Cours de Mathématiques

Module :

Complément de formation - Logique, Ensembles et Arithmétique

Nouira Redouane

Anné scolaire : 2024 - 2025

Table des matières

Chapitre 1

Ensembles et applications

1.1 Élements de logique

1.1.1 Proposition, négation d'une proposition

Définition. 1.1.1.

On appelle proposition, toute assertion qui peut prendre l'une des deux valeurs de vérité, vraie, ou fausse. À chaque proposition P, on fait associer sa table de vérité : $\begin{array}{|c|}\hline \text{P} \\ \hline \text{V} \\ \hline \end{array}$ si P est vraie, et $\begin{array}{|c|}\hline \text{P} \\ \hline \text{F} \\ \hline \end{array}$ si elle est fausse.

Exemples 1.1.1 1. *P : « L'homme est un animal sauvage » est une proposition fausse.*

2. *Q : « Rabat est la capitale du Maroc » est une proposition vraie.*

Remarque 1.1.1 *Les phrases interrogatives et exclamatives ne sont pas des propositions.*

Définition. 1.1.2.

On appelle négation d'une proposition P, la proposition notée $\urcorner$P dont la valeur de vérité est contraire de celui de P.

Exemples 1.1.2 1. *La négation de la proposition* $(P : 2 \leq 3)$ *est* $(\urcorner P : 2 > 3)$

2. *La négation de la proposition :*

$$Q : \textit{la fonction cosinus est croissante sur } \mathbb{R}$$

est

$$\urcorner Q : \textit{la fonction cosinus n'est pas croissante sur } \mathbb{R}.$$

Proposition. 1.1.1.

$\rceil\rceil P = P$

Preuve. En effet, d'après la table de vérité, ont les mêmes valeurs de vérité :

P	$\rceil$ P	$\rceil\rceil$ P
V	F	V
F	V	F

■

1.1.2 Connecteurs logique

À partir de deux propositions, on peut construire d'autres à l'aide de ce qu'on appelle des *connecteurs logiques*. Ces connecteurs sont : *La conjonction logique* (et), *la disjonction logique* (ou), *l'implication* ($\Rightarrow$) et *l'équivalence* ($\Leftrightarrow$).

Définition. 1.1.3.

Soient P, Q deux propositions.

1. (P et Q) est la proposition qui est vraie lorsque P et Q sont vraies, et qui est fausse sinon.
2. (P ou Q) est la proposition qui est fausse lorsque P et Q sont fausses, et qui est vraie sinon.
3. ($P \Longrightarrow Q$) est la proposition ($\rceil P$ ou Q)
4. ($P \Longleftrightarrow Q$) est la proposition $((P \Longrightarrow Q)$ et $(Q \Longrightarrow P))$.

P	Q	P et Q	P ou Q	$P \Longrightarrow Q$	$P \Longleftrightarrow Q$
V	V	V	V	V	V
V	F	F	V	F	F
F	V	F	V	V	F
F	F	F	F	V	V

Propriétés 1.1.1

Soient P, Q, R trois propositions. Alors on :

1. *Associativité*
   - *(a)* $(P$ *et* $(Q$ *et* $R)) = ((P$ *et* $Q)$ *et* $R)$
   - *(b)* $(P$ *ou* $(Q$ *ou* $R)) = ((P$ *ou* $Q)$ *ou* $R)$
   - *(c)* $(P \Longleftrightarrow (Q \Longleftrightarrow R)) = ((P \Longleftrightarrow Q) \Longleftrightarrow R)$
2. *Distributivité*
   - *(a)* $(P$ *et* $(Q$ *ou* $R)) = ((P$ *et* $Q)$ *ou* $(P$ *et* $R))$
   - *(b)* $(P$ *ou* $(Q$ *et* $R)) = ((P$ *ou* $Q)$ *et* $(P$ *ou* $R))$
3. *Négations*

(a) $\rceil (P \text{ et } Q) = (\rceil P \text{ ou } \rceil Q)$
(b) $\rceil (P \text{ ou } Q) = (\rceil P \text{ et } \rceil Q)$
(c) $\rceil (P \Longrightarrow Q) = (P \text{ et } \rceil Q)$

4. *Transitivité*
   (a) *Si* $(P \Longrightarrow Q)$ *et* $(Q \Longrightarrow R)$, *alors* $P \Longrightarrow R$
   (b) *Si* $(P \Longleftrightarrow Q)$ *et* $(Q \Longleftrightarrow R)$, *alors* $P \Longleftrightarrow R$

Remarques 1.1.1 1. *L'implication n'est pas associative. En effet, dans les cas où* P *est fausse,* Q *est vraie et* R *est fausse, alors* $P \Longrightarrow (Q \Longrightarrow R)$ *est vraie, alors que* $(P \Longrightarrow Q) \Longrightarrow R$ *est fausse.*
Pour cette raison, l'écriture sans parenthèses, $P \Longrightarrow Q \Longrightarrow R$, *n'est pas logique.*

2. *Au contraire, l'équivalence est bien associative et alors l'écriture* $P \Leftrightarrow Q \Leftrightarrow R$ *est logique. Cependant, il y a une différence entre*

$$P \Longleftrightarrow Q \Longleftrightarrow R,$$

et

$$(P \Longleftrightarrow Q) \text{ et } (Q \Longleftrightarrow R)$$

1.1.3 Le raisonnement

Le raisonnement direct

Il s'agit de démontrer une implication $P \Longrightarrow Q$. Dans le cas où P est fausse le problème ne se pose pas, pour cela, en pratique, pour ce faire, on suppose que P est vraie, et on démontre que Q est vraie. L'implication $P \Longrightarrow Q$ se lit : Si P alors Q.

Remarque 1.1.2

Pour démontrer une proposition Q, *on peut chercher une autre qui est vraie, et on démontrer que* $P \Longrightarrow Q$, *ou même que* $P \Longleftrightarrow Q$. *L'avantage de ce dernier choix, c'est qu'il nous donne la souplesse de commencer dans notre raisonnement par* Q, *puis arriver à* P.
Pour cela, Grâ ce à la transitivité de l'implication, on peut démontrer cela à l'aide des implications intermédiaires successives de la formes $P \Longrightarrow P_2$, $P_2 \Longrightarrow P_3, \cdots, P_{n-1} \Longrightarrow P_n$, *puis* $P_n \Longrightarrow Q$ *pour conclure que* $P \Longrightarrow Q$. *On écrit alors :*

$$\begin{array}{rl} P & \Longrightarrow P_1 \\ & \Longrightarrow P_2 \\ & \vdots \\ & \Longrightarrow P_n \\ & \Longrightarrow Q \end{array}$$

Et bien entendu, la même remarque s'applique pour montrer que $P \Leftrightarrow Q$ *à l'aide des équivalences successives.*

Exemple 1.1.1 *Soit* $x \in \mathbb{R}$. *Montrons que* $1 < x < 2 \Longrightarrow x^2 - 3x + 2 < 0$. *Supposons donc que*

$1 < x < 2$. *En remarquant que* $x^2 - 3x + 2 < 0 = \left(x - \frac{3}{2}\right)^2 - \frac{1}{4}$ *on a :*

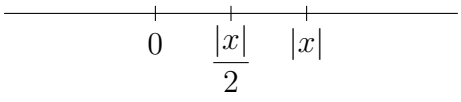
$$\begin{aligned} 1 < x < 2 &\Longrightarrow -\frac{1}{2} < x - \frac{3}{2} < \frac{1}{2} \\ &\Longrightarrow \left(x - \frac{3}{2}\right)^2 < \frac{1}{4} \\ &\Longrightarrow \left(x - \frac{3}{2}\right)^2 - \frac{1}{4} < 0 \\ &\Longrightarrow x^2 - 3x + 2 < 0 \end{aligned}$$

Le raisonnement par la contraposée

Principe : Si P, Q sont deux propositions, alors $P \Longrightarrow Q$ a la même valeur de vérité que $\rceil Q \Longrightarrow \rceil P$.

Donc, pour démontrer que $P \Longrightarrow Q$, la contraposée consiste à supposer que Q est fausse, et de prouver que P est fausse.

Exemple 1.1.2 *Soit* $x \in \mathbb{R}$. *Montrons par contraposée que si pour tout* $\varepsilon > 0$ *on a* $|x| < \varepsilon$, *alors* $x = 0$. *Supposons alors que* $x \neq 0$.



Dans ce cas, en prenant $\varepsilon = \frac{|x|}{2}$, *alors* $0 < \varepsilon = \frac{|x|}{2} < |x|$. *C'est ce qu'il faut démontrer.*

Le raisonnement par l'absurde

Principe : Si P, Q sont deux propositions, et si $\rceil P \Longrightarrow (Q \text{ et } \rceil Q)$ est vraie, alors P est vraie.

Donc, pour démontrer P, on supposer que P est fausse, et on aboutit à une contradiction de la forme Q et $\rceil Q$.

Exemple 1.1.3 *Montrer que si pour tout* $\sqrt{2} \notin \mathbb{Q}$.
Supposons que $\sqrt{2} \in \mathbb{Q}$. *Ils existent alors* $p, q \in \mathbb{N}^*$ *tels que* $p \wedge q = 1$ *et* $\sqrt{2} = \frac{p}{q}$. *Donc,* $p^2 = 2q^2$ *et alors* p^2 *est un nombre pair. On en déduit que* p *est pair ; donc de la forme* $p = 2k$ *avec* $k \in \mathbb{N}$. *Mais dans ce cas :*

$$\begin{aligned} p^2 = 2q^2 &\Longrightarrow 4k^2 = 2q^2 \\ &\Longrightarrow 2k^2 = q^2 \\ &\Longrightarrow 2 \textit{ divise } q^2 \\ &\Longrightarrow 2 \textit{ divise } q \\ &\Longrightarrow p \wedge q \neq 1 \end{aligned}$$

ce qui est contradictoire puisque $p \wedge q = 1$. *Ainsi* $\sqrt{2} \notin \mathbb{Q}$.

Le raisonnement par la récurrence

La récurrence simple

Principe : Si A est une partie de $\mathbb{N}$ telle que :

$$\left|\begin{array}{l} 0 \in A \\ \text{Pour tout } n \in \mathbb{N}, \text{ si } n \in A \text{ alors } n+1 \in A, \end{array}\right.$$

alors $A = \mathbb{N}$

Remarque 1.1.3 *Ce principe peut être formulé aussi sous la forme suivante : Si $P(n)$ est une propriété qui dépend d'un entier $n \in \mathbb{N}$, c'est à dir que pour chaque valeur fixée de n, $P(n)$ est une proposition, et si :*

$$\left|\begin{array}{l} P(0) \textit{ est vraie} \\ \textit{Pour tout } n \in \mathbb{N}, \textit{ si } P(n) \textit{ est vraie alors } P(n+1) \textit{ est vraie,} \end{array}\right.$$

alors pour tout $n \in \mathbb{N}$, $P(n)$ est vraie.

Exemple 1.1.4 *Montrer que pour tout $n \in \mathbb{N}$, $\displaystyle\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$.*

En effet, pour $n = 0$, le résultat est évident ; $\displaystyle\sum_{k=0}^{0} k = 0 = \frac{0(0+1)}{2}$.

Supposons que $\displaystyle\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$ pour un certain $n \in \mathbb{N}$ et montrons que $\displaystyle\sum_{k=0}^{n+1} k = \frac{(n+1)(n+2)}{2}$.

En effet ;

$$\begin{aligned} \sum_{k=0}^{n+1} k &= n+1+\sum_{k=0}^{n} k \\ &= n+1+\frac{n(n+1)}{2} \\ &= (n+1)\left(1+\frac{n}{2}\right) \\ &= \frac{(n+1)(n+2)}{2}. \end{aligned}$$

Conclusion,

$$\forall n \in \mathbb{N}, \ \sum_{k=0}^{n} k = \frac{n(n+1)}{2}.$$

La récurrence simple à deux pas

Principe : Si $P(n)$ est une propriété qui dépend d'un entier $n \in \mathbb{N}$ telle que :

$$\left|\begin{array}{l} P(0) \text{ et } P(1) \text{ sont vraies} \\ \text{Pour tout } n \in \mathbb{N}, \text{ si } P(n) \text{ et } P(n+1) \text{ sont vraies} \\ \text{ alors } P(n+2) \text{ est vraie,} \end{array}\right.$$

alors pour tout $n \in \mathbb{N}$, $P(n)$ est vraie.

De manière général, s'il existe $m \in \mathbb{N}$ tel que

$$\begin{array}{l} P(0), P(1), \cdots, P(m) \text{ sont vraies} \\ \text{Pour tout } n \in \mathbb{N}, \text{ si } P(n), P(n+1), \cdots, P(n+m) \text{ sont vraies} \\ \text{ alors } P(n+m+1) \text{ est vraie,} \end{array}$$

alors pour tout $n \in \mathbb{N}$, $P(n)$ est vraie.

Exemple 1.1.5 *Considérons la suite numérique définie par* $u_0 = 2,\ \ u_1 = 3$ *et* $u_{n+2} = 3u_{n+1} - 2u_n$. *Montrer que* $u_n = 2^n + 1$ *pour tout* $n \in \mathbb{N}$.
Pour $n = 0$ *et* $n = 1$ *le résultat est bien vérifié. Supposons que pour un* $n \in \mathbb{N}$ *on a* $u_n = 2^n + 1$ *et* $u_{n+1} = 2^{n+1} + 1$. *Il en découle alors que :*

$$\begin{aligned} u_{n+2} &= 3u_{n+1} - 2u_n \\ &= 3\left(2^{n+1} + 1\right) - 2\left(2^n + 1\right) \\ &= 3.2^{n+1} + 3 - 2^{n+1} - 2 \\ &= 2^{n+2} + 1 \end{aligned}$$

La récurrence forte
Principe : Si $P(n)$ est une propriété qui dépend d'un entier $n \in \mathbb{N}$ telle que :

> $P(0)$ est vraie
> Pour tout $n \in \mathbb{N},$ si $P(k)$ est vraie pour tout $k \in [\![0, n]\!]$ alors $P(n+1)$ est vraie,

alors pour tout $n \in \mathbb{N}$, $P(n)$ est vraie.

Exemple 1.1.6 *Montrer que tout entier naturel* $n \geq 2$ *admet un diviseur premier.*
Pour $n = 2$, *il n y a rien à démontrer ; 2 est divisible par lui même. Supposons que le résultat est vrai jusqu'à un certain* $n \geq 2$ *et montrons le pour* $n + 1$. *Si* $n + 1$ *est un nombre premier alors il n y a rien à prouver ; car il est divisible par lui même même. Sinon,* $n + 1$ *aura un diviseur* a *compris entre* 2 *et* n, *et dans ce cas, l'hypothèse de récurrence assure l'existence d'un diviseur premier* p *de* a. *Par transitivité de la divisibilité,* p *divise aussib* $n + 1$. *D'où le résultat.*

1.2 LES ENSEMBLES

1.2.1 Ensemble, élément d'un ensemble

Définition. 1.2.1.

On appelle ensemble E, toute collection d'objets. Ces objets sont appelés alors des élément de E. Si x est un élément de E, on dit que x appartient à E, que E contient x, et on écrit $x \in E$, sinon on écrit $x \notin E$.
On admet l'existence d'un ensemble ne contenant aucun élément. On l'appelle l'ensemble vide et on le note $\emptyset$.

Notation Si E est un ensemble dont les élément sont $x_1, ..., x_n$, alors on note $E = \{x_1, ..., x_n\}$

Dans toute la suite, E, F, G désignent trois ensembles quelconques.

1.2.2 Quantificateurs logiques

Quantificateurs logiques Soit $\mathcal{P}(x)$ une propriété qui dépend d'un élément variable dans E, c'est à dire que pour chaque valeur de x, $\mathcal{P}(x)$ devient une proposition. On définit alors les propositions $(\forall x \in E; \mathcal{P}(x))$, et $(\exists x \in E; \mathcal{P}(x))$ par :

1. $(\forall x \in E; \mathcal{P}(x))$ est la proposition qui est vraie si et seulement si $\mathcal{P}(x)$ est vraie pour toute valeur de x dans E

2. $(\exists x \in E : \mathcal{P}(x))$ est la proposition qui est vraie si et seulement si $\mathcal{P}(x)$ est vraie pour au moins une valeur de x dans E.

$(\forall)$ s'appelle le quantificateur universel, et $(\exists)$ s'appelle le quantificateur existentiel.

Remarque 1.2.1 *Une proposition peut contenir plusieurs quantificateurs, dans ce cas, l'ordre des quantificateurs, de natures différentes, est très important comme le montrent les exemples ci-dessous.*

Exemples 1.2.1
1. $\left(\forall x \in \mathbb{R};\ \ x^2 \geq 0\right)$ *est vraie*
2. $\left(\exists x \in \mathbb{Q};\ \ x^2 = 2\right)$ *est fausse.*
3. $(\forall x \in \mathbb{R};\ \ \exists y \in \mathbb{R} : x = y)$ *est vraie.*
4. $(\exists y \in \mathbb{R} : \forall x \in \mathbb{R};\ \ x = y)$ *est fausse.*

Propriétés 1.2.1

Si $\mathcal{P}(x)$ une propriété qui dépend d'un élément variable dans E alors :
1. $\rceil\,(\forall x \in E; \mathcal{P}(x)) = \exists x \in E; \rceil \mathcal{P}(x)$
2. $\rceil\,(\exists x \in E; \mathcal{P}(x)) = \forall x \in E; \rceil \mathcal{P}(x)$

Exemples 1.2.2 *Les négations des propositions précédentes sont :*
1. $\exists x \in \mathbb{R}; x^2 < 0.$
2. $\forall x \in \mathbb{Q}; x^2 \neq 2.$
3. $\exists x \in \mathbb{R}; \exists y \in \mathbb{R} : x \neq y.$
4. $\forall y \in \mathbb{R} : \forall x \in \mathbb{R}; x \neq y.$

1.2.3 Inclusion, partie d'un ensemble

Définition. 1.2.2.

On dit que l'ensemble E est inclus dans F, et on écrit $E \subset F$, si

$$\forall x \in E,\ \ x \in F.$$

Dans ce cas on dit aussi que E est une partie de F. Par convention, $\emptyset$ est supposé inclus dans tout ensemble.
On appelle ensemble de parties de E, l'ensemble dont les éléments sont toutes la es parties de E.

Exemples 1.2.3 *Pour $E = \{a, b\}$, $\mathcal{P}(E) = \{\emptyset, \{a\}, \{b\}, E\}$. Donc $\{a\}, \{b\}$ sont des éléments de $\mathcal{P}(E)$, et $\emptyset$ est à la fois une partie et un élément de $\mathcal{P}(E)$.*

Propriétés 1.2.2

Soient E, F, G trois ensembles quelconques, alors :
1. $E \subset F \Longleftrightarrow (\forall x \in E, x \in F)$
2. $(E \subset F \text{ et } F \subset G) \Longrightarrow E \subset G$

3. $E = F \iff (E \subset F \text{ et } F \subset E)$
4. $(E = F = G) \iff (E \subset F, F \subset G \text{ et } G \subset E)$
5. *Si F, G sont deux parties de E alors $F = G$ si cet seulement si ;*

$$\forall x \in E, \quad x \in F \iff x \in G$$

Remarque 1.2.2 *Si $P(x)$ est une propriété dépendante d'une variable $x \in E$, alors les élément x de E pour lesquelles $P(x)$ est vraie constituent une partie de E, éventuellement vide. Cette partie se note $\{x \in E : P(x)\}$. On dit que la partie est définie par une propriété, ou par compréhension.*

EXERCICE 1.2.1 *L'objectif de ce exercice est de démontrer que « l'ensemble de tous les ensembles » n'existe pas. Supposons par l'absurde qu'il existe un ensemble E qui contient tous les ensembles. Considérons alors la propriété $P(X)$, où $X \in E$, définie par*

$$P(X) \quad : \quad X \notin X,$$

et la partie A de E définie par

$$A = \Big\{ X \in E \quad : \quad P(X) \Big\} = \Big\{ X \in E \quad : \quad X \notin X \Big\}$$

Montrer que si $A \in A$ alors $A \notin A$, et que si $A \notin A$ alors $A \in A$ puis conclure

Solution 1 *Supposons que si $A \in A$. Alors par définition de A on a $A \notin A$. Et si $A \notin A$, toujours par définition de A on a $A \in A$. Dans les deux on a abouti à une contradiction, donc « l'ensemble de tous les ensembles » n'existe pas.*

1.2.4 Opérations sur les ensembles

Définition. 1.2.3.

Soient E un ensemble quelconque, et A, B deux parties de E.

1. On appelle intersection de A et B l'ensemble

$$A \cap B = \{x \in E : x \in A \text{ et } x \in B\}$$

2. On appelle réunion de A et B l'ensemble

$$A \cup B = \{x \in E : x \in A \text{ ou } x \in B\}$$

3. On appelle complémentaire de A l'ensemble

$$\overline{A} = \complement_E^A = \{x \in E : x \notin A\}$$

4. On appelle différence de A et B l'ensemble

$$A \setminus B = \{x \in E : x \in A \text{ ou } x \notin B\}$$

Propriétés 1.2.3

Si A, B, C sont des parties d'un ensemble E alors

1. $E \cap A = A$, $E \cup A = E$, $\emptyset \cup A = A$, $\emptyset \cap A = \emptyset$
2. $A \cap A = A \cup A = A$,
3. $A \cap B \subset A \subset A \cup B$
4. *Les assertions suivantes sont équivalentes :*
   (a) $A \subset B$.
   (b) $A \cap B = A$.
   (c) $A \cup B = B$.
   (d) $\overline{B} \subset \overline{A}$.
5. $A = B \iff \overline{A} = \overline{B}$
6. $A \subset B \Longrightarrow (A \cap C \subset B \cap C$ *et* $A \cup C \subset B \cup C)$
7. *Associativité de l'intersection et la réunion.*
   $(A \cap B) \cap C = A \cap (B \cap C)$ *et* $(A \cup B) \cup C = A \cup (B \cup C)$.
8. *Distributivité de l'intersection et la réunion.*
   $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *et* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
9. *Lois de Morgan.*
   $\overline{A \cap B} = \overline{A} \cup \overline{B}$ *et* $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Preuve. Laissée à titre d'exercice. ■

1.2.5 Produit cartésien

Définition. 1.2.4.

On appelle produit cartésien de deux ensembles non vides E et F, l'ensemble

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

Si $E \times F$, on note tout simplement E^2.

Remarque 1.2.3

1. *Sous les mêmes hypothèses, pour tous $(x, y), (x', y') \in E \times F$ on a $(x, y) = (x', y') \iff x = x'$ et $y = y'$*
2. *De la même faç on, on définit le produit cartésien de plusieurs ensembles $E_1, \cdots, E_n$ qu'on notera $E_1 \times E_2 \cdots \times E_n$, ou encore $\prod_{k=1}^{n} E_k$. Dans le cas où $E_1 = \cdots = E_n = E$ on note tout simplement E^n*
3. *Par convention, si E ou F est vide, $E \times F = \emptyset$*

1.3 LES RELATIONS

1.3.1 Relation binaire

Définition. 1.3.1.

Soient E, F deux ensembles non vides. On appelle relation $\mathcal{R}$ entre E et F, la donnée d'une partie G de $E \times F$. Dans ce cas, pour tout $x \in E$ et tout $y \in F$, si $(x, y) \in G$, on dit que x est en relation avec y et on écrit $x\mathcal{R}y$, sinon on écrit $x\not\mathcal{R}y$. Lorsque $E = F$, la relation est dite binaire.

Exemples 1.3.1 *Soit $\mathcal{R}$ définie sur $\mathbb{R}$ par : $x\mathcal{R}y \iff x^2 - y^2 = x - y$, pour tout $(x, y) \in \mathbb{R}$. Alors $1\mathcal{R}0$, mais $1\not\mathcal{R}2$.*

Définition. 1.3.2.

Soit $\mathcal{R}$ une relation binaire sur un ensemble E. On dit que la relation $\mathcal{R}$ est :

1. Réflexive si, $\forall x \in E, \quad x\mathcal{R}x$
2. symétrique si, $\forall x, y \in E, \quad x\mathcal{R}y \Longrightarrow y\mathcal{R}x$
3. antisymétrique si, $\forall x, y \in E, \quad (x\mathcal{R}y \text{ et } y\mathcal{R}x) \Longrightarrow x = y$
4. transitive si, $\forall x, y, z \in E, \quad (x\mathcal{R}y \text{ et } y\mathcal{R}z) \Longrightarrow x\mathcal{R}z$

Exemples 1.3.2

1. *La divisibilité dans $\mathbb{N}$ est une relation réflexive, antisymétrique et transitive.*
2. *Le parallélisme entre les droites est une relation réflexive, symétrique et transitive.*

1.3.2 Relation d'équivalence

Définition. 1.3.3.

On appelle relation d'équivalence, toute relation réflexive, symétrique et transitive.

Exemples 1.3.3

1. *Le parallélisme entre les droites est une relation d'équivalence.*
2. *La relation définie sur $\mathbb{R}$ par :*

$$(x, y) \in \mathbb{R}, \quad x\mathcal{R}y \iff x^2 - y^2 = x - y$$

est une relation d'équivalence.

3. *La congruence modulo un entier dans $\mathbb{Z}$: On dit que deux entiers relatifs a, b sont congrus modulo un entier $n \in \mathbb{N}^*$, et on écrit*

$$a \equiv b \quad [n],$$

si n divise $a - b$. La congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.

Définition. 1.3.4.

Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E, et soit $x \in E$. On appelle classe d'équivalence de x l'ensemble : $\{y \in E : x\mathcal{R}y\}$.

