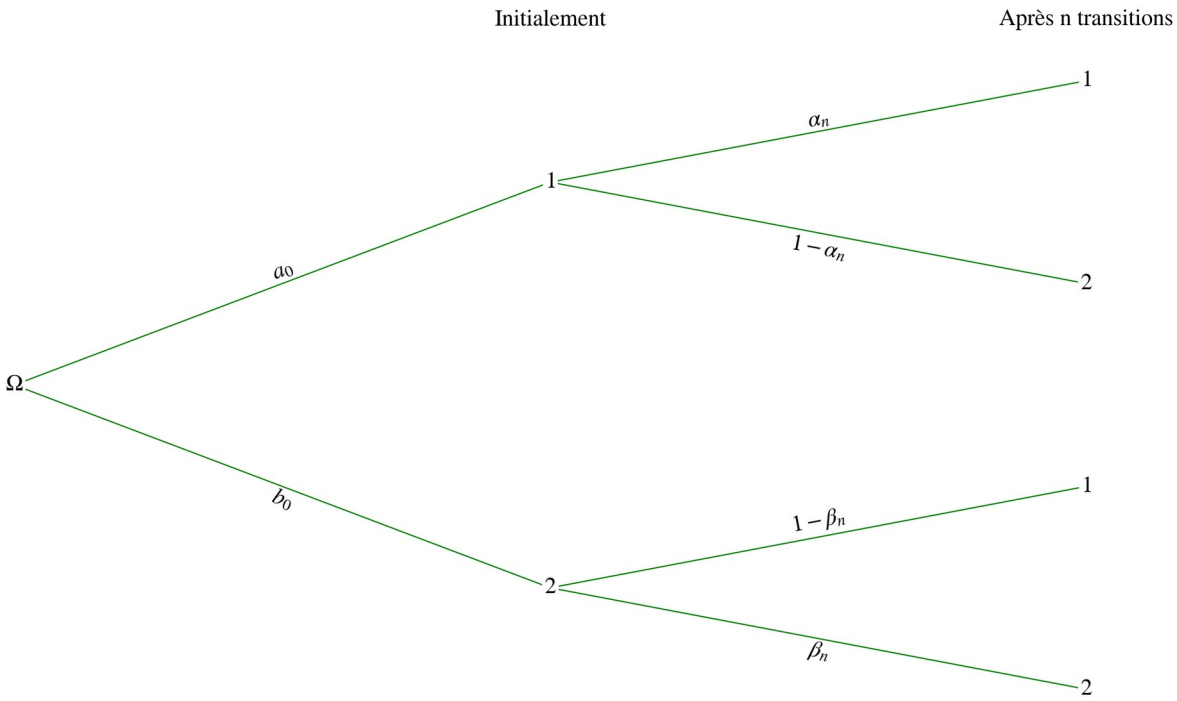
Conclusion : Pour tous états i et j et tout entier $n \geqslant 1$, le coefficient $\left(P^n\right)_{ij}$ est la probabilité de passer de l'état i à l'état j en n transitions.

Exemple : Avec l'exemple précédent, on a $P^5 = \begin{pmatrix} 0{,}41875 & 0{,}58125 \\ 0{,}3875 & 0{,}6125 \end{pmatrix}$. *On en déduit notamment que la probabilité de passer de l'état 2 à l'état 1 en 5 transitions (et donc d'une journée non pluvieuse à une journée pluvieuse cinq jours plus tard) est égale à 0,3875.*

Définition : La *distribution initiale*, notée π_0, est la loi de probabilité de la variable aléatoire X_0. La *distribution après n transitions*, notée π_n, est celle de la variable aléatoire X_n. Elles sont représentées par des matrices lignes.

Propriété : π_0 étant la distribution initiale d'une chaîne de Markov, alors pour tout $n \in \mathbb{N}$, la distribution π_n après n transitions vérifie $\pi_n = \pi_0 P^n$ et $\pi_{n+1} = \pi_n \times P$.

Preuve : Les propriétés sont évidentes pour $n=0$. Pour $n\geqslant 1$, on reprend les notations de la preuve précédente. Soit $\pi_n=\begin{pmatrix}a_n & b_n\end{pmatrix}$. Comme $P^n=\begin{pmatrix}\alpha_n & 1-\alpha_n\\ 1-\beta_n & \beta_n\end{pmatrix}$, on considère l'arbre ci-dessous.



