Cours arithmétique et groupes.
Licence première année

Rejeb Hadiji, Stéphane Jaffard, Jacques Printems, Stéphane Seuret

Année 2010-2011

Table des matières

Chapitre 1

Les ensembles de nombres

1.1 Les ensembles de nombres réels

1.1.1 L'ensemble $\mathbb{N}$

Naïvement, l'ensemble $\mathbb{N}$ des entiers positifs est l'ensemble des nombres

$$\{0, 1, 2, 3, \ldots\}.$$

Il est muni d'une relation d'ordre total notée $\leq$; cela signifie que, si a, b et c sont trois entiers quelconques, on a

$$a \leq b \quad \text{et} \quad b \leq c \quad \Longrightarrow a \leq c,$$

$$a \leq a$$

$$a \leq b \quad \text{et} \quad b \leq a \quad \Longrightarrow a = b,$$

et on a toujours $a \leq b$ ou $b \leq a$ (Nous reviendrons sur les relations d'ordre dans le chapitre 3).

De façon plus rigoureuse, on peut démontrer que, à une bijection respectant l'ordre près, il existe un seul ensemble vérifiant les quatre axiomes suivants :

Axiome 1 L'ensemble $\mathbb{N}$ est totalement ordonné, c'est-à-dire muni d'une relation d'ordre totale.

Axiome 2 Toute partie non vide de $\mathbb{N}$ a un plus petit élément.
(Ceci veut dire : Pour tout $x, y \in \mathbb{N}$, $x \leq y$ ou $y \leq x$, et : pour toute partie $A \subset \mathbb{N}, \exists x \in A$ $\forall y \in A : x \leq y$.)

Axiome 3 L'ensemble $\mathbb{N}$ n'a pas de plus grand élément.

Axiome 4 Tout élément $\mathbb{N}$ distinct du plus petit élément de $\mathbb{N}$ possède un "prédécesseur".

Rappelons qu'un prédécesseur de x est un entier $y < x$ tel que $\forall z \in \mathbb{N}$, tel que $y \leq z \leq x$, on a $z = x$ ou $z = y$; on le notera $x - 1$ (on montrera en exercice qu'un prédécesseur est nécessairement unique).

1.1.2 L'ensemble $\mathbb{Z}$

Nous utiliserons aussi $\mathbb{Z}$, l'ensemble des entiers relatifs (positifs ou négatifs). On verra comment on définit -1 comme l'inverse de 1 pour l'addition.

1.1.3 Nombres rationnels $\mathbb{Q}$

$\mathbb{Q}$ est l'ensemble des nombres fractionaires, ou rationnels ; ils s'écrivent sous la forme $r = \frac{p}{q}$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{N} \setminus \{0\}$.

On convient de la règle $\frac{a}{b} = \frac{a'}{b'}$ si $ab' = a'b$, et on identifie un entier relatif n avec la fraction $\frac{n}{1}$. L'addition et la multiplication sont définies par $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ et $\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$. $\mathbb{Q}$ est muni d'une relation d'ordre $\leq$ définie apr $\frac{a}{b} \leq \frac{a'}{b'}$ si $ab' \leq ba'$.

1.1.4 L'ensemble des nombres réels $\mathbb{R}$

Ce sont des nombres qui ne sont pas rationnels. Leur existence (et leurs propriétés) est admise.

Par exemple $\sqrt{2}$ est un nombre réel non rationnel.

1.2 Les nombres complexes

L'idée des nombres complexes est due aux mathématiciens italiens de l'université de Bologne : Dal Ferro, Tartaglia, Cardan. Il sont imaginé, vers 1550, une "racine carrée de -1" pour résoudre les équations du 3^e degré.
En 1777, Euler note i le nombre vérifiant $i^2 = -1$.

Définition 1.2.1 *On appelle* ***ensemble des nombres complexes*** *et on note $\mathbb{C}$ l'ensemble $\mathbb{R}^2$ muni des deux lois internes, notées $+$ et $\times$ (souvent on omet $\times$) définies par :*

$$\begin{array}{l} \forall (x,y) \in \mathbb{R}^2, \quad \forall (x',y') \in \mathbb{R}^2, \quad (x,y) + (x',y') = (x+x', y+y') \\ \forall (x,y) \in \mathbb{R}^2, \quad \forall (x',y') \in \mathbb{R}^2, \quad (x,y) \times (x',y') = (xx' - yy', xy' + x'y) \end{array}$$

Les éléments de $\mathbb{C}$ sont appelés les nombres complexes ou les complexes.

Remarque 1.2.2 *On a :* $\left\{ \begin{array}{l} \forall (x,x') \in \mathbb{R}^2, \quad (x,0) + (x',0) = (x+x', 0) \\ \forall (x,x') \in \mathbb{R}^2, \quad (x,0) \times (x',0) = (xx', 0) \end{array} \right.$.
On peut identifier le complexe $(x,0)$ au réel x, ce qui revient à considérer $\mathbb{R}$ comme une partie de $\mathbb{C}$. Le nombre complexe $(x,0)$ sera donc noté x.
Une fois cette identification effectuée, ces deux lois prolongent à $\mathbb{C}$ l'addition et la multiplication définies sur $\mathbb{R}$.

Notations :

Le nombre complexe $(0,1)$ est tel que $(0,1)^2 = (-1,0)$; nous le noterons i. Le calcul précédent montre que $i^2 = -1$. (De cette propriété "déconcertante" est issue le nom de nombre imaginaire donné a i).
On utilise souvent la lettre z pour désigner un nombre complexe. On a : $(x,y) = (x,0) + (0,y) = (x,0) + (0,1)(y,0)$.
L'écriture $z = (x,y)$ devient donc $z = x + iy$.

Remarque 1.2.3

1. *Grâce à l'identification précédente, le calcul dans $\mathbb{C}$ est identique à celui dans $\mathbb{R}$ avec la convention $i^2 = -1$. Plus précisément, on a :*

$$\begin{array}{rcl} (x+iy) + (x'+iy') & = & (x+x') + i(y+y') \\ (x+iy) \times (x'+iy') & = & (xx' - yy') + i(x'y + xy') \end{array}$$

2. *Pour tout $(x,x',y,y') \in \mathbb{R}^4$, on a $x + iy = x' + iy' \Leftrightarrow \left\{ \begin{array}{rcl} x & = & x' \\ y & = & y' \end{array} \right.$*

1.2.1 Conjugaison - partie réelle - partie imaginaire

Définition 1.2.4 *Soit $z = x + iy$. Le nombre réel x est appelé la* **partie réelle** *du nombre complexe z et on écrit $x = \mathcal{R}e\,(z)$. Si $\mathcal{R}e\,(z) = 0$ on dit que z est un* **nombre imaginaire pur**. *Le nombre réel y est la* **partie imaginaire** *du nombre complexe z et on écrit $y = \mathcal{I}m\,(z)$.*

On appelle **conjugué de** *z le nombre complexe $x - iy$, noté $\overline{z}$.*

On dit que les nombres complexes z et z' sont conjugués si $\overline{z}' = z$.

Proposition 1.2.5 *On a les propriétés élémentaires suivantes :*

1. $\forall (z, z') \in \mathbb{C}^2 \;\; \mathcal{R}e\,(z + z') = \mathcal{R}e\,(z) + \mathcal{R}e\,(z')' \quad et \quad \mathcal{I}m\,(z + z') = \mathcal{I}m\,(z) + \mathcal{I}m\,(z')$.
2. $\forall z \in \mathbb{C}, \;\; \forall \lambda \in \mathbb{R}, \;\; \mathcal{R}e\,(\lambda z) = \lambda \mathcal{R}e\,(z) \quad et \quad \mathcal{I}m\,(\lambda z) = \lambda \mathcal{I}m\,(z)$.
3. $\forall z \in \mathbb{C}, \;\; \mathcal{R}e\,(z) = \dfrac{z + \overline{z}}{2} \quad et \quad \mathcal{I}m\,(z) = \dfrac{z - \overline{z}}{2i}$.
4. $\forall z \in \mathbb{C}, \;\; z \in \mathbb{R} \Leftrightarrow z = \overline{z} \quad et \quad z \in i\mathbb{R} \Leftrightarrow z = -\overline{z}$.
5. $\forall z \in \mathbb{C}, \;\; \overline{\overline{z}} = z$.
6. $\forall (z, z') \in \mathbb{C}^2 \;\; \overline{z + z'} = \overline{z} + \overline{z}'$.
7. $\forall (z, z') \in \mathbb{C}^2 \;\; \overline{zz'} = \overline{z} \cdot \overline{z}'$
8. $\forall z \in \mathbb{C}, \;\; \forall \lambda \in \mathbb{R}, \;\; \overline{\lambda z} = \lambda \overline{z}$.
9. $\forall z \in \mathbb{C}, \;\; \forall z' \in \mathbb{C}^*, \;\; \overline{\left(\dfrac{1}{z'}\right)} = \dfrac{1}{\overline{z}'} \quad et \quad \overline{\left(\dfrac{z}{z'}\right)} = \dfrac{\overline{z}}{\overline{z}'}$.

On pourra démontrer ces propriétés en exercice.

Remarque 1.2.6 *En général $\mathcal{R}e\,(zz') \neq \mathcal{R}e\,(z) \cdot \mathcal{R}e\,(z') \qquad et \qquad \mathcal{I}m\,(zz') \neq \mathcal{I}m\,(z) \cdot \mathcal{I}m\,(z')$.*

1.2.2 Module-Arguments-Forme trigonométrique

Définition 1.2.7 *Soit $x + iy$ la forme algébrique du nombre complexe z.*
On appelle module de z le nombre réel positif $\sqrt{x^2 + y^2}$ que l'on note $|z|$.

Remarque 1.2.8 *Le module d'un nombre complexe est un prolongement de la notion de valeur absolue d'un nombre réel.*

Proposition 1.2.9 *On a les propriétés suivantes :*

1. $\forall z \in \mathbb{C}, \;\; |z| = 0 \quad si\ et\ seulement\ si \quad z = 0$.
2. $\forall z \in \mathbb{C}, \;\; |\overline{z}| = |z|$.
3. $\forall z \in \mathbb{C}, \;\; |z|^2 = z\overline{z} = \overline{z}z$. *En particulier pour tout $z \in \mathbb{C}^*$.*
   On a $|z| = 1 \Leftrightarrow \overline{z} = z^{-1}$ et pour tout $z \neq 0$, $z^{-1} = \dfrac{\overline{z}}{|z|^2}$.
4. $\forall (z, z') \in \mathbb{C}^2, \;\; |zz'| = |z||z'|$.
5. $\forall (z, z') \in \mathbb{C} \times \mathbb{C}^* \;\; \left|\dfrac{1}{z'}\right| = \dfrac{1}{|z'|} \quad et \quad \left|\dfrac{z}{z'}\right| = \dfrac{|z|}{|z'|}$.
6. $\forall z \in \mathbb{C}, \;\; |\mathcal{R}e\,(z)| \leq |z| \quad et \quad |\mathcal{I}m\,(z)| \leq |z|$.
7. $\forall (z, z') \in \mathbb{C}^2, \;\; |z + z'|^2 = |z|^2 + |z'|^2 + 2\mathcal{R}e\,(z\overline{z}')$.
8. $\forall (z, z') \in \mathbb{C}^2, \;\; |z + z'| \leq |z| + |z'|$.
9. $\forall (z, z') \in \mathbb{C}^2, \;\; ||z| - |z'|| \leq |z - z'|$.

Preuve :

- 1., 2., 3. et 6. découlent immédiatement de la définition du module.
- Pour prouver 4., on écrit $|zz'|^2 = zz'\overline{zz'} = zz'\overline{z}\overline{z}' = |z|^2|z'|^2$.
- Prouvons 5. Si $z' \neq 0$, le choix de $z = \frac{1}{z'}$ dans 4. donne $1 = \left|\frac{1}{z'}\right| |z'|$ et $\left|\frac{1}{z'}\right| = \frac{1}{|z'|}$.
  On a alors $\left|\frac{z}{z'}\right| = \left|z \times \frac{1}{z'}\right| = |z| \times \left|\frac{1}{z'}\right| = |z| \times \frac{1}{|z'|} = \frac{|z|}{|z'|}$.
- Montrons 7. On a $|z+z'|^2 = (z+z')(\overline{z+z'}) = (z+z')(\overline{z}+\overline{z}') = z\overline{z} + z\overline{z}' + z'\overline{z} + z'\overline{z}' = |z|^2 + |z'|^2 + (z\overline{z}' + \overline{z\overline{z}'})$. Compte tenu de la propriété 1. sur les conjugués, on a :

$$|z+z'|^2 = |z|^2 + |z'|^2 + 2\mathcal{R}e\,(z\overline{z}')$$

- D'après 7., on a $|z+z'|^2 \leq |z|^2 + |z'|^2 + 2|z\overline{z}'|$.
  On obtient $|z\overline{z}'| = |z| \cdot |\overline{z}'| = |z| \cdot |z'|$ en utilisant successivement (2) et (4).
  On a donc $|z+z'|^2 \leq |z|^2 + |z'|^2 + 2|z||z'|$ ou $|z+z'|^2 \leq (|z| + |z'|)^2$.
  Comme $|z+z'| \geq 0$ et $|z| + |z'| \geq 0$ on obtient $|z+z'| \leq |z| + |z'|$.
- Enfin, montrer 9. revient à montrer que $|z| \leq |z'| + |z-z'|$ et $|z'| \leq |z| + |z-z'|$.
  Comme $z = z' + (-z')$ d'après 8. on a $|z| \leq |z'| + |z-z'|$.
  En permutant dans ce qui précède z et z', on obtient l'ingalit complmentaire $|z'| \leq |z| + |z'-z|$.
  Comme $|z'-z| = |-(z-z')| = |-1||z-z'| = |z-z'|$, cela donne $|z'| \leq |z| + |z-z'|$.

■

Remarque : Le module est une norme sur $\mathbb{C}$, c'est-à -dire vérifie les trois propriétés :

$$\begin{aligned} \forall z \in \mathbb{C}, \quad & |z| = 0 \Rightarrow z = 0, \\ \forall z \in \mathbb{C},\ \forall \lambda \in \mathbb{R}, \quad & |\lambda z| = |\lambda||z| \\ \forall z, z' \in \mathbb{C}, \quad & |z+z'| \leq |z| + |z'|. \end{aligned}$$

Définition 1.2.10 (et Proposition) *Soit z un nombre complexe non nul. Il existe un unique réel $\theta \in [0, 2\pi[$ tel que*

$$\frac{z}{|z|} = \cos\theta + i\sin\theta; \tag{1.1}$$

ce réel s'appelle l'argument principal de z. L'ensemble des réels vérifiant (1.1) est $\{\theta + 2k\pi,\ k \in \mathbb{Z}\}$. Un tel θ s'appelle un argument de z, et est noté $\arg z$.

Preuve : Comme $\frac{z}{|z|}$ est un nombre complexe de module 1, on a

$$\frac{z}{|z|} = x + iy \text{ avec } x^2 + y^2 = 1.$$

Il existe donc un unique réel θ de $[0, 2\pi[$ tel que $x = \cos\theta \quad$ et $\quad y = \sin\theta$.
Soit maintenant $\theta' \in \mathbb{R}$ tel que $\cos\theta' + i\sin\theta' = \frac{z}{|z|}$. Par identification des parties réelles et imaginaires, $\cos\theta' + i\sin\theta' = \cos\theta + i\sin\theta$ équivaut à $\cos\theta' = \cos\theta$ et $\sin\theta' = \sin\theta$ i.e. $\theta' - \theta \in 2\pi\mathbb{Z}$. ■

Remarque 1.2.11 *Dans certains ouvrages, l'argument principal de z est défini comme l'unique réel de $]-\pi, \pi]$ vérifiant 1.1.*

On rappelle les formules trigonométriques suivantes (que l'on pourra redémontrer à titre d'exercice) :

$$\forall(\theta,\theta')\in\mathbb{R}^2,\quad \cos(\theta+\theta')=\cos\theta\cos\theta'-\sin\theta\sin\theta'$$
$$\forall(\theta,\theta')\in\mathbb{R}^2,\quad \sin(\theta+\theta')=\sin\theta\cos\theta'+\cos\theta\sin\theta'$$

(la deuxième se déduit de la première en changeant θ' en $\theta'+\frac{\pi}{2}$).
Pour tout réel θ, on note $e^{i\theta}=\cos\theta+i\sin\theta$. Cette notation est justifiée pour la raison suivante.

Proposition 1.2.12 *On a $e^{i\theta}e^{i\theta'}=e^{i(\theta+\theta')}$.*

Preuve : A l'aide des formules trigonométriques on obtient

$$e^{i\theta}e^{i\theta'}=(\cos\theta+i\sin\theta)(\cos\theta'+i\sin\theta')$$

$$=\big[(\cos\theta\cos\theta'-\sin\theta\sin\theta')+i(\cos\theta\sin\theta'+\sin\theta\sin\theta')\big]=(\cos(\theta+\theta')+i\sin(\theta+\theta')).$$

L'exponentielle d'un nombre imaginaire pur a donc la même propriété que l'exponentielle d'un nombre réel. Ceci permet de définir l'eponentielle d'un nombre complexe quelconque : Si $z=x+iy$, alors

$$e^z=e^xe^{iy}=e^x(\cos y+i\sin y).$$

On a alors : $\forall z,z'$, $e^{z+z'}=e^ze^{z'}$. ∎

Définition 1.2.13 *Soit z un nombre complexe non nul de module r et d'argument θ. On a $z=re^{i\theta}$. On dit que $re^{i\theta}$ est la forme trigonométrique de z.*

Proposition 1.2.14 *1. Pour tout complexe z non nul, on a l'équivalence suivante :*

$$re^{i\theta}=re^{i\theta'}\Leftrightarrow(r=r'\quad et\quad((\exists k\in\mathbb{Z}),\ \theta'=\theta+2k\pi)).$$

2. 0 peut s'écrire $re^{i\theta}$ avec $r=0$ et θ arbitraire. (l'argument de 0 n'est pas défini).

3. Pour tout $\theta\in\mathbb{R}$, $e^{i(\theta+\pi)}=-e^{i\theta}$ et $e^{i\left(\theta+\frac{\pi}{2}\right)}=ie^{i\theta}$.

Exemples de formes trigonométriques :

$$e^{i0}=1,\quad e^{i\pi}=-1,\quad e^{i\frac{\pi}{2}}=i,\quad e^{i\frac{3\pi}{2}}=-i$$

$$e^{i\frac{\pi}{6}}=\frac{\sqrt{3}}{2}+\frac{i}{2},\quad e^{i\frac{\pi}{4}}=\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2},\quad e^{i\frac{\pi}{3}}=\frac{1}{2}+i\frac{\sqrt{3}}{2}.$$

1.2.3 Interprétation géométrique

On appelle plan complexe un plan P rapporté à un repère orthonormé direct $(0,\vec{i},\vec{j})$. L'appellation

$$\begin{array}{rccc}\varphi: & \mathbb{C} & \longrightarrow & P\\ & z=x+iy & \longmapsto & M(x,y).\end{array}$$

est une bijection. Elle permet d'identifier $\mathbb{C}$ et P.
Pour tout $z\in\mathbb{C}$, M s'appelle l'image de z dans P ; pour tout $M\in P$, $z=\varphi^{-1}(M)$ s'appelle l'affixe de M.
On note $M(z)$ pour exprimer que z est l'affixe de M. Les axes $(O,\vec{i})$ et $(O,\vec{j})$ sont appelés respectivement axe des réels et axe des imaginaires. On voit alors que :

– $|z|$ représente la distance du point M à l'origine O.

$$|z| = \sqrt{x^2+y^2} = \|\overrightarrow{OM}\| = OM$$

– Si $z \neq 0$, l'argument de z est une mesure (en radians) de l'angle orienté $(\vec{i}, \overrightarrow{OM})$.

$$mes(\vec{i}, \overrightarrow{OM}) = \arg z + 2k\pi \quad \text{avec} \quad k \in \mathbb{Z}$$

$M(z)$ et $M(\overline{z})$ sont symétriques par rapport à l'axe des réels.

Interprétation de l'addition dans $\mathbb{C}$

Soient $(z, z') \in \mathbb{C}^2$, $M(z)$, $M(z')$, $S(z+z')$ et $D(z'-z)$. On a :

$$\overrightarrow{OS} = \overrightarrow{OM} + \overrightarrow{OM}'$$

$$\overrightarrow{OD} = \overrightarrow{OM}' - \overrightarrow{OM} = \overrightarrow{MM}$$

En particulier $MM' = \|\overrightarrow{MM}\| = \sqrt{(x'-x)^2+(y'-y)^2} = |z'-z|$.

La proposition suivante est une application des formules de trigonometrie (elle est fort utilisée en physique).

Proposition 1.2.15 *Soient a et b deux réels. Il existe un réel φ tel que :*

$$\forall x \in \mathbb{R}, \quad a\cos x + b\sin x = \sqrt{a^2+b^2}\cos(x-\varphi) \tag{1.2}$$

Si de plus $(a,b) \neq (0,0)$ on peut choisir pour φ l'unique réel de $[0, 2\pi[$ tel que $\cos\varphi = \frac{a}{\sqrt{a^2+b^2}}$ et $\sin\varphi = \frac{b}{\sqrt{a^2+b^2}}$. ($\varphi$ est l'argument principal de $a+ib$).

Preuve :

– Le cas $(a,b) = (0,0)$ est trivial.

– Supposons $(a,b) \neq (0,0)$.
Comme $\cos(x-\varphi) = \cos x\cos\varphi + \sin x\sin\varphi$, on déduit que la formule (1.2) est vérifiée si et seulement si

$$a = \sqrt{a^2+b^2}\cos\varphi \quad \text{et} \quad b = \sqrt{a^2+b^2}\sin\varphi$$

Comme $a+ib = \sqrt{a^2+b^2}\left(\frac{a}{\sqrt{a^2+b^2}} + i\frac{b}{\sqrt{a^2+b^2}}\right)$, il existe un unique $\varphi \in [0, 2\pi[$ tel que $\frac{a}{\sqrt{a^2+b^2}} = \cos\varphi$ et $\frac{b}{\sqrt{a^2+b^2}} = \sin\varphi$.

■

Les formules trigonométriques von également permettre de montrer des propriétés algébriques de l'argument.

Proposition 1.2.16 *1. Soient (θ, θ') un couple de réels positifs. On a :*

$$(re^{i\theta})(r'e^{i\theta'}) = rr'e^{i(\theta+\theta')}$$

2. Si z et z' sont deux nombres complexes non nuls alors il existe $k \in \mathbb{Z}$ tel que

$$\arg zz' = \arg z + \arg z' + 2k\pi \quad \textit{avec} \quad k \in \mathbb{Z}.$$

3. Si z est un nombre complexe nul alors on a :

$$\arg z^{-1} = -\arg z + 2k\pi \quad \textit{avec} \quad k \in \mathbb{Z}.$$

Si de plus $r \neq 0$, on a pour tout $n \in \mathbb{Z}$ $\quad (re^{\prime\theta})^n = r^n e^{in\theta}$.

Preuve : Le premier point est une conséquence immédiate de la proposition 1.2.12. Le second s'en déduit.

Reste le troisième, que l'on démontre par récurrence sur n : $\forall n \in \mathbb{N}$, montrons que $(re^{i\theta})^n = r^n e^{in\theta}$.

Si $n = 0$ ou $n = 1$ l'égalité ci-dessus est immédiate.
Soit $n \geq 1$ supposons que $(re^{i\theta})^1 = r^n e^{in\theta}$ et montrons que $(re^{i\theta})^{n+1} = r^{n+1}e^{i(n+1)\theta}$.
On a $(re^{i\theta})^{n+1} = (re^{i\theta})^n(re^{i\theta}) = (r^n e^{in\theta})re^{i\theta}$.
D'après ce qui précède $(r^n e^{in\theta})re^{i\theta} = r^{n+1}e^{i(n+1)\theta}$.
On a bien $(re^{i\theta})^{n+1} = r^{n+1}e^{i(n+1)\theta}$.

On a montré que $\forall n \in \mathbb{N}, \quad (re^{i\theta})^n = r^n e^{in\theta}$.

Il manque les entiers négatifs. Soit $n \in \mathbb{N}^*$, on a $(re^{i\theta})^{-n} = \frac{1}{(re^{i\theta})^n} = \frac{1}{r^n e^{in\theta}}$.
D'après les propriétés du module et de l'argument de l'inverse d'un nombre complexe, on a $\frac{1}{r^n e^{in\theta}} = r^{-n}e^{-in\theta}$ et $(re^{i\theta})^n = r^{-n}e^{-in\theta}$. On a le résultat. ■

En donnant à r la valeur 1 dans la dernière égalité de la proposition précédente, on obtient la formule de Moivre.