Remarque 1.3.1 *La classe d'équivalence de x est souvent notée $\dot{x}, \overline{x}$ ou $cl(x)$.*

Exemples 1.3.4 1. *Déterminons la classe d'équivalence de tout réel x pour la relation définie sur $\mathbb{R}$ par :*

$$(x,y) \in \mathbb{R}, \quad x\mathcal{R}y \iff x^2 - y^2 = x - y$$

Soit $x \in \mathbb{R}$. Pour tout $y \in \mathbb{R}$ on a :

$$\begin{aligned} y \in \dot{x} &\iff x\mathcal{R}y \\ &\iff x^2 - y^2 = x - y \\ &\iff (x-y)(x+y-1) = 0 \\ &\iff x = y \text{ ou } y = 1 - x \end{aligned}$$

Conclusion : $\dot{x} = \{x, 1-x\}$

2. *Déterminons les classes d'équivalence modulo un entier n dans $\mathbb{N}^*$. Pour tout $m, m' \in \mathbb{Z}$ on a*

$$m' \in \dot{m} \iff \exists k \in \mathbb{Z} \ : \ m' = m + kn$$

Donc : $\dot{m} = \{m + kn \ : \ k \in \mathbb{Z}\}$

Proposition. 1.3.1.

Étant donnée une relation d'équivalence $\mathcal{R}$ sur un ensemble E, et deux éléments $x, y \in E$, alors les assertions suivantes sont équivalentes :

1. $y \in \dot{x}$.
2. $x\mathcal{R}y$.
3. $x \in \dot{y}$.
4. $\dot{x} = \dot{y}$.

Preuve.

— Par définition même d'une classe d'équivalence, on a $(1) \Leftrightarrow (2) \Leftrightarrow (3)$.

— $(1) \Leftrightarrow (4)$. Supposons que $y \in \dot{x}$ et soit $z \in \dot{x}$. Alors $x\mathcal{R}y$ et $z\mathcal{R}x$, et par transitivité on a $z\mathcal{R}y$, puis $z \in \dot{y}$. Ceci montre que $\dot{x} \subset \dot{y}$. De la même manière on a $\dot{y} \subset \dot{x}$ et finalement $\dot{y} = \dot{x}$.

— $(4) \Leftrightarrow (1)$. Supposons que $\dot{x} = \dot{y}$. Comme $y \in \dot{y}$ alors $y \in \dot{x}$.

■

Proposition. 1.3.2.

Étant donnée une relation d'équivalence $\mathcal{R}$ sur un ensemble E, et deux éléments $x, y \in E$, alors soit $\dot{x} = \dot{y}$, soit $\dot{x} \cap \dot{y} = \emptyset$. C'est à dire que deux classes d'équivalences sont, soit égales, soit disjointes.

Preuve. Supposons que $\dot{x} \cap \dot{y} \neq \emptyset$ et soit $z \in \dot{x} \cap \dot{y}$. D'après la proposition précédente on a $\dot{x} = \dot{z} = \dot{y}$. D'où le résultat. ■

1.3.3 Relation d'ordre

Définition. 1.3.5.

On appelle relation d'ordre, toute relation réflexive, antisymétrique et transitive.

Exemples 1.3.5 *1. $\leq$ est une relation d'ordre dans $\mathbb{R}$, on l'appelle l'ordre usuel de $\mathbb{R}$.*

2. L'inclusion entre les parties d'un ensemble E, est une relation d'ordre dans $\mathcal{P}(E)$.

3. La divisibilité est une relation d'ordre dans $\mathbb{N}$, mais elle ne l'est pas dans $\mathbb{Z}$.

EXERCICE 1.3.1 *On définit dans $\mathbb{R}^2$ la relation $\mathcal{R}$ par :*

$$\forall (x,y),(x',y') \in \mathbb{R}^2;\ \ (x,y)\mathcal{R}(x',y') \Longleftrightarrow \left| \begin{array}{l} x < x', \\ \text{ou} \\ x = x' \text{ et } y \leq y' \end{array} \right.$$

Montrer qu'il s'agit d'une relation d'ordre. Cette relation s'appelle l'ordre lexicographique.

Définition. 1.3.6.

Soit $\mathcal{R}$ une relation d'ordre sur un ensemble E.

1. pour tout $(x,y) \in E^2$, on dit que x et y sont comparables, si $x\mathcal{R}y$ ou $y\mathcal{R}x$ Dans le cas contraire on dit qu'ils sont incomparables.
2. On dit que $\mathcal{R}$ est une relation d'ordre totale, si pour tout $(x,y) \in E^2$, x et y sont comparables. Si $\mathcal{R}$ n'est pas une relation d'ordre totale sinon, on dit qu'elle partielle.

Exemples 1.3.6 *1. L'ordre usuel de $\mathbb{R}$ est une relation d'ordre totale dans $\mathbb{R}$.*

2. L'inclusion entre les parties d'un ensemble E, est, en général, une relation d'ordre partielle. En effet, si E contient deux élément distincts a et b, alors $\{a\}$ et $\{b\}$ ne sont pas comparables.

3. La divisibilité est une relation d'ordre dans partielle $\mathbb{N}$; car 2 et 3 ne sont pas comparables.

EXERCICE 1.3.2 *Montrer que l'ordre lexicographique est une relation d'ordre totale dans $\mathbb{R}^2$.*

Définition. 1.3.7.

Soit $\mathcal{R}$ une relation d'ordre sur un ensemble E, $a \in E$ et $A \subset E$.

1. on dit que a est un majorant (resp : minorant) de A si pour tout $x \in A$ on a $x\mathcal{R}a$, (resp : $a\mathcal{R}x$).
2. on dit que a est le plus grand (resp : le plus petit) élément de A, et on écrit $a = \max A$, (resp : $\min A$), si $a \in A$ et a est un majorant (resp : minorant) de A.
3. on dit que a est la borne supérieure (resp : inférieure) de A, et on écrit $a = \sup A$, (resp : $\inf A$) si a est le plus petit des majorants (resp : le plus grand des minorants) de A.

Exemples 1.3.7 *1. Considérons dans $\mathbb{R}$, muni de son ordre usuel, les parties $A = [0,1]$ et $B =]0,1[$. Alors $\max A = 1$, $\min A = 0$, $\sup B = 1$, $\inf B = 0$, de plus, B n'admet ni plus grand ni plus petit élément.*

2. dans $\mathcal{P}(E)$, muni de inclusion, $\emptyset$ est le plus petit élément, et E est le plus grand élément.

3. *Munissons l'ensemble $\mathbb{N}$ de la divisibilité, et considérons la partie $A = \{2, 3, 4, 5\}$. Alors A n'admet ni plus grand, ni plus petit élément, mais elle admet 1 comme borne inférieure et 60 comme borne supérieure.*

Remarque 1.3.2 *les bornes supérieures et inférieures d'une partie A, en cas d'existence, contrairement aux plus grands et plus petits éléments, n'appartiennent pas forcément à A.*

Proposition. 1.3.3.

Soit $\mathcal{R}$ une relation d'ordre sur un ensemble E, $a \in E$ et $A \subset E$.

1. Si A admet un plus grand (resp : un plus petit) élément, a, alors A admet a comme borne supérieure (resp : inférieure).
2. la borne supérieure (resp : inférieure) de A, lorsqu'elle existe, elle est unique.

Preuve. On dira, pour $x, y \in E$, que y est supérieur à x, ou que x est inférieur à y, si $x\mathcal{R}y$. Remarquons que si on définit la relation $\mathcal{R}'$ dans E par

$$\forall (x, y) \in E^2, \quad x\mathcal{R}'y \Leftrightarrow y\mathcal{R}x$$

alors a est une borne inférieure (resp : un plus petit élément) de A pour la relation $\mathcal{R}'$ si et seulement si a est une borne supérieure (resp : un plus grand élément) de A pour la relation $\mathcal{R}$. Ainsi, il suffit de faire la preuve pour les cas de plus grand élément et de borne supérieure.

1. Supposons que A admet un plus grand élément a. Alors a est un majorant de A et $a \in A$. Donc, pour tout autre majorant de M de A on a $a\mathcal{R}M$, car $a \in A$. Donc a est le plus petit des majorants de A, c'est à dire que a est la borne supérieure de A.
2. Supposons que A admet borne supérieure a et b. Alors a est un majorant de A, et inférieur à tout autre majorant de A, en particulier $a\mathcal{R}b$. Comme a et b jouent des rô les symétriques, alors aussi $b\mathcal{R}a$ puis $a = b$. Ceci montre l'unicité de la borne supérieure. Et comme la borne plus grand élément de A est une supérieure de A, alors ce dernier est, lui aussi, lorsqu'il existe, il est unique.

■

Proposition. 1.3.4.

1. Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.
2. Toute partie de $\mathbb{N}$ non vide et majorée dans $\mathbb{N}$ admet un plus grand élément.

Preuve.

1. Soit A une partie non vide de $\mathbb{N}$. Supposons, par contraposée, que A n'admet pas de plus grand élément, et montrons que $A = \emptyset$. Pour cela, on va démontrer par récurrence forte que : $\forall n \in \mathbb{N}, \quad n \notin A$. En effet, $0 \notin A$, sinon, 0 est le plus petit élément de A. Supposons pour un certain $n \in \mathbb{N}$ on a :

$$\forall k \in \mathbb{N}, \quad 0 \leq k \leq n \Longrightarrow k \notin A.$$

Dans ce cas, si $n + 1 \in A$ alors $n + 1$ est le plus petit élément de A, ce qui est absurde. Ainsi,

$$\forall n \in \mathbb{N}, \quad n \notin A,$$

ou encore $A = \emptyset$. Fin de la démonstration.

2. Soit A une partie de $\mathbb{N}$ non vide et majorée par un certain $n \in \mathbb{N}$. Montrons par récurrence sur n, que A admet un plus grand élément.
Si $n = 0$ alors $A = \{0\}$ et A admet 0 comme plus grand élément. Supposons que ce résultat est vrai pour n et Supposons que A est majorée par $n+1$. Si $n+1 \in A$ alors $n+1$ est le plus grand élément de A, sinon, A est majorée par n, et d'après l'hypothèse de récurrence A admet un plus grand élément. D'où le résultat.

■

EXERCICE 1.3.3 *Montrer que tout entier $n \in \mathbb{N}^*$ s'écrit sous la forme $n = 2^p(2q+1)$*

1.4 LES APPLICATIONS

1.4.1 Notion d'application

Définition. 1.4.1.

Soient E, F deux ensembles non vides. On appelle application de E vers F, toute relation f de E vers F telle que pour tout $x \in E$ il existe un unique $y \in F$ vérifiant $x \ f \ y$; c'est à dire x en relation avec y. Dans ce cas, y s'appelle l'image de x par l'application f, et se note $f(x)$, et x s'appelle un antécédent de de y. On dit que E est l'ensemble de départ de l'application f, F son ensemble d'arrivée et $G = \{(x, f(x)) \ : \ x \in E\}$ son graphe. L'ensemble des applications de E vers F se note $\mathcal{F}(E,F)$ ou F^E.

Remarque 1.4.1 *En pratique, on définit une application en donnant son graphe ou en exprimant $f(x)$ en fonction de x pour tout $x \in E$, et on écrit :* $f : \begin{array}{ccc} E & \longrightarrow & F \\ x & \longmapsto & f(x) \end{array}$
On peut aussi représenter aussi f par un diagrammes cartésien ou sagittal.

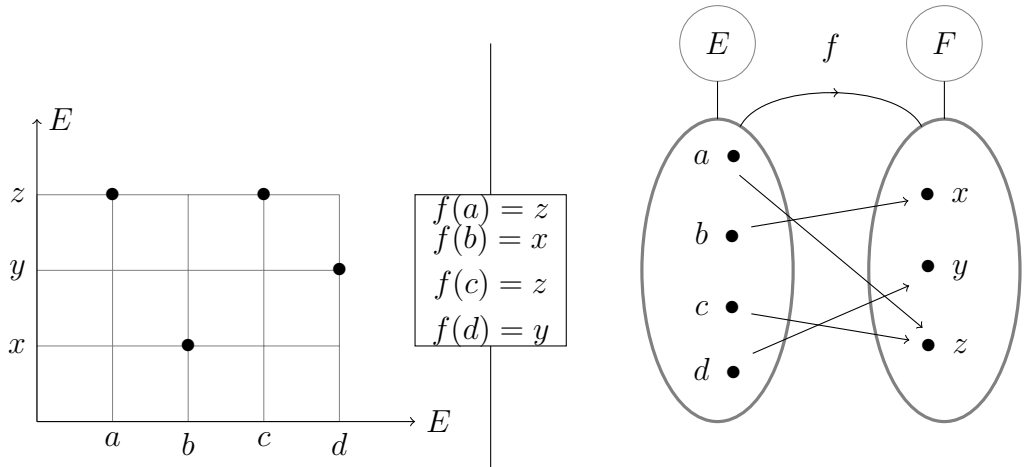


Diagramme cartésien de f Diagramme Sagittal de f

Exemples 1.4.1 *1.* $f : \begin{array}{ccc} \mathbb{N} & \longrightarrow & \mathbb{N} \\ n & \longmapsto & n^2 \end{array}$ *est une application.*

2. $f : \begin{array}{ccc} \mathbb{N} & \longrightarrow & \mathbb{N} \\ n & \longmapsto & \dfrac{n}{2} \end{array}$ *est-t-elle une application ?*

3. *L'identité d'un ensemble non vide E : C'est l'application id définie de E vers lui même par $id(x) = x$ pour tout $x \in E$.*

4. *Restriction et prolongement : Si $f : E \to F$ et $f : A \to F$ sont deux applications avec $A \subset E$, on dit que g est la restriction de f à A, et que f est un prolongement de g à E si*

$$\forall x \in A, \quad g(x) = f(x).$$

On note alors $g = f_{|A}$.

Proposition. 1.4.1.

Deux applications f et g sont égales si, et seulement si :

1. Elles ont le même ensemble de départ E.
2. Elles ont le même ensemble d'arrivée F
3. $\forall x \in E, \quad f(x) = g(x)$

EXERCICE 1.4.1 *Pour toute partie A de E on définie l'application χ_A, dite caractéristique de A, de E vers $\{0, 1\}$ par :*

$$\forall x \in E, \quad \chi_A(x) = \begin{cases} 1 \, ; \, si \; x \in A, \\ 0 \, ; \, sinon \end{cases}$$

1. *Montrer que : $\forall A, B \subset E, \quad A = B \iff \chi_A = \chi_A$.*
2. *Montrer que : $\forall A, B \subset E, \quad \chi_{A \cap B} = \chi_A \chi_B$.*

1.4.2 Composée de deux applications

Définition. 1.4.2.

Soit $f : E \to F$ et $g : F \to G$ deux applications. On définit l'application composée $g \circ f : E \to G$ par : $\forall x \in E, \quad g \circ f(x) = g\left(f(x)\right)$.

Exemples 1.4.2

1. *Si $f : E \to F$ est une application alors : $id_F \circ f = f = f \circ id_E$.*
2. *Soient les applications f et g définies de $\mathbb{R}$ vers lui même par $f(x) = x^2$ et $g(x) = 2x$ pour tout $x \in \mathbb{R}$. Pour tout $x \in \mathbb{R}$ on a $g \circ f(x) = 2x^2$ et $f \circ g(x) = 4x^2$.*

Remarque 1.4.2 *Comme le montre l'exemple ci-dessus, en général et sous réserve d'existence, $g \circ f \neq f \circ g$*

Proposition. 1.4.2.

Si $f : E \to F$, $g : F \to G$ et $h : G \to H$ sont trois applications, alors

$$(h \circ g) \circ f = h \circ (g \circ f)$$

Preuve. En effet, les deux applications ont le même ensemble de départ, E, et même ensemble d'arrivé, H, de plus, pour tout $x \in E$ on a :

$$\begin{aligned} (h \circ g) \circ f(x) &= (h \circ g)\left(f(x)\right) \\ &= h\left(g\left(f(x)\right)\right) \end{aligned}$$

et

$$\begin{aligned} h \circ (g \circ f)(x) &= h\left((g \circ f)(x)\right) \\ &= h\left(g\left(f(x)\right)\right) \end{aligned}$$

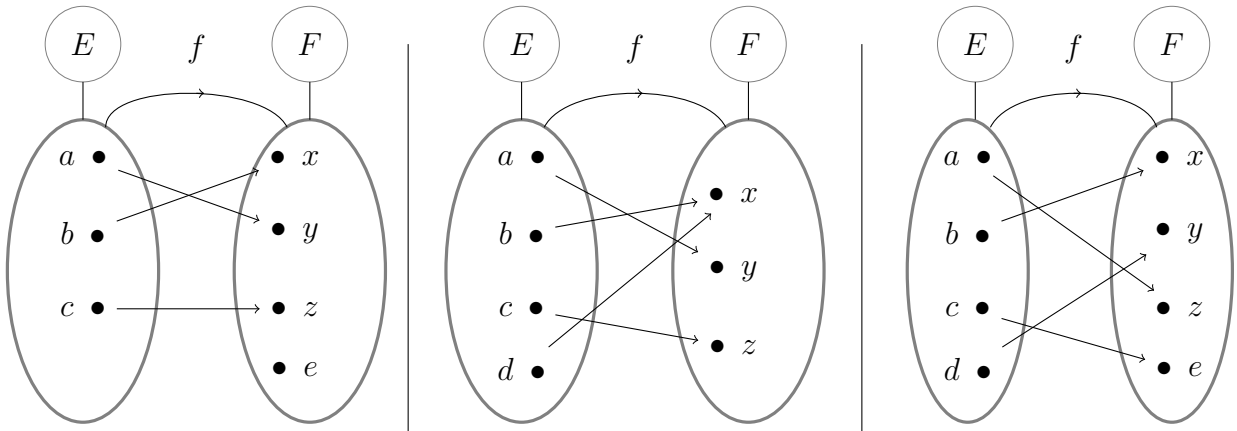
Donc $(h \circ g) \circ f = h \circ (g \circ f)$ ■

1.4.3 Injection, surjection, bijection

Définition. 1.4.3.

On dit qu'une application $f : E \to F$ est

1. injective lorsque :
$$\forall x_1, x_2 \in E \quad f(x_1) = f(x_2) \Longrightarrow x_1 = x_2$$
c'est-à-dire lorsque tout élément y de F a au plus un antécédent.
2. surjective lorsque :
$$\forall y \in F \quad \exists x \in E \quad f(x) = y$$
c'est-à-dire que tout élément y de F a au moins un antécédent.
3. bijective lorsqu'elle est injective et surjective, c'est-à-dire lorsque pour tout élément y de F a un unique antécédent.



Application injective non surjective | application surjective non injective | application bijective

Exemples 1.4.3 *1. L'application f définie de $\mathbb{R}$ vers lui même par $f(x) = x^2$ n'est, ni injective ni surjective. En effet, $f(-1) = f(1)$ avec $-1 \neq 1$, et -1 n'a pas d'antécédent.*

2. L'application f définie de $\mathbb{R}$ vers $\mathbb{R}_+$ par $f(x) = x^2$ est surjective, mais elle n'est pas injective.

3. L'application f définie de $\mathbb{R}_+$ vers $\mathbb{R}$ par $f(x) = x^2$ est injective, mais elle n'est pas surjective.

4. L'application f définie de $\mathbb{R}_+$ vers $\mathbb{R}_+$ par $f(x) = x^2$ est bijective.

EXERCICE 1.4.2 *Montrer que*

$$\begin{array}{rccc} f: & \mathbb{Q} \setminus \left\{2\right\} & \longrightarrow & \mathbb{Q} \setminus \left\{1\right\} \\ & x & \mapsto & f(x) = \dfrac{x-3}{x-2} \end{array}$$

définit une application bijective.

Solution 2 *D'abord, pour tout $x \in \mathbb{Q} \setminus \left\{2\right\}$ on a $\dfrac{x-3}{x-2}$ est bien un nombre rationnel ; car $x \neq 2$ et $x \in \mathbb{Q}$. De plus, $\dfrac{x-3}{x-2} \neq 1$, sinon, on aura :*

$$\begin{aligned} \frac{x-3}{x-2} = 1 &\Longrightarrow x - 3 = x - 2 \\ &\Longrightarrow -3 = -2 \end{aligned}$$

ce qui est faux. Donc f est bien une application.
Soit maintenant $y \in \mathbb{Q} \setminus \left\{1\right\}$. Pour tout $x \in \mathbb{Q} \setminus \left\{2\right\}$ on a :

$$\begin{aligned} f(x) = y &\iff \frac{x-3}{x-2} = y \\ &\iff x - 3 = xy - 2y \\ &\iff x = \frac{3-y}{1-y} \end{aligned}$$

Et on a bien $\frac{3-y}{1-y} \in \mathbb{Q} \setminus \left\{2\right\}$. En effet, $\frac{3-y}{1-y} \in \mathbb{Q}$ puisque $y \in \mathbb{Q}$, et $\frac{3-y}{1-y} \neq 2$ car sinon, comme précédemment on aura $y = 1$. Ainsi, y admet dans un unique antécédent dans $\mathbb{Q} \setminus \left\{2\right\}$. Comme conclusion, f est bijective

Propriétés 1.4.1

Soient $f : E \to F$ et $g : F \to G$ deux applications.

1. *si f et g sont injectives alors $g \circ f$ est injective.*
2. *si f et g sont surjectives alors $g \circ f$ est surjective.*
3. *si f et g sont bijectives alors $g \circ f$ est bijective.*

Preuve.

1. supposons que f et g sont injectives et soient $x, y \in E$ tels que $g \circ f(x) = g \circ f(y)$.

$$\begin{aligned} g \circ f(x) = g \circ f(y) &\implies f(x) = f(y) \text{ ; car } g \text{ est injective} \\ &\implies x = y \text{ ; car } f \text{ est injective} \end{aligned}$$

   Donc, $g \circ f$ est injective.
2. supposons que f et g sont surjectives et soit $z \in G$. Comme g est surjective, alors il existe $y \in F$ tel que $g(y) = z$. Et comme f est surjective, alors il existe $x \in E$ tel que $f(x) = y$. Ainsi $g \circ f(x) = z$ et $g \circ f$ est surjective.
3. C'est une conséquence de 1 et 2.

■

Définition. 1.4.4.

Soit $f : E \to F$ une application bijective. L'application $g : F \to E$, qui à chaque élément $y \in F$ fait correspondre son unique antécédent $x \in E$ par f, s'appelle l'application réciproque de f et se note f^{-1}.

Exemple 1.4.1 *Reprenons l'application*

$$\begin{array}{rccc} f : & \mathbb{Q} \setminus \left\{2\right\} & \longrightarrow & \mathbb{Q} \setminus \left\{1\right\} \\ & x & \mapsto & f(x) = \dfrac{x-3}{x-2} \end{array}$$

de l'exercice 1.4.2. Le calcul qui a été déjà fait montre au fait que $f^{-1}(x) = \frac{3-x}{1-x}$ pour tout $x \in \mathbb{Q} \setminus \left\{1\right\}$.

EXERCICE 1.4.3 *Montrer que l'application suivantes*

$$\begin{array}{rccc} f: & \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ & (x,y) & \mapsto & (x+y, x-y) \end{array}$$

est bijective et déterminer l'expression de f^{-1}.

Solution 3 *Soit* $(x,y) \in \mathbb{R}^2$. *Pour tout* $(a,b) \in \mathbb{R}^2$ *on a :*

$$\begin{aligned} f(a,b) = (x,y) &\iff (a+b, a-b) = (x,y) \\ &\iff \begin{cases} a+b = x \\ a-b = y \end{cases} \\ &\iff \begin{cases} a = \dfrac{x+y}{2} \\ \\ b = \dfrac{x-y}{2} \end{cases} \end{aligned}$$

Donc f *est bijective et* $f^{-1}(x,y) = \left(\dfrac{x+y}{2}, \dfrac{x-y}{2}\right)$ *pour tout* $(x,y) \in \mathbb{R}^2$.

Propriétés 1.4.2

Si $f : E \to F$ *est une application bijective alors* f^{-1} *est bijective et :*

$$\left(f^{-1}\right)^{-1} = f, \quad f \circ f^{-1} = id_F \text{ et } f^{-1} \circ f = id_E$$

Preuve. Évident. ■

Proposition. 1.4.3.

Soit $f : E \to F$ une application. Alors f est bijective si et seulement si il existe une application $g : F \mapsto E$ telle que :

$$g \circ f = \mathrm{id}_E \text{ et } f \circ g = \mathrm{id}_F$$

Si tel est le cas, alors $g = f^{-1}$.

Preuve. Si f est bijective alors il suffit de prendre $g = f^{-1}$. Réciproquement, supposons qu'il existe une application $g : F \mapsto E$ telle que :

$$g \circ f = \mathrm{id}_E \text{ et } f \circ g = \mathrm{id}_F$$

Pour tout $x, y \in E$, si $f(x) = f(y)$ alors $g \circ f(x) = g \circ f(y)$ puis $x = y$. Ainsi f est injective. Pour tout $y \in F$ on a $f\left(g(y)\right) = y$; donc $g(y)$ est un antécédent de y, et alors f est surjective. On en déduit que f est bijective et que $g = f^{-1}$. ■

Exemple 1.4.2 *Soient* E *un ensemble non vide et l'application*

$$\begin{array}{rccc} f: & \mathcal{P}(E) & \longrightarrow & \mathcal{P}(E) \\ & A & \mapsto & \complement_E^A. \end{array}$$

Remarquons que $f \circ f = id_E$. *On en déduit que* f *est bijective et* $f^{-1} = f$.

Proposition. 1.4.4.

Si $f : E \mapsto F$ et $g : F \mapsto G$ deux applications bijectives alors :

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

Preuve. Car $(g \circ f) \circ \left(f^{-1} \circ g^{-1}\right) = \mathrm{id}_G$ et $\left(f^{-1} \circ g^{-1}\right) \circ (g \circ f) = \mathrm{id}_E$ ■

1.4.4 Image directe et indirecte d'une partie par une application

Définition. 1.4.5.

Soit $f : E \to F$.

1. On appelle image réciproque d'une partie B de F par f, et on la note $f^{-1}(B)$, l'ensemble :
$$f^{-1}(B) = \left\{ x \in E \ : \ f(x) \in B \right\}$$
2. On appelle image directe d'une partie A de E par f, et on la note $f(A)$, l'ensemble :
$$f(A) = \left\{ f(x) \ : \ x \in A \right\}$$

Les propriétés suivantes sont faciles à prouver, et les quatre dernières seront énoncées dans le paragraphe suivant sous une forme plus générale ; voir propriétés 1.4.5.