On peut affirmer avec les probabilités totales que $\begin{cases}a_n=a_0\,\alpha_n+b_0(1-\beta_n)\\ b_n=a_0(1-\alpha_n)+b_0\beta_n\end{cases}$. Ainsi, pour tout $n\geqslant 1$, $\pi_n=P^n\pi_0$.

Donc, pour tout entier naturel n, $\pi_{n+1}=\pi_0\times P^{n+1}=\pi_0\times P^n\times P=\pi_n\times P$.

b) Distributions invariantes

Définition : Soit P la matrice de transition associée à une chaîne de Markov. π est une *distribution invariante* de la chaîne de Markov si et seulement si $\pi=\pi\times P$.

Exemple : Avec l'exemple précédent, on remarque que $\begin{pmatrix}0,4 & 0,6\end{pmatrix}\times P=\begin{pmatrix}0,4 & 0,6\end{pmatrix}\times\begin{pmatrix}0,7 & 0,3\\ 0,2 & 0,8\end{pmatrix}=\begin{pmatrix}0,4 & 0,6\end{pmatrix}$ *donc* $\pi=\begin{pmatrix}0,4 & 0,6\end{pmatrix}$ *est une distribution invariante de la chaîne de Markov. Ceci signifie que si un jour la probabilité de pluie est de 40 %, cette probabilité sera la même tous les jours suivants.*

Propriété admise : Soit P la matrice de transition associée à une chaîne de Markov de distribution initiale π_0.
S'il existe un entier naturel $k\geqslant 1$ tel que P^k ne comporte pas de zéro, alors la suite (π_n) converge vers une distribution π *invariante* et indépendante de π_0.
De plus, dans ce cas π est l'*unique* distribution invariante de cette chaîne de Markov.

Exemple : *Avec l'exemple précédent, comme* $P=\begin{pmatrix}0,7 & 0,3\\0,2 & 0,8\end{pmatrix}$ *ne comporte pas de zéro, alors la suite* (π_n) *converge vers l'unique distribution invariante de cette chaîne. On utilise deux méthodes.*

- ***Première méthode : Avec la relation*** $\pi=\pi\times P$

  $\pi=(x \quad y)$ *avec* $x+y=1$ *est invariante signifie que* $\pi P=\pi$ *. On a donc :*

  $(x \quad y)\begin{pmatrix}0,7 & 0,3\\0,2 & 0,8\end{pmatrix}=(x \quad y)\Leftrightarrow\begin{cases}0,7x+0,2y=x\\0,3x+0,8y=y\end{cases}\Leftrightarrow\begin{cases}-0,3x+0,2y=0\\0,3x-0,2y=0\end{cases}\Leftrightarrow -0,3x+0,2y=0$ *car les deux équations sont équivalentes. Or* $x+y=1$ *donc on résout* $\begin{cases}-0,3x+0,2y=0\\x+y=1\end{cases}\Leftrightarrow$

  $\begin{cases}x=\frac{2}{3}y\\\frac{2}{3}y+y=1\end{cases}\Leftrightarrow\begin{cases}x=0,4\\y=0,6\end{cases}$ *. On a donc* $\pi=(0,4 \quad 0,6)$ *.*

- ***Deuxième méthode : Avec l'étude de la distribution*** π_n

  On note $\pi_n=(a_n \quad b_n)$ *avec* $a_n+b_n=1$ *la distribution après* n *transitions.*

  On a donc pour tout $n\in\mathbb{N}$ $a_{n+1}=0,7a_n+0,2b_n\Leftrightarrow a_{n+1}=0,7a_n+0,2(1-a_n)\Leftrightarrow$ $a_{n+1}=0,5a_n+0,2$ *. On étudie ensuite cette suite arithmético-géométrique (détermination du point fixe, utilisation d'une suite auxiliaire géométrique et justification de la convergence de celle-ci) et on obtient que* $\lim\limits_{n\to+\infty} a_n=0,4$ *donc* $\pi=(0,4 \quad 0,6)$ *.*