Formule de Moivre :

$$\forall n \in \mathbb{Z}, \quad \forall \theta \in \mathbb{R} \quad (\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta.$$

En écrivant $e^{i\theta} = \cos\theta + i\sin\theta$, $e^{i\theta} = \cos\theta - i\sin\theta$ et en faisant la demi-somme et la demi-différence de ces expressions, on obtient les formules d'Euler.

Formule d'Euler :

$$\forall \theta \in \mathbb{R}, \quad \cos\theta = \frac{e^{i\theta} + e^{-i\theta}}{2} \quad \text{et} \quad \sin\theta = \frac{e^{i\theta} - e^{-i\theta}}{2i}$$

Applications :
La formule de Moivre permet de calculer $\cos nx$, $\sin nx$ avec $n \in \mathbb{N}^*$ en fonction de $\cos x$ et $\sin x$.
Les formules d'Euler permettent de linéariser des expressions du type $\cos^m x \ \sin^n x$ avec $(m, n) \in \mathbb{N}^2$ i.e. de les transformer en sommes de termes e la forme $a\cos kx$ et $b\sin kx$ avec $k \in \mathbb{N}$ et $(a, b) \in \mathbb{R}^2$.

Interprétation géométrique :
- Pour tout réel r non nul, l'image de rz se déduit de M par l'homothétie de centre O de rapport r.
- Soit M' l'image de $z' = e^{i\varphi}z$ avec φ réel donné.
  Comme $z = |z|e^{i\theta}$ on a $z' = |z|e^{i(\theta+\varphi)}$.
  $\theta+\varphi$ est une mesure (en radians) de l'angle orienté $(\vec{i}, \overrightarrow{OM'})$. D'après la relation de Chasles $\theta + \varphi - \theta$ est une mesure de l'angle orienté $(\overrightarrow{OM}, \overrightarrow{OM'})$. Par ailleurs $OM' = OM$. Donc, par définition, M' est l'image de M par la rotation de centre O et d'angle φ.

1.3 Retour sur les entiers naturels $\mathbb{N}$

On rappelle qu'à une bijection respectant l'ordre près, il existe un seul ensemble vérifiant les quatre axiomes suivants :

Axiome 1 L'ensemble $\mathbb{N}$ est totalement ordonné, c'est-à-dire muni d'une relation d'ordre totale.

Axiome 2 Toute partie non vide de $\mathbb{N}$ a un plus petit élément.
(Ceci veut dire : Pour tout $x, y \in \mathbb{N}$, $x \leq y$ ou $y \leq x$, et : pour toute partie $A \subset \mathbb{N}, \exists x \in A$ $\forall y \in A : x \leq y$.)

Axiome 3 L'ensemble $\mathbb{N}$ n'a pas de plus grand élément.

Axiome 4 Tout élément $\mathbb{N}$ distinct du plus petit élément de $\mathbb{N}$ possède un "prédécesseur".

1.3.1 Le Principe de récurrence

Soit $f(n)$ une propriété dépendant de n.

Théorème 1.3.1 *S'il existe un entier n_0 tel que $f(n_0)$ est vraie et si pour tout entier n, $n \geq n_0$, $f(n)$ entraîne $f(n+1)$ alors pour tout entier n, $n \geq n_0$, $f(n)$ est vraie.*
Soit en utilisant les quantificateurs :

$$[\exists n_0 \in \mathbb{N},\ f(n_0)] \text{ et } [\forall n \in \mathbb{N},\ n \geq n_0,\ (f(n) \Rightarrow f(n+1))] \Rightarrow [\forall n \in \mathbb{N},\ n \geq n_0,\ f(n)].$$

Preuve : On va effectuer un raisonnement par l'absurde : notons

$$A = \{n \geq n_0 : \quad f(n) \quad \text{est faux}\},$$

et supposons A non vide.
D'après l'axiome 2, A a un plus petit élément que nous noterons n_1. On a donc $n_1 - 1 \notin A$ et, de plus, $n_1 > n_0$ car, par hypothèse, $f(n_0)$ est vrai ; on a donc $n_1 - 1 \geq n_0$. Mais $n_1 - 1 \notin A$ signifie $f(n_1 - 1)$ vrai, donc, par hypothèse sur f, $f(n_1)$ vrai ; d'où une contradiction avec le fait que $n_1 \in A$. Donc A est vide. ■

Exemple : On va montrer que $\forall n \in \mathbb{N}^* \sum_{p=1}^{n} p^2 = \frac{n(n+1)(2n+1)}{6}$.
On note $f(n) : \sum_{p=1}^{n} p^2 = \frac{n(n+1)(2n+1)}{6}$.

1. Pour $n = 1$, $\frac{1(1+1)(2+1)}{6} = 1 = 1^2$ d'où $f(1)$ est vraie.

2. On suppose $f(n)$ vrai. Alors

$$\begin{aligned} \sum_{p=1}^{n} p^2 + (n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \frac{n+1}{6}(2n^2 + 7n + 6) = \frac{(n+1)(n+1+1)(2(n+1)+1)}{6}. \end{aligned}$$

Soit $(\forall n \in \mathbb{N}^*,\ f(n) \Rightarrow f(n+1))$ d'où le résultat.

1.3.2 La division euclidienne

Théorème 1.3.2 *Soient $a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\}$. Alors il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que*

$$a = bq + r \ \text{ où } 0 \leq r \leq |b| - 1.$$

q s'appelle le quotient de la division euclidienne de a par b, r s'appelle le reste de la division euclidienne de a par b. Cette opération s'appelle la division euclidienne de a par b.

Preuve : 1. Nous montrons d'abord l'existence du couple (q, r).

• Supposons $b \geq 1$ et définissons $A := \{a - bk, k \in \mathbb{Z}\} \cap \mathbb{N}$, alors $A \neq \emptyset$ (on peut prendre par exemple $k = -|a|$). On note donc $r := \min A$ et q tel que $a - bq = r$. Montrons que $r < b$.

Raisonnons par l'absurde : Si $r \geq b$, alors $0 \leq r - b = a - bq - b = a - (q+1)b$, donc $r - b \in A$ et $r - b < r$, contradiction avec la minimalité de r. On a par ailleurs $r \geq 0$ par hypothèse car $A \subset \mathbb{N}$.

• Si $b \leq -1$, nous appliquons le résultat précédent à a et $|b|$: $a = |b|q + r$, donc $a = b(-q) + r$.

2. Pour l'unicité, supposons que $a = bq + r = bq' + r'$ et $0 \leq r, r' \leq |b| - 1$. Alors $b(q - q') = r - r'$, donc $|b||q - q'| = |r' - r|$. Or, $|r' - r| \leq |b| - 1$, donc $|q - q'| = 0$, donc $q = q'$ et $r = r'$. ■

Chapitre 2

Groupes, corps, anneaux

2.1 Introduction

La formalisation des structures algébriques (groupes, anneaux, corps, espaces vectoriels) est relativement récente ; elle n'apparaît qu'en début du XIX siècle, mais l'idée est présente partout dans les sciences, en particulier les mathématiques.
Il s'agit grosso modo d'extraire des règles opératoires, valables indépendamment de la nature des objets considérés. Par exemple la somme de deux nombres, la somme de deux vecteurs du plan ou la composition de deux relations ont des propriétés similaires.

2.1.1 Groupes, exemples

Définition 2.1.1 *Une loi de composition interne (ℓci) sur un ensemble E est une application de $E \times E$ dans E.*

Exemple : La plupart des opérations usuelles sont des *lci*.
L'addition ou la multiplication sont des *lci* sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.
La soustraction définit une *lci* sur $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ mais pas sur $\mathbb{N}$.

Exemple : Le produit scalaire de deux vecteurs de $\mathbb{R}^d$ n'est pas une *lci* si $d \geq 2$.

Exemple : On note $\mathcal{F}(E,E)$ l'ensemble des applications de E dans E, l'application de

$$\begin{array}{rcl} \mathcal{F}(E,E) \times \mathcal{F}(E,E) & \to & \mathcal{F}(E,E) \\ (f,g) & \mapsto & f \circ g \end{array}$$

($f \circ g$ est défini par $\forall x \in E\ f \circ g(x) = f(g(x))$) est une *lci*.

Définition 2.1.2 *Un groupe est la donnée d'un ensemble G et d'une lci notée $*$*

$$\begin{array}{rcl} G \times G & \to & G \\ (x,y) & \mapsto & x * y \end{array}$$

telle que $(G,*)$ vérifie les trois propriétés suivantes :

1. *(Elément neutre) Il existe $e \in G$ tel que $\forall x \in G$, $e * x = x * e = x$.*
2. *(Associativité) Pour tout x, y, $z \in G$, $(x * y) * z = x * (y * z)$.*
3. *(Elément inverse) $\forall x \in G$, $\exists x' \in G$ tel que $x * x' = x' * x = e$.*
   Si de plus $\forall x, y \in G$, $x * y = y * x$, on dit que $*$ est commutative et que $(G,*)$ est un groupe commutatif ou abelien.

Remarque : On emploie aussi parfois le terme de symétrique au lieu de inverse.

Exemple :

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de l'addition sont des groupes abeliens : 0 est l'élément neutre, l'inverse de x est $-x$. Notons que $(\mathbb{N}, +)$ n'est pas un groupe car 3. n'est pas vérifié.

2. On note $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}, \mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. Alors $\mathbb{Q}^*$, $\mathbb{R}^*$ et $\mathbb{C}^*$ munis de la multiplication sont des groupes : 1 est l'élément neutre. Il en est de même de T, l'ensemble des nombres complexes de module 1. Si x est réel, alors l'inverse de x est $1/x$.
   Tout élément de $\mathbb{C}^*$ possède un inverse pour $\times$:

$$\forall z \in \mathbb{C}^*, \ \exists z' \in \mathbb{C}^*, \ z \times z' = z' \times z = 1$$

   $\Big($si $z = x + iy$ alors $z' = \frac{x-iy}{x^2+y^2} = \frac{1}{z} = z^{-1}\Big)$.

   Tous ces groupes sont des groupes commutatifs.
   Attention : $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ muni de la multiplication $\times$ n'est pas un groupe : $\nexists n \in \mathbb{Z}^*$ tel que $n \times 5 = 1$, donc 3. n'est pas vérifié. On voit que seuls 1 et -1 ont un inverse.

3. Soit E un ensemble et soit $S(E)$ l'ensemble des bijections de E sur E, soit $\circ$ la *lci* définie par la composition de deux bijections.
   Montrer à titre d'exercice que $(S(E), \circ)$ est un groupe, et qu'il est non-abélien si E a au moins trois elements.
   En particulier pour $n \in \mathbb{N}^*$, soit $E = \{1, 2, \cdots, n\}$. Alors $S(E)$ est noté S_n. S_n est un groupe de cardinal $n!$. On l'appelle le groupe des permutations sur n éléments (voir Section 2.2).

Proposition 2.1.3

1. *L'élément neutre est unique.*
2. *Dans un groupe l'inverse x' d'un élément x est unique.*
3. *L'inverse de l'inverse de x est x, i.e. $(x')' = x$.*
4. *$(x * y)' = y' * x'$.*

Preuve : 1. Soit $e' \in G$ un élément neutre. Puisque e est un élément neutre , on a $e' * e = e * e' = e'$. De même, puisque e' est un élément neutre , on a $e * e' = e' * e = e$ et par conséquent $e' = e$.

2. Soit $x'' \in G$ tel que $x'' * x = e$. On a alors $x" * x * x' = x'$ Donc $x" = x'$.
3. On a $x * x' = x' * x = e$ donc x est l'inverse de x', d'après 2. on a $x = (x')'$.
4. On a

$$(x * y) * (y' * x') = x * y * y' * x' = x * e * x' = e$$

donc $(x * y)' = y' * x'$.

Notation : Si $(G, *)$ est un groupe, on note souvent xy au lieu de $x * y$, 1 l'élément neutre, $x^{-1} = x'$.

Remarque 2.1.4 *Soit G un groupe. Alors $xy = 1$ implique $y = x^{-1}$. En effet,*

$$xy = 1 \Rightarrow x^{-1}(xy) = (x^{-1}x)y = y.$$

Attention, en général, nous avons dans un groupe $xy \neq yx$.

Notation : L'associativité donne un sens à x^n pour $x \in G$ et $n \in \mathbb{N}^*$: $x^2 = xx$, $x^3 = x^2x, \ldots, x^n = x^{n-1}x$ avec convention $x^0 = 1$.

Proposition 2.1.5 *Soit G un groupe, soient $x, y, z \in G$.*

1. $xy = xz \Rightarrow y = z$.
2. $yx = zx \Rightarrow y = z$.

C'est à dire dans un groupe on peut simplifier par x.

Preuve : On a

$$xy = xz \Rightarrow x'(xy) = x^{-1}(xz) \Rightarrow (x^{-1}x)y = (x^{-1}x)z \Rightarrow y = z.$$

Idem pour 2. ∎

2.1.2 Sous-groupes

Définition 2.1.6 *On dit que H est un sous-groupe de $(G, *)$ si H est un sous-ensemble de G tel que la loi $*$ restreint à $H \times H$ définisse une loi lci qui donne une loi de groupe sur H.*

Ainsi un sous-groupe est stable par la loi $*$, i.e. si x, $y \in H$ alors $x * y \in H$, l'élément neutre $e \in H$, et si $x \in H$ alors $x^{-1} \in H$.
Remarquons qu'il est inutile de vérifier l'associativité car on a $\forall x, y, z \in G$, $(x*y)*z = x*(y*z)$ donc $\forall x, y, z \in H$.
En fait, on peut même raccourcir ces vérifications.

Proposition 2.1.7 *Soit H un sous-ensemble d'un groupe G. Alors H est un sous-groupe de G si*

1. $e \in H$.
2. $\forall x, y \in H \quad xy^{-1} \in H$.

Preuve : Il est facile de voir que ces conditions sont nécessaires. Réciproquement, supposons que 1 et 2 sont vérifiées et montrons que H est sous-groupe. Si $y \in H$, $ey^{-1} = y^{-1} \in H$, donc tout élément de H admet un inverse. Soient maintenant $x \in H$, $y \in H$ alors $xy = x(y^{-1})^{-1} \in H$ d'après 2., donc la multiplication est *lci*. ∎

Exemple :

1. Si G est un groupe, G, $\{e\}$ sont deux sous-groupes de G. On les appelle les sous-groupes "triviaux".
2. L'ensemble μ_n $n \in \mathbb{N}^*$, des racines complexes de l'équation $x^n = 1$ muni de la multiplication est un sous-groupe de $\mathbb{C}^*$: En effet $1^n = 1$ et si $z \in \mu_n$, $z' \in \mu_n$ $(z(z')^{-1})^n = z^n(z')^{-n} = \frac{z^n}{(z')^n} = \frac{1}{1} = 1$ donc $z(z')^{-1} \in \mu_n$. On notera que μ_n a exactement n éléments qui sont les
$$e^{2i\pi k/n}, \qquad k = 0, 1, ..., n-1.$$
3. $T = \{z \in \mathbb{C} \text{ tel que } |z| = 1\}$ est un sous-groupe de $(\mathbb{C}^*, \times)$.
4. Les inclusions $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sont des inclusions de sous-groupes pour l'addition et $\{-1, 1\} \subset \mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$ sont des sous-groupes pour la multiplication.
5. $(\mathbb{R}_+^*, \times)$ est un sous-groupe de $(\mathbb{R}^*, \times)$ car $1 \in \mathbb{R}_+^*$ et si $x \in \mathbb{R}_+^*$, $y \in \mathbb{R}_+^*$, $x \times \frac{1}{y} \in \mathbb{R}_+^*$.
Attention, $\mathbb{R}_-^*$ n'est pas un sous-groupe de $\mathbb{R}^*$ car $(-2) \times (-3) \notin \mathbb{R}_-^*$.

6. Soit $n \in \mathbb{N}^*$, posons $n\mathbb{Z} := \{0, \pm n, \pm 2n, \cdots\} = \{kn, k \in \mathbb{Z}\}$. Alors $(n\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}, +)$.

   Réciproquement, on peut montrer que ce sont les seuls sous-grouprs de $(\mathbb{Z}, +)$

   Théorème 2.1.8 *Tous les sous-groupes de $(\mathbb{Z}, +)$ sont de la forme $(n\mathbb{Z}, +)$ pour un $n \in \mathbb{Z}$.*

   Preuve : Soit donc H un sous-groupe de $(\mathbb{Z}, +)$. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$. Sinon, $H \cap \mathbb{N}^*$ est non vide et admet donc un plus petit élément, que nous allons noter n. D'où $n\mathbb{Z} \subset H$. Montrons que $H \subset n\mathbb{Z}$. Soit $a \in H$. Effectuons la division euclidienne de a par n : $a = qn + r$ avec $0 \leq r < n$. Alors $a - qn = r \in H$ donc $r = 0$ par minimalité de n. Donc $a = qn$.

   ■

2.1.3 Sous-groupes engendrés

Proposition 2.1.9 *Soit $\{H_i\}_{i \in I}$ une famille quelconque (c'est-à-dire I quelconque) de sous-groupes d'un groupe G. Alors leur intersection est encore un sous-groupe de G.*

Preuve : On vérifie sans problèmes les deux assertions de la proposition 2.1.7. ■

Proposition 2.1.10 *Soit A une partie de G. On note $\mathcal{H}_A$ l'ensemble des sous-groupes de G contenant A et on pose*

$$\mathrm{Gr}(A) = \bigcap \{H, \quad H \in \mathcal{H}_A\}.$$

Alors $\mathrm{Gr}(A)$ est un sous-groupe de G contenant A et c'est le plus petit possèdant cette propriété. On dit que c'est le sous-groupe engendré par A.

Preuve : La propriété 2.1.9 montre que $\mathrm{Gr}(A)$ est un sous-groupe de G. Il contient A puisque $\forall H \in \mathcal{H}_A$, $A \subset H$, et donc $A \subset \cap_{H \in \mathcal{H}_A} H = Gr(A)$.

Réciproquement, soit H_0 un sous-groupe de G contenant A, i.e. H_0 est un élément de l'ensemble $\mathcal{H}_A$. Donc $\cap_{H \in \mathcal{H}_A} H \subset H_0$, puisque l'intersection est incluse dans l'une des parties qui est H_0. Or $\cap_{H \in \mathcal{H}_A} H$ est par définition égal à $\mathrm{Gr}(A)$, d'où la conclusion. ■

La proposition suivante nous apporte quelques précisions sur $\mathrm{Gr}(A)$:

Proposition 2.1.11 *Soit A une partie d'un groupe G. Alors $Gr(A)$ s'écrit comme*

$$\mathrm{Gr}(A) = \{g_1 * \cdots g_n, \quad n \geq 1, \quad g_i \in A \text{ ou } g_i^{-1} \in A\}.$$

Preuve : On désigne par K le membre de droite de la proposition 2.1.11. On a successivement

- K est un sous-groupe de G contenant A, donc il contient $\mathrm{Gr}(A)$.
- Soit H un sous-groupe de G contenant A. Contenant A, il contient les inverses des éléments de A, leurs produits (puisque c'est un groupe), donc contient K. Donc K est inclus dans tout sous-groupe H contenant A, il est donc inclus dans leur intersection, qui est $\mathrm{Gr}(A)$.

■

Remarque : Il y a en général deux façons de voir un sous-groupe de G engendré par une partie de G : par l'"extérieur", c'est le choix de la définition 2.1.10 ou par l'"intérieur", c'est la proposition précédente. Sa démonstration permet nous permet d'affirmer qu'elles sont équivalentes.

2.1.4 Morphismes

Définition 2.1.12 *Soient $(A,.)$ et $(B,*)$ deux ensembles munis d'une lci. Une application $f : A \longrightarrow B$ est appelé morphisme de $(A,.)$ dans $(B,*)$ si*

$$f(a.b) = f(a) * f(b).$$

Si $(A,.)$ et $(B,*)$ sont des groupes, on dit que f est un morphisme de groupe.
Si f est bijective, on dit que f est un isomorphisme.

Proposition 2.1.13 *Soient $(A,.)$ et $(B,*)$ deux groupes et f un morphisme de $(A,.)$ dans $(B,*)$. Alors*

1. $f(e_A) = e_B$
2. $\forall x \in A,\ f(x^{-1}) = f(x)^{-1}$.
3. $\forall (x,y) \in A^2,\ f(x \cdot y^{-1}) = f(x) * f(y)^{-1}$.
4. $\forall n \in \mathbb{Z},\ \forall x \in A,\ f(x^n) = f(x)^n$.

(Démonstration en exercice)

La proposition suivante montre qu'un morphisme est associé à des sous-groupes importants en pratique.

Définition 2.1.14 *Soit $f : (A,\cdot) \to (B,*)$ un morphisme de groupe. On note par*

$$\mathrm{Im}(f) = f(A) = \{f(x), \quad x \in A\},$$

l'image directe de A par f et par

$$\mathrm{Ker}(f) = f^{-1}(\{e_B\}) = \{a \in A, \quad f(x) = e_B\},$$

l'image réciproque de l'élément neutre e_B par f, encore appelé noyau de f.

On a la proposition suivante

Proposition 2.1.15 *Soit $f : (A,\cdot) \to (B,*)$ un morphisme de groupe. Alors*

1. Im*(f) est un sous-groupe de $B(,*)$.*
2. Ker*(f) est un sous-groupe de $(A,\cdot)$.*
3. *f est injective si et seulement si* $\mathrm{Ker}(f) = \{e_A\}$.

(Démonstration en exercice)

Exemples de morphismes

Le lecteur vérifiera que les applications f ci-dessous sont des morphismes de groupe :

1. Soient $(G,*)$ un groupe, et $a \in G$. On note f l'application de $(\mathbb{Z},+) \to (G,*)$ définie par $f(n) = a^n$ (l'image de f s'appelle le sous-groupe engendré par a).
2. L'application "exponentielle imaginaire pure" : $(\mathbb{R},+) \to (T,\times) : \varphi \to e^{i\varphi}$ (on rappelle que le tore T est l'ensemble des nombres complexes de module 1).
3. L'application "exponentielle complexe" : $(\mathbb{C},+) \to (\mathbb{C}^*,\times) : z \to e^z$.
4. Soient $(G,*)$ un groupe commutatif, et $n \in \mathbb{Z}$. On note f l'application de $(G,*) \to (G,*)$ définie par $f(a) = a^n$ (ce morphisme est différent de celui du point 1.).
5. L'application $z \to |z|$ de $(\mathbb{C}^*,\times)$ dans $(\mathbb{R}^*,\times)$.

2.2 Permutations d'un ensemble fini

2.2.1 Définitions

Définition 2.2.1 *Soit E_n l'ensemble fini à n éléments $\{1,\ 2,\ \ldots,\ n\}$. On appelle permutation de E_n (ou aussi "substitution") une* ***application φ bijective de E_n dans lui-même****. On note $GP(n)$ l'ensemble des permutations de E_n.*

On sait que $GP(n)$ form un groupe pour la composition. Pour caractériser entièrement une permutation $\varphi \in GP(n)$, il faut et il suffit de se donner les valeurs de φ sur les éléments de E_n, c'est-à-dire

$$\varphi(i) = \alpha_i, \quad i = 1,\ 2,\ \ldots,\ n$$

les α_i étant tous distincts et égaux, à l'ordre près, à $1,\ 2,\ \ldots,\ n$.

La permutation φ peut alors s'écrire conventionnellement sous la forme

$$\varphi = \begin{pmatrix} 1 & 2\ \ldots\ n \\ \alpha_1 & \alpha_2\ \ldots\ \alpha_n \end{pmatrix},$$

qui signifie que chaque $i \in E_n$ est envoyé par φ sur $\alpha_i \in E_n$.

La permutation la plus élémentaire est la permutation identité (ou "neutre") définie par $\varphi(i) = i,\ \forall\ i$: on la désigne par e :

$$e = \begin{pmatrix} 1 & 2\ \ldots\ i\ \ldots\ n \\ 1 & 2\ \ldots\ i \ldots\ n \end{pmatrix}$$

Rappelons qu'il y a $n\,!$ permutations de E_n (à démontrer en exercice).

Proposition 2.2.2 *Le groupe des permutations de E_n muni de la loi de composition $(GP(n), \circ)$ forme un groupe dont l'élément neutre est e, et où l'inverse de $\varphi \in GP(n)$ est la permutation*

$$\varphi^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2\ \ldots\ \alpha_n \\ 1 & 2\ \ldots\ n \end{pmatrix}$$

2.2.2 Transpositions

On suppose dans ce qui suit $n \geq 2$. On suppose dans ce qui suit $n \geq 2$.

Définition 2.2.3 *Une transposition de E_n est une permutation qui échange deux éléments i et j distincts de E_n, en laissant invariants les autres éléments de E_n. On peut le noter T_{ij}, avec la convention $T_{ii} = e$.*

On a donc

$$T_{ij}(i) = j, \quad T_{ij}(j) = i, \quad T_{ij}(p) = p \quad \text{si} \quad p \neq i \quad \text{et} \quad p \neq j$$

Exemple.