Propriétés 1.4.3

Soient $f : E \mapsto F$ une application, $A_1, A_2 \in E$ et $B_1, B_2 \in F$. Alors

1. $f(\emptyset) = \emptyset$.
2. $f^{-1}(\emptyset) = \emptyset$.
3. $f^{-1}(F) = E$.
4. $\forall x \in E, \ x \in f^{-1}(B) \iff f(x) \in B$.
5. $\forall y \in F, \ y \in f(A) \iff \exists x \in A \ : \ f(x) = y$.
6. $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.
7. $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$.
8. $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$.
9. $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.

EXERCICE 1.4.4 *Soit $f : E \mapsto F$ une application. Montrer que*

$$\forall A_1 \subset E, \ \forall A_2 \subset E, \ f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$$

si et seulement si f est injective.

Solution 4 *Supposons que*

$$\forall A_1 \subset E, \ \forall A_2 \subset E, \ f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$$

et soient $x, y \in E$ tels que $x \neq y$. Prenant $A_1 = \{x\}$ et $A_2 = \{y\}$. Comme $A_1 \cap A_2 = \emptyset$ alors $f(A_1) \cap f(A_2) = \emptyset$ et par la suite $f(x) \neq f(y)$. Ainsi f est injective.
Réciproquement, Supposons que f est injective et Soient $A_1, A_2 \in E$. On sait déjà que $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$. Soit donc $z \in f(A_1) \cap f(A_2)$. Ils existent alors $x \in A_1$ et $y \in A_2$ tels que $f(x) = f(y) = z$. Mais comme f est injective alors $x = y \in A_1 \cap A_2$, ce qui montre que $z \in f(A_1 \cap A_2)$, puis que $f(A_1) \cap f(A_2) = f(A_1 \cap A_2)$.

1.4.5 Familles

Définition. 1.4.6.

Étant donné deux ensemble non vides $\mathtt{I}$ et E, on appelle famille d'éléments de E indexée par les élément de $\mathtt{I}$ toute application $f : \mathtt{I} \to E$.

Notation Dans la pratique, une famille $f : \mathtt{I} \to E$ d'éléments de E indexée par les élément de $\mathtt{I}$ se note tout simplement $(f_i)_{i\in\mathtt{I}}$, et pour tout $i \in \mathtt{I}$, on note f_i au lieu de $f(i)$.

Exemples 1.4.4
1. *Toute suite $(x_n)_{n\in\mathbb{N}}$ à termes dans un ensemble non vide E est une famille.*
2. *En posant $\mathtt{I}_x = \left]-|x|, |x|\right[$ pour tout $x \in \mathbb{R}$, alors $(\mathtt{I}_x)_{x\in\mathbb{R}}$ est une famille d'intervalles de $\mathbb{R}$ indexés par des réels.*

Définition. 1.4.7.

Soient E un ensemble et $(A_i)_{i\in\mathtt{I}}$ une famille de parties de E. On appelle respectivement réunion et intersection de la famille $(A_i)_{i\in\mathtt{I}}$ les parties :

$$\bigcup_{i\in\mathtt{I}} A_i = \left\{x \in E \ : \ \exists i \in \mathtt{I} \ : \ x \in A_i\right\}$$
$$\bigcap_{i\in\mathtt{I}} A_i = \left\{x \in E \ : \ \forall i \in \mathtt{I}, \ x \in A_i\right\}$$

Remarque 1.4.3 *Dans le cas particulier $\mathtt{I} = \{1, 2, \cdots, n\}$, ces notations deviennent $\bigcup_{i=1}^{n} A_i$ et $\bigcap_{i=1}^{n} A_i$. Et dans le cas où $\mathtt{I} = \mathbb{N}$, on les note $\bigcup_{n=0}^{+\infty} A_n$ et $\bigcap_{n=0}^{+\infty} A_n$.*

Exemples 1.4.5 *Si on pose $\mathtt{I}_n =]-\frac{1}{n}, \frac{1}{n}[$ pour tout $n \in \mathbb{N}^*$, alors : $\bigcup_{n=1}^{+\infty} \mathtt{I}_n =]-1, 1[$ et $\bigcap_{n=1}^{+\infty} \mathtt{I}_n = \{0\}$.*

Propriétés 1.4.4

Si $A \subset F$ et $(A_i)_{i\in\mathtt{I}}$ est une famille de parties de E alors :

1. $A \bigcap \left(\bigcup_{i\in\mathtt{I}} A_i\right) = \bigcup_{i\in\mathtt{I}} \left(A \bigcap A_i\right)$
2. $A \bigcup \left(\bigcap_{i\in\mathtt{I}} A_i\right) = \bigcap_{i\in\mathtt{I}} \left(A \bigcup A_i\right)$
3. $\overline{\bigcap_{i\in\mathtt{I}} A_i} = \bigcup_{i\in\mathtt{I}} \overline{A_i}$
4. $\overline{\bigcup_{i\in\mathtt{I}} A_i} = \bigcap_{i\in\mathtt{I}} \overline{A_i}$

Preuve.

1 Soit $x \in A \bigcap \left(\bigcup_{i \in \mathtt{I}} A_i \right)$. Donc $x \in A$ et $x \in \bigcup_{i \in \mathtt{I}} A_i$. Il existe alors $j \in \mathtt{I}$ tel que $x \in A_j$, et donc $x \in A \cap A_j$. Ceci montre que $x \in \bigcup_{i \in \mathtt{I}} \left(A \bigcap A_i \right)$. Donc on a l'inclusion $A \bigcap \left(\bigcup_{i \in \mathtt{I}} A_i \right) \subset \bigcup_{i \in \mathtt{I}} \left(A \bigcap A_i \right)$.

Réciproquement, soit $x \in \bigcup_{i \in \mathtt{I}} \left(A \bigcap A_i \right)$. Il existe alors $j \in \mathtt{I}$ tel que $x \in A \cap A_j$. Donc, $x \in A$ et $x \in A_j$, et par la suite $x \in A$ et $x \in \bigcup_{i \in \mathtt{I}} A_i$, puis $x \in A \bigcap \left(\bigcup_{i \in \mathtt{I}} A_i \right)$.

Conclusion : $A \bigcap \left(\bigcup_{i \in \mathtt{I}} A_i \right) = \bigcup_{i \in \mathtt{I}} \left(A \bigcap A_i \right)$

3 Pour tout $x \in E$ on a

$$\begin{aligned} x \in \overline{\bigcap_{i \in \mathtt{I}} A_i} &\iff x \notin \bigcap_{i \in \mathtt{I}} A_i \\ &\iff \exists j \in \mathtt{I},\ x \notin A_j \\ &\iff \exists j \in \mathtt{I},\ x \in \overline{A_i} \\ &\iff x \in \bigcup_{i \in \mathtt{I}} \overline{A_i} \end{aligned}$$

Donc $\overline{\bigcap_{i \in \mathtt{I}} A_i} = \bigcup_{i \in \mathtt{I}} \overline{A_i}$

2 On peut faire comme dans (1), mais on préfère appliquer (3), en montrant que les complémentaires sont égaux. En effet,

$$\begin{aligned} \overline{A \bigcup \left(\bigcap_{i \in \mathtt{I}} A_i \right)} &= \overline{A} \bigcap \overline{\bigcap_{i \in \mathtt{I}} A_i} \\ &= \overline{A} \bigcap \bigcup_{i \in \mathtt{I}} \overline{A_i} \\ &= \bigcup_{i \in \mathtt{I}} \left(\overline{A} \bigcap \overline{A_i} \right) \\ &= \bigcup_{i \in \mathtt{I}} \left(\overline{A \bigcup A_i} \right) \\ &= \overline{\bigcap_{i \in \mathtt{I}} \left(A \bigcup A_i \right)} \end{aligned}$$

4 Il suffit de montrer qu'ils ont le même complémentaire. En effet

$$\begin{aligned} \overline{\overline{\bigcup_{i \in \mathtt{I}} A_i}} &= \bigcup_{i \in \mathtt{I}} A_i \\ &= \bigcup_{i \in \mathtt{I}} \overline{\overline{A_i}} \\ &= \overline{\bigcap_{i \in \mathtt{I}} \overline{A_i}} \end{aligned}$$

D'où le résultat.

■

Définition. 1.4.8.

Soient E un ensemble, et $\mathcal{F}$ une partie de $\mathcal{P}(E)$. On dit $\mathcal{F}$ est une partition de E, ou encore que les éléments de $\mathcal{F}$ forment une une partition de E, si :

1. Les éléments de $\mathcal{F}$ sont deux à deux disjoints, c'est à dire : $\forall A, B \in \mathcal{F}, A \neq B \Longrightarrow A \cap B = \emptyset$
2. $\bigcup_{A \in \mathcal{F}} A = E$

Exemple 1.4.3 *L'ensemble des entiers relatifs pairs et celui des entiers relatifs impairs forment une partition de $\mathbb{Z}$.*

Proposition. 1.4.5.

Les classes d'équivalence d'une relation d'équivalence sur un ensemble E forment une partition de E.

Preuve. On sait que deux classes d'équivalences sont soit égales, soit disjointes. De plus, tout élément de E appartient à sa classe d'équivalence. Ceci achève la preuve. ■

Propriétés 1.4.5

Soient $f : E \mapsto F$ une application, $(A_i)_{i \in \mathtt{I}}$ une famille de parties de E et $(B_i)_{i \in \mathtt{I}}$ une famille de parties de F. Alors :

1. $f\left(\bigcup_{i \in \mathtt{I}} A_i\right) = \bigcup_{i \in \mathtt{I}} f(A_i)$
2. $f\left(\bigcap_{i \in \mathtt{I}} A_i\right) \subset \bigcap_{i \in \mathtt{I}} f(A_i)$
3. $f^{-1}\left(\bigcup_{i \in \mathtt{I}} B_i\right) = \bigcup_{i \in \mathtt{I}} f^{-1}(B_i)$
4. $f^{-1}\left(\bigcap_{i \in \mathtt{I}} B_i\right) = \bigcap_{i \in \mathtt{I}} f^{-1}(B_i)$

Preuve.

1. Pour tout $j \in \mathtt{I}$ on a $A_j \subset \bigcup_{i \in \mathtt{I}} A_i$, donc $f(A_j) \subset f\left(\bigcup_{i \in \mathtt{I}} A_i\right)$ et par la suite $\bigcup_{i \in \mathtt{I}} f(A_i) \subset f\left(\bigcup_{i \in \mathtt{I}} A_i\right)$.

   Pour la réciproque, considérons $y \in f\left(\bigcup_{i \in \mathtt{I}} A_i\right)$. Il existe alors $x \in \bigcup_{i \in \mathtt{I}} A_i$ tel que $y = f(x)$. Il existe également $j \in \mathtt{I}$ tel que $x \in A_j$, et par conséquent $y \in f(A_j)$ puis $y \in \bigcup_{i \in \mathtt{I}} f(A_i)$.

   Conclusion : $f\left(\bigcup_{i \in \mathtt{I}} A_i\right) = \bigcup_{i \in \mathtt{I}} f(A_i)$

(2) ,(3) et(4) Laissés à titre d'exercice.

■

1.5 EXERCICES

1.5.1 Éléments de logique

EXERCICE 1 *Donner la valeur de vérité de chacune des propositions suivantes*

1. $0 = 0$ *et* $2 + 1 = 8$
2. $0 = 0$ *ou* $2 + 1 = 8$
3. $0 = 0 \Longrightarrow 2 + 1 = 8$
4. $0 = 1 \Longrightarrow 2 + 1 = 3$
5. $\forall x \in \mathbb{R}, (x \geq 0 \Longrightarrow 2 = 4)$
6. $(\forall x \in \mathbb{R}, x \geq 0) \Longrightarrow 2 = 4$

EXERCICE 2 *Soient les quatre assertions suivantes :*

a. $\exists x \in \mathbb{R}\ \forall y \in \mathbb{R} \quad x + y > 0$
b. $\forall x \in \mathbb{R}\ \exists y \in \mathbb{R} \quad x + y > 0$
c. $\forall x \in \mathbb{R}\ \forall y \in \mathbb{R} \quad x + y > 0$
d. $\exists x \in \mathbb{R}\ \forall y \in \mathbb{R} \quad y^2 > x$

1. *Les assertions* a, b, c, d *sont-elles vraies ou fausses ?*
2. *Donner leur négation.*

EXERCICE 3 *Soit* f, g *deux fonctions de* $\mathbb{R}$ *dans* $\mathbb{R}$. *Traduire en termes de quantificateurs les expressions suivantes :*

1. f *est majorée ;*
2. f *est bornée ;*
3. f *est paire ;*
4. f *est impaire ;*
5. f *ne s'annule jamais ;*
6. f *n'est pas la fonction nulle ;*
7. f *est périodique ;*
8. f *est croissante ;*
9. f *est strictement décroissante ;*
10. f *n'est pas surjective ;*
11. f *atteint toutes les valeurs de* $\mathbb{N}$ *;*
12. f *est inférieure à* g *;*
13. f *n'est pas inférieure à* g.

EXERCICE 4 *Compléter les pointillés par le connecteur logique qui s'impose :* $\Longleftrightarrow$, $\Leftarrow$, $\Rightarrow$.

1. $x \in \mathbb{R};\ x^2 = 4 \ \ldots\ldots\ x = 2$;
2. $z \in \mathbb{C};\ z = \overline{z} \ \ldots\ldots\ z \in \mathbb{R}$;
3. $x \in \mathbb{R}\ \ x = \pi \ \ldots\ldots\ e^{2ix} = 1$.

EXERCICE 5 *Nier les assertions suivantes :*

1. *tout triangle rectangle possède un angle droit ;*
2. *dans toutes les écuries, tous les chevaux sont noirs ;*
3. $\forall \epsilon > 0\ \exists \alpha > 0\ /\ |x - 7/5| < \alpha \Rightarrow |5x - 7| < \epsilon$.
4. *pour tout entier* x, *il existe un entier* y *tel que, pour tout entier* z, *la relation* $z < x$ *implique le relation* $z < x + 1 < y$ *;*

EXERCICE 6 *Soit* f *une application de* $\mathbb{R}$ *dans* $\mathbb{R}$. *Nier, de la manière la plus précise possible, les énoncés qui suivent :*

1. *Pour tout* $x \in \mathbb{R}\ f(x) \leq 1$.
2. *L'application* f *est croissante.*
3. *L'application* f *est croissante et positive.*

4. *Il existe $x \in \mathbb{R}^+$ tel que $f(x) \leq 0$.*
5. *Il existe $x \in \mathbb{R}$ tel que quel que soit $y \in \mathbb{R}$, si $x < y$ alors $f(x) > f(y)$.*

On ne demande pas de démontrer quoi que ce soit, juste d'écrire le contraire d'un énoncé.

EXERCICE 7 *Montrer que*

$$\forall \epsilon > 0,\ \exists N \in \mathbb{N}\ :\ \forall n \in \mathbb{N},\ n \geq N \Longrightarrow 2 - \epsilon < \frac{2n+1}{n+2} < 2 + \epsilon$$

EXERCICE 8 *Soit $(f_n)_{n\in\mathbb{N}}$ une suite d'applications de l'ensemble $\mathbb{N}$ dans lui-même. On définit une application f de $\mathbb{N}$ dans $\mathbb{N}$ en posant $f(n) = f_n(n) + 1$. Démontrer qu'il n'existe aucun $p \in \mathbb{N}$ tel que $f = f_p$.*

EXERCICE 9 *Soit $p_1, p_2, \ldots, p_r$, r nombres premiers.*

1. *Montrer que l'entier $N = p_1 p_2 \ldots p_r + 1$ n'est divisible par aucun des entiers p_i.*
2. *Utiliser la question précédente pour montrer par l'absurde qu'il existe une infinité de nombres premiers.*

EXERCICE 10

1. *Démontrer que la somme d'une suite convergente, et d'une suite divergente, est une suite divergente.*
2. *Que dire de la somme de deux suites divergentes ?*

EXERCICE 11

1. *Démontrer que la somme de deux nombres rationnels est un nombre rationnel.*
2. *Démontrer que la somme d'un nombre rationnel et un nombre irrationnel, est un nombre irrationnel.*
3. *Que dire de :*
   - *la somme de deux irrationnels ?*
   - *le produit d'un rationnel non nul par un irrationnel non nul*
   - *l'inverse d'un irrationnel ?*

EXERCICE 12 *Sachant que $\sqrt{30} \notin \mathbb{Q}$, montrer que $\sqrt{2} + \sqrt{3} + \sqrt{5} \notin \mathbb{Q}$.*

EXERCICE 13 *. Raisonnement par analyse et synthèse*
Montrer que toute application de $\mathbb{R}$ vers lui même s'écrit comme somme de deux applications, l'une paire et l'autre impaire.

EXERCICE 14 *Montrer que pour tout entier $n \geq 1$ on a :*

1. $1 + 2 + ... + n = \dfrac{n(n+1)}{2}$
2. $1^2 + 2^2 + ... + n^2 = \dfrac{n(n+1)(2n+1)}{6}$
3. $1^3 + 2^3 + ... + n^3 = \left(\dfrac{n(n+1)}{2}\right)^2$

EXERCICE 15 *Donner une expression simple de*

$$S_n = \sum_{p=0}^{n} \frac{1}{p^2 + 3p + 2}$$

1.5.2 Inclusion, opérations sur les ensembles

EXERCICE 16 *Soient E un ensemble, A, B, C et D des parties de E. Montrer que :*

1. $(A \cap B = A \cup C$ *et* $A \cup B = A \cap C) \Longrightarrow A = B = C$
2. $A \setminus B = A \Longleftrightarrow B \setminus A = B$
3. $(A \subset C,\ B \subset D,\ A \cup B = C \cup D$ *et* $C \cap D = \emptyset) \Longrightarrow (A = C$ *et* $B = D)$
4. $(A \cap B) \setminus C = (A \setminus C) \cap (B/C)$
5. $(A \cup B) \setminus C = (A/C) \cup (B \setminus C)$
6. $(A \setminus B) \setminus C = (A \setminus C) \setminus (B \setminus C) = A \setminus (B \cup C)$
7. $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$
8. $A = B \Longleftrightarrow A \cap B = A \cup B$
9. $A \cup B \subset A \cup C$ *et* $A \cap B \subset A \cap C \Longrightarrow B \subset C$

EXERCICE 17 *Soient , B des parties de E. Simplifier les expressions suivantes :*
1) $(A \cap B) \cup (\overline{A} \cap B) \cup (A \cap \overline{B}) \cup (\overline{A} \cap \overline{B})$.
2) $A \cup (\overline{A} \cap B) \cup (\overline{A} \cap \overline{B} \cap C)$
3) $A \backslash (A \backslash B)$.

EXERCICE 18 *Soit E un ensemble non vide. A chaque partie A de E, on fait assoicier l'application caractéristique χ_A définie par :*

$$\begin{array}{rccc} \chi_A : & E & \longrightarrow & \{0,1\} \\ & x & \longmapsto & \begin{cases} 1, & \text{si } x \in A \\ 0, & \text{si } x \notin A. \end{cases} \end{array}$$

Montrer que :

1. $A = B \Longleftrightarrow \chi_A = \chi_B$.
2. $\chi_{A \cap B} = \chi_A \chi_B$.
3. $\chi_{A \cup B} = \chi_A + \chi_B - \chi_A \chi_B$
4. $\chi_{\overline{A}} = 1 - \chi_A$
5. $\chi_{A \setminus B} = \chi_A - \chi_A \chi_B$.
6. $\chi_{A \triangle B} = |\chi_A - \chi_B|$

1.5.3 Applications injectives, surjectives, bijectives

EXERCICE 19 *Soient E , F et G des ensembles non vides, f une application de E dans F et g une application de F dans G .*

1. *Montrer que si gof est injective, alors f est injective .*
2. *Montrer que si gof est surjective, alors g est surjective.*

EXERCICE 20 *Soit E un ensemble, f, g et h des applications de E dans E. Montrer que :*

1. *Si gof et hog sont bijectives, alors f, g et h sont bijectives*
2. *Si $hogof$ et $gofoh$ sont surjectives et $fohog$ est injectives, alors f,g et h sont bijectives .*
3. *Si $fof = f$, et si f est surjective ou injective alors $f = id_E$*
4. *Si $fofof = f$ et f est surjective , alors f est bijective. quelle est sa application réciproque f^{-1} ?*

EXERCICE 21 *Montrer que l'application f définie de $\mathbb{N} \times \mathbb{N}$ dans $\mathbb{N}$ par*

$$f(p,q) = p^2 + 2pq + q^2 + p$$

est injective. Est-elle surjective ?

EXERCICE 22 **(a)** *Montrer que si f est une application injective de F vers G alors pour toutes applications g et h de E vers F on a $fog = foh \Longrightarrow g = h$.*
Que dire de la réciproque ?

(b) *Montrer que si f est une application surjective de E vers F alors pour toutes applications g et h de F vers G on a $gof = hof \Longrightarrow g = h$.*
Que dire de la réciproque ?

1.5.4 Image directe, image réciproque d'une partie par une application

EXERCICE 23 *Soient E et F deux ensembles non vides , f une application de E dans F , A_1 , A_2 deux parties de E , B_1 et B_2 deux parties de F. Montrer que :*

1. $A_1 \subset A_2 \Longrightarrow f(A_1) \subset f(A_2)$.
2. $B_1 \subset B_2 \Longrightarrow (f^{-1}(B_1) \subset f^{-1}(B_2)$
3. $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$ *. Peut-on génèraliser ce résultat ?*
4. $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$. *Peut-on génèraliser ce résultat ? A quelle condition on a l'egalité ?*
5. *Comparer* $\overline{f(A_1)}$ *et* $f(\overline{A_1})$
6. *Comparer* $\overline{f^{-1}(B_1)}$ *et* $f^{-1}(\overline{B_1})$

EXERCICE 24 *Soit f une application d'un ensemble E dans un ensembles F , A une partie de E et B une partie de F .*

1. *Montrer que* $A \subset f^{-1}(f(A))$
2. *Montrer que* $f(f^{-1}(f(A))) = f(A)$
3. *Montrer que* $f^{-1}(f(f^{-1}(B))) = f^{-1}(B)$
4. *Montrer que* $f(f^{-1}(B)) \subset B$.
5. *Montrer que* $(\forall A \in P(E) \ , \ f^{-1}(f(A)) = A) \Longleftrightarrow f$ *est injective .*
6. *Montrer que* $(\forall B \in P(F) \ , \ f(f^{-1}(B)) = B) \Longleftrightarrow f$ *est surjective.*

EXERCICE 25 *Soit E un ensemble non vide et f une application de E dans E. On pose $I_0 = E$ et pour tout entier non nul n, $I_{n+1} = f(I_n)$.*

1. *Prouver que ,* $\forall n \in \mathbb{N} \ , \ I_{n+1} \subset I_n$
2. *Prouver que s'il existe un entier i tel que $I_{i+1} = I_i$, alors , pour tout entier $n > i$ on a $I_n = I_i$.*
Que peut-on dire si f est surjective ?

1.5.5 Relations

EXERCICE 26 *Soient E un ensemble et f une application bijective de E dans E. Pour tout $n \in \mathbb{N}^\star$, on pose $f^n = fofo \ldots of$ (f répété n fois); de même : $f^{-n} = (f^{-1})^n$ et $f^0 = id_E$. On définit dans E la relation $\Re$ par :*

$$\forall (x,y) \in E^2 \ , \ x \Re y \Longleftrightarrow (\exists n \in \mathbb{Z} \ , \ y = f^n(x))$$

1. *Démontrer que $\Re$ est une relation d'équivalence sur E.*
(On admettra que $\forall (n,p) \in \mathbb{Z}^2 \ , \ f^n of^p = f^{n+p}$).

2. *Montrer que si C est une classe d'equivalence modulo $\Re$, alors $f(C) = C$*
3. *Démontrer que, réciproquement, toute partie X non vide de E telle que $f(X) = X$ est une réunion de classes déquivalence pour $\Re$*

EXERCICE 27 *Soit E un ensemble. Vérifier que la relation $\Re$ définie dans P par :*

$$A\Re B \Longleftrightarrow A = B \text{ ou } A = \overline{B}$$

est une relation d'équivalence

EXERCICE 28 *On définit sur $\mathbb{R}$ la relation :*

$$x\mathcal{R}y \Longleftrightarrow x^3 - y^3 = 3(x - y)$$

.

1. *Montrer que $\mathcal{R}$ est une relation d'équivalence.*
2. *Déterminer, pour tout réel x, le cardinal de la classe d'équivalence de x.*

EXERCICE 29 *Montrer que la relation $\Re$ définie dans $\mathbb{R}$ par :*

$$x\Re y \Longleftrightarrow xe^y = ye^x$$

est une relation d'équivalence.

EXERCICE 30 *Étudier la relation $\Re$ défini dans $\mathbb{N}$ par :*

$$x\Re y \Longleftrightarrow \exists n \in \mathbb{N}, y = x^n$$

EXERCICE 31 *Soit $(E, \leq)$ un ensemble ordonné. Pour tout $x \in E$ on définit la partie notée $\varphi(x)$ par : $\varphi(x) = \{t \in E \ / \ t \leq x\}$*

1. *Démontrer que $\forall (x, y) \in E^2 \ , \ x \leq y \iff \varphi(x) \subset \varphi(y)$*
2. *Démontrer que φ est une injection de E dans $P(E)$. Est-ce une surjection ?*
3. *Réciproquement, Soit ϕ une injection de E dans $P(E)$. On définit la relation $\Re$ par :*

$$\forall (x, y) \in E^2 \ , \ x\Re y \Longleftrightarrow \phi(x) \subset \phi(y)$$

Démontrer que $\Re$ est une relation d'ordre.

EXERCICE 32 *Soit $\mathcal{R}$ la relation binaire définie sur $\mathbb{R}^2$ par :*

$$(x, y))\mathcal{R}(x_0, y_0) \Longleftrightarrow |x - x_0| \leq y - y_0$$

1. *Montrer que $\mathcal{R}$ est une relation d'ordre*
2. *Soit $(a, b) \in \mathbb{R}^2$, déssiner $\{(x, y) \in \mathbb{R}^2 / (x, y)\mathcal{R}(a, b)\}$*

EXERCICE 33 *Soit $(E, \leq)$ un ensemble ordonnée dont toute partie non vide admet un plus petit élément. Si $(x, y) \in E^2$ est tel que $x \leq y$. $x \neq y$, on dit que x est strictement inférieur à y et on écrit $x < y$. On considère une bijection f de E vers F. On suppose que f est strictement croissante ; c'est à dire :*

$$\forall\, (x, y) \in E^2,\ x < y \Longrightarrow f\,(x) < f\,(y)$$

1. *Montrer que f^{-1} est strictement croissante.*
2. *Montrer que f l'application identique.*

Chapitre 2

Arithmétique des entiers

On rappelle que l'ensemble $\mathbb{Z}$ est l'ensemble des entiers relatifs formé des entiers naturels et de leurs opposés :

$$\mathbb{Z} = \{...., -2, -1, 0, 1, 2, ...\} = \mathbb{N} \cup (-\mathbb{N})$$

On munit cet ensemble de l'addition et de la multiplication habituelles.

2.1 Divisibilité et Division Euclidienne

Définition. 2.1.1.

Soient a et b deux entiers relatifs. S'il existe un entier relatif q vérifiant :

$$a = qb$$

alors il est équivalent de dire que : b **divise** a, a **est divisible par** b, b est un diviseur de a ou encore que a est un multiple de b.

Exemples 2.1.1

1. *Tous les entiers divisent* 0*, mais le seul entier divisible par* 0 *est* 0 *lui même.*
2. *L'entier* 1 *est un diviseur commun de tous les entiers ainsi que* -1*.*
3. *Les seuls diviseurs de* 1 *et de* -1 *sont* 1 *et* -1*.*
4. 6 *divise* 30 *et* 12 *ne le divise pas.*

Proposition. 2.1.1.

On définit ainsi une relation binaire sur $\mathbb{Z}$ réflexive et transitive mais n'est ni symétrique ni antisymétrique. La restriction de cette relation à l'ensemble des entiers naturels est une relation d'ordre partiel.

Propriétés 2.1.1

Pour tout $a, b, c, u, v \in \mathbb{Z}$ on a :

1. *b divise $a \Leftrightarrow |b|$ divise $|a|$.*
2. *a divise b et b divise $a \Leftrightarrow |a| = |b|$.*
3. *b divise $a \Rightarrow$ bc divise ac.*
4. *b divise $a \Rightarrow$ $a = 0$ ou bien $|b| \leq |a|$.*
5. *c divise a et $b \Longrightarrow c$ divise $au + bv$*

Remarque 2.1.1 *Deux entiers qui se divisent l'un l'autre sont dits **entiers associés** ce qui est équivalent à dire, d'après la propriété (2.), qu'ils sont égaux en valeur absolue.*

Notation Pour tout $a \in \mathbb{Z}$ on note $\mathcal{D}(a)$ l'ensemble des diviseurs positifs de a :

$$\mathcal{D}(a) = \{d \in \mathbb{N} : d \text{ divise } a\}$$

Propriétés 2.1.2

Pour tout $a, b \in \mathbb{Z}$:

1. *$\mathcal{D}(a) = \mathcal{D}(-a)$.*
2. *Pour $a \neq 0$ $\mathcal{D}(a)$ est fini.*
3. *Si b divise a alors $\mathcal{D}(b) \subset \mathcal{D}(a)$.*

Théorème. 2.1.1.

Division Euclidienne
Soient $a, b \in \mathbb{Z} \times \mathbb{Z}^*$ alors il existe un unique couple (q, r) d'entiers relatifs tels que :

$$\begin{cases} a = qb + r \\ 0 \leq r < |b| \end{cases}$$

On parle de la **division euclidienne** de a par b. q et r s'appellent respectivement le **quotient** et le **reste** de cette division, a est dit **dividende** et b le **diviseur**.

Preuve.

— Prouvons, d'abord, l'existence du couple (q, r) dans le cas où, $(a, b) \in \mathbb{N} \times \mathbb{N}^*$: On considère

$$I = \{q \in \mathbb{N} : a - qb \geq 0\}$$

I est une partie de $\mathbb{N}$ non vide (puisque 0 y appartient) et majorée par a. En effet : si, $q \in I$ alors et comme $b \geq 1$ on aura : $q \leq qb \leq a$. On en déduit que : I admet un plus grand élément qu'on notera q de sorte que par définition du plus grand élément on aura :

$$\begin{cases} qb \leq a \\ a < (q+1)b \end{cases}$$

En posant $r = a - qb$ on déduit l'existence du couple (q, r).

— Existence dans le cas où, $a \in (-\mathbb{N})$ et $b \in \mathbb{N}^*$: Dans ce cas $-a \in \mathbb{N}$ ce qui nous ramène au premier cas. Il existe donc un couple (q', r') d'entiers naturels vérifiant : $-a = q'b + r'$ avec $0 \leq r' < b$ par suite $a = -q'b - r'$. Alors deux cas se présentent : si $r' = 0$ il suffit de prendre $q = -q'$ et $r = 0$ sinon, on prend $q = -q' - 1$ et $r = b - r'$. D'où l'existence dans ce cas aussi.

— Existence dans le cas où $b \in -\mathbb{N}^*$: D'après les deux cas précédents, on peut effectuer la division euclidienne de a par $-b$ donc il existe un couple (q', r') d'entiers tels que : $a = q'(-b) + r'$ avec $0 \leq r' < (-b) = |b|$. Il suffit alors de prendre $q = -q'$ et $r = r'$. Ainsi l'existence du couple (q, r) est assurée dans tous les cas envisagés.

— Nous allons établir maintenant l'unicité : Considèrons deux couples (q, r) et (q', r') réalisant les conditions du théorème. Alors on a : $(q - q')b = r' - r$ ce qui signifie que b divise $(r' - r)$. Or $|(r' - r)| < |b|$ ce qui entraîne d'après la propriété (4.) précédente que $r' - r = 0$. D'où, l'unicité.

Ce qui achève la démonstration du théorème. ■

Exemple 2.1.1 *Effectuer la division euclidienne de* 451 *par* 41 *puis de* 3225 *par* 35.

2.2 PGCD et PPCM d'entiers

2.2.1 PGCD de deux entiers et algorithme d'Euclide

Théorème. 2.2.1.

(et définition)
Soient a et b deux entiers dont l'un des deux au moins n'est pas nul alors l'ensemble des diviseurs communs à a et b admet un plus grand élément (au sens de l'ordre de $\mathbb{Z}$) dit **plus grand commun diviseur** de a et b et noté $PGCD(a, b)$ ou $a \wedge b$.

Preuve. Suposons par exemple que a est non nul, alors $\mathcal{D}(a)$ est fini et par suite $\mathcal{D}(a) \cap \mathcal{D}(b)$ est une partie finie de $\mathbb{N}$ et de plus elle est non vide puisque $1 \in \mathcal{D}(a) \cap \mathcal{D}(b)$. Ainsi $\mathcal{D}(a) \cap \mathcal{D}(b)$ admet bien un plus grand élément. ■

Remarque 2.2.1 *Le* $PGCD$ *de deux entiers dont un au moins n'est pas nul est un entier naturel non nul. On peut convenir que* $a \wedge b = 0$ *lorsque* $a = b = 0$.

Remarque 2.2.2 *Si* $a \neq 0$ *alors* $a \wedge 0 = |a|$.

Propriétés 2.2.1

Soient a *et* b *deux entiers tel que* $b \neq 0$.

1. $a \wedge b = |a| \wedge |b|$; *On peut donc toujours se ramener au calcul du* $PGCD$ *d'entiers naturels.*
2. $a \wedge b = |b| \iff b$ *divise* a.
3. $a \wedge b = b \wedge a$.
4. $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ *pour tout entier* c.
5. $(ac) \wedge (bc) = |c|\,(a \wedge b)$; *Pour tout entier* c *non nul.*
6. $\left(\frac{a}{d}\right) \wedge \left(\frac{b}{d}\right) = \frac{a \wedge b}{|d|}$; *Pour tout diviseur* d *commun à* a *et* b.

Lemme 2.2.1 *(d'Euclide)*
Soient a, b, q *et* r *quatre entiers tels que :* $a = qb + r$. *Alors on a :*

$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(r)$$

ce qui entraîne, en particulier, lorsque a ou b n'est pas nul que :

$$a \wedge b = b \wedge r$$

En particulier, si $r = 0$ alors :

$$a \wedge b = |b|$$

Preuve. Il suffit de remarquer que $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(r)$. ■

Théorème. 2.2.2.

(de l'Algorithme d'Euclide)
Soient a et b deux entiers naturels tels que b n'est pas nul. Alors il existe un entier naturel non nul k et deux suites finies d'entiers $(q_1, ..., q_k)$ et $(r_0, ..., r_{k+1})$ tels que :

$$\begin{aligned} r_0 &= a,\ r_1 = b \\ r_{i-1} &= q_i r_i + r_{i+1}\ \forall 1 \leq i \leq k-1 \\ 0 &\leq r_{k-1} < r_{k-2} < ... < r_1 \\ r_k &\neq 0 \text{ et } r_{k+1} = 0 \end{aligned}$$

de sorte que :

$$a \wedge b = r_k$$

On dit que $a \wedge b$ coïncide avec le dernier reste non nul des divisions euclidiennes effectuées dans l'algorithme d'Euclide.

Preuve. On pose $r_0 = a$ et $r_1 = b$
Première étape :
On effectue la division euclidienne de $a = r_0$ par $b = r_1$:

$$\begin{cases} a = q_1 b + r_2 \\ 0 \leq r_2 < b \end{cases}$$

On déduit du lemme d'Euclide que : $a \wedge b = b \wedge r_2$. De sorte que, si $r_2 = 0$ alors $a \wedge b = b$ et l'algorithme s'arrête. Sinon, on passe à l'étape suivante :
Deuxième étape :
On réaapplique la première étape en remplaçant $a = r_0$ par $b = r_1$ et $b = r_1$ par r_2, on obtient :

$$\begin{cases} r_1 = b = q_2 r_2 + r_3 \\ 0 \leq r_3 < r_2 \end{cases}$$

et on a : $a \wedge b = r_1 \wedge r_2 = r_2 \wedge r_3$. Si, $r_3 = 0$ alors $a \wedge b = r_2$ et sinon, on recommence.
Ce processus doit s'arrêter au bout d'un nombre fini k d'étapes $(1 \leq k \leq b)$. Car sinon,, cela entraînerait l'existence de deux suites $(q_1, ..., q_b)$ et $(r_0, ..., r_{b+1})$ tels qu'on ait :

$$\begin{aligned} r_{i-1} &= q_i r_i + r_{i+1}\ \forall 1 \leq i \leq b \\ 0 &\leq r_{b+1} < r_b < ... < r_1 = b \end{aligned}$$

soit que $0 \leq r_{b+1} \leq -1$ ce qui est absurde. On déduit donc que l'algorithme s'arrête au bout d'un nombre fini k d'étapes, ce qui signifie l'existence des deux suites finies $(q_1, ..., q_k)$ et $(r_0, ..., r_{k+1})$ tels que :

$$\begin{aligned} r_0 &= a,\ r_1 = b \\ r_{i-1} &= q_i r_i + r_{i+1}\ \forall 1 \leq i \leq k-1 \\ 0 &\leq r_{k-1} < r_{k-2} < ... < r_1 \\ r_k &\neq 0 \text{ et } r_{k+1} = 0 \end{aligned}$$

Il s'en suit que : $a \wedge b = r_1 \wedge r_2 = ... = r_{k-1} \wedge r_k = r_k$. Ce qui achève la preuve du théorème. ■

Algorithme (Détermination pratique du $p\gcd$)
Soit $a, b \in \mathbb{Z}^*$ et $d = p\gcd(a, b)$. Comme $a \wedge b = |a| \wedge |b|$ on peut supposer que $a, b \in \mathbb{N}^*$.
$1^{er} test$: Si b divise a alors $d = b$
Sinon On effectue la division euclidienne de a par b et il existe $(q_0, r_1) \in \mathbb{Z}^2$ tels que :

$$\begin{aligned} a &= bq_0 + r_1 \\ 0 &\leq r_1 < b \end{aligned}$$

Et d'après le lemme d'Euclide $d = a \wedge b = b \wedge r_1$
$2^{ème} test$: Si r_1 divise b alors $d = a \wedge b = b \wedge r_1 = r_1$
Sinon On effectue la division euclidienne de b par r_1 et il existe $(q_1, r_2) \in \mathbb{Z}^2$ tels que :

$$\begin{aligned} b &= bq_1 + r_2 \\ 0 &\leq r_2 < r_1 < b \end{aligned}$$

Et d'après le lemme d'Euclide $d = a \wedge b = b \wedge r_1 = r_1 \wedge r_2$ et on recommence le test avec r_1 et r_2. Comme $\{0, 1, ..., b-1\}$ est fini cet algorithme s'arrête dans au plus b étapes (b divisions euclidiennes) et donc il existe $n \in \mathbb{N}^*$ et une suite d'entiers
$0 = r_n < r_{n-1} < r_{n-2} < ... < r_1 < r_0 = b$ et tel que $a \wedge b = b \wedge r_1 = r_1 \wedge r_2 = r_{n-1} \wedge r_n = r_{n-1}$.
En conclusion $a \wedge b$ est le dernier reste non dans l'algorithme d'Euclide ci-dessus.

Exemple 2.2.1 *de détermination du $PGCD$ de deux entiers :*
$235 \wedge 115 = 5$; $3527 \wedge 211 = 1$

235	115	5
5	0	

3527	211	151	60	31	29	2
151	60	31	29	2	1	

EXERCICE 2.2.1 1. *Écrire une fonction en python nommée "$PGCD$" prenant en argument deux entiers a et b et renvoyant leur PGCD quand c'est bien défini.*

2. *Qu'obtient-on en exécutant le script précédent si :*

   (a) $a = 0$ *et* $b = 2$.
   (b) $a = 3527$ *et* $b = 211$.
   (c) $a = 17643$ *et* $b = 2017$.
   (d) $a = 2017$ *et* $b = 17643$.

Théorème. 2.2.3.

(Relation de Bézout) Soient a, b deux entiers non tous les deux nuls et soit δ leur $PGCD$. Alors, il existe deux entiers u et v tel que $au + bv = \delta$

Preuve. Constructive s'appuyant sur un algorithme dit **algorithme d'Euclide étendu** :
On suppose par exemple que $b \neq 0$ (sinon, $\delta = |a|$ et il suffit de prendre $u = \pm 1$ selon si $a > 0$ ou $a < 0$ et $v = 0$). On reprend alors l'algorithme d'Euclide :

$$\begin{aligned} r_0 &= a,\ r_1 = b \\ r_{i-1} &= q_i r_i + r_{i+1}\ \forall 1 \leq i \leq k-1 \\ 0 &\leq r_{k-1} < r_{k-2} < ... < r_1 \\ r_k &\neq 0 \text{ et } r_{k+1} = 0 \end{aligned}$$

ce qui donne :

$$\delta = r_k = r_{k-2} - q_{k-1}r_{k-1}$$

et par une récurrence finie et descendante, on établit que pour tout $1 \leq i \leq k-1$, il existe un couple d'entiers (u_i, v_i) vérifiant :

$$\delta = r_{i-1}u_i + r_i v_i$$

En particulier, on a : $\delta = au_1 + bv_1$. Ce qui montre l'existence du couple (u, v). ■

Exemples 2.2.1 *Déterminer u et v tels que :*

1. $235u + 115v = 5$.
2. $3527u + 211v = 1$.
3. $17643u + 2017v = 1$

Remarque 2.2.3 *La réciproque du théorème précédent est fausse sauf si $\delta = 1$ comme on va le voir dans la section suivante. Contre exemple : En reprenant le premier exemple précédent et en prenant $u' = 2u$ et $v' = 2v$ on obtient : $235u' + 115v' = 10$ mais $235 \wedge 115 \neq 10$.*

EXERCICE 2.2.2

1. *Traduire l'algorithme d'Euclide étendu en un script Python.*
2. *Appliquer ce programme pour déterminer un couple d'entiers u et v vérifiant : $17643u + 2017v = 1$*

Proposition. 2.2.1.

$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a \wedge b)$: Tout diviseur commun à a et b divise $a \wedge b$. En d'autres termes $a \wedge b$ est le plus grand élément au sens de la divisibilité de l'ensemble des diviseurs positifs communs de a et b.

Preuve. Posons $\delta = a \wedge b$ et soit d un diviseur commun de a et b. En appliquant la relation de Bézout, il existe deux entiers u et v tel que : $au + bv = \delta$, et comme d est un diviseur commun de a et b il existe deux entiers k et k' tels que : $a = kd$ et $b = k'd$, de sorte que $\delta = d(ku + k'v)$, et donc d divise δ. Ainsi $\mathcal{D}(a) \cap \mathcal{D}(b) \subset \mathcal{D}(\delta)$. Inversement, il est claire que tout diviseur de δ est un diviseur commun à a et b ce qui montre l'inclusion inverse. D'où le résultat. ■

Corollaire. 2.2.1.

Soient a et b deux entiers non tous les deux nuls et soit δ un entier naturel. Alors on a :

$$\delta = a \wedge b \iff \begin{cases} \delta \text{ est un diviseur commun à } a \text{ et } b \\ \text{Tout diviseur commun à } a \text{ et } b \text{ divise } \delta \end{cases}$$

Preuve. $\Longrightarrow$) Si $\delta = a \wedge b$ alors et d'après la proposition précédente $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(\delta)$ ce qui démontre le premier sens

$\Longleftarrow$) On suppose que δ vérifie les deux conditions $\begin{cases} \delta \text{ est un diviseur commun à } a \text{ et } b \\ \text{Tout diviseur commun à } a \text{ et } b \text{ divise } \delta \end{cases}$.

Alors et comme δ est un diviseur commun à a et b on a : $\mathcal{D}(\delta) \subset \mathcal{D}(a) \cap \mathcal{D}(b)$. Puis la propriété : tout diviseur commun à a et b divise δ s'interpréte par : $\mathcal{D}(a) \cap \mathcal{D}(b) \subset \mathcal{D}(\delta)$. Ce qui entraîne l'égalité :$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(\delta)$ et achève la preuve. ■

2.2.2 Entiers premiers entre eux

Définition. 2.2.1.

Deux entiers a et b sont dits **premiers entre eux** lorsque $a \wedge b = 1$. Ce qui signifie en d'autres termes que les seuls diviseurs communs à a et b sont 1 et -1.

Exemple 2.2.2 *17643 et 2017 sont premiers entre eux.*

Théorème. 2.2.4.

(Caractérisation du $PGCD$)
Soient a et b deux entiers non tous les deux nuls et soit δ un entier naturel. Alors les assertions suivantes sont équivalentes :

1. $a \wedge b = \delta$
2. δ est un diviseur commun à a et b et $\left(\frac{a}{\delta}\right) \wedge \left(\frac{b}{\delta}\right) = 1$
3. Il existe deux entiers a' et b' premiers entre eux tels que : $\begin{cases} a = \delta a' \\ b = \delta b' \end{cases}$

Preuve. $1. \Longrightarrow 2.)$ On suppose que $a \wedge b = \delta$ donc δ est un diviseur commun et $\left(\frac{a}{\delta}\right) \wedge \left(\frac{b}{\delta}\right) = \frac{a \wedge b}{\delta} = 1$

$2. \Longrightarrow 3.)$ On suppose $(2.)$. Il suffit de prendre $a' = \frac{a}{\delta}$ et $b' = \frac{b}{\delta}$

$3.) \Longrightarrow 1.)$ On suppose $(3.)$. Alors $a \wedge b = \delta\,(a' \wedge b') = \delta$.

Ce qui achève la preuve. ■

Théorème. 2.2.5.

(De Bézout)
Deux entiers a et b sont premiers entre eux si et seulement s'il existe deux entiers u et v vérifiant :

$$au + bv = 1$$

l'identité précédente s'appelle **identité de Bézout** et les entiers u et v sont **ses coefficients**.

Preuve.

1. En appliquant l'algorithme d'Euclide étendu on démontre que la condition est bien nécessaire.
2. La condition est aussi suffisante : En effet, supposons l'existence d'entiers u et v tels que : $au + bv = 1$ et soit d un diviseur commun de a et b alors d divise $au + bv$ et donc divise 1. Ceci montrer que a et b sont premiers entre eux.

■

Remarque 2.2.4 *Le couple des coefficients de l'identité de Bézout quand il existe n'est pas unique.*

Propriétés 2.2.2

Soient a, b et c trois entiers.

1. *Si $au + bv = 1$ alors $a \wedge b = a \wedge v = b \wedge u = u \wedge v = 1$.*
2. *Si $a \wedge b = 1$ alors pour tous $n, m \in \mathbb{N}$ on a : $a^n \wedge b^m = 1$.*
3. *Si* $\left.\begin{array}{l} b \text{ divise } a \\ c \text{ divise } a \\ b \wedge c = 1 \end{array}\right\}$ *alors bc divise a.*

Preuve. La première propriété est une conséquence directe du théorème de $Bézout$.
Pour la deuxième : on montre d'abord par récurrence sur n que pour tout $n \in \mathbb{N}$ $a^n \wedge b = 1$: en effet, pour $n = 0$, on obtient $a^0 \wedge b = 1 \wedge b = 1$ puis si on suppose que $a^n \wedge b = 1$ pour un certain $n \in \mathbb{N}$ alors et par application du théorème de Bézout, il existe deux couples d'entiers (u, v) et (x, y) tels que : $a^n u + bv = ax + by = 1$. On multiplie les deux membres et on obtient : $a^{n+1}(ux) + b(avx + bvy + a^n uy) = 1$ ce qui montre que $a^{n+1} \wedge b = 1$. D'où la récurrence. Donc, pour tout $n \in \mathbb{N}$ on a : $a^n \wedge b = 1$. Maintenant en fixant n dans $\mathbb{N}$ on a : $a^n \wedge b = 1$ alors et en remplaçant a par b et b par a^n on obtient : Pour tout $m \in \mathbb{N}$, $a^n \wedge b^m = 1$. D'où le résultat escompté.
Pour la troisième propriété : Comme $b \wedge c = 1$ il existe un couple d'entiers (u, v) tel que $bu + cv = 1$, en multipliant de part et d'autre par a on obtient : $a = abu + acv$ mais comme b et c divisent a alors bc divise ac et ab et par suite il divise a en utilisant la propriété $(1.1.5)$. Ce qui achève la preuve. ■

Théorème. 2.2.6.

(Lemme de Gauss)
Soient a, b et c trois entiers tels que : $\left\{\begin{array}{c} a \text{ divise } bc \\ a \wedge b = 1 \end{array}\right.$. Alors a divise c.

Preuve. Ce grand résultat est une conséquence du théorème de Bézout. En effet, comme a et b sont premiers entre eux, il existe un couple d'entiers u et v tels que $au + bv = 1$. On multiplie de part et d'autre par c on obtient : $c = acu + bcv$ et comme a divise a et bc alors il divise $acu + bcv$ ce qui signifie que a divise c. ■

EXERCICE 2.2.3 *Soient a et b deux entiers premiers entre eux. On suppose $b \neq 0$ par exemple.*

1. *Montrer qu'il existe un unique couple d'entiers (u_0, v_0) vérifiant :*
$$\left\{\begin{array}{c} au_0 + bv_0 = 1 \\ 0 \leq u_0 < |b| \text{ et } |v_0| < |a| \end{array}\right.$$
2. *Résoudre, en fonction de (u_0, v_0), l'équation Diophantine en $(x, y) \in \mathbb{Z}^2$: $ax + by = 1$.*
3. *Résoudre dans $\mathbb{Z}^2$ l'équation : $17643x + 2017y = 1$*
4. *Déduire les solutions de l'équation : $176430x + 20170y = 10$*

Corollaire. 2.2.2.

(Forme irréductible d'un nombre rationnel)
Tout nombre rationnel r s'écrit de manière unique sous la forme :
$$r = \frac{p}{q}$$
tel que $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ et $p \wedge q = 1$. L'écriture précédente s'appelle **forme irréductible** ou **forme réduite** du rationnel r.

Preuve. Par définition d'un nombre irrationnel, il existe $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$ tel que : $r = \frac{a}{b}$. Soit $\delta = a \wedge b$ alors et d'après le théorème de caractérisation du PGCD il existe un couple d'entiers (a',b') premiers entre eux tels que : $\begin{cases} a = \delta a' \\ b = \delta b' \end{cases}$ de sorte que : $r = \frac{a'}{b'}$. Si $b > 0$ alors on prend $p = a'$ et $q = b'$ et si $b < 0$ on prendra $p = -a'$ et $q = -b'$. Ce qui montre l'existence du couple (p,q). Montrons maintenant son unicité : Soit (p',q') un autre couple de $\mathbb{Z} \times \mathbb{N}^*$ tels que $p' \wedge q' = 1$ et $r = \frac{p'}{q'}$. Alors et par définition de l'égalité de deux fractions rationnelles on obtient : $pq' = p'q$. Par suite q' divise $p'q$ avec $p' \wedge q' = 1$ alors et d'après le lemme de Gauss q' divise q. De même et comme q divise pq' on obtient q qui divise q'. Donc q et q' sont associés et comme de plus ce sont des entiers naturels on déduit que $q = q'$ ensuite on obtient $p = p'$. Ce qui montre l'unicité et achève la démonstration du corollaire. ■

2.2.3 PPCM de deux entiers

Pour tout $a \in \mathbb{Z}$ on note $\mathcal{M}(a)$ l'ensemble de tous les multiples de a :

$$\mathcal{M}(a) = \{ka : k \in \mathbb{Z}\}$$

Exemples 2.2.2 *$\mathcal{M}(0) = \{0\}$ et $\mathcal{M}(1) = \mathcal{M}(-1) = \mathbb{Z}$*

Remarque 2.2.5 *Pour tout entier a on a :*

1. $\mathcal{M}(a) = \mathcal{M}(-a)$
2. $0 \in \mathcal{M}(a)$
3. $a, -a \in \mathcal{M}(a)$

Théorème. 2.2.7.