Dans $E_5 = \{1,\ 2,\ 3,\ 4,\ 5\}$

$$T_{3,5} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix}$$

On pourra vérifier qu'une permutation est sa propre inverse, c'est-à-dire que $T_{ij} = T_{ji} = (T_{ij})^{-1}$ ou de manière équivalente $T_{i,j} \circ T_{i,j} = e$.

Le théorème suivant est fondamental :

Théorème 2.2.4 *Toute permutation $\varphi \in GP(n)$ de l'ensemble fini E_n peut se décomposer comme un produit de transpositions, c'est-à-dire qu'il existe un nombre fini M de transpositions T_1, T_2,..., T_M tels que*

$$\varphi = T_M \circ T_{M-1} \circ ... \circ T_1. \tag{2.1}$$

Preuve : Démontrons ce théorème par récurrence sur n, qui est le cardinal de E_n.

Si $n = 2$: alors il est clair que toute permutation de E_2 est soit l'identité, soit une transposition.

Supposons l'assertion vraie à l'ordre $n-1$. Soit $\varphi \in GP(n)$. Distinguons alors deux cas :
1. Si $\varphi(n) = n$: le point n est laissé invariant par φ. Donc la restriction de φ à E_{n-1} est en fait une permutation de l'ensemble E_{n-1}. Par hypothèse de récurrence, cette restriction se décompose en produit de transpositions, et il en est donc de même pour φ.
2. Si $\varphi(n) = p$ où p est différent de n : Considérons ψ la permutation définie comme le produit de φ avec la transposition $T = T_{np}$ qui inverse n et p. Plus précisément, on pose $\psi = T_{np} \circ \varphi$.
Par construction ψ vérifie $\psi(n) = n$. On peut donc appliquer le point 1. précédent à ψ. Grâce à la formule (2.1) on trouve qu'il existe un nombre fini M de transpositions T_1, T_2,..., T_M tels que

$$\psi = T_M \circ T_{M-1} \circ ... \circ T_1.$$

En utilisant que $T_{np} \circ T_{np} = e$, on voit alors que

$$\varphi = T_{np} \circ \psi = T_{np} \circ T_M \circ T_{M-1} \circ ... \circ T_1.$$

Donc φ est bien un produit de transpositions. Le théorème est démontré. ■

Remarquons qu'il n'y pas d'unicité dans la décomposition on transposition précdente.

2.2.3 Inversion d'une permutation. Parité. Signature

Définition 2.2.5 *Etant donné la permutation*

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_n \end{pmatrix},$$

on dit que α_i et α_j présentent une inversion dans φ si $i < j$ et $\alpha_i > \alpha_j$.

Définition 2.2.6 *Une permutation φ est dite paire si le nombre total des inversions qu'elle présente est pair, elle est dite impaire si ce nombre est impair.*
Si $I(\varphi)$ est ce nombre d'inversions, le nombre $\sigma(\varphi) = (-1)^{I(\varphi)}$ est appelé signature de φ.
La signature de φ vaut 1 ou -1 suivant que φ est respectivement paire ou impaire.

Exemple.

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

$$I(\varphi) = 8, \quad \varphi \text{ est paire}, \quad \sigma(\varphi) = 1.$$

Dans le cas des transpositions, on a le résultat suivant :

Proposition 2.2.7 *Toute transposition est impaire.*

Preuve : Soit $i \neq j$ et $T_{i,j}$ la transposition associée. On peut supposer sans perte de généralité que $i < j$. On considère d'abord le cas où i et j sont consécutifs, soit $j = i+1$. On a

$$T_{i,j} = \begin{pmatrix} 1 & \cdots & i-1 & i & i+1 & i+2 & \cdots & n \\ 1 & \cdots & i-1 & i+1 & i & i+2 & \cdots & n \end{pmatrix}.$$

Il est immédiat de constater qu'il n'y a qu'une seule inversion $(i, i+1)$ et donc que $T_{i,i+1}$ est impaire.

Pour le cas où $j \geq i+2$, on représente $T_{i,j}$ ci-dessous :

$$T_{i,j} = \begin{pmatrix} 1 & \cdots & i-1 & i & i+1 & \cdots & j-1 & j & j+1 & \cdots & n \\ 1 & \cdots & i-1 & j & i+1 & \cdots & j-1 & i & j+1 & \cdots & n \end{pmatrix}$$

Les couples $(i, i+1)$, $(i, i+2)$, ..., (i, j) (soit $j-i$ couples) présentent une inversion. De même, pour $(i+1, j)$, $(i+2, j)$, ..., $(j-1, j)$ (soit $j-i-1$ couples). Au total, on a $2(j-i)-1$ inversions, soit un nombre impair, $T_{i,j}$ est donc dans ce cas également impaire. ■

On peut démontrer les propriétés suivantes

Proposition 2.2.8 *Quand on compose une permutation quelconque par une transposition, on obtient une nouvelle permutation, de parité différente.*

Preuve : Commençons par le cas où la transposition T inverse deux éléments successifs, i.e. il existe un entier $i \in \{1, ..., n\}$ tel que $T = T_{i,i+1}$.

Soit $\varphi \in GP(n)$, qui s'écrit

$$\varphi = \begin{pmatrix} 1 & \cdots & j & \cdots & i & i+1 & \cdots & j' & \cdots & n \\ \alpha_1 & \cdots & \alpha_j & \cdots & \alpha_i & \alpha_{i+1} & \cdots & \alpha_{j'} & \cdots & \alpha_n \end{pmatrix}$$

Alors $\varphi \circ T_{i,i+1}$ s'écrit

$$\begin{aligned} \varphi \circ T_{i,i+1} &= \begin{pmatrix} 1 & \cdots & j & \cdots & i & i+1 & \cdots & j' & \cdots & n \\ \alpha_1 & \cdots & \alpha_j & \cdots & \alpha_{i+1} & \alpha_i & \cdots & \alpha_{j'} & \cdots & \alpha_n \end{pmatrix} \\ &= \begin{pmatrix} 1 & \cdots & j & \cdots & i & i+1 & \cdots & j' & \cdots & n \\ \alpha'_1 & \cdots & \alpha'_j & \cdots & \alpha'_i & \alpha'_{i+1} & \cdots & \alpha'_{j'} & \cdots & \alpha'_n \end{pmatrix}, \end{aligned}$$

où l'on a noté α'_p l'image de p par $\varphi \circ T_{i,i+1}$. On a donc $\alpha'_j = \alpha_j$ si $j < i$, $\alpha'_i = \alpha_{i+1}$, $\alpha'_{i+1} = \alpha_i$, et $\alpha'_{j'} = \alpha_{j'}$ pour $j' > i+1$.

Comparons les éventuelles inversions de φ et de $\varphi \circ T_{i,i+1}$.

1. Commençons par les inversions possibles entre les éléments i et $i+1$:
   (a) Supposons que φ présente une inversion entre i et $i+1$, alors $\alpha_i > \alpha_{i+1}$. Dans ce cas, $\varphi \circ T_{i,i+1}$ ne présente pas d'inversion entre i et $i+1$, car $\alpha'_i = \alpha_{i+1} < \alpha'_{i+1} = \alpha_i$.
   (b) Supposons que φ ne présente pas d'inversion entre i et $i+1$, alors $\alpha_i < \alpha_{i+1}$. Dans ce cas, $\varphi \circ T_{i,i+1}$ présente une inversion entre i et $i+1$, car $\alpha'_i = \alpha_{i+1} > \alpha'_{i+1} = \alpha_i$.
2. Étudions ensuite tous les autres cas possibles d'inversion :
   (a) Supposons que φ présente une inversion entre $j < i$ et i, alors $\alpha_j > \alpha_i$. Alors $\varphi \circ T_{i,i+1}$ présente une inversion entre j et $i+1$, car $\alpha'_j = \alpha_j > \alpha'_{i+1} = \alpha_i$. De même, s'il n'y avait pas d'inversion dans φ pour ces indices j et i, il n'y en aura pas dans $\varphi \circ T_{i,i+1}$ pour les indices j et $i+1$. Cette remarque s'applique également aux points b., c., d. et e. suivants.

(b) Supposons que φ présente une inversion entre $j < i$ et $i+1$, alors $\alpha_j > \alpha_{i+1}$. Alors $\varphi \circ T_{i,i+1}$ présente une inversion entre j et i, car $\alpha'_j = \alpha_j > \alpha'_i = \alpha_{i+1}$.

(c) Supposons que φ présente une inversion entre i et $j' > i+1$, alors $\alpha_{j'} < \alpha_i$. Alors $\varphi \circ T_{i,i+1}$ présente une inversion entre $i+1$ et j', car $\alpha'_{j'} = \alpha_{j'} < \alpha'_{i+1} = \alpha_i$.

(d) Supposons que φ présente une inversion entre $i+1$ et $j' > i+1$, alors $\alpha_{j'} < \alpha_{i+1}$. Alors $\varphi \circ T_{i,i+1}$ présente une inversion entre i et j', car $\alpha'_{j'} = \alpha_{j'} < \alpha'_i = \alpha_{i+1}$.

(e) Enfin, supposons que φ présente une inversion entre $j < i$ et $j' > i+1$, alors $\alpha_j > \alpha_{j'}$. Alors $\varphi \circ T_{i,i+1}$ présente une inversion entre j et j', car $\alpha'_j = \alpha_j > \alpha'_{j'} = \alpha_{j'}$.

Le lecteur vérifiera que l'on a bien étudié tous les cas possibles. Ainsi on a prouvé que le nombre d'inversions diminuait de 1 dans le cas 1.(a), et augmentait de 1 dans les cas 1.(b), tous les autres cas ne modifiant pas le nombre d'inversions entre φ et $\varphi \circ T_{i,i+1}$. Or on est nécessairement dans le cas 1.(a) ou dans le cas 1.(b). Donc on a changé la parité de la signature de φ en la composant par $T_{i,i+1}$.

Soit $T = T_{i,j}$ une inversion, avec $i < j$. Alors on remarque

$$\begin{aligned} T_{i,j} = \quad & T_{j,j-1} \circ T_{j-1,j-2} \circ \cdots \circ T_{i+2,i+1} \\ & \circ T_{i+1,i} \circ T_{i+2,i+1} \circ \cdots \circ T_{j-1,j-2} \circ T_{j,j-1}, \end{aligned}$$

c'est-à-dire que $T_{i,j}$ est le produit de $2(j-i)-1$ transpositions qui échangent deux éléments voisins. Comme la composition par une transposition qui échangent deux éléments voisins modifie la signature (c'est ce que l'on a démontré précédemment), lorsque l'on compose par T, on modifie $2(j-i)-1$ fois la signature. Étant donné que $2(j-i)-1$ est un nombre impair, φ et $\varphi \circ T_{i,j}$ n'ont pas la même signature. ∎

Par conséquent, le résultat précédent permet avec la décomposition (2.1) de montrer :

Proposition 2.2.9 *Pour qu'une permutation soit paire (respectivement, impaire), il faut et il suffit qu'elle soit le produit d'un nombre pair (respectivement, impair) de transpositions.*

Proposition 2.2.10 - *Si φ_1 et φ_2 sont deux permutations de même parité, $\varphi_1 \circ \varphi_2$ est paire ; si elles sont de parités différentes, $\varphi_1 \circ \varphi_2$ est impaire. Ainsi*

$$\sigma(\varphi_1 \circ \varphi_2) = \sigma(\varphi_1)\ \ \sigma(\varphi_2).$$

Donc l'application signature $\sigma : \varphi \in GP(n) \mapsto \sigma(\varphi)$ est un morphisme du groupe $(GP(n), \circ)$ vers le groupe $(\{-1, 1\}, \times)$ (muni de la multiplication classique). On en déduit que deux permutations inverses l'une de l'autre ont même parité puisque $\sigma(\varphi)\sigma(\varphi^{-1}) = \sigma(\varphi \circ \varphi^{-1}) = \sigma(e) = 1$.

Autre expression de la signature d'une permutation.

Proposition 2.2.11 *Soit $\varphi \in GP(n)$ avec $n \geq 2$. Alors on a*

$$\sigma(\varphi) = \prod_{1 \leq i < j \leq n} \frac{\varphi(j) - \varphi(i)}{j - i}. \tag{2.2}$$

(Noter que le produit précédent comprend tous les couples (i, j) tels que $1 \leq i < j \leq n$, soit C_n^2 facteurs.)

Preuve : Soit $i < j$ deux entiers de E_n. On pose

$$\begin{cases} h = \varphi(i) \\ k = \varphi(j) \quad \text{si } \varphi(i) < \varphi(j) \end{cases} \quad \text{et} \quad \begin{cases} h = \varphi(j) \\ k = \varphi(i) \quad \text{si } \varphi(j) < \varphi(i) \end{cases}$$

Pour des raisons de clarté, on omet de spécifier la dépendance en i et j de h et k. Le produit du membre de droite de (2.2) se décompose alors en

$$\prod_{1\le i<j\le n} \left(\frac{\varphi(j)-\varphi(i)}{j-i}\right) = \prod_{\substack{1 \le i < j \le n, \\ (i,j) \text{ pas d'inversion}}} \left(\frac{k-h}{j-i}\right) \prod_{\substack{1 \le i < j \le n, \\ (i,j) \text{ inversion}}} \left(\frac{h-k}{j-i}\right)$$

Le deuxième facteur du membre de droite comporte exactement $I(\varphi)$ facteurs. On retrouve donc

$$\prod_{1\le i<j\le n} \left(\frac{\varphi(j)-\varphi(i)}{j-i}\right) = (-1)^{I(\varphi)} \frac{\displaystyle\prod_{1\le i<j\le n} (k-h)}{\displaystyle\prod_{1\le i<j\le n} (i-j)}.$$

On conclut en remarquant que $(i,j) \to (h,k)$ est une bijection et donc que les deux produits du membre de droite sont identiques. ∎

Remarquons que l'on peut montrer facilement avec cette autre expression, la propriété de morphisme énoncée dans la proposition 2.2.10.

2.3 Structure d'anneau

2.3.1 Anneaux, exemples

Définition 2.3.1 *Un* anneau *est la donnée d'un ensemble A et de lois de composition $+$ (addition) et $*$ (multiplication) telles que :*

1. *$(A,+)$ est un groupe commutatif (dont on note l'élément neutre $0 = 0_A$)).*
2. *La loi $*$ est associative.*
3. *La loi $*$ possède un élément neutre (qu'on notera $1 = 1_A$).*
4. *La loi $*$ est distributive par rapport à l'addition :*

$$\forall x, y, z \in A,\ x*(y+z) = (x*y)+(x*z) \text{ et } (y+z)*x = (y*x)+(z*x)$$

Si de plus la loi $*$ est commutative, on dit que l'anneau A est commutatif.

Remarquons que l'on a toujours $x*0 = 0*x = 0$ dans un anneau ; en effet $x*0 = x*(0+0) = x*0 + x*0$ et donc (la loi $+$ est une loi de groupe) $x*0 = 0$.

Vocabulaire : Afin de ne pas introduire de confusion en ce qui concerne les "inverses" pour les deux lois, nous adoptons le vocabulaire hérité du cas de $(\mathbb{Z},+,\times)$, et nous appellerons "opposé" de x l'élément $-x$ et "inverse" de x (s'il existe) l'élément x^{-1}.

Attention : Dans un anneau $(A,+,*)$, un élément $x \in A$ possède un opposé, mais pas forcément pour la loi $*$. En effet, en général, $(A,*)$ ne forme pas un groupe !!

Le théorème suivant définit les règles de calcul dans les anneaux.

Théorème 2.3.2 *Soit $(A,+,*)$ un anneau.*

Pour tout triplet (x,y,y') de A^3, on a	*Pour tout triplet (x,x',y) de A^3, on a*
$x*0=0$,	$0*y=0$,
$x*(-y)=-(x*y)$,	$(-x)*y=-(x*y)$,
$x*(y-y')=x*y-x*y'$,	$(x-x')*y=x*y-x'*y$,
$\forall n\in\mathbb{Z}$, $x*(ny)=n(x*y)$.	$\forall n\in\mathbb{Z}$, $(nx)*y=n(x*y)$.

Preuve : Considérons pour $x\in A$ donné, l'application $f_x : A\to A$, $y\mapsto x*y$. f_x est un morphisme du groupe $(A,+)$ vers lui-même. On peut donc lui appliquer le formulaire de la proposition 2.1.13. ∎

Un anneau est donc un triplet $(A,+,*)$, l'ensemble A s'appelle l'ensemble *sous-jacent* à l'anneau ; toutefois on parle souvent de l'anneau A en sous-entendant les lois $+$ et $*$ quand il est clair dans le contexte de quelles lois il s'agit.

Exemple :

1. Nous étudierons tout spécialement l'anneau des entiers relatifs $(\mathbb{Z},+,\times)$ muni de ses lois usuelles.
2. $\mathbb{C}$ muni de l'addition et de la multiplication est un anneau commutatif (on pourra vérifier à titre d'exercice la distributivité de la multiplication des complexes par rapport à l'addition).
3. On note $\mathbb{R}[X]$ l'ensemble des polynômes à une variable, et à coefficients réels. Alors $(\mathbb{R}[X],+,\times)$ est un anneau.
4. L'anneau nul. On munit $A=\{a\}$ des lois $+$ et $*$ définies par $a+a=a$ et $a*a=a$. Alors $(A,+,*)$ est un anneau commutatif dans lequel $0_A=1_A=a$. C'est *l'anneau nul.*

Attention : dans un anneau, il n'est pas vrai en général que lorsque $x\in A\setminus\{0\}$ on ait $xy=xz\Rightarrow y=z$.

Si l'anneau est commutatif : $(xy)^n=x^ny^n$.

Définition 2.3.3 *On appelle* diviseurs de zéros *des éléments a et b d'un anneau $(A,+,*)$ tels que*

$$a\neq 0_A,\quad b\neq 0_A\quad \text{et } a*b=0_A.$$

Définition 2.3.4 *On appelle* anneau intègre *tout anneau distinct de l'anneau nul et qui n'a pas de diviseurs de zéros.*

Dans un anneau intègre $(A,+,*)$, on a

$$\forall (a,b)\in A^2,\quad a*b=0_A\Rightarrow a=0_A\quad \text{ou } b=0_A.$$

$\mathbb{Z}$ et $\mathbb{C}$ sont des anneaux intègres.

L'expression de la puissance n-ième d'une somme est souvent utile.

Théorème 2.3.5 *(Formule du binôme de Newton) Soient a,b deux éléments d'un anneau commutatif et soit n un entier ≥ 1, on a la formule :*

$$(a+b)^n=\sum_{p=0}^{n} C_n^p a^p b^{n-p}$$

où $C_n^p=\frac{n!}{p!(n-p)!}$ est le nombre de parties à p èlèments dans un ensemble à n éléments.
A cause de cette formule, les coefficients C_n^p sont aussi appelés coefficients binômiaux.

Les premiers exemples de cette formules s'écrivent :

$$\begin{aligned}(a+b)^1 &= a+b\\ (a+b)^2 &= a^2+2ab+b^2\\ (a+b)^3 &= a^3+3a^2b+3ab^2+b^3\\ (a+b)^4 &= a^4+4a^3b+6a^2b^2+4ab^3+b^4\\ (a+b)^5 &= a^5+5a^4b+10a^3b^2+10a^2b^3+5ab^4+b^5\end{aligned}$$

Preuve : La démonstration se fait par récurrence sur le nombre n : la formule est évidente pour $n=0$ ou $n=1$, on la suppose donc vraie pour l'entier n, pour tout a, b et on cherche à en déduire la formule pour l'entier $n+1$.
On a : $(a+b)^{n+1} = (a+b)(a+b)^n$ qui d'après l'hypothèse de récurrence vaut :

$$(a+b)\sum_{p=0}^{n} C_n^p a^p b^{n-p} = \sum_{p=0}^{n} C_n^p a^{p+1} b^{n-p} + \sum_{p=0}^{n} C_n^p a^p b^{n-p+1},$$

Cette dernière expression est égale à :

$$a^{n+1} + \sum_{h=1}^{n} (C_n^h + C_n^{h-1}) a^h b^{n+1-h} + b^{n+1}$$

et, si on rappelle que $C_n^h + C_n^{h-1} = C_{n+1}^h$ celle-ci vaut :

$$\sum_{h=0}^{n+1} C_{n+1}^h a^h b^{n+1-h}$$

ce qui est bien la formule de Newton pour l'entier $n+1$. ∎

Remarque 2.3.6 *L'hypothèse de commutativité ne peut pas être enlevée.*

2.3.2 Morphisme d'anneaux

Définition 2.3.7 *On appelle morphisme de l'anneau $(A,+,*)$ vers l'anneau $(B,+,*)$ toute application f de A vers B telle que*

1. $\forall (a,a') \in A^2,\ f(a+a') = f(a)+f(a')$.
2. $\forall (a,a') \in A^2,\ f(a*a') = f(a)*f(a')$.
3. $f(1_A) = 1_B$.

Conséquence de la définition : Un morphisme d'anneau est en particulier un morphisme de groupe (assertion 1), il s'en suit les propriétés habituelles (cf. propositions 2.1.13 et 2.1.15).

Proposition 2.3.8 *Soit f un morphisme de l'anneau $(A,+,*)$ vers l'anneau $(B,+,*)$, et a un élément inversible de A. Alors*

$$f(a^{-1}) = (f(a))^{-1}.$$

(Démonstration en exercice)

2.3.3 Sous-anneaux

Définition 2.3.9 *On appelle sous-anneau de l'anneau $(A,+,*)$ toute partie A' de A :*
- *stable pour les lois d'anneaux de A,*
- *qui, munie de ces lois est un anneau,*
- *et qui contient l'élément unité 1_A de l'anneau A.*

Une définition équivalente est de dire que A' est un sous-anneau de A ssi A' est un sous-groupe du groupe $(A,+)$ contenant l'unité 1_A et stable par la loi $*$. On en déduit facilement la caractérisation pratique suivante (cf. proposition 2.1.7).

Proposition 2.3.10 *Soit $(A,+,*)$ un anneau. Les assertions suivantes sont équivalentes*

1. *A' sous-anneau de A,*
2. $\begin{cases} A' \subset A \quad et\ 1_A \in A', \\ \forall (x,y) \in (A')^2, \quad x-y \in A', \\ \forall (x,y) \in (A')^2, \quad x*y \in A'. \end{cases}$

La proposition suivante s'intéresse aux images directes et réciproques d'un sous-anneau par un morphisme d'anneaux.

Proposition 2.3.11 *Soit $f : (A,+,*) \to (B,+,*)$ un morphisme d'anneaux. Alors,*
- *Pour tout sous-anneaux A' de A, $f(A')$ est un sous-anneau de B ;*
- *Pour tout sous-anneau B' de B, $f^{-1}(B')$ est un sous-anneau de A.*

(Démonstration en exercice)

En particulier, $\mathrm{Im}(f)$ est un sous-anneau de B. Attention, on ne peut rien dire en général sur $\mathrm{Ker}(f)$, car, si $1_A \neq 0_A$, alors $\{0\}$ n'est pas un sous-anneau de B.

Le lecteur vérifiera que le seul sous-anneau de $\mathbb{Z}$ est $\mathbb{Z}$ lui-même. La notion de sous-anneau peut donc sembler trop restrictive dans certains cas. On introduit une notion plus faible de sous-structures dans le paragraphe suivant.

2.3.4 Idéaux d'un anneau

Définition 2.3.12 *On appelle* idéal *de l'anneau $(A,+,*)$ toute partie I de A tel que*

1. *I sous-groupe de $(A,+)$,*
2. *$\forall a \in A$, $\forall i \in I$, $a*i \in I$ et $i*a \in I$.*

La proposition 2.1.7 nous fournit encore une caractérisation pratique des idéaux :

Proposition 2.3.13 *Soit $(A,+,*)$ un anneau. Les assertions suivantes sont équivalentes*

1. *I idéal de l'anneau A*
2. $\begin{cases} I \subset A \quad et\ I \neq \emptyset, \\ \forall (x,y) \in I^2, \quad x-y \in I, \\ \forall a \in A, \forall i \in I, a*i \in I\ et\ i*a \in I \end{cases}$

Exemple :

1. Soit A un anneau. Il admet deux idéaux dits *triviaux* : A et $\{0_A\}$.
2. Les seuls idéaux de l'anneau $(\mathbb{Z},+,\cdot)$ sont les ensembles de la forme $n\mathbb{Z}$ pour $n \in \mathbb{N}$.

On a le résultat simple mais important suivant

Proposition 2.3.14 *Soit I un idéal de l'anneau $(A,+,*)$. Si $1_A \in I$, alors $I = A$.*

(Démonstration en exercice)
Les liens entre morphismes d'anneaux et idéaux sont établis dans la proposition suivante.