(et définition)
Soient a et b deux entiers non nuls. Alors $\mathcal{M}(a) \cap \mathcal{M}(b) \cap \mathbb{N}^*$ admet un plus petit élément dit **le plus petit commun multiple** de a et b noté : $PPCM(a,b)$ ou encore $a \vee b$.

Preuve. En remarquant que $|ab| \in \mathcal{M}(a) \cap \mathcal{M}(b) \cap \mathbb{N}^*$ on déduit que $\mathcal{M}(a) \cap \mathcal{M}(b) \cap \mathbb{N}^*$ est une partie non vide de $\mathbb{N}$. Donc elle admet un plus petit élément. ■

Proposition. 2.2.2.

Soient a et b deux entiers non nuls. Alors $\mathcal{M}(a) \cap \mathcal{M}(b) = \mathcal{M}(a \vee b)$: En d'autres termes tout multiple commun de a et b est un multiple de $a \vee b$.

Théorème. 2.2.8.

(de Caractérisation)
Soient a et b deux entiers non nuls et soit m un entier naturel. Alors on a :

$$m = a \vee b \iff \begin{cases} m \text{ est un multiple commun de } a \text{ et } b \\ \text{Tout multiple commun de } a \text{ et } b \text{ est un multiple de } m \end{cases}$$

Preuve. $\Longrightarrow$) Si $m = a \vee b$ alors et d'après la proposition précédente $\mathcal{M}(a) \cap \mathcal{M}(b) = \mathcal{M}(m)$ ce qui démontre le premier sens

$\Longleftarrow$) On suppose que m vérifie les deux conditions $\begin{cases} m \text{ est un multiple commun de } a \text{ et } b \\ \text{Tout multiple commun de } a \text{ et } b \text{ est un multiple} \end{cases}$
Alors et comme m est un multiple commun de a et b on a : $\mathcal{M}(a)\cap\mathcal{M}(b) \subset \mathcal{M}(m)$. Puis la propriété : tout multiple commun de a et b est un multiple de m s'interpréte par : $\mathcal{M}(a)\cap\mathcal{M}(b) \subset \mathcal{M}(m)$. Ce qui entraîne l'égalité :$\mathcal{M}(a) \cap \mathcal{M}(b) = \mathcal{M}(m)$ et par suite $\mathcal{M}(a \vee b) = \mathcal{M}(m)$ cela signifie que $a \vee b$ et m sont deux entiers naturels associés donc égaux. Ceci achève la preuve. ■

Propriétés 2.2.3

Soient a et b deux entiers non nuls.

1. $a \vee b = |a| \vee |b|$; *On peut donc toujours se ramener au calcul du $PPCM$ d'entiers naturels.*
2. $a \vee b = |a| \Longleftrightarrow$ *b divise a.*
3. $a \vee b = b \vee a$.
4. $(a \vee b) \vee c = a \vee (b \vee c)$; *pour tout entier c non nul.*
5. $(ac) \vee (bc) = |c|\,(a \vee b)$; *Pour tout entier c non nul.*
6. $\left(\frac{a}{d}\right) \vee \left(\frac{b}{d}\right) = \frac{a \vee b}{|d|}$; *Pour tout diviseur d commun à a et b.*

Théorème. 2.2.9.

Soient a et b deux entiers non nuls. Alors on a :

$$(a \wedge b)\,(a \vee b) = |ab|$$

ce qui permet, en particulier, de déduire le $PPCM$ de a et b connaissant leur $PGCD$.

Preuve. Quitte à considérer leurs opposés, on peut supposer a et b des entiers naturels non nuls et on pose : $m = a \vee b$ et $\delta = a \wedge b$ et soients a' et b' les deux entiers premiers entre eux tels que : $a = \delta a'$ et $b = \delta b'$. Le problème revient à démontrer que $m = \delta a'b'$. Or, $\delta a'b'$ est un multiple commun de a et b et de plus, si k est un multiple commun de a et b alors l'entier $\frac{k}{\delta}$ est un multiple commun de a' et b' qui sont premier entre eux, donc $\frac{k}{\delta}$ est un multiple de $a'b'$ (d'après la propriété) et par suite k est un multiple de $\delta a'b'$. Ce qui montre, d'après le théorème de caractérisation du PPCM, que $\delta a'b' = a \vee b$ (en remarquant que $\delta a'b'$ est de plus positif). D'où, $|ab| = ab = \delta^2 a'b' = (a \wedge b)\,(a \vee b)$. ■

Corollaire. 2.2.3.

Deux entiers non nuls a et b sont premiers entre eux si et seulement si $a \vee b = |ab|$.

2.2.4 PGCD et PPCM de plusieurs entiers

Définition. 2.2.2.

Soient $a_1, ..., a_n$ n entiers, $n \in \mathbb{N} : n \geq 2$

1. On suppose qu'un au moins des a_k : $1 \leq k \leq n$ n'est pas nul. Le plus grand élément de $\bigcap_{k=1}^{n} \mathcal{D}(a_k)$ s'appelle **plus grand commun diviseur de** $a_1, ..., a_n$ et se note $\bigwedge_{k=1}^{n} a_k$ ou encore $PGCD(a_1, ..., a_n)$.
2. Lorsque tous les a_k sont non nuls, le plus petit élément positif de $\bigcap_{k=1}^{n} \mathcal{M}(a_k)$ s'appelle **plus petit commun multiple de** $a_1, ..., a_n$ et se note $\bigvee_{k=1}^{n} a_k$ ou encore $PPCM(a_1, ..., a_n)$.
3. Les entiers $a_1, ..., a_n$ sont dits **premiers entre eux (dans leur ensemble)** lorsque $\bigwedge_{k=1}^{n} a_k = 1$

Remarque 2.2.6 *Le calcul du $PGCD$ et du $PPCM$ de n entiers se fait par récurrence en se ramenant à celui de dux entiers puisqu'on a :*

$$\begin{aligned} \bigwedge_{k=1}^{n} a_k &= \left(\bigwedge_{k=1}^{n-1} a_k\right) \wedge a_n \\ \bigvee_{k=1}^{n} a_k &= \left(\bigvee_{k=1}^{n-1} a_k\right) \vee a_n \end{aligned}$$

Exemples 2.2.3 *1.* $6 \wedge 14 \wedge 21 = (6 \wedge 14) \wedge 21 = 2 \wedge 21 = 1$ *($6, 14$ et 21 sont premiers entre eux).*

2. $-3 \vee 7 \vee 14 \vee 6 = (-3 \vee 6) \vee (7 \vee 14) = 6 \vee 14 = 2 \times (3 \vee 7) = 2 \times 21 = 42.$

Théorème. 2.2.10.

(de caractérisation)
Soient $a_1, ..., a_n$ n entiers non nuls, $n \in \mathbb{N} : n \geq 2$.

1. On suppose qu'un au moins des a_k : $1 \leq k \leq n$ n'est pas nul et soit d un entier naturel non nul. Alors on a :

$$d = \bigwedge_{k=1}^{n} a_k \iff \begin{cases} \forall 1 \leq k \leq n \quad d \text{ divise } a_k \\ \text{tout diviseur commun de } a_1, ..., a_n \text{ divise } d \end{cases}.$$

2. On suppose tous les a_k sont non nuls et soit m un entier naturel non nul. Alors on a :

$$m = \bigvee_{k=1}^{n} a_k \iff \begin{cases} \forall 1 \leq k \leq n \quad m \text{ multiple de } a_k \\ \text{tout multiple commun de } a_1, ..., a_n \text{ est multiple de } m \end{cases}.$$

Preuve. Peut être établi par récurrence sur n. ■

Théorème. 2.2.11.

Soient $a_1, ..., a_n$ n entiers non nuls, $n \in \mathbb{N} : n \geq 2$ et soit δ leur $PGCD$ dans leur ensemble. Alors, il existe n enters $u_1, ..., u_n$ tels que :

$$\sum_{k=1}^{n} a_k u_k = \delta$$

La relation précédente est dite **relation de Bézout**. La réciproque est bien sêre fausse en général.

Preuve. Par récurrence :

— Pour $n = 2$ la propriété a été établi au paragraphe précédent.

— Soit n un entier > 2 telle que la propriété soit vraie pour $n-1$ et considèrons n entiers non nuls. Posons $\delta = \bigwedge_{k=1}^{n} a_k = \left(\bigwedge_{k=1}^{n-1} a_k\right) \wedge a_n$ donc d'après le cas particulier $n = 2$ il existerait deux entiers u et v tels que : $\left(\bigwedge_{k=1}^{n-1} a_k\right) u + a_n v = \delta$ et par hypothèse de récurrence il existe aussi, $n-1$ entiers $u'_1, ..., u'_{n-1}$ tel que : $\sum_{k=1}^{n-1} a_k u'_k = \bigwedge_{k=1}^{n-1} a_k$. On déduit alors la relation escomptée : $\sum_{k=1}^{n} a_k u_k = \delta$ en prenant : $\begin{cases} u_k = u'_k u \; \forall \, 1 \leq k \leq n-1 \\ u_n = v \end{cases}$

■

EXERCICE 2.2.4 *Déterminer $\delta = 45 \wedge 30 \wedge 72$ et déterminer trois entiers u, v et w tels que :* $45u + 30v + 72w = \delta$.

Corollaire. 2.2.4.

(Caractérisation d'entiers premiers entre eux)

Théorème. 2.2.12.

n entiers $a_1, ..., a_n$ sont **premiers entre eux (dans leur ensemble)** si et seulement s'il existe n entiers $u_1, ..., u_n$ tel que : $\sum_{k=1}^{n} a_k u_k = 1$.

Preuve. $\Longleftarrow$) On suppose qu'il existe n entiers $u_1, ..., u_n$ tel que : $\sum_{k=1}^{n} a_k u_k = 1$ et on considère un diviseur positif commun à $a_1, ..., a_n$. Alors et en généralisant par récurrence la propriété **??**5.on déduit que d divise 1 donc $d = 1$. Ce qui montre que $\bigwedge_{k=1}^{n} a_k = 1$.

$\Longrightarrow$) On suppose que $a_1, ..., a_n$ sont **premiers entre eux.** ■

Remarque 2.2.7 *n entiers $a_1, ..., a_n$ peuvent être premiers entre eux sans être premiers deux à deux.* 6, 14 *et* 21 *sont premiers entre eux mais non premiers deux à deux.*

2.3 Nombres premiers

2.3.1 Notion des nombres premiers

Définition. 2.3.1.

Un entier p est dit **premier** si $p \geq 2$ et ses seuls diviseurs dans $\mathbb{N}$ sont 1 et lui même : $\mathcal{D}(p) = \{-p, -1, 1, p\}$.

Exemples 2.3.1 $2, 3, 5, 7, 11, 13, 17, 19, 23$ *et* 29 *sont les dix premiers nombres premiers.* 1 *n'est pas un nombre premier ! !*

Notation On note $\mathcal{P}$ l'ensemble de tous les nombres premiers :

$$\mathcal{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...\}$$

Propriétés 2.3.1

1. *Pour tout entier a on a : p divise a ou bien p et a sont premiers entre eux.*
2. *Deux nombres premiers sont soient égaux soient premiers entre eux.*
3. *Soient p et q deux entiers premiers distincts. Alors pour tous entiers naturels α et β on a : $p^\alpha \wedge q^\beta = 1$.*
4. *Soient $a_1, ..., a_n$ n entiers et p un nombre premier tel que p divise $\prod_{k=1}^{n} a_k$ alors il existe $1 \leq k \leq n$ tel que p divise a_k.*
5. *Soient $p_1, ..., p_n$ et p $n+1$ nombres premiers tel que p divise $\prod_{k=1}^{n} p_k$ alors il existe $1 \leq k \leq n$ tel que $p = p_k$.*
6. *Soient $p_1, ..., p_n$ n nombres premiers distincts deux à deux et soit a un entier tel qu'il existe n entiers naturels $\alpha_1, ..., \alpha_n$ tels que : $\forall 1 \leq k \leq n$ $p_k^{\alpha_k}$ divise a alors $\prod_{k=1}^{n} p_k^{\alpha_k}$ divise a.*

Théorème. 2.3.1.

(Crible d'**Eratosthène**)
Un entier $p \geq 2$ est premier si et seulement si p n'est divisible par aucun entier naturel $\leq \sqrt{p}$

EXERCICE 2.3.1 *Écrire un algorithme de test de primalité utilisant le crible d'**Eratosthène**. Traduire cet algorithme en un script python.*

2.3.2 Décomposition d'un entier en produit de facteurs premiers

Lemme 2.3.1 *Tout entier $n \geq 2$ admet au moins un diviseur premier.*

Preuve. On raisonne par récurrence sur $n \geq 2$:

— Pour $n = 2$: 2 est un diviseur premier de lui même

— Soit n un entier > 2 pour lequel on suppose la propriété vérifiée pour tout entier $2 \leq k < n$ et on montre la propriété pour n. Si n est premier, c'est terminé puisque ça sera un diviseur premier de lui même. Sinon, cela signifie qu'il admet un diviseur $2 \leq d < n$ alors et par l'hypothèse de récurrence d admet un diviseur premier p.

■

Proposition. 2.3.1.

L'ensemble $\mathcal{P}$ des nombres premiers est infini.

Preuve. On raisonne par l'absurde et on suppose $\mathcal{P}$ fini de cardinal n : $\mathcal{P} = \{p_1, ..., p_n\}$ et considèrons l'entier $N = \left(\prod_{k=1}^{n} p_k\right)! + 1$. D'après le lemme N admet un diviseur premier p qui appartient à $\mathcal{P}$ donc p divise $\prod_{k=1}^{n} p_k$ et par suite p divise 1 ce qui contredit le fait que p soit premier. D'où, la proposition. ■

Notation L'ensemble des diviseurs premiers d'un entier a se note $\mathcal{P}(a)$.

Proposition. 2.3.2.

(et définition)
Soit n un entier ≥ 2 et soit p un nombre premier alors il existe un plus grand entier naturel k vérifiant p^k divise n noté $v_p(n)$ dit **valuation p-adique de** a :

$$v_p(n) = \max\{k \in \mathbb{N} : p^k \text{ divise } n\}.$$

Preuve. $\{k \in \mathbb{N} : p^k$ divise $n\}$ est une partie de $\mathbb{N}$, non vide (elle contient 0) et majorée par n. En effet : Comme p est ≥ 2 alors pour tout entier naturel k on a : $k \leq p^k$. Or, si p^k divise n alors $p^k \leq n$ et donc $k \leq n$. Ainsi $\{k \in \mathbb{N} : p^k$ divise $n\}$ admet un plus grand élément. Ce qui justifie l'existence de $v_p(n)$. ■

Exemple 2.3.1 $v_2(100) = 2$, $v_5(100) = 2$ *et* $v_3(100) = 0$.

Proposition. 2.3.3.

Soit p un nombre premier et k un entier naturel. Alors $1, p, ..., p^k$ sont exactement les diviseurs de p^k dans $\mathbb{N}$.

Théorème. 2.3.2.

(de caractérisation)
Soit n un entier ≥ 2 et $k \in \mathbb{N}$. Alors les trois propriétés suivantes sont équivalentes :

1. $k = v_p(n)$
2. $\begin{cases} p^k \text{ divise } n \\ p^{k+1} \text{ ne divise pas } n \end{cases}$
3. Il existe $q \in \mathbb{N}$ telle que : $\begin{cases} n = qp^k \\ p \text{ ne divise pas } q \end{cases}$

en particulier : p divise n si et seulement si $v_p(n) \neq 0$.

Preuve. Notons $I = \{i \in \mathbb{N} : p^i \text{ divise } n\}$.

1. $\Longrightarrow$ 2.) On suppose $k = v_p(n)$, donc et par définition du plus grand élément d'une partie, $k \in I$ et $k+1 \notin I$ ce qui est équivalent à dire que $\begin{cases} p^k \text{ divise } n \\ p^{k+1} \text{ ne divise pas } n \end{cases}$.

2. $\Longleftarrow$ 3.) On suppose qu'on a : $\begin{cases} p^k \text{ divise } n \\ p^{k+1} \text{ ne divise pas } n \end{cases}$ alors d'un côté, il existe $q \in \mathbb{N}$ telle que : $n = qp^k$ d'un autre côté p ne divise pas q car sinon, on aura p^{k+1} divise n ce qui est absurde. D'où, l'implication.

3. $\Longrightarrow$ 1.) On suppose l'existence de $q \in \mathbb{N}$ telle que : $n = qp^k$ avec p qui ne divise pas q. Alors d'un côté p^k divise n et donc $k \in I$. Et d'un autre côté, pour tout $i \in I$, on a p^i divise $n = qp^i$ et comme p est premier et ne divise pas q alors $p \wedge q = 1$ et donc $p^i \wedge q = 1$ par suite et d'après le lemme de Gauss on obtient p^i divise p^kce qui implique que $i \leq k$ et donc I est majorée par k. Ainsi, k est le plus grand élément de I et $k = v_p(n)$. Ce qui achève la démonstration. ■

Propriétés 2.3.2

Soit p un nombre premier. Alors :

1. *Pour tous entiers n et m on a : $v_p(nm) = v_p(n) + v_p(m)$.*
2. *Pour tous entier n et entier naturel r on.a : $v_p(n^r) = rv_p(n)$.*

Preuve.

1. On pose $k = v_p(n)$ et $k' = v_p(m)$ donc il existe deux entiers q et q' tels que : $n = qp^k$ et $m = q'p^{k'}$ avec p ne divise ni q ni q' donc premier avec les deux. Par suite p ne divise pas leur produit qq' et on a $nm = (qq')\, p^{k+k'}$ alors et d'après le théorème de caractérisation précédent on déduit que $v_p(nm) = k + k'$.
2. On raisonne par récurrence sur r en exploitant la propriété précédente.

■

Théorème. 2.3.3.

(de décomposition d'un entier en produit de facteurs premiers)
Soit n un entier ≥ 2 et soient $p_1, p_2, ..., p_r$ les diviseurs premiers de n. Alors on a :

$$n = \prod_{k=1}^{r} p_k^{v_{p_k}(n)} = \prod_{p \in \mathcal{P}(n)} p^{v_p(n)}$$

cette décomposition est l'unique décomposition, à l'ordre des facteurs près, de n en produit de facteurs premiers.

Preuve.

— Décomoposition : Par définition de la p-valuation, on a pour tout $1 \leq k \leq r$, $p_k^{v_{p_k}(n)}$ divise n et comme $p_1, ..., p_r$ sont des nombres premiers distincts deux à deux ils sont premiers entre eux deux à deux et par suite : $p_1^{v_{p_1}(n)}, ..., p_r^{v_{p_r}(n)}$ sont premiers entre eux deux à deux. On en déduit que leur produit $\prod_{k=1}^{r} p_k^{v_{p_k}(n)}$ divise n. Donc il existe $q \in \mathbb{N}$ telle que $n = q\prod_{k=1}^{r} p_k^{v_{p_k}(n)}$. Si q était ≥ 2 alors il admettrait un diviseur premier p qui divise

donc n aussi donc il existerait un indice $1 \leq i \leq r$ tel que $p = p_i$. On obtient alors que $p_i^{v_{pi}(n)+1}$ divise n ce qui contredit la définition de la p-valuation.

— Unicité : On suppose que n admet une autre décomposition en produit de nombres premiers distincts : $n = \prod_{k=1}^{s} q_k^{\beta_k}$ où $q_1, ..., q_s$ sont des nombres premiers distincts deux à deux et $\beta_1, ..., \beta_s$ sont des entiers naturels non nuls. On peut aussi supposer que $q_1 < ... < q_s$ et de même que $p_1 < ... < p_r$. Il s'agit alors de montrer que $r = s$ et que pour tout $1 \leq i \leq r$ $p_i = q_i$ et $\beta_i = v_{p_i}(n)$. Pour cela on remarque que pour tout $1 \leq i \leq r$ on a : p_i divise $n = \prod_{k=1}^{s} q_k^{\beta_k}$ et comme $q_1, ..., q_s$ sont des nombres premiers distincts deux à deux alors il existe $1 \leq j \leq s$ tel que $p_i = q_j$ et donc $\{p_1, ..., p_r\} \subset \{q_1, ..., q_s\}$. En inversant les rôles des p_i et des q_k on obtient l'inclusion inverse, ce qui montre que les deux ensembles sont égaux et en particulier ont le même cardinal. Ainsi $r = s$ d'un côté, d'autre part et comme les p_i et les q_i sont ordonnés dans le sens croissant on obtient que : $p_i = q_i$ pour tout $1 \leq i \leq r$. Ainsi $n = \prod_{k=1}^{r} p_k^{\beta_k} = \prod_{k=1}^{r} p_k^{v_{p_k}(n)}$. Reste à montrer que, pour $1 \leq i \leq r$ $\beta_i = v_{p_i}(n)$: or, on a par hypothèse $p_i^{\beta_i}$ divise n donc, et par définition de $v_{pi}(n)$, $\beta_i \leq v_{p_i}(n)$. Réciproquement si $\beta_i < v_{pi}(n)$ alors, et en divisant les deux membres de l'égalité $\prod_{k=1}^{r} p_k^{\beta_k} = \prod_{k=1}^{r} p_k^{v_{p_k}(n)}$ par $p_i^{\beta_i}$, on obtient $p_i^{v_{p_i}(n)-\beta_i}$ divise $\prod_{k=1,k\neq i}^{r} p_k^{\beta_k}$ ce qui va entraîner l'existence d'un entier $k \neq i$ tel que $p_i = p_k$ ce qui est absurde. D'où, $\forall 1 \leq i \leq r$ $\beta_i = v_{p_i}(n)$. Ce qui achève la démonstration du théorème.

■

Remarque 2.3.1 *En remarquant que* $\mathcal{P}(1) = \emptyset$, *on convient que l'écriture* $1 = \prod_{p \in \mathcal{P}(1)} p^{v_p(1)}$ *est l'unique décomposition de* 1 *en produit de facteurs premiers.*

Exemple 2.3.2 *Décomposer* 2018 *en produit de facteurs premiers.*

Corollaire. 2.3.1.

(Caractérisation de la divisibilité)
Soient a et b deux entiers naurels non nuls. Alors on a :

$$b \text{ divise } a \iff \begin{cases} \mathcal{P}(b) \subset \mathcal{P}(a) \\ \forall p \in \mathcal{P}(a) \quad v_p(b) \leq v_p(a) \end{cases}$$

Preuve. Posons $\mathcal{P}(a) = \{p_1, ..., p_r\}$ et $\alpha_k = v_{p_k}(a)$ où $p_1, ..., p_r$ sont distincts deux à deux.
$\Longleftarrow$) On suppose que $\begin{cases} \mathcal{P}(b) \subset \mathcal{P}(a) \\ \forall p \in \mathcal{P}(b) \quad v_p(b) \leq v_p(a) \end{cases}$. Posons $\beta_k = v_{p_k}(b)$ pour tout $1 \leq k \leq r$. On écrit alors $a = qb$ avec $q = \prod_{k=1}^{r} p_k^{\alpha_k - \beta_k} \in \mathbb{N}$ ce qui montre que b divise a.

$\Longrightarrow$) on suppose que b divise a. Si $b = 1$ alors on a : $\mathcal{P}(b) = \emptyset \subset \mathcal{P}(a)$ et pour tout $p \in \mathcal{P}(a)$ $0 = v_p(b) \leq v_p(a)$. Sinon, tout diviseur premier de b est un diviseur de a et donc on a bien $\mathcal{P}(b) \subset \mathcal{P}(a)$. Puis, pour tout $p \in \mathcal{P}(a)$, on a, par définition de $v_p(b)$, $p^{v_p(b)}$ divise b qui divise a donc $p^{v_p(b)}$ divise a alors, et par définition de $v_p(a)$, $v_p(b) \leq v_p(a)$. Ce qui achève la preuve.
■

EXERCICE 2.3.2 *Soit n un entier ≥ 2 dont la décomposition en produit de facteurs premiers est donnée par :*

$$n = \prod_{k=1}^{r} p_k^{v_{p_k}(n)}$$

On note $\mathcal{D}(n)$ l'ensemble des diviseurs de n dans $\mathbb{N}$.

1. *On pose :*

$$\varphi : \begin{array}{c} \prod_{k=1}^{r} [|0, \alpha_k|] \longrightarrow \mathcal{D}(n) \\ (\beta_1, ..., \beta_r) \longmapsto \prod_{k=1}^{r} p_k^{\beta_k} \end{array}$$

   Justifier qu'on définit ainsi une application bijective.

2. *En déduire le nombre de diviseurs positifs de n.*

Corollaire. 2.3.2.

(Application au calcul du $PGCD$ et du $PPCM$)
Soient a et b deux entiers naurels non nuls. Alors on a :

$$\begin{aligned} a \wedge b &= \prod_{p \in \mathcal{P}(b) \cap \mathcal{P}(a)} p^{\min(v_p(a), v_p(b))} \\ a \vee b &= \prod_{p \in \mathcal{P}(b) \cup \mathcal{P}(a)} p^{\max(v_p(a), v_p(b))} \end{aligned}$$

2.4 Congruence modulo un entier

Soit n un entier.

Définition. 2.4.1.

(Relation de congruence modulo n)
Deux entiers a et b sont dits **congrus modulo** n s'il existe $k \in \mathbb{Z}$ tel que $a - b = kn$ ce qui signifie que n divise $a - b$. On note dans ce cas $a \equiv b\ [n]$.

Remarque 2.4.1 *La congruence modulo n coïncide avec la congruence modulo $(-n)$. Pour cela, dans la suite on suppose n entier naturel.*

Proposition. 2.4.1.

On définit ainsi une relation d'équivalence sur $\mathbb{Z}$ dite **congruence modulo** n.

Preuve.

— Réflexivité : Pour tout entier a on a : n divise $0 = a - a$ donc $a \equiv a\ [n]$. D'où, la réflexivité.

— Symétrie : Soient $a, b \in \mathbb{Z}$ telle que : $a \equiv b\ [n]$ ce qui signifie que n divise $a - b$ par suite n divise aussi $b - a$ et donc : $b \equiv a\ [n]$. d'où, la symétrie.

— Transitivité : Soient $a, b, c \in \mathbb{Z}$ telle que : $a \equiv b\ [n]$ et $b \equiv c\ [n]$, ce qui signifie que n divise $a - b$ et $b - c$. Alors n divise leur somme $a - c$ et donc $a \equiv c\ [n]$. D'où, la transitivité. Ce qui montre que la congruence modulo n est bien une relation d'équivalence.

■

Définition. 2.4.2.

Pour tout $a \in \mathbb{Z}$ on notera $cl_n(a)$ ou simplement $\overline{a}$ la classe d'équivalence de a :

$$\overline{a} = \{a + kn : k \in \mathbb{Z}\}$$

L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble de ces classes :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{a} \text{ tel que } a \in \mathbb{Z}\}$$

Théorème. 2.4.1.

1. Pour $n = 0$ on a : $\mathbb{Z}/n\mathbb{Z} = \{\{a\} \text{ tel que } a \in \mathbb{Z}\}$
2. Pour $n \geq 1$, $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$ de cardinal fini n.

Preuve.

1. Pour $n = 0$, on a, pour tout $a, b \in \mathbb{Z}$:

$$\begin{aligned} b \quad \in \quad & \overline{a} \Longleftrightarrow a \equiv b\ [0] \\ \Longleftrightarrow \quad & 0 \text{ divise } a - b \\ \Longleftrightarrow \quad & a - b = 0 \end{aligned}$$

   donc, pour tout $a \in \mathbb{Z}$, $\overline{a} = \{a\}$ et par suite $\mathbb{Z}/0\mathbb{Z} = \{\overline{a} \text{ tel que } a \in \mathbb{Z}\} = \{\{a\} \text{ tel que } a \in \mathbb{Z}\}$.

2. Pour $n \geq 1$. Il est clair que $\{\overline{0}, \overline{1}, ..., \overline{n-1}\} \subset \mathbb{Z}/n\mathbb{Z}$ et inversement : soit $a \in \mathbb{Z}$. Effectuons la division euclidienne de a par n et soient q et r le quotient et le reste respectifs de cette division euclidienne de sorte que :

$$a - r = qn \text{ et } 0 \leq r \leq n - 1$$

   ce qui montre que $a \equiv r\ [n]$ et donc a et r ont la même classe d'équivalence, en d'autres termes $\overline{a} = \overline{r}$ et $r \in \{0, ..., n-1\}$. Ainsi, $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$. Reste à montrer que cet ensemble contient exactement n éléments. Cela revient à montrer que ses éléments $\overline{0}, \overline{1}, ..., \overline{n-1}$ sont distincts deux à deux. Pour cela, on va raisonner par contre-apposée : Soient donc $r, r' \in \{0, ..., n-1\}$ tels que $\overline{r} = \overline{r'}$ ce qui est équivalent à $r \equiv r'\ [n]$ ou encore n divise $r - r'$. Or, $|r - r'| < n$ donc nécessairement $r - r\prime = 0$. Ce qu'il fallait démontrer.

■

Propriétés 2.4.1

On suppose n un entieret ≥ 2. Alors, pour tout $a, b, a', b' \in \mathbb{Z}$ tels que $a \equiv a'\ [n]$ et $b \equiv b'\ [n]$. Alors on a :

1. $a + b \equiv a' + b'\ [n]$.
2. $ab \equiv a'b'\ [n]$.
3. *Pour tout* $k \in \mathbb{Z}$ $ka \equiv ka'\ [kn]$

Preuve. Par hypothèse il existe $k, k' \in \mathbb{Z}$ tels que : $a - a' = kn$ et $b - b' = k'n$ de sorte qu'en sommant on obtient : $(a+b) - (a'+b') = (k+k')n$ et par suite n divise $(a+b) - (a'+b')$ ce qui est équivalent à $a + b \equiv a' + b'\ [n]$. De même en écrivant : $ab - a'b' = (a-a')b + a'(b-b')$ on obtient que n divise $ab - a'b'$ et donc $ab \equiv a'b'\ [n]$. Pour le troisième point, pour $k \in \mathbb{Z}$, on a : $ka - ka' = k(a-a')$ et comme n divise $a - a'$, kn divise $k(a-a') = ka - ka'$ ce qui montre que $ka \equiv ka'\ [n]$. ■

Lemme 2.4.1 *Soit p un nombre premier. Alors pour tout entier $1 \leq k \leq p-1$ on a : p divise* $\begin{pmatrix} p \\ k \end{pmatrix}$.

Preuve. On rappelle que pour un tel k on a :

$$\begin{pmatrix} p \\ k \end{pmatrix} = \frac{p!}{k!(p-k)!} = \frac{p}{k}\begin{pmatrix} p-1 \\ k-1 \end{pmatrix}$$

de sorte que : p divise $k\begin{pmatrix} p \\ k \end{pmatrix}$ et comme p est un nombre premier et $1 \leq k \leq p-1$ alors $p \wedge k = 1$. Donc, et d'après le lemme de Gauss, p divise $\begin{pmatrix} p \\ k \end{pmatrix}$. ■

Théorème. 2.4.2.

(Petit théorème de Fermat)
Soit p un nombre premier. Alors pour tout entier a on a :

1. $a^p \equiv a\ [p]$
2. Si $a \wedge p = 1$ alors $a^{p-1} \equiv 1\ [p]$

Preuve.

1. Pour $a \in \mathbb{N}$, on raisonne par récurrence : Pour $a = 0$, il n'y a rien à montrer. On suppose la propriété vraie pour un certain $a \in \mathbb{N}$ alors et par application du formule du Binôme de Newton on obtient :
$$(a+1)^p = \sum_{k=0}^{p} \begin{pmatrix} p \\ k \end{pmatrix} a^k$$
or, et d'après le lemme précédent, pour tout $1 \leq k \leq p-1$ p divise $\begin{pmatrix} p \\ k \end{pmatrix}$ par suite p divise $(a+1)^p - (1+a)$ ce qui signifie que : $(a+1)^p \equiv (a+1)\ [p]$ ce qui montre la récurrence. Ainsi, $\forall a \in \mathbb{N}\ \ a^p \equiv a\ [p]$. D'autre part, et comme pour p premier impair, on a : $(-1)^p = -1$ on déduit que : $\forall a \in \mathbb{N}$ $(-a)^p \equiv -a\ [p]$ ce qui montre la propriété pour tout $a \in \mathbb{Z}$. Pour p premier pair c'est à dire $p = 2$, on remarque que : $\forall a \in \mathbb{Z}\ \ -a \equiv a\ [2]$ et comme $\forall a \in \mathbb{N}\ \ a^2 \equiv a\ [2]$ on obtient : $\forall a \in \mathbb{N}\ \ (-a)^2 = a^2 \equiv a \equiv -a\ [2]$ et par suite la propriété est encore vraie pour $p = 2$.
2. On suppose maintenant que $a \wedge p = 1$. La propriété précédente montre que p divise $a(a^{p-1} - 1)$ alors et en appliquant le lemme de Gauss, on déduit que p divise $a^{p-1} - 1$ ce qui signifie que : $a^{p-1} \equiv 1\ [p]$. D'où, le théorème.

■

EXERCICE 2.4.1 *Montrer que pour tout $m, n \in \mathbb{N}$ $mn(m^{60} - n^{60}) \equiv 0\ [56730]$*

EXERCICE 2.4.2 *(Lemme chinois)*
Soient n et m deux entiers premiers entre eux.

1. *En utilisant l'identité de Bézout, montrer que pour tout entiers a et b le systéme* $\begin{cases} x \equiv a\ [n] \\ x \equiv b\ [m] \end{cases}$ *admet toujours des solutions.*
2. *On pose* $f : \begin{array}{l} \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ cl_{nm}(x) \mapsto (cl_n(x), cl_m(x)) \end{array}$
   (a) *Vérifier que f définit une application.*
   (b) *Montrer que f est injective*
   (c) *En déduire que f est une bijection*
3. *Exemple : Résoudre* $\begin{cases} x \equiv 3\ [41] \\ x \equiv 2\ [7] \end{cases}$

EXERCICE 2.4.3 *(Indicateur d'Euler)*
Pour tout entier $n \geq 2$, on pose :

$$\varphi(n) = card\{k \in \{0, 1, ..., n-1\} \text{ tel que } k \wedge n = 1\}$$

On définit ainsi une application φ de l'ensemble des entiers ≥ 2 dans $\mathbb{N}$ dite ***indicateur d'Euler****. Montrer que :*

1. *Pour tout entier premier p $\varphi(p) = p - 1$.*
2. *Si n est un entier primair (c'est á dire de la forme p^α oú p est un nombre premier et $\alpha \in \mathbb{N}^*$) alors : $\varphi(n) = p^\alpha - p^{\alpha-1}$.*
3. *Pour tous entiers n et m premiers entre eux $\varphi(nm) = \varphi(n)\varphi(m)$.*
4. *Pour tout entier $n \geq 2$,* $\varphi(n) = n \prod_{p \in \mathcal{P}(n)} (1 - \frac{1}{p})$.
5. *Exemple : Calculer $\varphi(99999)$.*

Chapitre 3

Les polynômes

Tout au long de ce chapitre, on désigne par $\mathbb{K}$ un sous corps de $\mathbb{C}$, principalement $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

3.1 Généralités

3.1.1 L'algèbre des polynômes

Définition. 3.1.1.

On appelle polynôme à coefficients dans $\mathbb{K}$ toute suite $(a_n)_{n\geq 0} = (a_0, a_1, \cdots, a_r, 0, \cdots)$ d'éléments de $\mathbb{K}$ nulle à partir d'un certain rang $r \in \mathbb{N}$, c'est = dire que $a_n = 0$ pour tout $n \geq r$. On définit les opérations suivantes sur les polynômes. On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$.

Exemples 3.1.1 *La suite $(a_n)_{n\geq 0}$ définie par $a_n = \left\lfloor \dfrac{3n+1}{n^2+1} \right\rfloor$ pour tout $n \in \mathbb{N}$, où $\lfloor x \rfloor$ désigne la partie entière de tout réel $x \in \mathbb{R}$, est un polynôme à coefficients dans $\mathbb{Q}$, car elle est nulle dès que $n \geq 4$.*

Proposition. 3.1.1. et définition

Si $P = (a_n)_{n\geq 0}$, $Q = (b_n)_{n\geq 0}$ sont deux polynômes à coefficients dans $\mathbb{K}$, et $\lambda \in \mathbb{K}$, alors les suites $P + Q = (a_n + b_n)_{n\geq 0}$, $\lambda.P = (\lambda a_n)_{n\geq 0}$ $P \times Q = (c_n)_{n\geq 0}$, où les coefficients c_n sont définis par la formule

$$\forall n \in \mathbb{N}, \quad c_n = \sum_{k=0}^{n} a_k b_{n-k}$$

sont de polynômes. On les appelle respectivement : la somme de P et Q, le produit de P par le scalaire λ et le produit de P et Q.

Preuve. En effet, $(a_n)_{n\geq 0}$ est nul à partir d'un certain rang $p \in \mathbb{N}$, et $(b_n)_{n\geq 0}$ est nul à partir d'un certain rang $q \in \mathbb{N}$ alors il est clair que :

— $\forall n > \max(p,q),\ \ a_n + b_n = 0$,

— $\forall n > p,\ \ \lambda.a_n = 0$

— $\forall n > p+q,\ \ c_n = \sum_{k=0}^{n} a_k b_{n-k} = 0$, car, pour tout $n > p+q$ et tout $k \in [\![0,n]\!]$, soit $k > p$, soit $n-k > q$, donc ; soit $a_k = 0$, soit $b_{n-k} = 0$ et par suite $a_k b_{n-k} = 0$.

■

Proposition. 3.1.2.

$(\mathbb{K}[X], +, ., \times)$ est une algèbre commutative.

Preuve. Exercice ■

Proposition. 3.1.3.

$\mathbb{K}$ est isomorphisme d'une sous-algèbre de

Preuve. En effet, il est facile de montrer que $(\mathbb{K}[X], +, ., \times)$. L'application de

$$\begin{array}{rccc} \phi : & (\mathbb{K}, +, ., \times) & \to & (\mathbb{K}[X], +, ., \times) \\ & \alpha & \longmapsto & (\alpha, 0, 0, \cdots, \cdots) \end{array}$$

est un morphisme d'algèbre injectif. ■

Remarque 3.1.1 *L'isomorphisme entre $\mathbb{K}$ et son image par ϕ permet de confondre tout élément $\alpha \in \mathbb{K}$ et son image $\phi(\alpha) = (\alpha, 0, 0, \cdots, \cdots)$, et par suite considérer $\mathbb{K}$ comme une partie de $\mathbb{K}[X]$. Ainsi, désormais, tout polynôme de la forme $\phi(\alpha) = (\alpha, 0, 0, \cdots, \cdots)$ sera noté α tout court, et sera appelé un polynôme constant.*

3.1.2 L'indéterminée X

Notation On note $X = (0, 1, 0, \cdots)$, $X^0 = (1, 0, 0, \cdots)$, et $X^n = \underbrace{X \times X \times \cdots \times X}_{n-fois}$ pour tout $n \in \mathbb{N}^*$. On dit que X est une indéterminée.

Proposition. 3.1.4.

Pour tout entier naturel $n \in \mathbb{N}$ on a,

$$X^n = (0, \cdots, 0, \underset{\substack{\uparrow \\ (n+1)-\text{ème place}}}{1}, 0 \cdots).$$

Preuve. En effet il est facile de montrer que pour tout polynôme de la forme $P = (a_0, a_1, , \cdots, \cdots)$ on a $XP = (0, a_0, a_1, , \cdots, \cdots)$. ■

Ainsi, tout polynôme $P = (a_0, a_1, \cdots, a_n, 0, \cdots)$ s'écrit sous la forme :

$$P = a_0 + a_1 X, \cdots, a_n X^n = \sum_{k=0}^{n} a_k X^k.$$

Dans ce cas, pour tout $k \in \mathbb{N}$, a_k s'appelle le coefficient de X^k dans P, et a_0 son coefficient constant. On appelle monôme tout polynôme de la forme $a_k X^k$ pour un certain $k \in \mathbb{N}$ et $a_k \in \mathbb{K}$.

Corollaire. 3.1.1.

La famille $(X^n)_{n\in\mathbb{N}} = \left(1, X, X^2, \cdots, \right)$ est base de $\mathbb{K}[X]$. On l'appelle la base canonique de $\mathbb{K}[X]$.

3.1.3 Composée de deux polynômes

Définition. 3.1.2.

Soit P, Q deux polynômes. Si $= a_0 + a_1X, \cdots, a_nX^n = \sum_{k=0}^{n} a_kX^k$, on appelle composée de P et Q le polynôme noté par $P \circ Q$ ou $P(Q)$ défini par :

$$P \circ Q = \sum_{k=0}^{n} a_kQ^k$$

Propriétés 3.1.1

- *La composée de polynômes est associative,*
- *Pour tout polynôme P on a $P(X) = P$.*
- $\forall P, Q, R \in \mathbb{K}[X],\ \ (P + Q) \circ R = P \circ R + Q \circ R$

Remarque 3.1.2 *En général, $P \circ (Q + R) \neq P \circ Q + P \circ R$*

3.1.4 Degré et valuation

Proposition. 3.1.5. et définition

Si $P = (a_k)_{k\in\mathbb{N}} \in \mathbb{K}[X]$ est un polynôme non nul, alors l'ensemble

$$\{k \in \mathbb{N} \ : \ a_k \neq 0\}$$

admet un plus grand et un plus élément dans $\mathbb{N}$. On appelle degré de P, et on le note par $\deg P$ ou d^oP, le nombre

$$\deg P = \max\{k \in \mathbb{N} \ : \ a_k \neq 0\}.$$

On appelle valuation de P, et on le note par $\mathrm{Val}(P)$, le nombre

$$\mathrm{Val}(P) = \min\{k \in \mathbb{N} \ : \ a_k \neq 0\}.$$

Par convention, le degré du polynôme nul est égal à $-\infty$, et son évaluation est égal à $+\infty$.

Remarque 3.1.3 *Étant donné un polynôme non nul, P, et $n, p \in \mathbb{N}$, alors :*

- $\deg P = n$ *si et seulement si P s'écrit sous la forme*

$$P = a_0 + a_1X, \cdots, a_nX^n,$$

avec $a_0, a_1, \cdots, a_n \in \mathbb{K}$ et $a_n \neq 0$.

— $\deg P = n$ *et* $\mathrm{Val}(P) = p$ *si et seulement si* P *s'écrit sous la forme*

$$P = a_p + a_1 X, \cdots, a_n X^n,$$

avec $a_0, a_1, \cdots, a_n \in \mathbb{K}$, $a_p \neq 0$ *et* $a_n \neq 0$.

Le coefficient a_n *s'appelle le coefficient dominant de* P, *et* $a_n X^n$ *son monôme dominant. Dans le cas où* $a_n = 1$, *on dit que* P *est un polynôme unitaire ou normalisé. Remarquer alors que le polynôme* $\frac{1}{a_n} P$ *est un polynôme unitaire ; on l'appelle le polynôme normalisé de* P, *et on le note souvent* $\widehat{P}$.

Proposition. 3.1.6.

Si P, Q sont deux polynômes alors :

1. $\deg(P+Q) \leq \max(\deg P, \deg Q)$, avec égalité si $\deg P \neq \deg Q$,
2. $\mathrm{Val}(P+Q) \geq \max(\mathrm{Val}(P), \mathrm{Val}(Q))$, avec égalité si $\mathrm{Val}P \neq \mathrm{Val}Q$,
3. $\deg(PQ) = \deg P + \deg Q$,
4. $\deg(P \circ Q) = \deg P \times \deg Q$ si $Q \neq 0$.

Preuve. Exercice ■

Corollaire. 3.1.2.

Les éléments inversible de l'anneau $(\mathbb{K}[X], +, \times)$ sont les polynômes constants non nuls.

Preuve. Soit P un polynôme inversible d'inverse Q. Donc, $PQ = 1$, et par suite $\deg P + \deg Q = 0$ puis $\deg P = \deg Q = 0$, ce qui montre que P est un polynôme constants non nul. La réciproque est évidente. ■

Corollaire. 3.1.3.

$(\mathbb{K}[X], +, \times)$ est un anneau intègre.

Preuve. Soit P, Q deux polynômes tels que $PQ = 0$. Dans ce cas, $\deg P + \deg Q = -\infty$ et par suite $\deg P = -\infty$ ou $\deg Q = -\infty$, c'est à dire que $P = 0$ ou $Q = 0$. ■

Proposition. 3.1.7.

Étant donné un entier naturel $n \in \mathbb{N}$, l'ensemble des polynômes de degrés inférieurs ou égal à n, qu'on notera par $\mathbb{K}_n[X]$, est un sous espace vectoriel de $(\mathbb{K}[X], +, .)$ de dimension $n+1$, et ayant la famille $\left(X^k\right)_{0 \leq k \leq n} = (1, X, \cdots, X^n)$ comme base. On l'appelle la base canonique de $\mathbb{K}_n[X]$.

3.1.5 Dérivation

Définition. 3.1.3.

On appelle polynôme dérivé d'un polynôme $P = \sum_{k=0}^{n} a_k X^k$, avec $n \geq 1$ et $a_0, \cdots, a_n \in \mathbb{K}$, le polynôme noté P' ou $P^{(1)}$ défini par : $P' = \sum_{k=0}^{n} k a_k X^{k-1}$.

Remarque 3.1.4 *Rappelons nous qu'un polynôme est une suite et non pas une fonction. Ainsi, la dérivation d'un polynôme n'est pas une dérivation de fonctions ; c'est juste une dérivation formelle.*

Propriétés 3.1.2

Si P, Q sont deux polynômes alors :

1. $\deg P' \leq \deg P$. *Plus précisément,*

$$\deg P' = \begin{cases} \deg P - 1 & , si\ \deg P \geq 1 \\ -\infty & , si\ \deg P \leq 0, \end{cases}$$

2. $(P+Q)' = P' + Q'$,
3. $\forall \alpha \in \mathbb{K},\ \ (\alpha.P)' = \alpha.P'$,
4. $(PQ)' = P.Q' + P'Q$.

Preuve. Facile ■

Remarque 3.1.5 *Comme pour pour le cas des fonctions, on définit les dérivées d'ordres supérieurs d'un polynôme P par récurrence. Ainsi, la dérivée d'ordre $k \geq 2$ de P est $P^{(k)} = \left(P^{(k-1)}\right)'$. Remarque qu'on a aussi $P^{(k)} = (P')^{(k-1)}$. De plus, si $P = \sum_{i=0}^{n} a_i X^i$, avec $n \geq 1$, alors*

$$P^{(k)} = \begin{cases} 0 & , si\ n < k \\ \sum_{k=0}^{n} i(i-1).\cdots.(i-k+1) a_i X^{i-k} = \sum_{i=k}^{n} k! \binom{i}{k} a_i X^{i-k} & , si\ n \geq k. \end{cases}$$

On notera aussi $P'' = P^{(2)}$, $P''' = P^{(3)}$ et par convention, $P^{(0)} = P$.

Théorème. 3.1.1. de Leibniz

Pour tous polynômes P, Q et tout $n \in \mathbb{N}$ on a :

$$(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}.$$

Preuve. C'est une simple récurrence sur n. ■

3.1.6 fonction polynomiale

Définition. 3.1.4.

À tout polynôme $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$, on associe l'application :

$$\begin{array}{rccc} \tilde{P}: & \mathbb{K} & \longrightarrow & \mathbb{K} \\ & x & \longmapsto & \tilde{P}(x) = \sum_{k=0}^{n} a_k x^k \end{array}$$

$\tilde{P}$ est appelée *l'application polynômiale* associée à P.

Propriétés 3.1.3

Si P, Q sont deux polynômes alors :

1. *L'application*
$$\begin{array}{rccc} \varphi : & (\mathbb{K}[X], +, ., \times) & \longrightarrow & (\mathbb{K}^{\mathbb{K}}, +, ., \times) \\ & P & \longmapsto & \widetilde{P} \end{array}$$
est un morphisme d'algèbre, c'est à dire que :
   (a) $\widetilde{P+Q} = \widetilde{P} + \widetilde{Q}$,
   (b) $\forall \alpha \in \mathbb{K},\ \widetilde{\alpha.P} = \alpha.\widetilde{P}$,
   (c) $\widetilde{PQ} = \widetilde{P}.\widetilde{Q}$,
2. $\widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}$,
3. $(\widetilde{P})' = \widetilde{P'}$, *et plus généralement :* $\forall k \in \mathbb{N},\ (\widetilde{P})^{(k)} = \widetilde{P^{(k)}}$.

Preuve. Facile ■

Théorème. 3.1.2. Formule de Talor

Pour tout polynôme $P \in \mathbb{K}_n[X]$, $n \in \mathbb{N}$, et tout $a \in \mathbb{K}$ on a :

$$P(a+X) = \sum_{k=0}^{n} \frac{\widetilde{P}^{(k)}(a)}{k!} x^k$$

En particulier,

$$P(X) = \sum_{k=0}^{n} \frac{\widetilde{P}^{(k)}(0)}{k!} x^k$$

Preuve. On se ramène au cas particulier où $P = X^n$. ■

Corollaire. 3.1.4.

L'application qui, à chaque polynôme fait correspondre sa fonction polynômiale, est un isomorphisme d'algèbre entre l'algèbre $\mathbb{K}_n[X]$ et celle des applications polynômiales.

Preuve. Il suffit de montrer que l'application φ (définit dans **Propriétés** 3.1.3) est injectif. En effet, si $P \in \ker \varphi$ alors $\widetilde{P}^{(k)}(0) = 0$ pour tout $k \in \mathbb{N}$, et par suite, d'après la formule de *Taylor*, $P = 0$. ■

Remarque 3.1.6 *L'isomorphisme précédent, permet de confondre un polynôme avec sa fonction polynômiale.*

3.1.7 Schéma de Hörner

Lorsqu'on cherche à évaluer un polynôme $\widetilde{P}(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$nen un point $x \in \mathbb{K}$, il n'est pas optimal de calculer chaque $a_k x^k$, puis de les ajouter. En effet, pour calculer $a_n x^n$, il est intéressant de se souvenir que l'on a déjà calculé $a_{n-1}x^{n-1}$, et donc x^{n-1}. Le mathématicien anglais *Horner* a mis au point une méthode efficace utilisant cette remarque. Pour un polynôme $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, on écrit

$$P(x) = (\cdots(((a_n x + a_{n-1})x + a_{n-2})x + a_{n-3})\cdots)x + a_0.$$

Cela revient à poser $b_n = a_n$, $b_{n-1} = a_{n-1} + b_n x, \cdots, b_1 = a_1 + b_2 x,\ b_0 = a_0 + b_1 x$, et alors $\tilde{P}(x) = b_0$. Le calcul nécessitera simplement n multiplications et n additions.

Exemple 3.1.1 *Pour calculer* $\tilde{P}(x) = 5x^4 - 4x^3 + 3x^2 - 2x + 1$, *on écrit* $\tilde{P}(x) = (x(x(x(5x-4)+3)-2)+1)$. *On calcule alors successivement* $a = 5$, $b = xa-4 = 5x-4$, $c = xb+3 = (x(5x-4)+3$, $d = xc - 2$, *et enfin* $\tilde{P}(x) = e = xd + 1$.