Proposition 2.3.15 *Soit $f : (A, +, *) \to (B, +, *)$ un morphisme d'anneau. Alors*

1. *I idéal de A implique $f(I)$ idéal de $\mathrm{Im}(f)$,*
2. *J idéal de B implique $f^{-1}(J)$ idéal de A.*

(Démonstration en exercice)
En particulier, $\mathrm{Ker}(f)$ est un idéal de l'anneau A.

2.3.5 Idéal engendré par une partie. Idéal principal. Anneau principal

La fin de ce paragraphe consacré aux anneaux introduit la notion d'idéaux engendré par une partie d'un anneau et à la notion, centrale en arithmétique, d'anneau principal.

Proposition 2.3.16 *Soit $\{I_j\}_{j\in J}$ une famille quelconque (c'est-à-dire J quelconque) d'idéaux d'un anneau A. Alors leur intersection est encore un idéal de A.*

Preuve : On vérifie sans problèmes les deux assertions de la proposition 2.3.13. ■

La dernière proposition légitime la définition suivante.

Définition 2.3.17 *Soit X une partie de A. On note $\mathcal{I}_X$ l'ensemble des idéaux de A contenant X et on pose*

$$(X) = \bigcap \{I, \quad I \in \mathcal{I}_X\}.$$

*Alors (X) est un idéal de A contenant X et c'est le plus petit possèdant cette propriété. On dit que c'est l'*idéal engendré par *X.*

On se place dans le cas d'un anneau commutatif A. Soit $a \in A$. On pose $M = \{a*x, \quad x \in A\}$. On vérifie facilement que M est un idéal de A contenant a et que de plus c'est le plus petit idéal de A contenant a. Soit en effet J un idéal de A contenant $\{a\}$ et m un élément de M. L'élément m est donc de la forme $a * x$ où $x \in A$. Alors, par définition de l'idéal, $a * x \in J$ car $a \in J$. Donc $M \subset J$.

C'est donc l'idéal engendré par $\{a\}$. On le note souvent (a) (plutôt que $(\{a\})$). On a prouvé

$$(a) = \{a * x, \quad x \in A\}. \tag{2.3}$$

Définition 2.3.18 (Éléments associés) *Soit $(A, +, *)$ un anneau. Soit a, b deux éléments de A. On dit que a et b sont associés ssi*

$$(a) = (b).$$

Dans un anneau intègre, il est possible de caractériser les éléments associés. Auparavant, notons $\mathbb{U}(A)$ l'ensemble des éléments inversibles de l'anneau A (pour la loi $*$). On sait (cf. exercice) que munit de la loi $*$, c'est un groupe. On l'appelle *le groupe des unités de l'anneau.*

Proposition 2.3.19 *Soit A un anneau commutatif et* intègre. *Soit a et b deux éléments de A. Alors*

$$a \text{ et } b \quad \text{associés} \iff \exists\, u \in \mathbb{U}(A) \text{ tel que } \; b = ua$$

Preuve : L'implication de droite à gauche est évidente. Soit maintenant a et b tels que $(a) = (b)$. Il existe alors q_1 et q_2 dans A tels que $a = b\,q_1$ et $b = a\,q_2$. On a alors

$$a = a\,q_2 q_1 \quad \text{ou encore} \quad a\,(1_A - q_2 q_1) = 0_A.$$

Soit $a = 0_A$. Auquel cas, $b = 0_A$. Soit $a \neq 0_A$ et alors, comme A est intègre, $q_2\,q_1 = 1_A$. ■

Définition 2.3.20 *On appelle* idéal principal *tout idéal engendré par un singleton $X = \{a\}$.*

Définition 2.3.21 *On appelle* anneau principal *tout anneau A tel que*

1. *A est intègre,*
2. *tout idéal de A est principal.*

L'arithmétique abordée dans le chapitre 4 se fonde en partie sur le théorème suivant :

Théorème 2.3.22 *L'anneau $(\mathbb{Z}, +, \cdot)$ des entiers relatifs munis des lois usuelles est un anneau principal.*

Preuve : Les seuls sous-groupes de $(\mathbb{Z}, +)$ sont $n\mathbb{Z}$ pour n entier. On vérifie sans peine que $n\mathbb{Z}$ est bien un idéal de $\mathbb{Z}$ et qu'il est engendré par n (cf. (2.3)). ■

2.4 Structure de corps

2.4.1 Corps, exemples

Définition 2.4.1 *Un* corps $(K, +, \cdot)$ *(commutatif) est un anneau tel que :*

1. *K distinct de l'anneau nul,*
2. *la loi $\cdot$ est commutative,*
3. *tout élément $x \in K \setminus \{0_K\}$ possède un inverse.*

Exemple :

1. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sont des corps.
2. L'anneau $(\mathbb{Z}, +, \times)$ n'est donc pas un corps car les seuls éléments de $\mathbb{Z}$ possédant un inverse pour la multiplication sont $+1$ et -1.

Les corps les plus importants que nous étudierons sont le corps des nombres rationnels $\mathbb{Q}$, le corps des nombres réels $\mathbb{R}$ et le corps des nombres complexes $\mathbb{C}$. Nous verrons aussi que, si K désigne $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, l'ensemble des polynômes à coefficients dans K, que l'on note $K[X]$, muni de l'addition et de la multiplication naturelles, forme un anneau qui possède beaucoup de propriétés communes avec $\mathbb{Z}$. Tous ces anneaux sont commutatifs.

Les propriétés suivantes sont immédiates.

Proposition 2.4.2 *Soit $(K, +, \cdot)$ un corps.*

1. *K possède au moins deux éléments.*
2. *K est intègre, c'est-à-dire*

$$\forall (a, b) \in K^2, \quad a \cdot b = 0_K \Rightarrow a = 0_K \text{ ou } b = 0_K.$$

Preuve :

1. Il s'agit de 0_K et 1_K puisque $0_K \neq 1_K$ (K distinct de l'anneau nul).
2. Un corps K ne possède pas de diviseurs de zéros. En effet,

$$a \neq 0_K, \quad b \neq 0_K \Rightarrow a \cdot b \neq 0_K,$$

car $K \setminus \{0_K\}$ est stable pour $\cdot$ (en fait, $K \setminus \{0_K\}$ est un groupe). Pour le voir, il suffit de constater que $K \setminus \{0_K\} = \mathbb{U}(K)$, l'ensemble des éléments inversibles de K. L'inclusion directe est une conséquence de la définition de corps. Quant à l'inclusion réciproque, si x est inversible pour $\cdot$ alors $x \neq 0_K$ car $0_K \cdot y = 0_K \neq 1_K$ pour tout $y \in K$.

■

2.4.2 Sous-corps

Définition 2.4.3 *On appelle* sous-corps *d'un corps, tout anneau de ce corps qui est un corps pour les lois induites.*

De même que précédemment, on a les caractérisations pratiques suivantes :

Proposition 2.4.4 *Soit $(K,+,\cdot)$ un corps.*

$$\begin{aligned} K' \text{ sous-corps de } K &\iff K' \text{ sous-anneau de } K \text{ et } \forall x \in K'\backslash\{0_K\},\ x^{-1} \in K' \\ &\iff \begin{cases} K' \subset K \text{ et } 1_K \in K', \\ \forall (x,y) \in K',\ x-y \in K' \text{ et } x\cdot y \in K' \\ \forall x \in K'\backslash\{0_K\},\ x^{-1} \in K' \end{cases} \\ &\iff \begin{array}{l} K' \text{ est un sous-groupe de } (K,+) \text{ et} \\ K'\backslash\{0_K\} \text{ sous-groupe de } (K\backslash\{0_K\},\cdot). \end{array} \end{aligned}$$

Si K' est un sous-corps de K, alors K est appelé *sur-corps* de K' ou encore *extension* de K.

2.4.3 Idéaux d'un corps

Théorème 2.4.5 *Tout corps n'a que des idéaux triviaux.*

Preuve : D'abord, K et $\{0_K\}$ sont bien des idéaux (triviaux) de K. Il n'y en a pas d'autre. Car si I est un idéal de K distinct de l'idéal nul $\{0_K\}$, montrons que $I = K$. Comme I n'est pas l'idéal nul, il existe un élément i de I distinct de 0_K. Soit i^{-1} son inverse dans K. Alors $i \cdot i^{-1} = 1_K \in I$ par définition d'un idéal. On conclut par la proposition 2.3.14. ■

2.4.4 Morphisme de corps

Définition 2.4.6 *On appelle morphisme du corps $(K,+,\cdot)$ vers le corps $(L,+,\cdot)$ toute application f de K vers L telle que*

1. $\forall (x,y) \in K^2,\ f(x+y) = f(x) + f(y)$.
2. $\forall (x,y) \in K^2,\ f(x\cdot y) = f(x)\cdot f(y)$.
3. $f(1_K) = 1_L$.

Les conséquences immédiates sont que tout morphisme de corps f est un morphisme du groupe $(K,+)$ vers le groupe $(L,+)$. De plus, f est également un morphisme du groupe $(K\backslash\{0_K\},\cdot)$ vers le groupe $(L\backslash\{0_L\},\cdot)$. On remarquera qu'il s'agit bien d'une application ici car si x est inversible pour $\cdot$ dans K alors $f(x)$ est inversible pour $\cdot$ dans L (propriété d'anneau).

Les corps sont finalement des objets assez contraints comme le souligne le résultat suivant.

Théorème 2.4.7 *Tout morphisme de corps est injectif.*

Preuve : Soit $f : K \to L$ un morphisme de corps. Alors $\mathrm{Ker}(f)$ est un idéal du corps K. Donc $\mathrm{Ker}(f)$ ne peut-être que l'idéal nul ou l'idéal plein (cf. le théorème 2.4.5). Or $\mathrm{Ker}(f) = K$ est absurde car $f(1_K) = 1_L \neq 0_L$. Donc $1_K \notin \mathrm{Ker}(f)$. Donc $\mathrm{Ker}(f) = \{0_K\}$, c'est-à-dire f injectif. ■

Concernant l'image directe d'un corps par un morphisme de corps, on a le résultat suivant.

Proposition 2.4.8 *Soit $f : K \to L$ un morphisme de corps. Alors* $\mathrm{Im}(f)$ *est un sous-corps du corps L.*

Preuve : Tout d'abord, $\mathrm{Im}(f)$ est déjà un sous-anneau de l'anneau L (cf. proposition 2.3.11). Ensuite, grâce à la caractérisation 2.4.4, il suffit de montrer que pour tout $y \in \mathrm{Im}(f)$, $y \neq 0_L$, y^{-1} appartient à $\mathrm{Im}(f)$. Or, il existe $x \in K$ tel que $y = f(x)$ avec $x \neq 0_K$. Mais alors $y^{-1} = (f(x))^{-1} = f(x^{-1})$ (propriété de morphisme d'anneaux pour les éléments inversibles). Donc $y^{-1} \in \mathrm{Im}(f)$. ■

En conclusion, tout morphisme de corps $f : K \to L$ induit un isomorphisme de corps de K sur $\mathrm{Im}(f)$.

2.5 Compléments sur les nombres complexes

2.5.1 Racines n-ièmes de l'unité

Définition 2.5.1 *Soient $n \in \mathbb{N}^*$, $(z, z) \in \mathbb{C}^2$.*
On dit que z est racine n-ième de Z si $z^n = Z$.
On dit que z est racine n-ième de l'unité si $z^n = 1$. Lorsque $n = 2$ on parle de racine carrée de Z si $z^2 = Z$ et de racine carrée de l'unité si $z^2 = 1$.

Proposition 2.5.2 *Soit $n \in \mathbb{N}^*$. Il y a exactement n racines $n^{ièmes}$ de l'unité (2 à 2 distinctes), a savoir les nombres complexes $w_k = e^{2\frac{ik\pi}{n}} = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$ avec $k \in \{0, 1, \ldots, n-1\}$*

Preuve : Soit z une racine n-ème de l'unité que nous écrivons sous la forme trigonométrique $z = |z|e^{i\theta}$.
$|Z|^n e^{in\theta} = 1\dot{e}^{i\theta}$ s'écrit $\left\{ \begin{array}{lcl} |z|^n & = & 1 \\ n\theta & = & 2k\pi \quad \text{avec} \quad k \in \mathbb{Z} \end{array} \right.$ Comme $|z|^n - 1 = (|z|-1)(|z|^{n-1} + \cdots + |z| + 1)$ et $|z| \geq 0$, on a $|z|^n = 1$ si et seulement si $|z| = 1$.
Les racines n$^{\text{ièmes}}$ de 1 sont les nombres complexes $w_k = e^{\frac{2ik\pi}{n}}$ avec $k \in \mathbb{N}$.
$e^{\frac{2ik\pi}{n}} = e^{\frac{2ik'\pi}{n}}$ si et seulement si $\frac{2k'\pi}{n} - \frac{2k\pi}{n} = 2p\pi$ avec $p \in \mathbb{Z}$.
$w_k = w_k$, si et seulement si $k' = k + np$ avec $p \in \mathbb{Z}$.
On obtient donc toutes les racines n$^{\text{ièmes}}$ de 1 en donnant à k, n valeurs consécutives par exemple $k \in \{0, 1, \ldots, n-1\}$ (et elles sont bien distinctes). ■

Interprétation géométrique

Les points M_k d'affixe $w_k = e^{\frac{2ik\pi}{n}}$ sont les points du cercle unité tels que $\frac{2k\pi}{n}$ soit une mesure (en radians) de l'angle orienté $(\vec{i}, \overrightarrow{OM}_k)$.
M_{k+1} est l'image de M_k par la rotation de centre O et d'angle $\frac{2\pi}{n}$. On a $M_0M_1 = M_1M_2 = \cdots = M_{n-1}M_0 = \left|e^{\frac{2i\pi}{n}} - 1\right| = 2\sin\frac{\pi}{n}$.
$\left(\text{on remarque que } \left|e^{\frac{2i\pi}{n}} - 1\right| = \left|e^{\frac{i\pi}{n}}\right| \left|e^{\frac{i\pi}{n}} - e^{-\frac{i\pi}{n}}\right| = 2\sin\frac{\pi}{n}\right)$.

Exemples :

1. Les racines cubiques de l'unité sont 1, $j = e^{\frac{2i\pi}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, $j^2 = \overline{j} = e^{-\frac{2i\pi}{3}}$. Leurs images forment un triangle équilatéral.
2. Les racines quatrièmes de l'unité sont 1, $i = e^{i\frac{\pi}{2}}$, $-1 = e^{i\pi}$, $-i = e^{-i\frac{\pi}{2}}$. Leurs images forment un carré.

Proposition 2.5.3 *La somme des racines $n^{ièmes}$ de l'unité est nulle.*

Preuve : D'après la formule donnant la somme des n premiers termes d'une suite géométrique, on a :

$$\sum_{k=0}^{n-1} e^{\frac{2ik\pi}{n}} = \frac{1-e^{2i\frac{n\pi}{n}}}{1-e^{i\frac{2\pi}{n}}} = 0$$

■

2.5.2 Racines n$^{\text{ièmes}}$ d'un nombre complexe

Si $Z = 0$, 0 est la seule racine n$^{\text{ième}}$ de Z.

Proposition 2.5.4 *Tout nombre complexe non nul Z d'argument α possède exactement n racines $n^{ièmes}$, à savoir les nombres complexes $z_k = \sqrt[n]{|z|}e^{i\theta_k}$ où $\theta_k = \frac{\alpha}{n} + \frac{2k\pi}{n}$ avec $k \in \{0, 1, \ldots, n-1\}$.*

Preuve : Soit z une racine n$^{\text{ième}}$ de Z sous sa forme trigonométrique $z = |z|e^{i\theta}$. On a l'écriture trigonométrique $Z = |Z|e^{i\alpha}$. $|z|^n e^{in\theta} = |Z|e^{i\alpha}$ s'écrit $\left\{ \begin{array}{lcl} |z|^n & = & |Z| \\ n\theta & = & \alpha + 2k\pi \quad \text{avec} \quad k \in \mathbb{Z} \end{array} \right.$.
En S2 dans le cours "Fonction de la variable réelle", on montrera que pour tout $n \in \mathbb{N}$ et pour tout $r \in \mathbb{R}_+^*$ il existe un unique réel positif appelé racine n$^{\text{ième}}$ de r et noté $\sqrt[n]{r}$ ou $(r)^{\frac{1}{n}}$ tel que $(r)^n = r$.
Ainsi, comme $|z| \geq 0$, $\quad |z|^n = Z$ équivaut à $|z| = \sqrt[n]{|Z|}$. Les racines n$^{\text{ièmes}}$ de Z sont les nombres complexes $z_k = \sqrt[n]{|Z|}e^{i\frac{\alpha}{n}+\frac{2ik\pi}{n}}$ avec $k \in \mathbb{Z}$.
On a $z_k = z_0 w_k$ avec $z_0 = \sqrt[n]{|Z|}e^{i\frac{\alpha}{n}}$ et $w_k = e^{\frac{2ik\pi}{n}}$. Comme $z_0 \neq 0$, $z_k = z_{k'}$ si et seulement si $w_k = w_{k'}$.
D'après la démonstration précédente $z_k = z_{k'}$ si et seulement si $k' = k + np$ avec $p \in \mathbb{Z}$.
On obtient toutes les racines n$^{\text{ièmes}}$ de z en donnant à k, n valeurs consécutives par exemple $k \in \{0, 1, \ldots, n-1\}$. ■

Corollaire 2.5.5 *Si a est une racine $n^{ième}$ de Z avec $z \neq 0$ alors les racines $n^{ièmes}$ de Z sont les nombres complexes a, aw_1, $aw_1^2, \ldots,$ aw_1^{n-1} avec $w_1 = e^{\frac{2i\pi}{n}}$.*

Corollaire 2.5.6 *La somme des racines $n^{ièmes}$ d'un nombre complexe non nul est nulle.*

2.5.3 Racines carrées d'un nombre complexe

D'après ce qui précède, tout nombre complexe non nul Z possède deux racines carrées opposées. (L'une se déduit de l'autre en multipliant par $e^{i\pi}$). Leur calcul effectif à l'aide de la méthode précédente n'est possible que si l'on peut écrire facilement z sous la forme trigonométrique, ce qui est rare. La méthode suivante a l'avantage d'être plus systématique.
Posons $Z = X + iY$, avec $(X, Y) \in \mathbb{R}^2$ et cherchons $z = x + iy$, avec $(x, y) \in \mathbb{R}^2$ tel que $z^2 = Z$.

$$x^2 - y^2 + 2ixy = X + iY \quad \text{s'écrit} \quad \left\{ \begin{array}{lcll} x^2 - y^2 & = & X & (1) \\ 2xy & = & Y & (2) \end{array} \right.$$

De plus, $|z|^2 = |Z| \quad$ s'écrit $\quad x^2 + y^2 = \sqrt{X^2 + Y^2} \quad$ (3).
Les relations (1) et (3) donnent x et y au signe près. La relation (2) permet d'apparier les signes de x et de y.

2.5.4 Equation du second degré

On cherche à résoudre (E) $az^2+bz+c=0$ avec $a\neq 0$ et $(a,b,c)\in\mathbb{C}^3$. On note Δ le nombre complexe b^2-4ac.
Δ est appelé le discriminant complexe du trinôme $T(2)=az^2+bz+c$.

Proposition 2.5.7 *Si $\Delta=0$ alors (E) admet une unique solution $z=-\frac{b}{2a}$.*
Si $\Delta\neq 0$ alors (E) admet deux solutions distinctes z_1 et z_2 qui sont données par les formules :

$$z_1=-\frac{b}{2a}+\frac{\delta}{2a} \quad \text{et} \quad z_2=-\frac{b}{2a}+\frac{\delta}{2a} \quad \text{avec } \delta \text{ racine carrée de } \Delta.$$

Preuve : On peut écrire le trinôme sous sa forme canonique.

$$az^2+bz+c=a\left(z+\frac{b}{2a}\right)^2-\frac{b^2}{4a}+c$$

(E) équivaut à $\left(z+\frac{b}{2a}\right)^2=\frac{b^2-4ac}{4a^2}=\frac{\Delta}{(2a)^2}$.
Si $\Delta=0$, l'équation a une seule solution $z=-\frac{b}{2a}$.
Si $\Delta\neq 0$, le nombre complexe Δ a deux racines carrées δ et $-\delta$. L'équation a deux solutions $z_1=\frac{-b+\delta}{2a}$ et $z_2=\frac{-b-\delta}{2a}$. ■

Remarque 2.5.8 *Les formules sont les mêmes que celles donnant les solutions d'une équation du second degré à coefficients réels ; mais le calcul des racines carrées du discriminant complexe constitue une étape supplémentaire.*

Proposition 2.5.9 *L'application $\theta\to e^{i\theta}$ est un morphisme du groupe $(\mathbb{R},+)$ dans le groupe des nombres complexes de module 1 muni de la multiplication.*

On démontrera ce résultat en exercice.

Chapitre 3

Relations

Définition 3.0.10 *Soient E et F deux ensembles. Une relation R correspond à une propriété caractéristique des éléments d'une partie $G \subset E \times F$. G est appelé le graphe de la relation R. Autrement dit : Dire que $(x, y) \in G$ correspond à "x et y vérifient la relation R" ce qui sera noté xRy. Donc*

$$G = \{(x, y) \in E \times F : xRy\}.$$

Exemple : $E = F = \{1, 2, 3\}$, $R =<$. Nous avons que $1 < 2$, $1 < 3$, $2 < 3$ donc $G = \{(1, 2), (1, 3), (2, 3)\}$.

Définition 3.0.11 *Si $E = F$, on dit que l'on a une relation R sur l'ensemble E.*

Définition 3.0.12 *Une relation R sur un ensemble E est dite*
- *reflexive si pour tout $x \in E$, xRx.*
- *symétrique si pour tous $x, y \in E$, xRy implique yRx.*
- *antisymétrique si pour tous $x, y \in E$, xRy et yRx implique $x = y$.*
- *transitive si pour tous $x, y, z \in E$, (xRy et yRz) implique xRz.*

3.1 Relations d'ordre

Définition 3.1.1 *On dit qu'une relation R sur E est une relation d'ordre si R est reflexive, antisymétrique et transitive.*

Exemple : La relation xRy définie sur $\mathbb{R}$ par $xRy \iff x \leq y$ est une relation d'ordre sur $\mathbb{R}$.

Définition 3.1.2 *On dit qu'une relation d'ordre R est totale si pour tous $x, y \in E$ xRy ou yRx.*

Exemple : $x \leq y$ est une relation d'ordre totale sur $\mathbb{R}$.

Exemple : Sur $\mathbb{R}^2$ l'on introduit l'ordre lexicographique

$$(x, y)R(x', y') \iff (x < x' \text{ ou } (x = x' \text{ et } y \leq y')).$$

Il s'agit bien d'une relation d'ordre sur $\mathbb{R}^2$.

Preuve : Il est évident que R est reflexive. Montrons que R est antisymétrique : Supposons que $(x, y)R(x', y')$ et $(x', y')R(x, y)$. Alors $x \leq x'$ et $x' \leq x$, donc $x = x'$. Par définition de R, nous avons alors $y \leq y'$ et $y' \leq y$, donc $y = y'$. Montrons finalement que R est transitive : Supposons que $(x, y)R(x', y')$ et $(x', y')R(x'', y'')$. Alors $x \leq x'$ et $x' \leq x''$, donc $x \leq x''$. Si $x < x'$ et $x' < x''$, alors $x < x''$ et c'est terminé. Si $x = x' = x''$, alors $y \leq y' \leq y''$, donc $y \leq y''$, et nous avons encore $(x, y)R(x'', y'')$. Sinon, $x = x'$ et $x' < x''$, donc $x < x''$, donc c'est bon. Pareil pour $x < x'$ et $x' = x''$. ∎

Exemple : Soit $\mathcal{P}(E)$ l'ensemble des parties (c'est-à-dire des sous-ensembles) d'un ensemble E. On considère la relation R sur $\mathcal{P}(E)$ définie par ARB si et seulement si $A \subset B$.

On vérifie qu'il s'agit d'une relation d'ordre qui n'est pas totale si E possède au moins deux éléments. En effet, si $a \neq b \in E$, alors $A = \{a\}$ et $B = \{b\}$ ne sont pas en relation.

3.2 Relations d'équivalence

Définition 3.2.1 *On dit qu'une relation R sur E est une relation d'équivalence si R est reflexive, symétrique et transitive. Dans ce cas, on notera aussi bien xRy ou $x \equiv y(modR)$.*

Exemple :

1. Soit $E = \mathbb{R}$ et $xRy \iff x = y$. Il s'agit bien d'une relation d'équivalence.
2. Soit $E = \mathbb{R}$ et $xRy \iff |x| = |y|$. Il s'agit bien d'une relation d'équivalence.