3.2 Arithmétique des polynômes

3.2.1 Divisibilité dans l'anneau des polynômes

Définition. 3.2.1.

Soit $A, B \in \mathbb{K}[X]$. On dit que A divise B, et on écrit A/B, lorsqu'il existe $P \in \mathbb{K}[X]$ tel que $B = PA$.

Exemples 3.2.1

1. *Pour tout* $n \in \mathbb{N}$, $1 - X$ *divise* $1 - X^n$ *dans* $\mathbb{K}[X]$,
2. $X - j$ *et* $X - j^2$ *divisent le polynôme* $X^2 + X + 1$ *dans* $\mathbb{C}[X]$, *où* $j = e^{\frac{2i\pi}{3}}$, *car* $X^2 + X + 1 = (X - j)(X - j^2)$.

Remarque 3.2.1 *Si un polynôme* A *divise un autre polynôme* B, *on dit aussi que* A *est un diviseur de* B, *ou encore que* B *est un multiple de* A.

Propriétés 3.2.1

1. *Le polynôme constant* 1 *divise tous les polynômes,*
2. *Tous les polynômes divisent le polynôme nul,*
3. *La divisibilité est une relation réflexive et transitive dans* $\mathbb{K}[X]$, *c'est à dire que pour tous polynômes* $A, B, C \in \mathbb{K}[X]$ *on a*
   - A/A
   - $(A/B$ *et* $B/C) \Rightarrow A/C$.
4. *Pour tout* $A, B \in \mathbb{K}[X]$ *on a :*

$$A/B \Longrightarrow B = 0 \text{ ou } \deg(A) \leq / \deg(B).$$

Proposition. 3.2.1. et définition

Étant donné deux polynômes $A, B \in \mathbb{K}[X]$, les propriétés suivantes sont équivalentes :

1. A/B et B/A,
2. Il existe un scalaire non nul $\alpha \in \mathbb{K} \setminus 0$ tel que $A = \alpha.B$,
3. Il existe un scalaire non nul $\alpha \in \mathbb{K} \setminus 0$ tel que $B = \alpha.A$,

Dans ce cas, on dit que A et B sont associés et on écrit $A \equiv B$

Preuve. Il est clair que $(2) \Leftrightarrow (3)$, $(2) \Rightarrow B/A$ et $(3) \Rightarrow A/B$, et donc $(2) \Leftrightarrow (3) \Rightarrow (1)$. Supposons maintenant que A/B et B/A. Il existe alors deux polynômes $U, V \in \mathbb{K}[X]$ de sorte que $A = UB$ et $B = VA$. Ainsi, $A = UVA$. Si $A \neq 0$ alors $UV = 1$. Sachant que seuls les polynômes constat non nuls qui sont inversibles, alors U est une constante non nulle α. Dans le cas $A = 0$, on a aussi $B = A = 0$, et on peut prendre $\alpha = 1$. Ceci achève la preuve. ■

Propriétés 3.2.2

Étant donné deux polynômes $A, B \in \mathbb{K}[X]$ alors

1. *A et B sont associés si, et seulement si, A/B et $\deg(A) = \deg(B)$,*
2. *Si A et B sont unitaires, alors A et B sont associés si et seulement si $A = B$.*

Proposition. 3.2.2. et définition

Étant donné un polynôme non nul $A \in \mathbb{K}[X]$, il existe un unique polynôme unitaire $\widehat{A}$ associé avec A. On l'appelle le polynôme normalisé de A

Preuve. Facile ; $\widehat{A} = \dfrac{1}{\gamma}.A$, où γ est le coefficient dominant de A. ■

Théorème. 3.2.1. Dévision Euclidienne

Soit $A, B \in \mathbb{K}[X]$ deux polynômes. Si B est non nul, alors il existe un unique couple (Q, R) de polynômes tels que $A = QB + R$ et $\deg(R) < \deg(B)$. Dans ce cas, le polynôme Q est appelé le quotient, et R le reste de la division euclidienne de A par B.

Preuve.

— L'unicité : Supposons que $A = Q_1B + R_1 = Q_2B + R_2$, avec $Q_1, Q_2, R_2, R_2 \in \mathbb{K}[X]$, $\deg(R_1) < \deg(B)$ et $\deg(R_2) < \deg(B)$. Dans ce cas, $(Q_1 - Q_2)\, B = R_2 - R_1$ et par suite $\deg(B) + \deg(Q_1 - Q_2) = \deg(R_2 - R_1) < \deg(B)$. Ceci entraine que $\deg(Q_1 - Q_2) < 0$, ce qui signifie que $Q_1 = Q_2$ puis $R_1 = R_2$.

— L'existence :

  — Si $A = 0$ alors il suffit de prendre $Q = R = 0$.

  — Supposons que $A \neq 0$, et montrons le résultat par récurrence sur le degré de A.

    — Si $\deg A < \deg B$ alors il suffit de prendre $Q = 0$ et $R = A$.

    — Supposons que le résultat est vrai pour tout polynôme de degré inférieur à un certain entier $n \geq \deg B$, et que $\deg A = n + 1$. Si on note $m = \deg B$,a le coefficient dominant de A et b celui de B, alors $\deg\left(A - \dfrac{a}{b}X^{n+1-m}B\right) \leq n$. Ainsi, d'après l'hypothèse de récurrence, il existe un couple (U, R) de polynômes tels que $A - \dfrac{a}{b}X^{n+1-m}B = UB + R$ et $\deg(R) < \deg(B)$. Il suffit alors de prendre $Q = U + \dfrac{a}{b}X^{n+1-m}$.

■

Remarque 3.2.2 *La construction du couple (Q, R) dans la preuve constitue un algorithme pratique pour déterminer un tel couple.*

Exemple 3.2.1

$$\begin{array}{rl|l} & X^3+X^2+2X+1 & X^2+1 \\ - & X^3+X & \hline & & X+1 \\ \hline & X^2+X+1 & \\ - & X^2+1 & \\ \hline & X & \end{array}$$

Donc, $X^3+X^2+2X+1=(X^2+1)(X+1)+1$.

Proposition. 3.2.3.

Soit $A, B \in \mathbb{K}[X]$ deux polynômes, B étant non nul, et R le reste de la division euclidienne de A par B. Alors A divise B si et seulement si $R=0$.

3.2.2 Racine d'un polynôme, multiplicité d'une racine

Définition. 3.2.2.

Soit $A \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. On dit que a est une racine de A, si $\tilde{A}(a)=0$.

Exemples 3.2.2 *j et j^2 sont deux racines de $1+X+X^2$, et pour tout $n \in \mathbb{N}$, 1 est une racine de $1-X^n$.*

Proposition. 3.2.4.

Soit $A \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors a est une racine de A si et seulement si $X-a$ divise A, c'est à dire :

$$\tilde{A}(a)=0 \Longleftrightarrow X-a/a.$$

Preuve. En effet, si Q est le quotient, et R le reste de la division euclidienne de A par $X-a$ alors, comme $\deg R < \deg(X-a)=1$, R est une constante $c \in$. Sachant que $A=(X-a)Q+c$ on a $\tilde{A}(a)=c$, et par suite $\tilde{A}(a)=0 \Longleftrightarrow c=0$. ■

Définition. 3.2.3. multiplicité d'une racine

Soit $A \in \mathbb{K}[X]$ un polynôme non nul, a une racine de A et $m \in \mathbb{N}^*$. On dit que a est une racine de A de multiplicité m, si $(X-a)^m$ divise A et $(X-a)^{m+1}$ ne divise pas A, c'est à dire que : $m=\max\left\{k \in \mathbb{N} \ : \ (X-a)^k/A\right\}$.
Si $m=1$ (resp. $m=2,3\cdots$), on parle de racine simple (resp. double, triple, ...).

Remarque 3.2.3

— *Toute racine d'un polynôme non nul admet une unique multiplicité,*

— *Si un élément $a \in \mathbb{K}$ n'est pas une racine de A, on dit parfois que c'est une racine de A de multiplicité nulle,*

— *Pour $A \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}$, il est clair que a est une racine de A de multiplicité m si et seulement si A s'écrit sous la forme $A=(X-a)^m Q$, où Q est un polynôme tel que : $\tilde{Q}(a) \neq 0$.*

Exemple 3.2.2 *j est une racine simple de X^3-1, et 0 est une racine double de X^2+X^3*

Proposition. 3.2.5.

Soit $A \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}^*$. Alors a est une racine de A de multiplicité m si, et seulement si, $\tilde{A}(a) = \tilde{A}'(a) = \cdots = \tilde{A}^{(m-1)}(a) = 0$ et $\tilde{A}^{(m)}(a) \neq 0$.

Preuve. La formule de Taylor s'écrit : $A(X) = \sum_{k=0}^{n} \frac{\tilde{A}^{(k)}(a)}{k!}(X-a)^k$, avec $n = \deg A$.Ainsi, les restes de la division Euclidienne de A par $(X-a)^m$ et $(X-a)^{m+1}$ sont respectivement $R_1 = \sum_{k=0}^{m-1} \frac{\tilde{A}^{(k)}(a)}{k!}(X-a)^k$ et $R_2 = \sum_{k=0}^{m} \frac{\tilde{A}^{(k)}(a)}{k!}(X-a)^k = R_1 + \frac{\tilde{A}^{(m)}(a)}{m!}(X-a)^m$. Il en découle que a est une racine de A de multiplicité m si et seulement $R_1 = 0$ et $R_2 \neq 0$, ce qui donne le résultat. ■

Exemple 3.2.3 *1 est une racine simple de $A = X^n - 1$, où $n \in \mathbb{N}^*$. En effet, il est clair que $\tilde{A}(1) = 0$ et $\tilde{A}'(1) = n \neq 0$, car $A' = nX^{n-1}$.*

Proposition. 3.2.6.

Si $a_1, \cdots, a_r$ sont des racines de multiplicités respectives $m_1, \cdots, m_r$ d'un polynôme non nul A, où $r \in \mathbb{N}^*$, alors $\prod_{i=1}^{r}(X-a_i)^{m_i}$ divise A. Plus précisément, A s'écrit sous la forme :

$$A = \prod_{i=1}^{r}(X-a_i)^{m_i} Q,$$

où Q est un polynôme vérifiant $\tilde{Q}(a_i) \neq 0$ pour tout $i \in [\![1, r]\!]$.

Preuve. C'est une récurrence sur r. Le cas $r = 1$ étant clair, supposons que ce résultat est vrai pour un certain $r \geq 1$, et que $a_1, \cdots, a_{r+1}$ sont des racines de multiplicités respectives $m_1, \cdots, m_{r+1}$ de A. L'hypothèse de récurrence permet d'écrire A sous la forme : $A = \prod_{i=1}^{r}(X-a_i)^{m_i} Q$, où Q est un polynôme vérifiant $\tilde{Q}(a_i) \neq 0$ pour tout $i \in [\![1, r]\!]$. Il est clair que a_{r+1} est une racine de Q. Soit α la multiplicité de a_{r+1} en tant que racine de Q. On peut écrire donc $Q = (X-a_{r+1})^{\alpha} R$, où R est un polynôme vérifiant $\tilde{R}(a_{r+1}) \neq 0$, et par conséquent $A = (X-a_{r+1})^{\alpha} \prod_{i=1}^{r}(X-a_i)^{m_i} R$, ce qui montre que α est aussi la multiplicité de a_{r+1} en tant que racine de A, i.e., $\alpha = m_{r+1}$. Ainsi, $A = \prod_{i=1}^{r+1}(X-a_i)^{m_i} R$, et $\tilde{R}(a_i) \neq 0$ pour tout $i \in [\![1, r+1]\!]$, ce qui achève la preuve. ■

Conséquences Soit $A \in \mathbb{K}[X]$.

1. Si $\deg A = n$, alors A admet au plus n racines deux à deux distinctes,
2. Si A admet n racines deux à deux distinctes, alors $\deg A \leq n$,
3. Si $\deg A \leq n$ et A admet $n+1$ racines deux à deux distinctes, alors $A = 0$,
4. Si A admet un infinité de racines, alors $A = 0$,
5. L'application de l'algèbre des polynôme vers celle des fonctions polynômiales à coefficients dans $\mathbb{K}$ qui, à chaque polynôme fait correspondre sa fonction polynômiale, est un isomorphisme d'algèbre.

3.2.3 Plus grand commun diviseur et plus petit commun multiple

Notation On note l'ensemble des multiples d'un polynôme P par (P). Étant donné deux polynômes P et Q, on note également,
$(P)+(Q)=\{A+B \ : \ A\in(P) \text{ et } B\in(Q)\}=\{AP+BQ \ : \ A,B\in\mathbb{K}[X]\}$.

Propriétés 3.2.3

1. *Pour tout $P\in\mathbb{K}[X]\}$, l'ensemble (P) est un idéal de $\mathbb{K}[X]$, c'est à dire que*
   - *(P) est un sous-groupe de $(\mathbb{K}[X],+)$ et,*
   - *$\forall A\in(P),\ \forall B\in\mathbb{K}[X],\ AB\in(P)$,*
2. *Pour tout $P,Q\in\mathbb{K}[X]\}$, les ensembles $(P)+(Q)$ et $(P)\cap(Q)$ est un idéal de $\mathbb{K}[X]$.*

Théorème. 3.2.2.

$(\mathbb{K}[X],+,\times)$ est un idéal principal, c'est à dire que tout idéal I de $(\mathbb{K}[X],+,\times)$ est de la forme $I=(P)$ pour un certain polynôme $P\in\mathbb{K}[X]$. Si de plus I est non nul, i.e., $I\neq\{0\}$, alors il existe un unique polynôme unitaire P vérifiant $I=(P)$.

Preuve. Sil $I=\{0\}$ alors le problème est résolu, car $I=(0)$. Supposons que I est non nul et posons $d=\min\left\{\deg A \ : \ A\in I \text{ et } A\neq 0\right\}$. Remarquer que d existe, car c'est le plus petit élément d'une partie non vide de $\mathbb{N}$. Soit $P\in I$ un polynôme de I ayant d pour degrés. Quitte à remplacer P par son normalisé, qui appartient à tour à I, on peut supposer que P est unitaire. Il suffit de montrer alors que $I=(P)$. Comme $P\in I$ et I est un idéal de $\mathbb{K}[X]$, alors $(P)\subset I$. Soit maintenant $A\in I$. La division Euclidienne de A par P s'écrit $A=PQ+R$ avec $\deg R<\deg P=d$. Remarquions alors que $R=A-PQ\in I$, et par suite $R=0$. Ceci montre que $A\in(P)$. Comme conséquence, $I=(P)$. Pour l'unicité, suppsons que s'écrit sous la forme $I=(P)=(Q)$, où P et Q sont des polynôme unitaires. Dans ce cas, P/Q et Q/P et par suite $P=Q$. ■

Proposition. 3.2.7. et définition

Soit $P,Q\in\mathbb{K}[X]\}$ deux polynômes.

1. Si $P\neq 0$ ou $Q\neq 0$ alors il existe un unique polynôme unitaire D vérifiant $(P)+(Q)=(D)$. Le polynôme (D) s'appelle le plus grand commun diviseur de P et Q et se note PGCD$(P;Q)$ ou encore $P\wedge Q$.
2. Si $P\neq 0$ et $Q\neq 0$ alors il existe un unique polynôme unitaire M vérifiant $(P)\cap(Q)=(M)$. Le polynôme (M) s'appelle le plus petit commun multiple de P et Q et se note PPCM$(P;Q)$ ou encore $P\vee Q$.

Preuve. C'est une application directe de la proposition précédente puisque $(P)+(Q)$ et $(P)\cap(Q)$ sont des idéaux de $\mathbb{K}[X]$. ■

Remarque 3.2.4

1. *Par convention, $0\wedge 0=P\vee 0=0\vee Q=0$. Ce choix est justifié par le fait que $(0)+(0)=(P)\cap(0)=(0)$.*

2. *La définition du PGCD et du PPCM s'étend sans difficulté à une famille finie $P_1, \cdots, P_n$. On a alors les identités :*

$$(P_1) + \cdots + (P_n) = pgcd(P_1, \cdots, P_n) = (\overset{n}{\underset{i=1}{\wedge}} P_i) \text{ et } \bigcap_{i=1}^{n}(P_i) = ppcm(P_1, \cdots, P_n) = (\overset{n}{\underset{i=1}{\vee}} P_i).$$

Propriétés 3.2.4

Propriétés 3.2.5

Soient $P, Q, R \in \mathbb{K}[X]$

1. *$(P \wedge Q) \wedge R = P \wedge (Q \wedge R) = P \wedge Q \wedge R$ et $(P \vee Q) \vee R = P \vee (Q \vee R) = P \vee Q \vee R$,*
2. *Ils existent deux polynômes $U, V \in \mathbb{K}[X]$; appelés coefficients de Bezout, tels que*

$$PU + QV = P \wedge Q,$$

3. *Si $P \neq 0$ ou $Q \neq 0$, et R est polynôme unitaire alors les assertions suivantes sont équivalentes :*
   - *(a)* $R = P \wedge Q$.
   - *(b)* $\begin{cases} R \text{ est un diviseur commun de } P \text{ et } Q, \\ \text{Tout diviseur commun de } P \text{ et } Q \text{ divise aussi } R. \end{cases}$
   - *(c)* $\begin{cases} R \text{ est un diviseur commun de } P \text{ et } Q, \\ \text{Pour tout diviseur commun } D \text{ de } P \text{ et } Q \text{ on a } \deg(D) \leq \deg(R). \end{cases}$
4. *Si R est polynôme unitaire alors les assertions suivantes sont équivalentes :*
   - *(a)* $R = P \vee Q$.
   - *(b)* $\begin{cases} R \text{ est un multiple commun de } P \text{ et } Q, \\ \\ \text{Tout multiple commun de } P \text{ et } Q \text{ est un multiple de } R. \end{cases}$
   - *(c)* $\begin{cases} R \text{ est un multiple commun de } P \text{ et } Q, \\ \\ \text{Si } M \text{ est un multiple commun non nul de } P \text{ et } Q \text{ alors} \\ \deg(R) \leq \deg(M). \end{cases}$

Preuve.

1. Car $((P) + (Q)) + (R) = (P) + ((Q) + (R)) = (P) + (Q) + (R)$ et $((P) \cap (Q)) \cap (R) = (P) \cap ((Q) \cap (R)) = (P) \cap (Q) \cap (R)$
2. comme $P \wedge Q \in (P) + (Q)$, alors ils existent deux polynômes $U, V \in \mathbb{K}[X]$ tels que $PU + QV = P \wedge Q$.
3. — Supposons que $R = P \wedge Q$. Puisque $P \in (P) + (Q) = (R)$ et $Q \in (P) + (Q) = (R)$ alors R divise P et Q. Soit maintenant un diviseur commun D de P et Q. En écrivant R sous la forme $R = PU + QV =$ on s'aperçoit facilement que D divise R, et aussi $\deg D \leq \deg R$.

— Réciproquement, supposons avoir (b) ou (c). Alors d'après ce qui a été démontré, R divise $P \wedge Q$ et $\deg R \leq \deg P \wedge Q$. Ainsi, si $P \wedge Q$ divise R ou si $\deg(P \wedge Q) \leq \deg R$ on a $R = P \wedge Q$.

4. — Supposons que $R = P \vee Q$. Puisque $R \in (P) \cap (Q) \subset (P)$ et $R \in (P) \cap (Q) \subset (Q)$ alors R est un multiple de P et Q. Soit maintenant un multiple commun M de P et Q. Donc $M \in (P) \cap (Q) = (R)$, et par conséquent M est un multiple de R et $\deg R \leq \deg M$.

— Réciproquement, supposons avoir (b) ou (c). Comme précédemment, on peut déduire que R est un multiple de $P \vee Q$ et $\deg(P \vee Q) \leq \deg R$. Ainsi, si on suppose que $P \vee Q$ est un multiple de R ou si $\deg R \leq \deg(P \wedge Q)$ on aura $R = P \wedge Q$.

■

Remarque 3.2.5
1. *La propriété 1 montre que le pgcd et le ppcm d'une famille finie de polynômes peut être définie aussi par récurrence.*
2. *Les propriétés 2 et 3 ainsi que 4 s'étendent au cas d'une famille finie de polynômes.*
3. *Les propriétés 3 et 4 montrent que le PGCD et le PPCM de polynômes méritent bien leurs noms.*

Proposition. 3.2.8.

Soient $P, Q, D, R \in \mathbb{K}[X]$. Si $P = QD + R$ alors $P \wedge Q = Q \wedge R$.

Preuve. Posons $A = P \wedge Q$ et $B = Q \wedge R$. Alors A divise P et Q et par la suite aussi $P - QD = R$; ainsi A est un diviseur commun de Q et R, ce qui permet de déduire que A divise $B = Q \wedge R$. Un raisonnement analogue prouve que B divise A, et alors $A = B$. ■

Application : L'algorithme d'*Euclide*. Soient P, Q deux polynômes non nuls.

— On calcul le reste R de la division Euclidienne de P par Q.

—
- Si $R_1 = 0$ on s'arrête ; $P \wedge Q = Q$.
- Sinon, on calcul le reste R_2 de la division Euclidienne de Q par R_1, et on répète le même processus, qui s'arrête au bout d'un nombre fini d'itérations.

Le pgcd de P et Q est donc le polynôme normalisé du dernier reste non nul dans cet algorithme appelé l'algorithme d'*Euclide*.

Remarque 3.2.6 *L'algorithme d'Euclide permet de trouver aussi le PGCD et des coefficients de Bézout de deux polynômes.*

Exemples 3.2.3 *Calculons le pgcd D des polynômes $A = X^4 - 4X^3 + 2X^2 + X + 6$ et $B = X^4 - 3X^3 + 2X^2 + X + 5$. L'algorithme d'Euclide donne :*

$$\begin{aligned} X^4 - 4X^3 + 2X^2 + X + 6 &= (X^4 - 3X^3 + 2X^2 + X + 5) + (-X^3 + 1) \\ X^4 - 3X^3 + 2X^2 + X + 5 &= (-X^3 + 1)(-X + 3) + (2X^2 + 2X + 2) \\ -X^3 + 1 &= (2X^2 + 2X + 2)(-\frac{1}{2}X + \frac{1}{2}) + 0 \end{aligned}$$

Le dernier reste non nul dans cet algorithme est $2X^2 + 2X + 2$, donc $D = X^2 + X + 1$. De plus, en remontant l'algorithme précédent, on a successivement :

$$\begin{aligned} 2D &= (-X^3 + 1)(X - 3) + B \\ &= (A - B)(X - 3) + B \\ &= A.(X - 3) + (-X + 4)B \end{aligned}$$

On peut donc choisir $U = \frac{1}{2}X - \frac{3}{2}$ et $V = -\frac{1}{2}X + 2$

3.2.4 Polynômes premiers entre eux

Définition. 3.2.4.

On dit que des polynômes $P_1, \cdots, P_n$ sont premiers entre eux, si $\bigwedge_{i=1}^{n} P_i = 1$.
On dit qu'ils sont sont premiers entre eux deux à deux si $P_i \wedge P_j = 1$ pour tout $i, j \in [\![1, n]\!]$ avec $i \neq j$.

Remarque 3.2.7 *Si $P_1, \cdots, P_n$ sont premiers entre eux deux à deux, alors ils sont sont premiers entre eux, mais la réciproque est fausse si $n \geq 3$.*

Théorème. 3.2.3. de Bézout

Des polynômes $P_1, P_2, \cdots, P_n$ sont premiers entre eux dans l'ensemble si et seulement s'ils existent des polynômes $U_1, U_2, \cdots, U_n$ tels que $\sum_{i=1}^{n} U_i P_i = 1$.

Preuve. Le sens direct étant évident ; c'est la définition même du pgcd de polynômes, on suppose qu'ils existent des polynômes $U_1, U_2, \cdots, U_n$ tels que $\sum_{i=1}^{n} U_i P_i = 1$. Comme $\bigwedge_{i=1}^{n} P_i$ est un diviseur commun des P_i, alors il divise aussi $\sum_{i=1}^{n} U_i P_i = 1$ et par suite $\bigwedge_{i=1}^{n} P_i = 1$. ■

Théorème. 3.2.4. de Gauss

Soient $P, Q, L \in \mathbb{K}[X]$. Si P/QL et $P \wedge Q = 1$ alors P/L.

Preuve. Les hypothèses permettent d'écrire $UP + VQ = 1$ et $OL = PW$, où $U, V, W \in \mathbb{K}[X]$. Ainsi

$$L = UPL + VQL = (UL + VW)P$$

et la conclusion en découle. ■

Proposition. 3.2.9.

Soient $P, Q, L \in \mathbb{K}[X]$. Si $P \wedge Q = P \wedge L = 1$ alors $P \wedge QL = 1$.

Preuve. Car si $U, V, W, R \in \mathbb{K}[X]$ sont des polynômes tels que $UP + VQ = PW + LR = 1$. Donc, $(UPW + ULR + VQW)U + VRLQ = 1$, et d'après le théorème de Bezout, $P \wedge QL = 1$.
■

Proposition. 3.2.10.

Soient $P, Q \in \mathbb{K}[X]$. Si $P \wedge Q = 1$ alors $P^n \wedge Q^m = 1$, pour tout $m, n \in \mathbb{N}$.

Preuve. Car si $U, V, W, R \in \mathbb{K}[X]$ sont des polynômes tels que $UP + VQ = PW + LR = 1$. Donc, $(UPW + ULR + VQW)U + VRLQ = 1$, et d'après le théorème de Bezout, $P \wedge QL = 1$.
■

Proposition. 3.2.11.

Soient $P, Q, L \in \mathbb{K}[X]$. Si P/L, Q/L et $P \wedge Q = 1$ alors PQ/L.

Preuve. Car si $U, V, W, R \in \mathbb{K}[X]$ sont des polynômes tels que $UP + VQ = 1$, $L = PW$ et $L = QR$, alors

$$L = UPL + VQL = PQ(UR + VW).$$

■

Proposition. 3.2.12.