Exemple :

1. Soit $E = \mathbb{Z}$. La relation définie par xRy si et seulement si $x - y$ est un multiple de 2 est une relation d'équivalence.
2. Sur $\mathbb{Z}$, xRy ssi $x - y$ est impair n'est pas une relation d'équivalence (pas de reflexivité).
3. Soit $k \in \mathbb{N}$ fixé. La relation R définie sur $\mathbb{Z}$ par xRy ssi $x - y$ est un multiple de k est une relation d'équivalence que l'on note $x \equiv y[\text{ mod } k]$. On dira aussi x est congru à y modulo k.

3.3 Classes d'équivalence

Définition 3.3.1 *Soit R une relation d'équivalence sur E et $a \in E$. On note $\dot{a} := \{y \in E : yRa\}$. On dit que $\dot{a}$ est la classe d'équivalence de a.*

Proposition 3.3.2 *Si $b \in \dot{a}$, alors $\dot{b} = \dot{a}$.*

Preuve : Soit $c \in \dot{a}$. Alors cRa. Or bRa, donc par transitivité cRb donc $c \in \dot{b}$. D'où $\dot{a} \subset \dot{b}$. On montre de la même manière que $\dot{b} \subset \dot{a}$. ∎

3.4 Partitions

Soit I un ensemble non vide, appelé *ensemble d'indices*, et E un ensemble. Une *famille d'ensembles inclus dans E indexée par I* est une application Φ de I dans $\mathcal{P}(E)$. Si $i \in I$, on note $A_i = \Phi(i)$ l'image de i. Alors $A_i \subset E$.

Exemple : Si $I = \{1, \ldots, n\}$, nous avons donc $A_1, \ldots, A_n$.

Notation : Nous notons

$$\bigcup_{i \in I} A_i := \{x \in E : \exists i \in I : x \in A_i\},$$

$$\bigcap_{i \in I} A_i := \{x \in E : \forall i \in I,\ x \in A_i\}.$$

Définition 3.4.1 *On appelle* partition de E *toute famille $(A_i)_{i \in I}$ de sous-ensembles de E indexée par I vérifiant que pour tout $i \neq j$ $A_i \cap A_j = \emptyset$ et $\bigcup_{i \in I} A_i = E$.*

Théorème 3.4.2 *Soit R une relation d'équivalence sur E. Alors les classes d'équivalence de R forment une partition de E.*

Preuve : Montrons d'abord que $\dot{a} \cap \dot{b} = \emptyset$ ou bien $\dot{a} = \dot{b}$: Si $x \in \dot{a} \cap \dot{b}$ alors xRa et xRb donc aRb donc $\dot{a} = \dot{b}$. De plus, pour tout $x \in E$, $x \in \dot{x}$, donc E est bien la réunion de toutes les classes d'équivalence. ■

Exemple : Considérons sur $\mathbb{Z}$ la relation d'équivalence définie par xRy ssi $x - y$ est multiple de 2. Alors on a deux classes d'équivalence $\dot{0} = \{2n : n \in \mathbb{Z}\}$ et $\dot{1} = \{2n + 1 : n \in \mathbb{Z}\}$.

Théorème 3.4.3 *Soit $(A_i)_{i\in I}$ une partition de E. Alors il existe une relation d'équivalence R sur E dont les A_i sont les classes d'équivalence.*

Preuve : Définissons R par

$$xRy \text{ ssi } \exists i : (x \in A_i \text{ et } y \in A_i).$$

■

Les deux théorèmes précédents signifient donc que se donner une relation d'équivalence sur un ensemble E est la même chose que se donner une partition de cet ensemble.

Définition 3.4.4 *L'ensemble des classes d'équivalence de E pour la relation R est noté E/R et appelé ensemble quotient de E par R.*

Exemple : Soit R la relation d'équivalence sur $\mathbb{Z}$ définie par xRy ssi $x - y$ est un multiple de k. On note $k\mathbb{Z} := \{kn : n \in \mathbb{Z}\}$. L'ensemble quotient de $\mathbb{Z}$ par R est noté $\mathbb{Z}/k\mathbb{Z}$.

Proposition 3.4.5 *Soit $k \in \mathbb{N}$. $\mathbb{Z}/k\mathbb{Z}$ possède k éléments :*

$$\mathbb{Z}/k\mathbb{Z} = \{\dot{0}, \dot{1}, \ldots, (\dot{k-1})\} = \{k\mathbb{Z}, 1 + k\mathbb{Z}, \ldots, (k-1) + k\mathbb{Z}\}.$$

Preuve : Soit $n \in \mathbb{Z}$. On effectue la division euclidienne de n par k : $n = qk + r$ où $0 \leq r \leq k - 1$. Alors $n \in \dot{r}$. Par ailleurs, $\dot{0}, \dot{1}, \ldots, (\dot{k-1})$ définissent des classes distinctes ; en effet, supposons que $\dot{n} = \dot{m}$ avec $0 \leq n \leq k - 1$ et $0 \leq m \leq k - 1$; on a donc $-(k - 1) \leq n - m \leq k - 1$. Comme $n - m$ est multiple de k, la seule possibilité est $n - m = 0$. ■

3.5 Compatibilité d'une relation d'équivalence avec une loi interne $*$ sur E

Définition 3.5.1 *Soit $*$ une loi interne sur E. On dit que R est compatible avec $*$ si pour tout a, b aRb implique que pour tout $x \in E$, $(a * x)R(b * x)$ et $(x * a)R(x * b)$.*

Définition 3.5.2 (et Proposition) *Si R est compatible avec $*$, on peut définir sur E/R la loi $\dot{*}$ de la façon suivante : Soient $\dot{c}$ et $\dot{c'} \in E/R$. Choisissons $a \in \dot{c}$ et $a' \in \dot{c'}$. Posons*

$$\dot{c}\dot{*}\dot{c'} := (\dot{a * a'}).$$

Preuve : Pour définir correctement la loi $\dot{*}$, il faut vérifier que cette définition ne dépend pas du choix de a et a' : Soient $b \in \dot{c}$ et $b' \in \dot{c'}$. Alors $(\dot{b * b'}) = (\dot{b * a'})$ car $b'Ra'$ implique que $(b * b')R(b * a')$. Ensuite $(\dot{b * a'}) = (\dot{a * a'})$ car bRa implique $(b * a')R(a * a')$.

La classe d'équivalence $\dot{c}\dot{*}\dot{c'}$ ne dépend donc pas du représentant choisi dans les classes de $\dot{c}$ et $\dot{c'}$. ■

Exemple : Considérons $\mathbb{Z}$ que l'on munit de l'addition classique et de la relation $x\mathcal{R}y \Leftrightarrow (x-y$ est un multiple de 3). Alors on sait que $\mathbb{Z}/3\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}\}$. Vérifions que cette relation est compatible avec l'addition :

Soient $(a,b) \in \mathbb{Z}^2$ tels que $a\mathcal{R}b$, et soit $x \in \mathbb{Z}$. On a $(a+x)-(b+x) = a-b$, dont on sait qu'il est multiple de 3. Donc $(a+x)\mathcal{R}(b+x)$.

Dans ce cas, cela donne la loi $\dot{+}$ suivante : $\dot{0}\dot{+}\dot{1} = (0 \dot{+} 1) = \dot{1}$.
$\dot{1}\dot{+}\dot{1} = (1 \dot{+} 1) = \dot{2}$.
$\dot{1}\dot{+}\dot{2} = (1 \dot{+} 2) = \dot{3} = \dot{0}$.
$\dot{2}\dot{+}\dot{2} = \dot{4} = \dot{1}$.

Proposition 3.5.3 *Si $(E,*)$ est un groupe et si R est compatible avec $*$, alors $(E/R, \dot{*})$ est un groupe. De plus, si $*$ est commutative, alors $\dot{*}$ l'est.*

Preuve : $\dot{*}$ est clairement une loi de composition interne associative (car $*$ est associative).

Soit e l'élément neutre pour $*$, et montrons que $\dot{e}$ est l'élément neutre pour $\dot{*}$ sur $E/\mathcal{R}$. Soit $\dot{x}$ une classe d'équivalence, dont un représentant est x. Alors $\dot{x}\dot{*}\dot{e} = (x * e) = \dot{x}$, et de même on a $\dot{e}\dot{*}\dot{x} = (e * x) = \dot{x}$, donc $\dot{e}$ est élément neutre.

Soit $\dot{x}$ une classe d'équivalence, dont un représentant est x. Considérons x', l'inverse de x pour $*$. Alors $\dot{x}\dot{*}\dot{x'} = (x * x') = \dot{e}$, et $\dot{x'}\dot{*}\dot{x} = (x' * x) = \dot{e}$. Donc $\dot{x'}$ est la classe d'équivalence inverse de $\dot{x}$ pour $\dot{*}$. Tout élément de $E/\mathcal{R}$ a donc un inverse. ■

De même on a le résultat suivant concernant les anneaux :

Proposition 3.5.4 *Si $(A,+,*)$ est un anneau et si R est compatible avec $+$ et $*$, alors $(A/R, \dot{+}, \dot{*})$ est un anneau. De plus, si $*$ est commutative, alors $\dot{*}$ l'est également.*

Preuve : La preuve est la même que dans la proposition précédente. ■

3.6 Application aux groupes : le théorème de Lagrange

La notion de relation d'équivalence permet de démontrer un assez joli résultat qui met en lumière les relations entre théorie des groupes (finis) et arithmétique, à savoir que le cardinal d'un sous-groupe divise le cardinal du groupe. Nous allons le montrer ci-dessous. Auparavant, rappelons que l'on appelle *groupe fini* tout groupe ne comportant qu'un nombre fini d'éléments. On notera $\mathrm{Card}(E)$ le nombre d'éléments d'un ensemble fini E.

Théorème 3.6.1 (Théorème de Lagrange) *Soit $(G,\cdot)$ un groupe fini et H un sous-groupe de G. Alors $\mathrm{Card}(H)$ est un diviseur de $\mathrm{Card}(G)$.*

Preuve : On note e l'élément neutre de G. Pour x et y dans G, on note xRy la relation "il existe un élément a de H tel que $y = ax$".

On montre facilement qu'il s'agit d'une relation d'équivalence sur G. En effet, d'une part, pour tout $x \in G$, xRx car il suffit de prendre $a = e \in H$ dans la définition de R car H est un sous-groupe donc contient e. La relation R est donc *réflexive*.

D'autre part, si xRy, il existe $a \in H$ tel que $y = ax$. Il existe donc $b = a^{-1} \in H$ car H s.g., donc contient les inverses de ses éléments, tel que $x = a^{-1}y = by$. Donc R est *symétrique*.

Enfin, si xRy, il existe $a \in H$ tel que $y = ax$. Si yRz, il existe $b \in H$ tel que $z = by$. On pose alors $c = ba$. On a $z = by = bax = cx$ avec $c \in H$ car H s.g.. Donc R est *transitive*.

La relation R est donc une relation d'équivalence. On sait donc grâce au théorème 3.4.2 que l'ensemble des classes d'équivalence modulo R forment une partition de G.

Soit $\dot{x}$ une telle classe pour un représentant $x \in G$ et soit f_x l'application de H dans $\dot{x}$ définie par $f_x(a) = ax$. L'application f_x est clairement à valeurs dans $\dot{x}$. D'autre part, f_x est injective. En effet,

$$f_x(a) = f_x(a') \Rightarrow ax = a'x \Rightarrow a = a'.$$

De plus, $\mathrm{Card}(H)$ est fini. Donc f_x est injective ssi elle est bijective. En définitive, $\mathrm{Card}(\dot{x}) = \mathrm{Card}(H)$. Toutes les classes d'équivalences ont donc le même nombre d'éléments : le nombre d'éléments de H. Si on désigne par n leur nombre, on a donc

$$\mathrm{Card}(G) = n\,\mathrm{Card}(H).$$

■

Corollaire 3.6.2 *Soit G un groupe dont le cardinal est un nombre premier. Alors G ne possède pas d'autres sous-groupes que ses sous-groupes triviaux.*

Chapitre 4

Nombres premiers, PPCM, PGCD

4.1 Nombres premiers, Décomposition en facteurs premiers

Définition 4.1.1 *Soient $n, m \in \mathbb{Z}^*$. On dit que n divise m (et on note $n|m$) si le reste de la division euclidienne de m par n est nul.*

Définition 4.1.2 *Soit $n \in \mathbb{Z}^*$. On note D_n l'ensemble des diviseurs de n. On a toujours $\{-1, 1, -n, n\} \subset D_n$. On dit que $n \neq 0, 1$, est premier ssi $D_n = \{-1, 1, -n, n\}$.*

Exemple : $2, 3, 5, 7, 11, 13, 17, \ldots$ sont des nombres premiers.

Proposition 4.1.3 *Tout entier naturel $n \geq 2$ admet au moins un diviseur premier. Tout entier naturel $n \geq 2$ non premier admet au moins un diviseur premier p tel que $p^2 \leq n$. Il en est de même pour les entiers ≤ -2.*

Preuve : Notons D_n^+ les diviseurs de n plus grands que 2. Nous avons $n \in D_n^+$, donc $D_n^+ \neq \emptyset$, $D_n^+ \subset \mathbb{N}$. Par les axiomes de $\mathbb{N}$ (voir chapitre 1), D_n^+ possède donc un plus petit élément m. Montrons que m est premier.

Raisonnons par l'absurde : Si d divise m, et si $d \geq 2$, alors d divise n. Donc $d \in \Delta_n$, donc $d \geq m$, contradiction.

Soit maintenant $n \geq 2$, n non premier. Soit p le plus petit diviseur de n. Donc $n = pd$ et d divise n, donc $d \geq p$, donc $n \geq p^2$. ∎

Proposition 4.1.4 *L'ensemble des nombres premiers est infini.*

Preuve : Raisonnons par l'absurde et notons $\{p_1, \ldots, p_N\}$ l'ensemble des nombres premiers. Alors $n := p_1 \cdot \ldots \cdot p_N + 1$ doit admettre un diviseur premier p. Mais le reste de la division euclidienne de n par p_i est toujours égal à 1. Contradiction. ∎

Théorème 4.1.5 (Décomposition en facteurs premiers) *Tout entier naturel $n \neq 0, 1$ peut s'écrire comme produit fini de nombres premiers. Il en est de même pour les entiers ≤ -2.*

De plus, cette décomposition est unique, à l'ordre des facteurs près.

Preuve : Récurrence sur n. Pour $n = 2$, nous avons $2 = 2$, donc l'affirmation est vraie. On suppose le résultat vrai pour tout entier appartenant à $\{1, \ldots, n\}$. Considérons $n + 1$. Si $n + 1$ est premier, il n'y a rien à montrer. Sinon, on sait qu'il existe p premier qui divise $n + 1$. Mais $p \geq 2$, donc $(n + 1)/p \leq n$. L'hypothèse de récurrence s'applique. Donc $(n + 1)/p = p_1 \cdot \ldots \cdot p_k$, d'où $n + 1 = p \cdot p_1 \cdot \ldots \cdot p_k$.

L'unicité de la décomposition sera démontrée dans la section 4.5. ∎

4.2 Etude de $\mathbb{Z}/n\mathbb{Z}$

Rappelons la relation d'équivalence suivante sur $\mathbb{Z}$: Soit $n \in \mathbb{N}$ fixé, alors

$$xRy \text{ si et seulement si } x - y \text{ est un multiple de } n.$$

L'ensemble quotient de $\mathbb{Z}$ par R est noté $\mathbb{Z}/n\mathbb{Z}$.

De plus, $(\mathbb{Z}, +, \times)$ est un anneau muni des opérations $+$ et $\times$ usuelles.

Proposition 4.2.1 *Les lois $+$ et $\times$ sont compatibles avec R sur $\mathbb{Z}$.*

Preuve : Soient $(a, b) \in \mathbb{Z}^2$ tels que $a\mathcal{R}b$, et soit $x \in \mathbb{Z}$.

On a $(a + x) - (b + x) = a - b$, dont on sait qu'il est multiple de n. Donc $(a + x)\mathcal{R}(b + x)$, et $+$ est compatible avec R.

On a aussi $a \times x - b \times x = (a - b) \times x$. Comme $a - b$ est un multiple de n, $a \times x - b \times x$ est encore un multiple de n. Par suite, $(a \times x)R(b \times x)$, et $\times$ est compatible avec R. ■

Rappelons alors que sur $\mathbb{Z}/n\mathbb{Z}$, on peut définir deux lois internes $\dot{+}$ et $\dot{\times}$ par

$$\dot{k}\dot{+}\dot{k'} := (\dot{k + k'})$$

et

$$\dot{k}\dot{\times}\dot{k'} := (\dot{k \times k'}).$$

Ces définitions ne dépendent pas des représentants choisis.

On obtient donc, comme application de la proposition 3.5.4 :

Proposition 4.2.2 $(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times})$ *est un anneau commutatif unitaire.*

Remarque 4.2.3 *Le lecteur vérifiera que $(\mathbb{Z}/n\mathbb{Z}, \dot{+})$ est isomorphe au groupe des racines n-ièmes de l'unité muni de la multiplication.*

Remarque 4.2.4 *Nous omettrons à partir de maintenant d'indiquer les $\dot{}$ et noterons $+$ au lieu de $\dot{+}$, $\times$ ou $\cdot$ au lieu de $\dot{\times}$. Remarquons que $\dot{1}$ est un élément neutre pour la multiplication dans $\mathbb{Z}/n\mathbb{Z}$.*

Nous rappellons qu'un anneau A est dit *intègre* si $(\forall a, b \in A : ab = 0) \Leftrightarrow (a = 0 \text{ ou } b = 0)$.

Proposition 4.2.5 $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$, $n \neq 0, 1$ *est un anneau intègre ssi n est premier.*

Preuve :

- Si n n'est pas premier, alors $n = pq$ avec $p \neq n$, $q \neq n$. Alors $\dot{n} = \dot{p}\dot{q} = \dot{0}$ et $\dot{p} \neq \dot{0}$, $\dot{q} \neq \dot{0}$.
- Choisissons p le plus petit entier strictement positif vérifiant $\dot{p}\dot{q} = \dot{0}$ pour un certain q, avec $0 < p, q < n$. Effectuons la division euclidienne de n par p ; on a $n = ap + b$, $0 \leq b < p$. En multipliant cette égalité par q, et en prenant les classes d'équivalence, on obtient
$$(\dot{qn}) = (\dot{apq}) + (\dot{bq}),$$
or $(\dot{qn}) = (\dot{apq}) = \dot{0}$, donc $(\dot{bq}) = \dot{b} \cdot \dot{q} = \dot{0}$. Grâce à la minimalité de p, on en déduit que nécessairement $\dot{b} = \dot{0}$. Comme $b < n$, on a $b = 0$, ce qui implique que $n = ap$, donc n n'est pas premier.

■

Corollaire 4.2.6 *Un nombre premier p divise $n \cdot m$ ssi p divise n ou p divise m.*

Preuve : Supposons que p divise le produit $n \cdot m$. Alors $\dot{n}\dot{m} = \dot{0}$ dans $\mathbb{Z}/p\mathbb{Z}$ ce qui est équivalent à $\dot{n} = \dot{0}$ ou $\dot{m} = \dot{0}$ dans $\mathbb{Z}/p\mathbb{Z}$. ■

Proposition 4.2.7 *$(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ est un corps ssi p est premier.*

Preuve : Si c'est un corps, alors il est intègre, et la proposition 4.2.5 nous dit que p est premier.

Il reste à montrer que si p premier, alors $\mathbb{Z}/p\mathbb{Z}$ est un un corps. Soit n tel que $\dot{n} \neq \dot{0}$. Il faut trouver un élément inverse pour la multiplication dans $\mathbb{Z}/p\mathbb{Z}$. Considérons la fonction $\Phi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ définie par $\Phi(\dot{m}) := \dot{n}\dot{m}$. Alors Φ est injective : $\Phi(\dot{m}) = \Phi(\dot{m'})$ ssi $\dot{n}(m - m') = \dot{0}$ ssi $\dot{m} = \dot{m'}$, car $\mathbb{Z}/p\mathbb{Z}$ intègre. Φ est donc nécessairement bijective. En particulier, il existe $\dot{m}$ tel que $\Phi(\dot{m}) = \dot{1}$ donc $\dot{m}\dot{n} = \dot{1}$. ■

Dorénavant, on notera $m = n\ [p]$ pour dire que deux nombres entiers n et m sont dans la même classe d'équivalence dans $\mathbb{Z}/p\mathbb{Z}$.

Théorème 4.2.8 (Petit théorème de Fermat) *Soit p premier et $a \in \mathbb{Z}$ non multiple de p. Alors $a^{p-1} \equiv 1[p]$.*

Preuve : a non multiple de p, donc $\dot{a} \neq \dot{0}$ dans $\mathbb{Z}/p\mathbb{Z}$. Or $a^{p-1} \equiv 1[modp]$ est équivalent à $\dot{a}^{p-1} = \dot{1}$ dans $\mathbb{Z}/p\mathbb{Z}$. Comme $\dot{a} \neq \dot{0}$, la fonction définie par

$$\Phi(\dot{n}) := \dot{a}\dot{n}$$

est bijective. Nous avons donc que

$$\Phi(\dot{1}) \cdot \ldots \cdot \Phi((p \dot{-} 1)) = \dot{a}\dot{1} \cdot \ldots \cdot \dot{a}(p \dot{-} 1) = \dot{a}^{p-1}(\dot{1} \cdot \ldots \cdot (p \dot{-} 1)).$$

Or, comme Φ bijective et $\Phi(\dot{0}) = \dot{0}$, alors

$$\Phi(\dot{1}) \cdot \ldots \cdot \Phi((p \dot{-} 1)) = \dot{1} \cdot \ldots \cdot (p \dot{-} 1)$$

d'où $\dot{a}^{p-1} = \dot{1}$. ■

4.3 Le PPCM : plus petit commun multiple

Remarque 4.3.1 *Rappels sur les groupes : Soit $(G, +)$ un groupe.*

1. *Si H_1 et H_2 sont des sous-groupes de $(G, +)$, alors $H_1 + H_2 = \{x \in G :$ il existe $v \in H_1$ et $w \in H_2$ tels que $x = v + w\}$ forme un sous-groupe de $(G, +)$.*
2. *Si H_1 et H_2 sont des sous-groupes de $(G, +)$, alors $H_1 \cap H_2 = \{x \in G : x \in H_1$ et $x \in H_2\}$ forme un sous-groupe de $(G, +)$.*

Remarque 4.3.2 *Rappel sur $(\mathbb{Z}, +)$:*

1. *Tous les sous-groupes de $(\mathbb{Z}, +)$ sont de la forme $a\mathbb{Z}$, avec $a \in \mathbb{N}$.*
2. *a divise b ssi $b\mathbb{Z} \subset a\mathbb{Z}$.*

Définition 4.3.3 *Soient $(a_1, a_2) \in (\mathbb{Z}^*)^2$, alors $a_1\mathbb{Z} \cap a_2\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, il est donc de la forme $a\mathbb{Z}$, avec $a \in \mathbb{N}$.*

a est appelé le PPCM de a_1 et de a_2. On note $a = a_1 \vee a_2$.

Attention, on définit le PGCD de deux nombres entiers comme un nombre positif, même si ces deux nombres sont négatifs.

Exemple : Pour $a_1 = -4$, $a_2 = 6$, nous avons

$$a_1\mathbb{Z} = \{\ldots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\}$$

et

$$a_2\mathbb{Z} = \{\ldots, -18, -12, -6, 0, 6, 12, 18, \ldots\},$$

donc $a = 12$. Remarquons que $6 = 2 \cdot 3$ et $-4 = -2 \cdot 2$, et $a = 2 \cdot 2 \cdot 3$.

Proposition 4.3.4 *On a les propriétés suivantes :*

1. $a \vee a = |a|$. *et* $a \vee 0 = 0$.
2. $a \vee b = b \vee a$.
3. $a \vee (b \vee c) = (a \vee b) \vee c$.
4. $c(a \vee b) = ca \vee cb$.
5. a *et* b *divisent* m *implique que* $a \vee b$ *divise* m.

Preuve : 1., 2. et 3. découlent de la définition du ppcm.

4. L'affirmation est évidente pour $c = 0$.

Soit $c \neq 0$. Alors $n \in ca\mathbb{Z} \cap cb\mathbb{Z}$ est équivalent à $n = cak = cbk'$ donc $n/c \in a\mathbb{Z} \cap b\mathbb{Z}$ ce qui revient à dire que $n \in c(a\mathbb{Z} \cap b\mathbb{Z})$.

5. a et b divisent m ssi $m\mathbb{Z} \subset a\mathbb{Z}$ et $m\mathbb{Z} \subset b\mathbb{Z}$ donc $m\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$. ■

4.4 Le PGCD : plus grand commun diviseur

Définition 4.4.1 *Soient* $(a_1, a_2) \in (\mathbb{Z}^*)^2$. *On remarque que* $(a_1\mathbb{Z} + a_2\mathbb{Z}, +)$ *est un sous-groupe de* $(\mathbb{Z}, +)$. *Il est donc de la forme* $d\mathbb{Z}$, *pour un certain* $d \in \mathbb{N}$.

On note $d = a_1 \wedge a_2$, *et* d *est appelé le PGCD de* a_1 *et de* a_2.

On a donc $a_1\mathbb{Z} + a_2\mathbb{Z} = d\mathbb{Z}$.

Attention, on définit le PGCD de deux nombres entiers comme un nombre positif, même si ces deux nombres sont négatifs.

Exemple : $a_1 = 4$, $a_2 = 6$. Alors $2 = 6 - 4 \in a_1\mathbb{Z} + a_2\mathbb{Z}$, donc $2\mathbb{Z} \subset a_1\mathbb{Z} + a_2\mathbb{Z}$. D'autre part, tous les éléments de $a_1\mathbb{Z}$ et de $a_2\mathbb{Z}$ sont divisibles par 2, donc $a_1\mathbb{Z} + a_2\mathbb{Z} \subset 2\mathbb{Z}$.

Proposition 4.4.2 *On a les propriétés suivantes :*

1. $a \wedge a = |a|$, $a \wedge 0 = |a|$, $a \wedge 1 = 1$, $(a \wedge b) \wedge c = a \wedge (b \wedge c)$, $a \wedge b = b \wedge a$.
2. $a \wedge b$ *divise* a *et divise* b.
3. a *divise* b *ssi* $a \wedge b = |a|$.
4. $c(a \wedge b) = ca \wedge cb$.
5. *(*c *divise* $a \wedge b$*) ssi (*c *divise* a *et* c *divise* b*)*.

Preuve : 1. découle directement de la définition de PGCD.

2. Remarquons que $a\mathbb{Z}$ est toujours un sous-groupe de $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, donc d divise a. De même, d divise b.

3. Si a divise b, alors $b\mathbb{Z} \subset a\mathbb{Z}$ donc $a\mathbb{Z} + b\mathbb{Z} = a\mathbb{Z}$. Inversement, si $a \wedge b = |a|$, alors $a\mathbb{Z} + b\mathbb{Z} = a\mathbb{Z}$, donc $b\mathbb{Z} \subset a\mathbb{Z}$, donc a divise b.

4. est facile.

5. On sait que c divise $a \wedge b$ ssi $(a \wedge b)\mathbb{Z} \subset c\mathbb{Z}$. Donc $a\mathbb{Z} \subset c\mathbb{Z}$ et $b\mathbb{Z} \subset c\mathbb{Z}$. c divise donc a et aussi b. Inversement, si $a\mathbb{Z} \subset c\mathbb{Z}$ et $b\mathbb{Z} \subset c\mathbb{Z}$, alors $a\mathbb{Z} + b\mathbb{Z} \subset c\mathbb{Z}$. Donc c divise $a \wedge b$. ■

4.5 Nombres premiers entre eux, Théorème de Bezout, Théorème chinois

Proposition 4.5.1 *On sait que $d = a \wedge b$ ssi $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. En particulier, comme $d \in d\mathbb{Z}$, on peut donc trouver $k, l \in \mathbb{Z}$ tels que*

$$d = ak + bl.$$

Ceci est l'identité de Bezout.

Réciproquement : *Si $(\exists k, l \in \mathbb{Z} : ak + bl$ divise a et $b)$ alors $a \wedge b = ak + bl$.*

Preuve : Le sens direct est évident.

Pour la réciproque : Notons $f := ak+bl$. Donc $f \in a\mathbb{Z}+b\mathbb{Z}$. D'où $f\mathbb{Z} \subset a\mathbb{Z}+b\mathbb{Z} = (a\wedge b)\mathbb{Z}$. Par conséquent, $a \wedge b$ divise f. D'autre part, comme f divise a et b, f divise aussi $a \wedge b$. Comme la relation "est divisible par" est une relation d'ordre, f divise $a \wedge b$ et $a \wedge b$ divise f implique que $f = a \wedge b$. ■

Définition 4.5.2 *On dit que a et b sont premiers entre eux ssi $a \wedge b = 1$. On dit que $a_1, \ldots, a_n$ sont premiers entre eux si $a_1 \wedge \ldots \wedge a_n = 1$.*

Le théorème suivant est une conséquence immédiate de l'identité de Bezout.

Théorème 4.5.3 (Théorème de Bezout)

$$a \wedge b = 1 \Leftrightarrow \exists k, l \in \mathbb{Z} : 1 = ak + bl.$$

Remarque 4.5.4 *Il n'y a pas unicité de k, l car $a(k + ub) + b(l - ua) = 1$ pour tout $u \in \mathbb{Z}$.*

Théorème 4.5.5 (Théorème de Gauss) *Si $a \wedge b = 1$ et si a divise bc, alors a divise c.*

Preuve : D'après l'égalité de Bezout, $a \wedge b = 1$ est équivalent à $\exists u, v \in \mathbb{Z}$ tels que $au + bv = 1$. Donc $c = cau + cbv$. Or, a divise bc et a divise cau, donc a divise c. ■

Théorème 4.5.6 (Application du Théorème de Gauss) *La décomposition d'un nombre entier $n \geq 2$ en facteurs premiers est unique (à l'ordre des facteurs près).*

Ce théorème signifie que tout entier n supérieur ou égal à 2 s'écrit sous la forme

$$n = p_1^{\alpha_1} \ldots p_k^{\alpha_k},$$

avec p_1, ..., p_k suite strictement croissante de nombres premiers et chaque α_i étant supérieur ou égal à 1.

Théorème 4.5.7 (Théorème chinois) *Soit n et m deux nombres premiers entre eux. Alors $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est isomorphe à $\mathbb{Z}/nm\mathbb{Z}$ par un isomorphisme d'anneaux.*

Preuve : Considérons l'application

$$\begin{aligned} f : \mathbb{Z}/nm\mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ q &\mapsto (q\ [n], q\ [m]). \end{aligned}$$

On peut définir sur $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ des lois $+$ et $\times$ en faisant agir les lois sur chaque coordonnée.

Alors f est clairement un morphisme d'anneaux entre $(\mathbb{Z}/nm\mathbb{Z}, +, \times)$ et $(\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}, +, \times)$.

Remarquons que le cardinal de $\mathbb{Z}/nm\mathbb{Z}$ est le même que celui de $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$, c'est-à-dire nm. Pour obtenir le résultat, il reste à montrer que f est injectif.

Supposons que $f(q) = (0, 0)$. Alors q est un multiple de n et de m. Comme n et m sont premiers entre eux, par le théorème de Gauss, q est un multiple de nm, donc $q = 0\ [nm]$.

■

4.6 Formules explicites pour les PPCM et PGCD

Retrouvons maintenant la formule connue depuis le lycée pour le PPCM de deux nombres entiers.

Proposition 4.6.1 *Si $a = p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}$, $\alpha_i \geq 0$, et $b = p_1^{\beta_1} \cdot \ldots \cdot p_n^{\beta_n}$, $\beta_i \geq 0$, p_i premiers, alors*

$$a \vee b = p_1^{\max(\alpha_1,\beta_1)} \cdot \ldots \cdot p_n^{\max(\alpha_n,\beta_n)}. \tag{4.1}$$

Preuve : Notons $c := p_1^{\max(\alpha_1,\beta_1)} \cdot \ldots \cdot p_n^{\max(\alpha_n,\beta_n)}$. Il est clair que c est un multiple de a et de b, donc de $a \vee b$.
Notons $a \vee b = p_1^{\gamma_1} \cdot \ldots \cdot p_n^{\gamma_n}$. Alors a divise $a \vee b$. Comme $p_1^{\alpha_1} \wedge (p_2^{\gamma_2} \cdot \ldots \cdot p_n^{\gamma_n}) = 1$, le théorème de Gauss implique que $p_1^{\alpha_1}$ divise $p_1^{\gamma_1}$. Donc $\gamma_1 \geq \alpha_1$. De même : $\gamma_i \geq \alpha_i$ $\forall i$. On montre de la même manière que $\gamma_i \geq \beta_i$ pour tout i. Donc $\gamma_i \geq \max(\alpha_i, \beta_i)$. $a \vee b$ est donc un multiple de c. c étant le plus petit multiple de a et de b, on a égalité. ■

Faisons le même travail que pour le PPCM, et retrouvons la formule donnant le PGCD à partir des décompositions en facteurs premiers de a et b :

Proposition 4.6.2 *Si $a = p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}$, $\alpha_i \geq 0$, et $b = p_1^{\beta_1} \cdot \ldots \cdot p_n^{\beta_n}$, $\beta_i \geq 0$, p_i premiers, alors*

$$a \wedge b = p_1^{\min(\alpha_1,\beta_1)} \cdot \ldots \cdot p_n^{\min(\alpha_n,\beta_n)}. \tag{4.2}$$

Preuve : On note $c := p_1^{\min(\alpha_1,\beta_1)} \cdot \ldots \cdot p_n^{\min(\alpha_n,\beta_n)}$. c divise a et b donc aussi $a \wedge b$. Ecrivons $a \wedge b = p_1^{\gamma_1} \cdot \ldots \cdot p_n^{\gamma_n}$. Alors $p_1^{\gamma_1}$ divise a. Comme $p_1^{\gamma_1} \wedge (p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}) = 1$, le théorème de Gauss implique que $p_1^{\gamma_1}$ divise $p_1^{\alpha_1}$. Donc $\gamma_1 \leq \alpha_1$. Pareil : $\gamma_i \leq \alpha_i$ $\forall i$. On montre de la même manière que $\gamma_i \leq \beta_i$ pour tout i. Donc $\gamma_i \leq \min(\alpha_i, \beta_i)$. $a \wedge b$ divise donc c. Conclusion : $a \wedge b = c$. ■

Comme application des propositions 4.6.1 et 4.6.2, on voit :

Proposition 4.6.3 *Pour tous nombres entiers (a, b) supérieurs à 1, on a $(a \vee b)(a \wedge b) = ab$. Si a et b sont de signe quelconque, on a $(a \vee b)(a \wedge b) = |ab|$.*

Preuve : Cela découle du fait que pour tous nombres réels p et q, $\min(p, q) + \max(p, q) = p + q$. ■

4.7 L'algorithme d'Euclide

On suppose $a > b \geq 0$. Nous effectuons des divisions euclidiennes successives.

$$\begin{array}{rcl}
\text{de } a \text{ par } b : & a = bq_1 + r_1, & \text{avec } 0 \leq r_1 < b, \\
\text{de } b \text{ par } r_1 : & b = r_1 q_2 + r_2, & \text{avec } 0 \leq r_2 < r_1, \\
\text{de } r_1 \text{ par } r_2 : & r_1 = r_2 q_3 + r_3, & \text{avec } 0 \leq r_3 < r_2, \\
\text{etc jusqu'à} & \ldots & \\
\text{de } r_{n-3} \text{ par } r_{n-2} : & r_{n-3} = r_{n-2} q_{n-1} + r_{n-1}, & \text{avec } 0 \leq r_{n-3} < r_{n-2}, \\
\text{de } r_{n-2} \text{ par } r_{n-1} : & r_{n-2} = r_{n-1} q_n + r_n, & \text{avec } 0 \leq r_{n-2} < r_{n-1}, \\
\text{de } r_{n-1} \text{ par } r_n : & r_{n-1} = r_n q_{n+1} + 0, & \text{avec } r_{n+1} = 0.
\end{array}$$

Proposition 4.7.1 *On a $a \wedge b = r_n$, i.e. le PGCD de a et b et le dernier reste non nul dans cette série de divisions euclidiennes.*

Preuve : Montrons tout d'abord qu'il existe bien un rang n tel que $r_{n+1} = 0$. Par construction, $\forall p \geq 1$, $0 \leq r_{p+1} < r_p$. La suite $(r_p)_{p\geq 1}$ est donc positive, et strictement décroissante tant qu'elle n'est pas égale à 0. Il existe donc bien un rang à partir n tel que $\forall p \geq n+1$, $r_p = 0$.

On a que $a\mathbb{Z} + b\mathbb{Z} = b\mathbb{Z} + r_1\mathbb{Z}$, car a s'écrit comme un multiple de b et un multiple de r_1.

De même, $b\mathbb{Z} + r_1\mathbb{Z} = r_1\mathbb{Z} + r_2\mathbb{Z}$, car b s'écrit comme un multiple de $r_1 + r_2$.

En itérant ce raisonnement, on trouve que $a\mathbb{Z} + b\mathbb{Z} = b\mathbb{Z} + r_1\mathbb{Z} = r_1\mathbb{Z} + r_2\mathbb{Z} = \ldots = r_{n-1}\mathbb{Z} + r_n\mathbb{Z} = r_n\mathbb{Z}$, car $r_{n+1} = 0$.

Par définition, $a\mathbb{Z} + b\mathbb{Z} = r_n\mathbb{Z}$ signifie que $r_n = a \wedge b$. ■

Exemple : Prenons $a = 125$ et $b = 35$. Alors

$$125 = 35 \cdot 3 + 20,$$

$$35 = 20 \cdot 1 + 15,$$

$$20 = 15 \cdot 1 + 5,$$

$$15 = 5 \cdot 3 + 0.$$

Donc $a \wedge b = 5$.

Chapitre 5

Polynômes

5.1 L'ensemble des polynômes à une indéterminée

5.1.1 Définitions

Définition 5.1.1 *On appelle* **polynôme à une indéterminée et coefficients dans** $\mathbb{K}$ *ou plus simplement polynôme, toute expression algébrique de la forme*

$$a_p X^p + a_{p-1} X^{p-1} + \cdots + a_1 X + a_0,$$

avec $a_i \in \mathbb{K}$ *pour tout* $i \in \{0, \cdots, p\}$.

- *Les scalaires* a_i *sont appelés* **coefficients** *du polynôme.*
- *S'il existe, le plus grand indice* i *tel que* $a_i \neq 0$ *s'appelle* **degré de** P *et est noté* $\deg P$.
- *Si tous les coefficients* a_i *sont nuls,* P *est appelé* **polynôme nul** *et est noté* 0. *Par convention,* $\deg 0 = -\infty$.
- *Un polynôme de la forme* $P = a_0$ *avec* $a_0 \in \mathbb{K}$ *est appelé* **polynôme constant**. *Si* $a_0 \neq 0$, *son degré est* 0.

L'ensemble des polynôme à une indéterminée et coefficients dans $\mathbb{K}$ *est noté* $\mathbb{K}[X]$.

Exemples :

- $X^3 - \pi X + 3/2$ est un polynôme de degré 3.
- Si $n \in \mathbb{N}^*$, $X^n - 1$ est un polynôme de degré n
- 1 est un polynôme de degré 0.

Remarque 5.1.2 *Nous serons amenés par la suite à additionner des degrés de polynômes. Comme l'application* deg *est à valeurs dans* $\mathbb{N} \cup \{-\infty\}$, *il faut étendre la définition de l'addition. On adopte la convention suivante pour* $n \in \mathbb{N} \cup \{-\infty\}$ *:*

$$-\infty + n = -\infty.$$

Définition 5.1.3 *Les polynômes ne comportant qu'un seul terme non nul (i.e du type* $P = a_p X^p$*) sont appelés* **monômes**.

Remarque : Tout polynôme est donc une somme finie de monômes.

Définition 5.1.4 *Soit* $P = a_p X^p + \cdots + a_0$ *avec* $a_p \neq 0$ *un polynôme. On appelle* **terme dominant** *de* P *le monôme* $a_p X^p$. *Si le coefficient* a_p *du terme dominant est* 1, *on dit que* P *est un* **polynôme unitaire**.

Remarque 5.1.5 *On adopte la convention que l'on ne change pas un polynôme* P *en lui ajoutant un ou plusieurs monômes à coefficients nuls. Par exemple, on ne fera pas la distinction entre*

$$X^4 - X + 1 \quad et \quad 0X^5 + X^4 + 0X^2 - X + 1.$$

5.1.2 Opérations sur $\mathbb{K}[X]$

Nous allons munir $\mathbb{K}[X]$ de deux lois internes "+" et "$*$", et d'une loi externe "$\cdot$".

a) Addition de deux polynômes :

Définition 5.1.6 *Soit $P = a_nX^n + \cdots + a_0$ et $Q = b_nX^n + \cdots + b_0$ avec $n \in \mathbb{N}$. On définit alors le polynôme $P + Q$ par*

$$P + Q \stackrel{\text{déf}}{=} (a_n + b_n)X^n + \cdots + (a_1 + b_1)X + (a_0 + b_0).$$

Remarque : Dans la définition ci-dessus, il n'est pas restrictif de faire commencer les expressions des polynômes P et Q par un monôme de même degré n (voir la remarque 5.1.5 ci-dessus)

Proposition 5.1.7 *Soit P et Q deux polynômes de $\mathbb{K}[X]$. Alors on a*

$$\deg(P + Q) \leq \max(\deg P, \deg Q).$$

De plus, si $\deg P \neq \deg Q$ alors $\deg(P + Q) = \max(\deg P, \deg Q)$.

Preuve : Notons $p = \deg P$ et $q = \deg Q$.
- Si $p > q$, le coefficient du terme dominant de $P + Q$ est a_p donc $\deg(P + Q) = \deg P$.
- Si $p < q$, le coefficient du terme dominant de $P + Q$ est b_q donc $\deg(P + Q) = \deg Q$.
- Si $p = q$, le monôme de plus haut degré dans l'expression de $P + Q$ est $(a_p + b_p)X^p$. Donc $\deg(P + Q) \leq p$. Si $b_p = -a_p$, ce monôme est nul et l'on a donc $\deg(P + Q) < p$.

■

b) Multiplication de deux polynômes :

Considérons deux monômes $P = a_pX^p$ et $Q = b_qX^q$. Si l'on interprète ces deux monômes comme des fonctions de la variable réelle ou complexe X, il est naturel de définir le produit de P par Q comme étant le monôme $P * Q \stackrel{\text{déf}}{=} a_pb_qX^{p+q}$.

Plus généralement, on définit le produit de deux polynômes de la façon suivante :

Définition 5.1.8 *Étant donnés deux polynômes $P = a_pX^p + \cdots + a_0$ et $Q = b_qX^q + \cdots + b_0$, on définit le polynôme $P * Q$ par $P * Q = c_rX^r + \cdots + c_0$ avec $r = p + q$ et, pour $k \in \{0, \cdots, r\}$,*

$$c_k = \sum_{i+j=k} a_ib_j = \sum_{i=0}^{k} a_ib_{k-i} = \sum_{j=0}^{k} a_{k-j}b_j.$$

Remarque : Si P ou Q est nul, on a donc $P * Q = 0$.

La proposition suivante est une conséquence immédiate de la définition de "$*$" :

Proposition 5.1.9 *Soit P et Q deux polynômes de $\mathbb{K}[X]$. Alors on a*

$$\deg(P * Q) = \deg P + \deg Q.$$

c) Multiplication d'un polynôme par un scalaire :

Définition 5.1.10 *Soit $P = a_pX^p + \cdots + a_0$ un polynôme de $\mathbb{K}[X]$, et $\lambda \in \mathbb{K}$. On définit alors le polynôme $\lambda \cdot P$ par*

$$\lambda \cdot P \stackrel{\text{déf}}{=} \sum_{i=0}^{p} \lambda a_iX^i.$$

Le lecteur prouvera sans difficulté le résultat suivant :

Proposition 5.1.11 *Soit P un polynôme et λ un scalaire <u>non nul</u>. Alors $\deg(\lambda \cdot P) = \deg P$.*

5.1.3 Propriétés algébriques de $\mathbb{K}[X]$

Proposition 5.1.12 *$(\mathbb{K}[X], +, *)$ est un anneau commutatif.*

Preuve : Montrons déjà que $(\mathbb{K}[X], +)$ est un groupe commutatif.
- Le polynôme nul est clairement l'élément neutre pour l'addition.
- Si $P = a_pX^p + \cdots + a_0$, le polynôme $-P \overset{\text{déf}}{=} -a_pX^p + \cdots - a_1X - a_0$ vérifie $P + (-P) = 0$.
- L'associativité et la commutativité résultent de celles de l'addition sur $\mathbb{K}$.

Reste à étudier les propriétés de la multiplication "$*$".
- De la définition de la multiplication sur $\mathbb{K}[X]$, on déduit facilement que le polynôme $P = 1$ est l'élément neutre pour "$*$".
- Commutativité : considérons $P = a_pX^p + \cdots + a_0$ et $Q = b_qX^q + \cdots + b_0$. Notons $r = p + q$, $P * Q = c_rX^r + \cdots + c_0$ et $Q * P = d_rX^r + \cdots + d_0$. Alors on a

$$\forall k \in \{0, \cdots, r\},\ c_k = \sum_{i+j=k} a_ib_j = \sum_{j+i=k} b_ja_i = d_k$$

  Donc $P * Q = Q * P$.
- Associativité : Soit $P = a_pX^p + \cdots + a_0$, $Q = b_qX^q + \cdots + b_0$ et $R = c_rX^r + \cdots + c_0$. Soit $U \overset{\text{déf}}{=} (P * Q) * R$ et $V \overset{\text{déf}}{=} P * (Q * R)$. Notons d_ℓ les coefficients de U, et e_m ceux de V. Enfin, notons f_s les coefficients de $P * Q$, et g_t ceux de $Q * R$. Alors on a

$$\begin{array}{rcl} d_\ell &=& \sum_{s+k=\ell} f_sc_k \\ &=& \sum_{s+k=\ell} \left(\sum_{i+j=s} a_ib_j\right) c_k \\ &=& \sum_{i+j+k=\ell} a_ib_jc_k. \end{array} \quad \left| \quad \begin{array}{rcl} e_\ell &=& \sum_{i+t=\ell} a_ig_t \\ &=& \sum_{i+t=\ell} a_i \left(\sum_{j+k=t} b_jc_k\right) \\ &=& \sum_{i+j+k=\ell} a_ib_jc_k. \end{array} \right.$$

  Donc $d_\ell = e_\ell$, d'où $U = V$.
- Distributivité de la multiplication sur l'addition : Définissons P, Q, R comme ci-dessus et posons $U \overset{\text{déf}}{=} (P + Q) * R$ et $V \overset{\text{déf}}{=} P * R + Q * R$. Notons encore d_ℓ les coefficients de U, et e_m ceux de V. Alors on a

$$d_\ell = \sum_{i+j=\ell} (a_i + b_i)c_j = \sum_{i+j=\ell} (a_ic_j + b_ic_j) = \sum_{i+j=\ell} a_ic_j + \sum_{i+j=\ell} b_ic_j = e_\ell.$$

  Donc $U = V$.

■

À titre d'exercice, le lecteur pourra établir la

Proposition 5.1.13 *L'anneau $(\mathbb{K}[X], +, *)$ vérifie les propriétés supplémentaires suivantes pour tout $(\lambda, \mu) \in \mathbb{K}2$ et $(P, Q) \in \mathbb{K}[X]^2$:*

1. $(\lambda + \mu) \cdot P = \lambda \cdot P + \mu \cdot P$,
2. $\lambda \cdot (P + Q) = \lambda \cdot P + \lambda \cdot Q$,
3. $\lambda \cdot (\mu \cdot P) = (\lambda\mu) \cdot P$,
4. $1 \cdot P = P$,
5. $\lambda \cdot (P * Q) = (\lambda \cdot P) * Q = P * (\lambda \cdot Q)$.

On dit que $(\mathbb{K}[X], +, *, \cdot)$ est une **algèbre**.

Ainsi, multiplier un polynôme P par un scalaire λ est équivalent à le multiplier par le polynôme constant $\lambda \cdot 1$. On peut donc sans danger noter la multiplication interne $*$ et la multiplication externe $\cdot$ par le même symbole.

Enfin, $(\mathbb{K}[X], +, *, \cdot)$ jouit de la propriété suivante qui est primordiale :

Proposition 5.1.14 *Soit (P, Q) un couple de polynômes tel que $P * Q = 0$. Alors $P = 0$ ou $Q = 0$. On dit que $(\mathbb{K}[X], +, *, \cdot)$ est une* **algèbre intègre**.

Preuve : Soit donc (P, Q) tel que $P * Q = 0$. Alors on a $\deg P + \deg Q = \deg(P * Q) = -\infty$. Donc $\deg P$ ou $\deg Q$ vaut $-\infty$, ce qui est exactement la propriété demandée. ■

Notations : Dorénavant, on omettra les symboles "$*$" et "$\cdot$". Ainsi PQ désignera $P * Q$, et λP désignera $\lambda \cdot P$.

5.2 Division des polynômes

Définition 5.2.1 *On dit que le polynôme A est* **divisible** *par le polynôme B s'il existe un polynôme Q tel que $A = BQ$. Dans ce cas, on note $B \mid A$ (voir remarque[1]) et l'on dit que A est* **multiple** *de B (ou que B est* **diviseur** *de A). Le polynôme Q est parfois noté $\frac{A}{B}$ ou A/B.*

Remarques :

1. Le polynôme nul est divisible par tous les polynômes. En revanche seul le polynôme nul est divisible par le polynôme nul.
2. Dans le cas où A et B sont tous les deux non nuls, $B|A$ entraîne $\deg B \leq \deg A$.

Proposition 5.2.2 *Soit A et B, deux polynômes non nuls. Si $A \mid B$ et $B \mid A$ alors A et B sont proportionnels, c'est-à-dire qu'il existe $\lambda \in \mathbb{K}^*$ tel que $A = \lambda B$. On dit que A et B sont* **associés**.

Preuve : D'après la remarque ci-dessus, on a à la fois $\deg A \leq \deg B$ et $\deg B \leq \deg A$. Donc A et B sont de même degré. Comme $B \mid A$, on en déduit que $A = BQ$ avec $\deg Q = 0$. Autrement dit Q est un polynôme constant (et non nul car A n'est pas nul). ■

Remarque 5.2.3 *Deux polynômes unitaires associés sont forcément égaux.*

Exercice : Prouver la remarque ci-dessus.

Proposition 5.2.4 *Soit B un polynôme non nul, et A un multiple de B de même degré que B. Alors A et B sont associés.*

Preuve : Elle reprend la dernière partie de celle de la proposition 5.2.2. ■

Théorème 5.2.5 (Division euclidienne) *Soit A et B deux polynômes avec B non nul. Alors il existe un unique couple (Q, R) de polynômes tel que*

$$A = BQ + R \quad et \quad \deg R < \deg B.$$

Le polynôme Q est appelé **quotient** *de la division de A par B, R est le* **reste**, *B, le diviseur, et A, le* **dividende**.

Preuve : On va d'abord prouver l'unicité du couple (Q, R), puis son existence.

Unicité : Supposons que $A = BQ + R = BQ' + R'$ avec $\deg R < \deg B$ et $\deg R' < \deg B$. Alors on a $R - R' = B(Q' - Q)$. Donc $\deg(R - R') = \deg B + \deg(Q' - Q)$.

Si $Q \neq Q'$, alors on en déduit que $\deg(R - R') \geq \deg B$.

Donc d'après la proposition 5.1.7, $\max(\deg R, \deg R') \geq \deg B$, ce qui contredit la définition de R ou de R'. Donc $Q = Q'$, puis $R = R'$.

1. Lire "B divise A" et non pas le contraire !

Existence : Fixons un polynôme $B = b_m X^m + \cdots + b_0$ de degré $m \geq 1$ (le cas B constant non nul étant évident). L'existence du couple (Q, R) vérifiant les propriétés voulues se montre par récurrence sur le degré de A. Pour $n \in \mathbb{N}$, on note $(\mathcal{P}_n)$ l'hypothèse de récurrence suivante :

$$(\mathcal{P}_n)\ \ (\forall A \in \mathbb{K}[X], \deg A \leq n) \Rightarrow (\exists Q \in \mathbb{K}[X], \exists R \in \mathbb{K}[X] \mid A = BQ + R \text{ et } \deg R < \deg B)\,.$$

Il est clair que $(\mathcal{P}_{m-1})$ est vraie. En effet, il suffit de choisir $Q = 0$ et $R = A$.
Soit maintenant $n \geq m$. Supposons $(\mathcal{P}_{n-1})$ vraie et démontrons $(\mathcal{P}_n)$. Le polynôme A est de la forme $A = a_n X^n + \cdots + a_0$ avec $a_n \neq 0$. Comme $n \geq m$ et $b_m \neq 0$, l'expression

$$A' \overset{\text{déf}}{=} A - \frac{a_n}{b_m} X^{n-m} B$$

est bien un polynôme, et son degré est au plus $n-1$. D'après $(\mathcal{P}_{n-1})$, il existe donc deux polynômes Q' et R' tels que $A' = Q'B + R'$ et $\deg R' < \deg B$. On en déduit que

$$A = \underbrace{\left(\frac{a_n}{b_m} X^{n-m} + Q'\right)}_{\overset{\text{déf}}{=} Q} B \ + \ \underbrace{R'}_{\overset{\text{déf}}{=} R}\ ,$$

ce qui démontre $(\mathcal{P}_n)$. ∎

La démonstration ci-dessus suggère un procédé de construction itératif permettant de calculer Q et R. En effet, au cours de la récurrence, on a vu comment ramener la division d'un polynôme de degré n à celle d'un polynôme de degré moins élevé (au plus $n-1$). En pratique, on peut donc calculer le couple (Q, R) en "posant" la division comme dans $\mathbb{N}$, les puissances de X jouant le rôle des puissances de 10.

Illustrons nos propos par un exemple.

Exemple : Division de $4X^5 - 7X^3 + 8X^2 - 1$ par $X^3 - 4X^2 + 2X + 3$.

$$\begin{array}{rrrrrr|l}
4X^5 + & 0X^4 - & 7X^3 + & 8X^2 + & 0X - & 1 & X^3 - 4X^2 + 2X + 3 \\
\cline{7-7}
 & 16X^4 - & 15X^3 - & 4X^2 + & 0X - & 1 & \\
 & & 49X^3 - & 36X^2 - & 48X - & 1 & 4X^2 + 16X + 49 = Q \\
 & & R = & 160X^2 - & 146X - & 148 &
\end{array}$$

Donc $4X^5 - 7X^3 + 8X^2 - 1 = (X^3 - 4X^2 + 2X + 3)(4X^2 + 16X + 49) + 160X^2 - 146X - 148$.

Définition 5.2.6 *On rappelle qu'un sous-ensemble I de $\mathbb{K}[X]$ est un* **idéal** *de $(\mathbb{K}[X], +, *)$ si*

1. *I est un sous-groupe de $(\mathbb{K}[X], +)$,*
2. *I est stable par multiplication par n'importe quel polynôme de $\mathbb{K}[X]$.*

Exemple : Pour $B \in \mathbb{K}[X]$, on note $B\mathbb{K}[X]$ l'ensemble des multiples de B. Il est facile de vérifier que $B\mathbb{K}[X]$ est un idéal de $\mathbb{K}[X]$. En particulier, le singleton $\{0\}$ est un idéal.

Nous laissons au lecteur le soin de montrer la proposition suivante :

Proposition 5.2.7 *Soit A et B deux polynômes. Alors $A \mid B$ si et seulement si $B\mathbb{K}[X] \subset A\mathbb{K}[X]$.*

Théorème 5.2.8 *Soit I un idéal de $(\mathbb{K}[X], +, *)$ non réduit à $\{0\}$. Alors il existe un unique polynôme P unitaire tel que $I = P\mathbb{K}[X]$. Le polynôme P est appelé* **générateur unitaire** *de I.*

On dit que $(\mathbb{K}[X], +, *)$ est un **idéal principal** *.*

Preuve : Soit I un idéal de $(\mathbb{K}[X], +, *)$ non réduit à $\{0\}$. On note

$$E = \{\deg A \mid A \in I \backslash \{0\}\}.$$

L'ensemble E est une partie non vide de $\mathbb{N}$, donc admet un plus petit élément. On en déduit que I admet un polynôme P non nul et de degré minimal. Comme pour tout $\lambda \in \mathbb{K}$, le polynôme λP appartient aussi à I, on peut toujours choisir P unitaire. La stabilité de I par multiplication par les éléments de $\mathbb{K}[X]$ assure que $P\mathbb{K}[X] \subset I$.

Reste à montrer que $I \subset P\mathbb{K}[X]$. Soit donc $A \in I$. Écrivons la division euclidienne de A par P :

$$A = PQ + R \quad \text{avec} \quad \deg R < \deg P.$$

Comme A et PQ appartiennent à I, on a aussi $R \in I$. Mais par ailleurs $\deg R < \deg P$. Vu la définition de P, on conclut que $R = 0$. ■

5.3 PGCD et PPCM

La division euclidienne va nous permettre de définir les notions de PGCD et de PPCM dans l'ensemble des polynômes.

5.3.1 PGCD

Proposition 5.3.1 *Soit A et B deux polynômes non tous les deux nuls. L'ensemble*

$$A\mathbb{K}[X] + B\mathbb{K}[X] \overset{\text{déf}}{=} \left\{AP + BQ \mid P \in \mathbb{K}[X],\ Q \in \mathbb{K}[X]\right\}$$

est un idéal de $\mathbb{K}[X]$ non réduit à $\{0\}$. Son générateur unitaire[2] *D est appelé* **Plus Grand Commun Diviseur** *(ou plus simplement PGCD) de A et de B, et est noté* $\mathrm{PGCD}(A, B)$.

Preuve : Notons $J \overset{\text{déf}}{=} A\mathbb{K}[X] + B\mathbb{K}[X]$. Remarquons que J n'est pas réduit à $\{0\}$ car contient A et B, et que l'un de ces deux polynômes n'est pas nul par hypothèse. Reste à montrer que J est un idéal.

1. Montrons que J est un sous-groupe de $(\mathbb{K}[X], +)$:
   - Il est évident que $0 \in J$.
   - Soit C et C' deux polynômes de J. Alors il existe quatre polynômes P, P', Q et Q' tels que $C = AP + BQ$ et $C' = AP' + BQ'$. Donc
   $$C + C' = A(P+P') + B(Q+Q') \in J.$$
   - Enfin, si $C = AP + BQ$, il est clair que $-C = A(-P) + B(-Q)$, donc $-C \in J$.
2. Stabilité de J par produit :
   Soit $C = AP + BQ$ un élément de J, et R un polynôme quelconque. Alors $RC = A(PR) + B(QR)$ donc $RC \in J$.

On conclut que J est un idéal non réduit à $\{0\}$. Le théorème 5.2.8 assure l'existence d'un unique polynôme unitaire D tel que $A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$. ■

Remarque : On convient que $\mathrm{PGCD}(0, 0) = 0$. Pour tout couple de polynômes (A, B), on a donc $A\mathbb{K}[X] + B\mathbb{K}[X] = \mathrm{PGCD}(A, B)\,\mathbb{K}[X]$.

La proposition suivante justifie l'appellation "PGCD" donnée au générateur unitaire de $A\mathbb{K}[X] + B\mathbb{K}[X]$.

2. Dans certains ouvrages, le caractère unitaire n'est pas imposé au PGCD.

Proposition 5.3.2 *Soit (A, B) un couple de polynômes distinct de $(0, 0)$. Alors* $\mathrm{PGCD}\,(A, B)$ *est l'unique polynôme unitaire vérifiant*

$$\mathrm{PGCD}\,(A,B) \mid A, \quad \mathrm{PGCD}\,(A,B) \mid B \quad et \quad (P \mid A \text{ et } P \mid B) \Rightarrow P \mid \mathrm{PGCD}\,(A,B). \tag{5.1}$$

Preuve : Notons $D = \mathrm{PGCD}\,(A, B)$ et montrons que D vérifie (5.1).

Par définition, $D\mathbb{K}[X] = A\mathbb{K}[X] + B\mathbb{K}[X]$. Comme A et B appartiennent tous les deux à l'ensemble de droite, A et B sont bien des multiples de D. Enfin, si P divise A et B alors, d'après la proposition 5.2.7, $A\mathbb{K}[X] \subset P\mathbb{K}[X]$ et $B\mathbb{K}[X] \subset P\mathbb{K}[X]$. Donc $D\mathbb{K}[X] = A\mathbb{K}[X] + B\mathbb{K}[X] \subset P\mathbb{K}[X]$. Donc P divise D.

Pour montrer l'unicité, considérons un polynôme D' unitaire vérifiant (5.1). On a donc en particulier $D \mid D'$. Mais bien sûr $D' \mid D$ donc D et D' sont associés (cf prop. 5.2.2). Comme D et D' sont unitaires, on a $D = D'$. ∎

Proposition 5.3.3 *Si A et B ne sont pas simultanément nuls et si C est unitaire alors on a*

$$\mathrm{PGCD}\,(AC, BC) = C\,\mathrm{PGCD}\,(A, B).$$

Preuve : Notons $D = \mathrm{PGCD}\,(A, B)$ et $\Delta = \mathrm{PGCD}\,(AC, BC)$. Il suffit alors de remarquer que

$$\Delta\mathbb{K}[X] = AC\mathbb{K}[X] + BC\mathbb{K}[X] = C\,(A\mathbb{K}[X] + B\mathbb{K}[X]) = CD\mathbb{K}[X].$$

∎

Définition 5.3.4 *On dit que deux polynômes A et B sont* **premiers entre eux** *si leur PGCD vaut 1.*

Théorème 5.3.5 (de Bezout) *Deux polynômes A et B sont premiers entre eux si et seulement si il existe deux polynômes U et V tels que $AU + BV = 1$.*

Preuve : $\Longrightarrow$ Si $\mathrm{PGCD}\,(A, B) = 1$ alors par définition du PGCD, on a $A\mathbb{K}[X] + B\mathbb{K}[X] = \mathbb{K}[X]$. Donc $1 \in A\mathbb{K}[X] + B\mathbb{K}[X]$, ce qui signifie qu'il existe U et V tels que $AU + BV = 1$.

$\Longleftarrow$ Si $AU + BV = 1$ alors $1 \in A\mathbb{K}[X] + B\mathbb{K}[X]$. Le générateur unitaire de $A\mathbb{K}[X] + B\mathbb{K}[X]$ est donc un diviseur de 1, donc 1 lui-même. On a donc bien $1 = \mathrm{PGCD}\,(A, B)$. ∎

Proposition 5.3.6 *Pour que le polynôme unitaire D soit le PGCD de A et de B, il faut et il suffit que*

$$D \mid A, \quad D \mid B \quad et \quad \mathrm{PGCD}\,(\frac{A}{D}, \frac{B}{D}) = 1. \tag{5.2}$$

Preuve : Si $D = \mathrm{PGCD}\,(A, B)$, on a bien sûr $D \mid A$ et $D \mid B$. Notons $P = \frac{A}{D}$ et $Q = \frac{B}{D}$. D'après la proposition 5.3.3, on a

$$D = \mathrm{PGCD}\,(A, B) = \mathrm{PGCD}\,(DP, DQ) = D\,\mathrm{PGCD}\,(P, Q).$$

Comme D n'est pas nul, on conclut que $\mathrm{PGCD}\,(P, Q) = 1$.

Réciproquement, supposons que (5.2) soit satisfaite. Alors, la proposition 5.3.3 entraîne

$$\mathrm{PGCD}\,(A, B) = \mathrm{PGCD}\,(D\frac{A}{D}, D\frac{B}{D}) = D\mathrm{PGCD}\,(\frac{A}{D}, \frac{B}{D}) = D.$$

∎

Théorème 5.3.7 (de Bezout généralisé) *Supposons que D unitaire divise A et B avec A et B non tous les deux nuls. Alors on a*

$$D = \mathrm{PGCD}\,(A, B) \iff \exists U \in \mathbb{K}[X],\ \exists V \in \mathbb{K}[X],\ AU + BV = D.$$

Preuve : En appliquant la proposition 5.3.6, on a

$$D = \mathrm{PGCD}\,(A, B) \iff 1 = \mathrm{PGCD}\,(\frac{A}{D}, \frac{B}{D}).$$

Or d'après le théorème de Bezout, on a

$$\mathrm{PGCD}\,(\frac{A}{D}, \frac{B}{D}) = 1 \iff \exists U \in \mathbb{K}[X],\ \exists V \in \mathbb{K}[X],\ \frac{A}{D}U + \frac{B}{D}V = 1,$$

ce qui achève la preuve du théorème. ■

Théorème 5.3.8 (de Gauss) *Si P divise AB et est premier avec A alors P divise B.*

Preuve : Soit B' le polynôme unitaire associé à B. On a

$$\mathrm{PGCD}\,(PB, AB) = B'\,\mathrm{PGCD}\,(P, A) = B'.$$

Par hypothèse, P divise AB, et il est clair que P divise aussi PB. Donc P divise B' et, partant, B. ■

Proposition 5.3.9 *Un polynôme P est premier avec un produit AB si et seulement si P est premier avec A et avec B.*

Preuve : $\Rightarrow$ Supposons P premier avec AB. Soit P' divisant P et A. Alors P' divise aussi AB. Donc $P' \mid \mathrm{PGCD}\,(AB, P)$, i.e $P'|1$. On en déduit que P' est un polynôme constant. Donc P est premier avec A. On établit de même que P est premier avec B.

$\Leftarrow$ On prouve la réciproque par contraposition. Supposons que P ne soit pas premier avec AB. Alors il existe P' divisant P et AB, et tel que $\deg P' \geq 1$. Si P est premier avec A alors P' également. D'après le théorème de Gauss, P' divise donc B. On a donc montré que P' divise à la fois P et B. Comme $\deg P' \geq 1$, cela signifie que P et B ne sont pas premiers entre eux. ■

Remarque 5.3.10 *Une récurrence élémentaire permet de montrer plus généralement qu'un polynôme P est premier avec un produit de polynôme $A_1 \cdots A_k$ si et seulement si il est premier avec chacun des facteurs A_i. Les détails sont laissés en* **exercice**.

5.3.2 L'algorithme d'Euclide

L'*algorithme d'Euclide* est un moyen systématique permettant de calculer le PGCD de deux polynômes. L'outil de base est la *division euclidienne*. L'algorithme repose sur le lemme suivant :

Lemme 5.3.11 *Soit B un polynôme non nul, et A un polynôme quelconque. Notons Q et R le quotient et le reste de la division euclidienne de A par B. Alors on a*

$$\mathrm{PGCD}\,(A, B) = \mathrm{PGCD}\,(B, R).$$

Preuve : Soit D divisant A et B. Comme $R = A - BQ$, le polynôme D divise aussi R. Donc D divise $\mathrm{PGCD}(B, R)$. En choisissant $D = \mathrm{PGCD}(A, B)$, on conclut que $\mathrm{PGCD}(A, B) \mid \mathrm{PGCD}(B, R)$.

Soit maintenant D un polynôme divisant B et R. Comme $A = BQ + R$, on a aussi $D \mid A$. Donc $D \mid \mathrm{PGCD}(A, B)$. On a donc finalement $\mathrm{PGCD}(B, R) \mid \mathrm{PGCD}(A, B)$.

Les deux polynômes $\mathrm{PGCD}(B, R)$ et $\mathrm{PGCD}(A, B)$ sont unitaires et associés. Ils sont donc égaux. ■

Ce lemme indique clairement la stratégie à suivre pour calculer $\mathrm{PGCD}(A, B)$. Quitte à permuter A et B, on peut toujours supposer que $\deg A \geq \deg B$. On procède alors comme suit :

- Si $B = 0$, il n'y a rien à faire : $\mathrm{PGCD}(A, B)$ est égal au polynôme unitaire associé à A.
- Si B n'est pas nul, on effectue la division euclidienne de A par B, ce qui donne deux polynômes Q_0 et R_1 tels que $A = BQ_0 + R_1$ et $\deg R_1 < \deg B$.

Le lemme 5.3.11 montre que $\mathrm{PGCD}(A, B) = \mathrm{PGCD}(B, R_1)$. On reprend le calcul ci-dessus en remplaçant A par B, et B par R_1. En itérant le procédé, on construit deux suites $R_1, R_2, \cdots$ et $Q_0, Q_1, \cdots$ telles que :

$$\begin{array}{lllll}
A & = BQ_0 + R_1 & \text{avec} & \deg R_1 < \deg B, \\
B & = R_1Q_1 + R_2 & \text{avec} & \deg R_2 < \deg R_1, \\
R_1 & = R_2Q_2 + R_3 & \text{avec} & \deg R_3 < \deg R_2, \\
\cdots & \cdots & \cdots & \cdots \\
R_{k-1} & = R_kQ_k + R_{k+1} & \text{avec} & \deg R_{k+1} < \deg R_k, \\
\cdots & \cdots & \cdots & \cdots \\
R_{n-1} & = R_nQ_n + 0. & &
\end{array}$$

Le procédé s'arrête nécessairement au bout d'au plus $\deg P$ étapes car chaque itération diminue d'au moins 1 le degré du reste de la division euclidienne. On a donc finalement

$$\boxed{\mathrm{PGCD}(A, B) = \mathrm{PGCD}(B, R_1) = \cdots = \mathrm{PGCD}(R_k, R_{k+1}) = \cdots = \mathrm{PGCD}(R_n, 0) = R_n.}$$

Exemple : Calculer $\mathrm{PGCD}(X^4 - 1, X^3 - 1)$.

Posons la division euclidienne de $X^4 - 1$ par $X^3 - 1$.

$$\begin{array}{rrrrr|l}
X^4 + & 0X^3 + & 0X^2 + & 0X - & 1 & X^3 + \quad 0X^2 + \quad 0X - \quad 1 \\
\cline{6-6}
 & & & X - & 1 & \quad X
\end{array}$$

Donc $\mathrm{PGCD}(X^4 - 1, X^3 - 1) = \mathrm{PGCD}(X^3 - 1, X - 1)$.

On remarque ensuite que $X^3 - 1$ est divisible par $X - 1$ donc finalement

$$\boxed{\mathrm{PGCD}(X^4 - 1, X^3 - 1) = \mathrm{PGCD}(X^3 - 1, X - 1) = \mathrm{PGCD}(X - 1, 0) = X - 1.}$$

5.3.3 PPCM

Nous laissons au lecteur le soin de prouver le résultat suivant :

Proposition 5.3.12 *Considérons deux polynômes non nuls A et B. Alors l'ensemble $A\mathbb{K}[X] \cap B\mathbb{K}[X]$ est un idéal non réduit à $\{0\}$. Son générateur unitaire*[3] *est appelé* **Plus Petit Commun Multiple** *(ou plus simplement* **PPCM***) de A et B. On le note* $\mathrm{PPCM}(A, B)$.

Remarque : Si A ou B est nul, on a $A\mathbb{K}[X] \cap B\mathbb{K}[X] = \{0\}$. On adopte alors la convention que $\mathrm{PPCM}(A, B) = 0$. Ainsi, on aura toujours $A\mathbb{K}[X] \cap B\mathbb{K}[X] = \mathrm{PPCM}(A, B)\,\mathbb{K}[X]$.

3. Dans certains ouvrages, on n'impose pas au PPCM d'être unitaire

En s'inspirant de la preuve de la proposition 5.1, on obtient le résultat suivant qui explique l'appellation "Plus Petit Commun Multiple" donnée au générateur unitaire de $A\mathbb{K}[X] \cap B\mathbb{K}[X]$.

Proposition 5.3.13 *Soit A et B deux polynômes non nuls. Le PPCM de A et de B est l'unique polynôme unitaire vérifiant la propriété suivante :*

$$A \mid \mathrm{PPCM}\,(A,B), \quad B \mid \mathrm{PPCM}\,(A,B) \quad et \quad (A \mid M \text{ et } B \mid M) \Rightarrow \mathrm{PPCM}\,(A,B) \mid M.$$

À certains égards, le PPCM et le PGCD ont des propriétés très similaires. On a par exemple :

Proposition 5.3.14 *Soit C un polynôme unitaire et A, B deux polynômes. Alors on a*

$$\mathrm{PPCM}\,(AC,BC) = C\,\mathrm{PPCM}\,(A,B).$$

Preuve : Il suffit de remarquer que

$$AC\mathbb{K}[X] \cap BC\mathbb{K}[X] = C\left(A\mathbb{K}[X] \cap B\mathbb{K}[X]\right).$$

■

Proposition 5.3.15 *Soit A et B deux polynômes non nuls. Pour que M unitaire soit le PPCM de A et de B, il faut et il suffit que*

$$A \mid M, \quad B \mid M \quad et \quad \mathrm{PGCD}\left(\frac{M}{A}, \frac{M}{B}\right) = 1.$$

Preuve : $\Rightarrow$ Notons M le PPCM de A et de B. Alors $M\mathbb{K}[X]$ est inclus dans $A\mathbb{K}[X]$ et dans $B\mathbb{K}[X]$. Donc M divise bien A et B. Soit D unitaire divisant M/A et M/B. Alors $AD|M$ et $BD|M$. Donc $\mathrm{PPCM}\,(AD,BD)|M$. Mais d'après la proposition 5.3.14, $\mathrm{PPCM}\,(AD,BD) = D\,\mathrm{PPCM}\,(A,B) = DM$. Donc $D = 1$.

$\Leftarrow$ Soit M un multiple commun unitaire de A et de B vérifiant de plus $\mathrm{PGCD}\,(\frac{M}{A}, \frac{M}{B}) = 1$. D'après le théorème de Bezout, il existe deux polynômes U et V tels que

$$\frac{M}{A}U + \frac{M}{B}V = 1.$$

Multiplions les deux membres de cette égalité par $\mathrm{PPCM}\,(A,B)$. On trouve

$$M\left(U\frac{\mathrm{PPCM}\,(A,B)}{A} + V\frac{\mathrm{PPCM}\,(A,B)}{B}\right) = \mathrm{PPCM}\,(A,B).$$

Donc M divise $\mathrm{PPCM}\,(A,B)$. Comme M est unitaire et est multiple de A et de B, on conclut que $M = \mathrm{PPCM}\,(A,B)$. ■

Proposition 5.3.16 *Soit A et B deux polynômes. Il existe une constante λ non nulle telle que*

$$\lambda AB = \mathrm{PGCD}\,(A,B)\,\mathrm{PPCM}\,(A,B).$$

- *Si de plus A et B sont unitaires, alors $\lambda = 1$.*
- *Si A et B sont premiers entre eux alors AB et $\mathrm{PPCM}\,(A,B)$ sont associés.*

Preuve : Écartons le cas évident où l'un des deux polynômes A et B est nul. On peut alors appliquer la proposition 5.3.15. On en déduit que

$$\mathrm{PGCD}\left(\frac{\mathrm{PPCM}\,(A,B)}{A}, \frac{\mathrm{PPCM}\,(A,B)}{B}\right) = 1. \tag{5.3}$$

Notons λ l'inverse du coefficient du terme dominant de AB. Alors λAB est unitaire, et la proposition 5.3.14 combinée avec (5.3) montre que

$$\mathrm{PGCD}\left(\lambda AB\left(\frac{\mathrm{PPCM}\,(A,B)}{A}\right), \lambda AB\left(\frac{\mathrm{PPCM}\,(A,B)}{B}\right)\right) = \lambda AB.$$

En appliquant la proposition 5.3.3, on constate que le membre de gauche de cette égalité vaut $\mathrm{PPCM}\,(A,B)\,\mathrm{PGCD}\,(A,B)$. ■

5.3.4 Polynômes irréductibles

Au cours des sections qui précèdent, le lecteur a pu constater que l'ensemble $\mathbb{K}[X]$ avait beaucoup de similarités avec l'ensemble $\mathbb{Z}$ des entiers relatifs : les deux ensembles sont des anneaux principaux intègres sur lesquels on peut définir la division euclidienne, le PGCD et le PPCM. Dans cette section, nous allons introduire une classe de polynômes qui jouent dans $\mathbb{K}[X]$ le même rôle que les nombres premiers dans $\mathbb{Z}$: les polynômes irréductibles.

Définition 5.3.17 *On dit qu'un polynôme P est* **irréductible** *si ses seuls diviseurs sont les constantes et les polynômes qui lui sont associés.*

Remarques :

1. À la différence des nombres premiers, les polynômes irréductibles ont une infinité de diviseurs. Mais on notera que ces diviseurs sont triviaux !
2. Tout polynôme de degré 1 est irréductible. En effet, soit P de degré 1, et Q un diviseur de P. Alors $\deg Q \in \{0, 1\}$. Si $\deg Q = 0$ alors Q est une constante, si $\deg Q = 1$ alors $\deg Q = \deg P$ donc P et Q sont associés.

La proposition suivante constitue une "loi du tout ou rien" pour la division par les polynômes irréductibles.

Proposition 5.3.18 *Soit A un polynôme et P un polynôme irréductible ne divisant pas A. Alors P est premier avec A.*

Preuve : Soit B un diviseur commun de A et de P. Comme P est irréductible, B doit être constant, ou associé à P. Le deuxième cas est exclus car on a supposé que P ne divisait pas A. Donc B est constant. On a donc bien $\mathrm{PGCD}\,(A, P) = 1$. ∎

De même que tout entier possède une décomposition en facteurs premiers, tout polynôme a une décomposition en facteurs irréductibles.

Théorème 5.3.19 (Décomposition en facteurs irréductibles) *Soit P un polynôme non constant. Alors il existe un entier $k \geq 1$, k entiers $\alpha_1, \cdots, \alpha_k$ non nuls, k polynômes irréductibles unitaires $P_1, \cdots, P_k$ deux à deux distincts, et $\lambda \in \mathbb{K}\backslash\{0\}$ tels que*

$$P = \lambda \prod_{i=1}^{k} P_i^{\alpha_i}.$$

Cette décomposition, appelée décomposition en facteurs irréductibles, est unique à ordre des facteurs près.

Preuve : On prouve d'abord l'existence puis l'unicité à ordre des facteurs près.

Existence : Elle se fait par récurrence sur le degré de P.

- Si $\deg P = 1$ alors P est irréductible. On pose $k = 1$, $\alpha_1 = 1$ et l'on prend pour P_1 le polynôme unitaire associé à P. Il est de degré 1 donc irréductible.
- Supposons maintenant que le théorème de décomposition soit valable pour tout polynôme de degré compris entre 1 et n. Soit P de degré $n+1$ et $P' \overset{\text{déf}}{=} P/\lambda$ avec λ coefficient du terme dominant de P. Le polynôme P' est unitaire et de degré $n+1$. S'il est irréductible, $P = \lambda P'$ constitue une décomposition de P en facteurs premiers. Sinon, il existe un polynôme A unitaire de degré compris entre 1 et n et divisant P'. On a donc $P' = AB$ avec A et B unitaires et de degré compris entre 1 et

n. D'après l'hypothèse de récurrence, A et B admettent chacun une décomposition en facteurs premiers :

$$A = \prod_{i=1}^{k} A_i^{\alpha_i} \quad \text{et} \quad B = \prod_{i=1}^{\ell} B_i^{\beta_i}.$$

Donc

$$P = \lambda \left(\prod_{i=1}^{k} A_i^{\alpha_i} \right) \left(\prod_{i=1}^{\ell} B_i^{\beta_i} \right).$$

Il ne reste plus qu'à renuméroter les facteurs de la décomposition pour obtenir le résultat voulu.

Unicité : Supposons que P admette *deux* décompositions en facteurs irréductibles :

$$P = \lambda \prod_{i=1}^{k} P_i^{\alpha_i} = \mu \prod_{i=1}^{\ell} Q_i^{\beta_i}.$$

Comme tous les facteurs irréductibles sont unitaires, λ et μ sont égaux au coefficient du terme dominant de P. Donc $\lambda = \mu$. De ce fait, on a

$$\prod_{i=1}^{k} P_i^{\alpha_i} = \prod_{i=1}^{\ell} Q_i^{\beta_i}. \tag{5.4}$$

Par ailleurs, P_1 divise la somme de droite. De la remarque 5.3.10, on déduit que P_1 n'est pas premier avec au moins un des Q_j : il existe j_1 tel que Q_{j_1} et P_1 ne soient pas premiers entre eux. Comme par ailleurs Q_{j_1} et P_1 sont irréductibles et unitaires, cela signifie que $P_1 = Q_{j_1}$. En vertu du caractère intègre de $\mathbb{K}[X]$, on peut donc simplifier l'expression (5.4) par P_1. On itère ce procédé et en $\alpha_1 + \cdots + \alpha_k$ étapes, on parvient à une expression du type $1 = \prod_{j=1}^{\ell} Q_j^{\beta'_j}$ avec $\beta'_j = \beta_j - \alpha_j$. Cela permet de conclure que tous les β'_j sont nuls. Donc les deux décompositions sont identiques à ordre près des facteurs.

■

5.4 Fonctions polynômes

5.4.1 Définition des fonctions polynômes

Jusqu'à présent, nous avons traité les polynômes comme des objets algébriques "abstraits". Ce point de vue permet de manipuler de façon unifiée des objets mathématiques très différents dès lors qu'ils peuvent être interprétés comme des polynômes. Dans cette section, nous allons nous borner à remplacer la variable muette X par des nombres réels ou complexes. Mais vous verrez en deuxième année que l'on peut fort bien remplacer X par une matrice...

Définition 5.4.1 *Soit $P = a_n X^n + \cdots + a_1 X + a_0$ un polynôme de $\mathbb{K}[X]$, et $t \in \mathbb{K}$. On définit alors l'élément $P(t)$ de $\mathbb{K}$ par*

$$P(t) = a_n t^n + \cdots + a_1 t + a_0.$$

On dit que $P(t)$ est obtenu par substitution de t à X.

Proposition 5.4.2 *Soit $t \in \mathbb{K}$ un scalaire fixé. Alors on a pour tous polynômes P et Q, et pour tout scalaire λ :*

1. $P(t)+Q(t)=(P+Q)(t)$,
2. $P(t)Q(t)=(PQ)(t)$,
3. $\lambda P(t)=(\lambda P)(t)$,
4. $1(t)=1$.

Preuve : Vérifions la deuxième relation. Les autres sont immédiates.

Rappelons que si $P=a_pX^p+\cdots+a_1X+a_0$ et $Q=b_qX^q+\cdots+b_1X+b_0$ alors

$$PQ=\sum_{j=0}^{p+q}\Big(\sum_{k+\ell=j}a_kb_\ell\Big)X^j. \tag{5.5}$$

Donc

$$\begin{aligned}(PQ)(t) &= \textstyle\sum_{j=0}^{p+q}\Big(\sum_{k+\ell=j}a_kb_\ell\Big)t^j,\\ &= \textstyle\sum_{j=0}^{p+q}\Big(\sum_{k+\ell=j}(a_kt^k)(b_\ell t^\ell)\Big),\\ &= \Big(\textstyle\sum_{k=0}^{p}a_kt^k\Big)\Big(\sum_{\ell=0}^{q}b_\ell t^\ell\Big)=P(t)Q(t).\end{aligned}$$

■

Définition 5.4.3 *Soit $P\in\mathbb{K}[X]$. L'application*

$$\widetilde{P}\ :\ \left\{\begin{array}{ccc}\mathbb{K} & \longrightarrow & \mathbb{K}\\ t & \longmapsto & P(t)\end{array}\right.$$

est appelée fonction polynôme définie par P sur $\mathbb{K}$.

Remarque : Dans la suite du cours, on ne fera plus la distinction entre le polynôme P qui est un objet algébrique et la fonction polynôme $\widetilde{P}$ qui lui est associée [4].

5.4.2 Racines

Définition 5.4.4 *Soit $a\in\mathbb{K}$ et $P\in\mathbb{K}[X]$. On dit que a est* **racine** *ou* **zéro** *de P si $P(a)=0$.*

Proposition 5.4.5 *Soit $a\in\mathbb{K}$ et $P\in\mathbb{K}[X]$. Pour que a soit une racine de P, il faut et il suffit que $X-a$ divise P.*

Preuve : $\Rightarrow$ Supposons que $P(a)=0$. La division euclidienne de P par $X-a$ donne

$$P=Q(X-a)+R\quad\text{avec}\quad\deg R\leq 0.$$

En substituant a à X dans la relation ci-dessus, on trouve $R(a)=0$. Comme la fonction polynôme R est constante, on conclut que $R=0$.

$\Leftarrow$ Si $X-a\mid P$ alors il existe Q tel que $P=Q(X-a)$, ce qui donne en particulier $P(a)=Q(a)(a-a)=0$. ■

Définition 5.4.6 *Soit $P\in\mathbb{K}[X]$, $a\in\mathbb{K}$ et $k\in\mathbb{N}^*$. On dit que a est racine de P de multiplicité k si $(X-a)^k\mid P$.*

- *Si $k=1$, on parle de racine simple,*
- *Si $k=2$, on dit que a est racine double,*
- *Si $k=3$, on dit que a est racine triple, etc.*

4. La proposition 5.4.2 nous autorise à faire cet abus de notation.

Proposition 5.4.7 *Soit P un polynôme non nul admettant les racines $a_1, \cdots, a_k$ avec multiplicité $\alpha_1, \cdots, \alpha_k$. Alors $\prod_{i=1}^{k}(X-a_i)^{\alpha_i}$ divise P.*

Preuve :

- On sait déjà que $(X-a_1)^{\alpha_1}$ divise P.
- Supposons que $\prod_{i=1}^{j-1}(X-a_i)^{\alpha_i}$ divise P (avec $j \leq k$). Comme les a_i sont deux à deux distincts, les polynômes $(X-a_i)^{\alpha_i}$ sont premiers entre eux deux à deux. La remarque 5.3.10 permet donc d'affirmer que $(X-a_j)^{\alpha_j}$ est premier avec $\prod_{i=1}^{j-1}(X-a_i)^{\alpha_i}$. Comme P est multiple de $(X-a_j)^{\alpha_j}$ par hypothèse, et de $\prod_{i=1}^{j-1}(X-a_i)^{\alpha_i}$, P est également multiple du PPCM de ces deux polynômes qui, d'après la proposition 5.3.16, vaut $\prod_{i=1}^{j}(X-a_i)^{\alpha_i}$.

Nous venons donc de montrer par récurrence sur j que $\prod_{i=1}^{k}(X-a_i)^{\alpha_i}$ divise P. ■

Remarque 5.4.8 *En particulier, si $P \neq 0$, toutes les racines de P sont de multiplicité inférieure ou égale à* $\deg P$.

Exercice : Justifier la remarque 5.4.8.

Proposition 5.4.9 *Un polynôme de degré $n \in \mathbb{N}$ admet au plus n racines comptées avec leur ordre de multiplicité : $\{a_1, \cdots, a_k\}$ est l'ensemble des racines de P, et α_i est la multiplicité de a_i, alors on a $\alpha_1 + \cdots + \alpha_k \leq n$.*

Preuve : D'après la proposition 5.4.8, on a $\prod_{i=1}^{k}(X-a_i)^{\alpha_i} \mid P$. Donc

$$\sum_{i=1}^{k} \deg(X-a_i)^{\alpha_i} \leq \deg P.$$

Le membre de gauche vaut $\sum_{i=1}^{k}\alpha_i$, d'où le résultat. ■

Remarque 5.4.10 *Le seul polynôme ayant une infinité de racines est le polynôme nul.*

5.4.3 Polynômes dérivés

Définition 5.4.11 *Soit $P = a_kX^k + \cdots + a_1X + a_0$ un polynôme de $\mathbb{K}[X]$. On appelle* **polynôme dérivé** *noté P' le polynôme suivant :*

$$P' = ka_kX^{k-1} + \cdots + a_1 = \sum_{j=1}^{k} ja_jX^{j-1}.$$

Proposition 5.4.12 *Soit P et Q deux polynômes, et $\lambda \in \mathbb{K}$.*

1. *Si $\deg P > 0$ alors $\deg P' = \deg P - 1$,*
2. *Si P est constant alors $P' = 0$,*
3. *$(P+Q)' = P' + Q'$,*
4. *$(\lambda P)' = \lambda P'$,*
5. *$(PQ)' = P'Q + PQ'$.*

Preuve : Les quatre premiers points sont évidents. Prouvons le cinquième.

Soit $P = a_pX^p + \cdots + a_1X + a_0$ et $Q = b_qX^q + \cdots + b_1X + b_0$. En appliquant la définition du polynôme dérivé à la relation (5.5), on trouve

$$(PQ)' = \sum_{j=1}^{p+q} j\Big(\sum_{k+\ell=j} a_kb_\ell\Big)X^{j-1}.$$

Des calculs élémentaires montrent donc que

$$\begin{aligned}(PQ)' &= \sum_{j=1}^{p+q}\sum_{k+\ell=j}\Big(ka_kX^{k-1}b_\ell X^\ell + a_kX^k\ell b_\ell X^{\ell-1}\Big),\\ &= \sum_{j=1}^{p+q}\Big(\sum_{k+\ell=j} ka_kX^{k-1}\, b_\ell X^\ell\Big) + \sum_{j=1}^{p+q}\Big(\sum_{k+\ell=j} a_kX^k\,\ell b_\ell X^{\ell-1}\Big),\\ &= \Big(\sum_{k=1}^{p} ka_kX^{k-1}\Big)\Big(\sum_{\ell=0}^{q} b_\ell X^\ell\Big) + \Big(\sum_{k=0}^{p} a_kX^k\Big)\Big(\sum_{\ell=1}^{q}\ell b_\ell X^{\ell-1}\Big),\\ &= P'Q + PQ'.\end{aligned}$$

■

Proposition 5.4.13 *Soit P un polynôme non nul, et a une racine de P. Alors a est une racine simple si et seulement si $P'(a) \neq 0$.*

Preuve : Nous allons prouver la négation de l'équivalence : i.e a est une racine double de P si et seulement si $P(a) = P'(a) = 0$.

Supposons donc que a est une racine double de P. Alors $(X-a)2 \mid P$. Donc P s'écrit $P = Q(X-a)2$ pour un certain polynôme Q. Il est donc immédiat que $P(a) = 0$. En dérivant, on trouve $P' = Q'(X-a)2 + 2(X-a)Q$, donc $P'(a) = 0$.

Réciproquement, supposons que $P(a) = P'(a) = 0$. La division euclidienne de P par $(X-a)2$ s'écrit $P = Q(X-a)2 + R$ avec $\deg R \leq 1$. Comme $P(a) = 0$, on a $R(a) = 0$. En dérivant la relation $P = Q(X-a)2 + R$, on obtient $R'(a) = 0$. Comme R' est un polynôme constant, on a $R' = 0$, puis, comme $R(a) = 0$, R est nul aussi. ■

5.5 Polynômes scindés

5.5.1 Le théorème fondamental de l'algèbre

Définition 5.5.1 *On dit qu'un polynôme non constant est scindé si la somme des ordres de multiplicité de ses racines est égal à son degré.*

Remarque : Autrement dit, P *de degré* n est scindé si et seulement si il existe un n-uplet $(\lambda_1, \cdots, \lambda_n)$ de $\mathbb{K}^n$ tel que P soit associé à $(X-\lambda_1)\cdots(X-\lambda_n)$.

Proposition 5.5.2 *Soit P un polynôme scindé <u>unitaire</u> d'expression $X^n + a_{n-1}X^{n-1} + \cdots + a_0$. Notons λ_i ses racines comptées avec leur ordre de multiplicité. Alors on a les relations suivantes entre les racines et les coefficients :*

$$a_0 = (-1)^n \prod_{i=1}^{n} \lambda_i \quad \textit{et} \quad a_{n-1} = -\sum_{i=1}^{n} \lambda_i.$$

Preuve : On développe l'expression $(X-\lambda_1)\cdots(X-\lambda_n)$ et on identifie les termes du développement avec ceux de l'expression $X^n + a_{n-1}X^{n-1} + \cdots + a_0$. ■

Remarque : Dans le cas où $P = X^2 + a_1X + a_0$ a pour racines λ_1 et λ_2, on retrouve les relations

$$a_0 = \lambda_1\lambda_2 \quad \text{et} \quad a_1 = -(\lambda_1 + \lambda_2).$$

Le très important résultat suivant est connu sous le nom de **théorème fondamental de l'algèbre** ou **théorème de d'Alembert-Gauss**. Il en existe de nombreuses preuves, mais toutes dépassent le cadre du programme.

Théorème 5.5.3 *Tout polynôme <u>de $\mathbb{C}[X]$</u> est scindé*[5].

5. On dit que $\mathbb{C}$ est un **corps algébriquement clos.**

Remarque : On a vu que toutes les équations de degré 2 avaient deux solutions (éventuellement confondues) dans $\mathbb{C}$. Le théorème fondamental exprime que toute équation de degré n admet n solutions (éventuellement confondues) dans $\mathbb{C}$. Dans le cas $n = 3$ ou 4, il existe des formules (assez compliquées) donnant les solutions en fonction des coefficients. Pour une équation de degré supérieur ou égal à 5, il a été prouvé par un jeune mathématicien du XIX ème siècle, E. Galois, que de telles formules n'existent pas !

5.5.2 Polynômes irréductibles de $\mathbb{C}[X]$

Théorème 5.5.4 *Un polynôme P est irréductible dans $\mathbb{C}$ si et seulement si* $\deg P = 1$.

Preuve : On a déjà vu que tout polynôme de degré 1 était irréductible (que ce soit dans $\mathbb{C}$ ou dans $\mathbb{R}$).

Pour montrer la réciproque, donnons-nous un polynôme P de degré au moins 2. Le théorème fondamental de l'algèbre nous dit que P admet au moins une racine λ_1. Donc P est divisible par $X - \lambda_1$. Clairement $X - \lambda_1$ n'est pas constant et n'est pas associé à P car de degré strictement inférieur à 2. Donc P n'est pas irréductible. ■

En appliquant le théorème général de décomposition irréductible, on en déduit :

Corollaire 5.5.5 *Tout polynôme P non nul de $\mathbb{C}[X]$ admet une décomposition en facteurs irréductibles du type suivant :*

$$P = \lambda \prod_{i=1}^{k} (X - \lambda_i)^{\alpha_i},$$

où $\{\lambda_1, \cdots, \lambda_k\}$ est l'ensemble des racines de P, α_i est la multiplicité de λ_i, et λ est le coefficient du terme dominant de P.

5.5.3 Polynômes irréductibles de $\mathbb{R}[X]$

Dans $\mathbb{R}[X]$, la situation est un peu plus compliquée. On sait d'ores et déjà que tous les polynômes irréductibles ne sont pas de degré 1. Par exemple, $X^2 + 1$ ne saurait être irréductible dans $\mathbb{R}[X]$ car n'a pas de racine réelle (la fonction polynôme associée est minorée par 1, donc ne s'annule jamais).

On peut cependant dresser une liste de tous les polynômes irréductibles de $\mathbb{R}[X]$:

Théorème 5.5.6 *Les polynômes irréductibles de $\mathbb{R}[X]$ sont :*

- *Les polynômes de degré 1,*
- *Les polynômes de degré 2 à discriminant strictement négatif : $P = aX^2 + bX + c$ avec $a \neq 0$ et $\Delta \stackrel{\text{déf}}{=} b^2 - 4ac < 0$.*

La preuve de ce théorème repose sur le lemme suivant :

Lemme 5.5.7 *Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme de $\mathbb{C}[X]$. Notons $\overline{P} = \sum_{k=0}^{n} \overline{a_k} X^k$ le polynôme conjugué. Alors λ est racine de P de multiplicité α si et seulement si $\overline{\lambda}$ est racine de $\overline{P}$ de multiplicité α.*

Preuve : Soit λ une racine de P de multiplicité α. Alors il existe un polynôme Q tel que $P = Q(X - \lambda)^\alpha$. En prenant le conjugué de cette expression, on obtient $\overline{P} = \overline{Q}(X - \overline{\lambda})^\alpha$. Donc $\overline{\lambda}$ est racine de $\overline{P}$ de multiplicité $\overline{\alpha} \geq \alpha$.

En échangeant les rôles de P et $\overline{P}$, λ et $\overline{\lambda}$, α et $\overline{\alpha}$, on obtient $\overline{\alpha} \leq \alpha$, d'où le résultat. ■

Preuve du théorème 5.5.6 :

On sait déjà que les polynômes de degré 1 sont irréductibles. Soit maintenant $P = aX^2 + bX + c$ à discriminant strictement négatif. La fonction $t \mapsto P(t)$ associée ne s'annule pas sur $\mathbb{R}$ (elle est du signe de a), et donc aucun polynôme de degré 1 ne saurait diviser P. Par ailleurs, on a vu que toute équation de degré 2 à coefficients réels et discriminant positif ou nul admettait au moins une solution réelle. Donc les polynômes de degré 2 à discriminant positif ne sont pas irréductibles dans $\mathbb{R}[X]$.

Soit maintenant $P \in \mathbb{R}[X]$ un polynôme de degré au moins 3. Supposons que P n'ait pas de racine réelle (sinon P n'est pas irréductible dans $\mathbb{R}[X]$). D'après le lemme 5.5.7, les racines complexes non réelles de P sont deux à deux conjuguées (avec ordres de multiplicité égaux deux à deux). Le corollaire 5.5.5 assure donc l'existence de nombres complexes (non réels) $\mu_1, \cdots, \mu_p$, d'entiers $\alpha_1, \cdots, \alpha_p$, et d'un réel α, tels que

$$P = \alpha \prod_{i=1}^{p} \Big[(X - \mu_i)^{\alpha_i} (X - \bar{\mu}_i)^{\alpha_i} \Big].$$

Mais un calcul facile montre que

$$(X - \mu_i)^{\alpha_i} (X - \bar{\mu}_i)^{\alpha_i} = (X^2 - 2\mathcal{R}e\, \mu_i\, X + |\mu_i|^2)^{\alpha_i}$$

Donc P est divisible par le polynôme *réel* $X^2 - 2\mathcal{R}e\, \mu_i\, X + |\mu_i|^2$ (de degré 2) et n'est donc pas irréductible. ■

En reprenant la preuve ci-dessus, on déduit facilement le résultat suivant.

Corollaire 5.5.8 *Tout polynôme à coefficients réels admet dans $\mathbb{R}[X]$ une décomposition en facteurs irréductibles du type suivant :*

$$P = \lambda \Big(\prod_{i=1}^{k} (X - \lambda_i)^{\alpha_i} \Big) \Big(\prod_{j=1}^{\ell} (X^2 - 2\mathcal{R}e\, \mu_j\, X + |\mu_j|^2)^{\beta_j} \Big),$$

où λ est le coefficient du terme dominant de P, $\{\lambda_1, \cdots, \lambda_k\}$ est l'ensemble des racines réelles de P, α_i, multiplicité de λ_i, et $\{\mu_1, \cdots, \mu_\ell\}$ est l'ensemble des racines complexes et non réelles de P et β_j, la multiplicité de μ_j.