Pour tous polynômes $P, Q, \in \mathbb{K}[X]$, il existe deux polynômes $U, V, \in \mathbb{K}[X]$ tels que $P = DU$, $Q = DV$ et $U \wedge V = 1$, avec $D = P \wedge Q$.

Preuve. Posons $D = P \wedge Q$. Il existe alors deux polynômes $U, V, \in \mathbb{K}[X]$ tels que $P = DU$, $Q = DV$. Donc, $D = P \wedge Q = (DU) \wedge (DV) = D(U \wedge V)$. Si $D \neq 0$ alors $U \wedge V = 1$, sinon, $P = Q = 0$, et dans ce cas, on peut prendre $U = V = 1$, et donc $U \wedge V = 1$. ■

Proposition. 3.2.13.

Pour tous polynômes $P, Q, \in \mathbb{K}[X]$,

$$\widehat{PQ} = (P \wedge Q)(P \vee Q).$$

Preuve. Soit $U, V, \in \mathbb{K}[X]$ tels que $P = DU$, $Q = DV$ et $U \wedge V = 1$, avec $D = P \wedge Q$. Ainsi on a $PQ = D^2UV$ et $(P \wedge Q)(P \vee Q) = D^2.(U \vee V)$. Il suffit donc de montrer que $U \vee V = UV$. En effet, UV est déjà un multiple commun de U et V, et si L est un autre multiple commun de U et V, alors d'après la Proposition 3.2.4, L est aussi un multiple de UV, ce qui signifie que $U \vee V = UV$. ■

3.2.5 Polynômes irréductibles

Définition. 3.2.5.

On dit qu'un polynôme non constant à coefficient dans $\mathbb{K}$ est irréductible dans $\mathbb{K}[X]$, si ses seuls diviseurs sont les polynômes constants non nuls et ses associés.

Exemples 3.2.4

1. *Tout polynôme de degré* 1 *est irréductible.*
2. *Si un polynôme de degré supérieur ou égal à* 2 *admet une racine dans* $a \in \mathbb{K}$ *alors il n'est pas irréductible dans* $\mathbb{K}$*; car divisible par* $X - a$*. Pour la réciproque, elle est fausse si le degré est supérieur ou égal à* 4*; prendre par exemple* $\left(X^2 + 1\right)^2$ *dans* $\mathbb{R}[X]$.
3. *Un polynôme* P *de degré* 2 *ou* 3 *est pas irréductible dans* $\mathbb{K}$ *si et seulement s'il n'admet pas de racine réelle. En effet, il n'est pas irréductible si et seulement s'il s'écrit sous la forme* $P = AB$*, où* A, B *sont des polynômes tels que* $\deg A \geq 1$ *et* $\deg B \geq 1$*. Comme* $\deg A + \deg B = \deg P \leq 3$*, alors forcément* $\deg A = 1$ *ou* $\deg B = 1$*, ce qui signifie que* P *admet une racine dans* $\mathbb{K}$.
4. *Dans* $\mathbb{R}[X]$*, un trinôme; c'est à dire un polynôme de degré* 2*, est irréductible si, et seulement si son discriminant est strictement négatif.*
5. *Dans* $\mathbb{R}[X]$*, un polynôme de degré* 3 *n'est pas irréductible, car, en vertu du théorème des valeurs intermédiaires, il admet une racine réelle.*

EXERCICE 3.2.1 *Montrer que* $X^3 + X^2 + X + 3$ *est irréductible dans* $\mathbb{Q}$.

Remarque 3.2.8 *La notion d'irréductibilité dépend du corps de base. Par exemple* $1 + X^2$ *est irréductible dans* $\mathbb{R}$ *mais il ne l'est pas dans* $\mathbb{C}$*, et* $X^2 - 2$ *est irréductible dans* $\mathbb{Q}$ *mais il ne l'est pas dans* $\mathbb{R}$.

Proposition. 3.2.14.

Soient $P, Q \in \mathbb{K}[X]$. Si P est irréductible alors P/Q ou $P \wedge Q = 1$.

Preuve. Supposons que P est irréductible. Puisque $P \wedge Q$ divise P, alors :

— soit c'est une constante non nulle, et dans ce cas $P \wedge Q = 1$; car $P \wedge Q$ est unitaire,

— soit c'est un associé de P ; c'est à dire de la forme γP où $\gamma \in \mathbb{K}^*$.

Donc P/Q ou $P \wedge Q = 1$. ■

Proposition. 3.2.15.

Soient $P, Q, L \in \mathbb{K}[X]$. Si P et Q sont irréductibles non associés, P/L et Q/L alors PQ/L.

Preuve. En effet, d'après la proposition précédente, $P \wedge Q = 1$, et par suite PQ/L. ■

Proposition. 3.2.16.

Tout polynôme non constant admet au moins un diviseur irréductible.

Preuve. C'est une simple récurrence sur le degré. ■

Théorème. 3.2.5.

Tout polynôme non constant $P \in \mathbb{K}[X]$ se décompose de manière unique (à un ordre prés) sous la forme

$$P = \gamma \prod_{k=1}^{n} P_k$$

où $\gamma \in \mathbb{K}^*$ et les P_k sont des polynômes irréductibles unitaires. Dan ce cas γ est le coefficient dominant de P.

Preuve.

— Pour l'existence, on raisonne par récurrence forte sur le degrés du polynôme P. Lorsque $\deg P = 1$, il est déjà irréductible. On écrit alors $P = \gamma \widehat{P}$, où γ est le coefficient dominant de P et $\widehat{P}$ est son polynôme normalisé ; qui est unitaire et irréductible.
Supposons que ce résultat est vrai chaque fois que $\deg P < d$ avec $d \in \mathbb{N}^*$. Si P est déjà irréductible, le problème ne se pose pas ; on fait fait comme précédemment, sinon, il s'écrit $P = QL$ où Q, L sont deux polynômes de degrés compris entre 1 et $d-1$. Il suffit alors d'appliquer l'hypothèse de récurrence à Q et L.

— Pour l'unicité, supposons qu'un certain polynôme P s'écrit sous cette forme de deux manières différentes :

$$P = \gamma \prod_{k=1}^{n} P_k = \gamma' \prod_{k=1}^{m} Q_k.$$

Sans quoi, $\gamma = \gamma'$; c'est le coefficient dominant de P. Après simplifications, on se ramène à l'une des deux situations suivantes :

— $\prod_{k=1}^{n} P_k = 1$, ce qui est contradictoire puisque le degré de 1 est nul,

— $\prod_{k=1}^{n} P_k = \prod_{k=1}^{m} Q_k$ avec $P_i \neq Q_j$ pour tout $i \in [\![1, n]\!]$ et $j \in [\![1, m]\!]$. Là aussi, on arrive à une contradiction : En effet, comme P_1 divise $\prod_{k=1}^{n} Q_k$, alors il divise au moins un Q_j où $j \in [\![1, m]\!]$, et par suite $P_1 = Q_j$.

■

Corollaire. 3.2.1.

Tout polynôme non constant $P \in \mathbb{K}[X]$ se décompose de manière unique (à un ordre prés) sous la forme

$$P = \gamma \prod_{k=1}^{n} P_k^{\alpha_k}$$

où γ est son coefficient dominant, les α_k sont des entiers naturels non nuls et les P_k sont des polynômes irréductibles unitaires distincts deux à deux.

Application. Si $P, Q \in \mathbb{K}[X]$ sont deux polynômes non constants dont les décompositions en facteurs irréductibles sont :

$$P = \gamma \prod_{k=1}^{n} P_k^{\alpha_k} \text{ et } Q = \gamma' \prod_{k=1}^{n} P_k^{\beta}$$

où γ est son coefficient dominant, les α_k sont des entiers naturels (éventuellement nuls) et les P_k sont des polynômes irréductibles unitaires distincts deux à deux, alors :

— $P \wedge A = \prod_{k=1}^{n} P_k^{\min(\alpha_k, \beta_k)}$ et $P \vee A = \prod_{k=1}^{n} P_k^{\max(\alpha_k, \beta_k)}$.

— P divise Q si et seulement si $\alpha_k \leq \beta_k$ pour tout $k \in [\![1, n]\!]$.

Théorème. 3.2.6. de D'Alembert-Gauss.

Tout polynôme non constant à coefficients complexes, admet au moins une racine complexe.

Preuve. Soit $P = \sum_{k=0}^{p} a_k X^k$ un polynôme de $\mathbb{C}[X]$ de degré $p > 0$. Il est clair que l'application définie sur $\mathbb{C}$ par $z \mapsto |P(z)|$ admet une ne borne inférieure qu'on notera α. Ceci découle du fait que l'ensemble $P = \{|P(z)|; z \in \mathbb{C}\}$ est une partie de $\mathbb{R}$ non vide et minorée par 0. Dans le reste de preuve, on va montrer que cette borne inférieure est atteint en un point $w \in \mathbb{C}$, puis que $\alpha = 0$. Ceci achèvera la démonstration. D'abord, on montre que $\lim_{|z| \to +\infty} |P(z)| = +\infty$. En effet, pour tout $r > 0$, et tout nombre complexe z de module r on a

$$|P(z)| = \left|\sum_{k=0}^{p} a_k z^k\right| \geq |a_p z^p| - \left|\sum_{k=0}^{p-1} a_k z^k\right| . \geq |a_p| r^p - \sum_{k=0}^{p-1} |a_k| r^k.$$

Ainsi, comme $\lim_{r \to +\infty} |a_p| r^p - \sum_{k=0}^{p-1} |a_k| r^k = +\infty.$, on a $\lim_{|z| \to +\infty} |P(z)| = +\infty$. Comme conséquence, il existe un réel $r_1 > 0$ tel que si $|z| > r_1$, alors $|P(z)| > \alpha + 2$. D'autre part, d'après la caractérisation séquentielle de la borne inférieure, il existe une suite $(y_n) \in \mathbb{C}$ tel que $|P(y_n)|$

converge vers α. Ainsi, il existe un entier n_0 tel que pour tout $n > n_0$, $|P(y_n)| \in [\alpha - 1, \alpha + 1]$. On en déduit que, pour tout $n \in \mathbb{N}$, $|y_n| \leq r_1$, et alors la suite $(y_n)_{n\in\mathbb{N}}$ est bornée de $\mathbb{C}$. Donc, d'après le théorème de Bolzano-Weierstrass, $(y_n)_{n\in\mathbb{N}}$ admet une sous-suite convergente. Notons $(z_n)_{n\in\mathbb{N}}$ cette suite extraite et w sa limite.

Comme $(|P(z_n)|)_{n\in\mathbb{N}}$ est une suite extraite de $(|P(y_n)|)_{n\in\mathbb{N}}$, la suite $(|P(z_n)|)_{n\in\mathbb{N}}$ converge vers α. Or, $\lim\limits_{n\to+\infty} |P(z_n)| = |P(w)|$, et par suite $|P(w)| = \alpha$. Reste à démontrer que $\alpha = 0$. Pour cela, supposons que $\alpha \neq 0$ et posons $Q = \dfrac{P(X + z_0)}{P(z_0)}$. Il est clair que $\inf\limits_{z\in\mathbb{C}} |Q(z)| = |Q(0)| = 1$. Donc, on peut écrire Q sous la forme

$$Q = 1 - b_q X^q + \sum_{k=q+1}^{p} b_k X^k.$$

avec $q \in \{1, \ldots, p\}$ et $b_q \neq 0$. En posant $b_q = \rho e^{-i\theta}$, et en prenant $z = re^{i\theta/q}$ on obtient $|Q(z)| \leq |1 - \rho r^q| + \sum\limits_{k=q+1}^{p} |b_k| r^k$, et pour r assez petit, $\rho r^q \leq 1$ et

$$|Q(z)| \leq 1 - \rho r^q + \sum_{k=q+1}^{p} |b_k| r^k.$$

Or, lorsque r tend vers 0,

$$-\rho r^q + \sum_{k=q+1}^{p} |b_k| r^k \underset{0}{\sim} -\rho r^q < 0,$$

donc, pour r assez petit, $|Q(z)| - 1 < 0$, soit $|Q(z)| < 1$.

Or, ceci est impossible car $1 = \inf\limits_{z\in\mathbb{C}} |Q(z)|$. On obtient ainsi une contradiction, et par conséquent

$$\alpha = 0.$$

■

Corollaire. 3.2.2.

- Les polynômes irréductibles de $\mathbb{C}[X]$ sont ceux de degré 1,
- les polynômes irréductibles de $\mathbb{R}[X]$ sont
  - Ceux de degré 1
  - Ceux de degré 2 de discriminants strictement négatifs.

Preuve.

- Dans $\mathbb{C}[X]$, le problème est réglé par le théorème de D'Alembert-Gauss.
- dans $\mathbb{R}$, on sait que les polynômes de degré 1ainsi que ceux de degré 2 de discriminants strictement négatifs sont irréducibles. pour la réciproque, considérons un polynôme P irréductible dans $\mathbb{R}[X]$. D'après le théorème de D'Alembert-Gauss, il admet une racine complexe $\alpha \in \mathbb{C}$. Si $\alpha \in \mathbb{R}$, alors $X - \alpha$ divise P, et par suite $\deg P = 1$; car P et $X - \alpha$ sont dans ce cas associés. Sinon, comme P est à coefficients réels, $\overline{\alpha}$ est aussi racine de P. Donc, $X - \alpha$ et $X - \overline{\alpha}$ divisent P dans $\mathbb{C}$, ce qui montre qui $X^2 - 2\mathrm{Re}(\alpha)X + |\alpha| = (X - \alpha)(X - \overline{\alpha})$, qui est à coefficients réels, divise aussi P dans $\mathbb{C}$. D'autre part, le reste de la division Euclidienne P par $X^2 - 2\mathrm{Re}(\alpha)X + |\alpha|$ dans $\mathbb{R}$ est le même que celui dans $\mathbb{R}$. Donc, $X^2 - 2\mathrm{Re}(\alpha)X + |\alpha|$ divise P dans $\mathbb{R}$. Étant irréductible, P est associé avec $X^2 - 2\mathrm{Re}(\alpha)X + |\alpha|$, qui est un polynôme de degré 2 de discriminant strictement négatif ; puisqu'il n'a pas de racine réelle.

■

Corollaire. 3.2.3.

— Tout polynôme non constant P à coefficients complexes est décomposable en facteurs de degré 1 sur $\mathbb{C}$, donc de la forme :

$$P = \gamma \prod_{k=1}^{d} (X - a_i)$$

où $\gamma \in \mathbb{C}^*$ et $a_0, a_1, \cdots, a_d \in \mathbb{C}$.

— Tout polynôme non nul P à coefficients réels est décomposable en facteurs irréductibles sur $\mathbb{R}$ sous la forme suivante :

$$P = \gamma \prod_{k=1}^{d} (X - a_i) \prod_{k=1}^{d'} X^2 + b_i X + c_i)$$

avec $\gamma \in \mathbb{R}^*$, $a_0, a_1, \cdots, a_d, a_0, b_1, \cdots, b_{d'}, c_1, \cdots, c_{d'} \in \mathbb{R}$, et $b_i^2 - 4c_i < 0$ pour tout $i \in [\![1, d']\!]$.

Exemples 3.2.5 1. *Dans $\mathbb{C}$ on a $X^3 - 1 = (X-1)(X-j)(X-j^2)$, et dans $\mathbb{R}$ on a $X^3 - 1 = (X-1)(X^2+X+1)$.*

2. *Dans $\mathbb{C}$ on a $X^4 - 1 = (X-1)(X+1)(X-i)(X+i)$, et dans $\mathbb{R}$ on a $X^4 - 1 = (X-1)(X+1)(X^2+1)$.*

3.2.6 Relations entre coefficients et racines d'un polynôme scindé

Définition. 3.2.6.

On dit qu'un polynôme non constant $P \in \mathbb{K}[X]$ est scindé sur $\mathbb{K}$, s'il peut s'écrire sous la forme de produit de polynômes de degré un sur $\mathbb{K}$, c'est à dire de la forme :

$$P = \gamma \prod_{k=1}^{d} (X - a_i)$$

où $\gamma \in \mathbb{K}^*$ et $a_0, a_1, \cdots, a_d \in \mathbb{K}$.

Ainsi, un polynôme de degré $n \geq 1$ est scindé dans $\mathbb{K}$ si et seulement s'il admet n racines distinctes deux. D'après le théorème de *Gauss*, tout polynôme non constant à coefficients complexes est scindé sur $\mathbb{C}$.

Définition. 3.2.7.

Soit $n \in \mathbb{N}^*$ et $x_1, x_2, \cdots, x_n \in \mathbb{K}$. On appelle fonctions symétriques élémentaires de $x_1, x_2, \cdots, x_n$, les expressions

$$\sigma_p = \sum_{i_1<\cdots<i_p} \prod_{k=1}^{p} x_{i_k}$$

pour tout $p \in [\![1, n]\!]$. C'est à dire :

$$\sigma_1 = \sum_{i=1}^{n} x_i, \quad \sigma_2 = \sum_{1\leq i<j\leq n} x_i x_j, \quad \sigma_3 = \sum_{1\ i<j<k\leq n} x_i x_j x_k, \quad \cdots, \quad \sigma_n = \prod_{i=1}^{n} x_i.$$

Proposition. 3.2.17.

Soit $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{K}[X]$ un polynôme non constant et scindé dont la décomposition en facteurs irréductibles est : $P = a_n \prod_{k=1}^{n}(X - x_i)$, où $a_n \in \mathbb{K}^*$ et $a_0, a_1, \cdots, a_n \in \mathbb{K}$. En posant $\sigma_1, \sigma_2, \cdots, \sigma_n$ fonctions symétriques élémentaires de $x_1, x_2, \cdots, x_n$, alors

$$\forall p \in [\![1, n]\!], \quad \sigma_p = (-1)^p \frac{a_{n-p}}{a_n}.$$

En particulier,

$$\sum_{i=1}^{n} x_i = -\frac{a_{n-1}}{a_n} \text{ et } \prod_{i=1}^{n} x_i = (-1)^p \frac{a_{n-1}}{a_n}.$$

EXERCICE 3.2.2 *Calculer a^2+ab^2+3ab sachant que a, b sont deux racines distinctes de z^3+3z^2+z.*

Solution 5 *Soit c la troisième racine de $zs+3z^2+z$. Alors $a^2b+ab^2+3ab = ab(a+b+3) = -abc = 1$.*

Chapitre 4

Les fractions rationnelles

Tout au long de ce chapitre, on désigne par $\mathbb{K}$ un sous corps de $\mathbb{C}$, principalement $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

4.1 Construction de l'ensemble des fractions rationnelles

4.1.1 Définition d'une fraction rationnelle

Dans l'ensemble

$$\mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\}) = \{(P, Q) \mid P, Q \in \mathbb{K}[X], Q \neq 0\},$$

on définit la relation $\mathcal{R}$ en posant :

$$(P, Q)\, R\, (R, S) \iff P \cdot S = Q \cdot R.$$

On vérifie que la relation $\mathcal{R}$ est une relation d'équivalence dans $\mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\})$. La transitivité de la relation utilise l'intégrité de $\mathbb{K}[X]$.

Définition. 4.1.1.

On appelle *fraction rationnelle à coefficients dans* $\mathbb{K}$ toute classe d'équivalence pour la relation $\mathcal{R}$. La classe de (P, Q) est notée $\dfrac{P}{Q}$ (avec P le numérateur et Q le dénominateur), on a donc :

$$\frac{P}{Q} = \{(R, S) \in \mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\}) \mid P \cdot S = Q \cdot R\}.$$

On dit que (P, Q) est un représentant de la fraction $\dfrac{P}{Q}$.

L'ensemble des fractions rationnelles est noté $\mathbb{K}(X)$ et la relation $\mathcal{R}$ est appelée *égalité des fractions rationnelles*.

4.1.2 Opérations sur les fractions

Définition. 4.1.2.

Soient $\frac{P}{Q}$ et $\frac{R}{S}$ deux fractions rationnelles et soit $\lambda \in \mathbb{K}$. On pose :

$$\frac{P}{Q}+\frac{R}{S}=\frac{PS+QR}{QS}, \quad \frac{P}{Q}\times\frac{R}{S}=\frac{PR}{QS}, \quad \text{et} \quad \lambda\frac{P}{Q}=\frac{\lambda P}{Q}.$$

Pour que la définition ait un sens, il faut que le résultat ne dépende pas des représentants choisis pour les fractions. C'est-à-dire, si $\frac{P}{Q}=\frac{P'}{Q'}$ et $\frac{R}{S}=\frac{R'}{S'}$, alors :

$$\frac{PS+QR}{QS}=\frac{P'S'+Q'R'}{Q'S'}, \quad \frac{PR}{QS}=\frac{P'R'}{Q'S'}, \quad \text{et} \quad \lambda\frac{P}{Q}=\lambda\frac{P'}{Q'}.$$

Cette vérification est simple et laissée en exercice.

Remarque 4.1.1 *Pour tous polynômes non nuls P et Q, on a $\frac{0}{P}=\frac{0}{Q}$, et $\frac{P}{P}=\frac{Q}{Q}$.*

Propriétés 4.1.1

a) ***Pour l'addition :***
- *Elle est associative et commutative.*
- *Elle admet un élément neutre, la fraction $\frac{0}{Q}$, où Q est un polynôme non nul.*
- *Toute fraction $\frac{P}{Q}$ admet un opposé et $-\frac{P}{Q}=\frac{-P}{Q}=\frac{P}{-Q}$.*

b) ***Pour la multiplication :***
- *Elle est associative et commutative.*
- *Elle admet un élément neutre qui est la fraction $\frac{P}{P}$, où Q est un polynôme non nul.*
- *Toute fraction $\frac{P}{Q}$ non nulle (i.e., $P \neq 0$) admet un inverse, et $\left(\frac{P}{Q}\right)^{-1}=\frac{Q}{P}$.*
- *Elle est distributive sur l'addition.*

c) ***Pour le produit par un scalaire :***
- $\forall \lambda, \mu \in \mathbb{K}, \forall F, G \in \mathbb{K}(X)$:
  - $1 \cdot F = F$;
  - $\lambda \cdot (F+G) = \lambda \cdot F + \lambda \cdot G$;
  - $(\lambda+\mu) \cdot F = \lambda \cdot F + \mu \cdot F$;
  - $(\lambda\mu) \cdot F = \lambda \cdot (\mu \cdot F)$;
  - $\lambda \cdot (F \times G) = (\lambda \cdot F) \times G = F \times (\lambda \cdot G)$.

Corollaire. 4.1.1.

$(\mathbb{K}(X), +, \times)$ est un corps commutatif et $(\mathbb{K}(X), +, \times, \cdot)$ est une $\mathbb{K}$-algèbre commutative.

4.1.3 Représentants irréductibles

Théorème. 4.1.1. plongement des polynômes dans $\mathbb{K}(X)$

L'application $\varphi : \mathbb{K}[X] \to \mathbb{K}(X)$ définie par $\varphi(P) = \dfrac{P}{1}$ est un morphisme d'algèbres injectif.

Preuve. Facile. ■

Par conséquent, on peut identifier le polynôme P avec la fraction $\dfrac{P}{1}$, ce qui fait que l'on peut considérer que $\mathbb{K}[X] \subset \mathbb{K}(X)$. En particulier, la fraction nulle (en vertu de l'égalité des fractions) est identifiée au polynôme nul 0, et la fraction unité est identifiée au polynôme constant 1.

Définition. 4.1.3.

Soit $F = \dfrac{P}{Q}$ une fraction, on dit que $\dfrac{P}{Q}$ est un représentant irréductible lorsque $pgcd(P, Q) = 1$ et que Q est unitaire.

Exemple 4.1.1 *Soit* $F = \dfrac{X^3 - 1}{X^2 - 1}$. *Un représentant irréductible est* $\dfrac{X^2 + X + 1}{X + 1}$.

4.2 Degré, pôles et racines d'une fraction

4.2.1 Notion de degré

Soit F une fraction non nulle et $\dfrac{P}{Q}$, $\dfrac{R}{S}$ deux représentants de F (i.e., $F = \dfrac{P}{Q} = \dfrac{R}{S}$), on a donc $PS = QR$, d'où $\deg(P) - \deg(Q) = \deg(R) - \deg(S)$. Autrement dit, la différence entre le degré du numérateur et le degré du dénominateur ne dépend pas du représentant de F, mais seulement de F.

Définition. 4.2.1.

Soit $F = \dfrac{P}{Q}$ une fraction, on pose $\deg(F) = -\infty$ si $F = 0$, et $\deg(F) = \deg(P) - \deg(Q)$ sinon. Le degré d'une fraction est donc un élément de $\mathbb{Z} \cup \{-\infty\}$.

Remarque 4.2.1 *Soit P un polynôme, en tant que polynôme son degré est* $\deg(P)$, *mais en tant que fraction, son degré est* $\deg\left(\dfrac{P}{1}\right) = \deg(P) - \deg(1) = \deg(P)$. *On trouve bien la même chose.*

Exemple 4.2.1 $\deg\left(\dfrac{X^2 + X + 1}{X + 1}\right) = 1$ *et* $\deg\left(\dfrac{X}{X^3 - X^2 + 2}\right) = -2$.

Théorème. 4.2.1.

Soient $F, G \in \mathbb{K}(X)$, on a : $\deg(F+G) \leq \max(\deg(F), \deg(G))$, et $\deg(F \times G) = \deg(F) + \deg(G)$. On retrouve les mêmes propriétés que pour les polynômes.

Preuve. Posons $F = \dfrac{P}{Q}$ et $G = \dfrac{R}{S}$, alors $F \times G = \dfrac{PR}{QS}$, donc $\deg(F \times G) = \deg(PR) - \deg(QS) = \deg(P) - \deg(Q) + \deg(R) - \deg(S) = \deg(F) + \deg(G)$. De même, $\deg(F+G) = \deg(PS+QR) - \deg(QS)$, or $\deg(PS+QR) \leq \max(\deg(PS), \deg(QR))$, donc on a $\deg(F+G) \leq \deg(PS) - \deg(QS)$ ou $\deg(F+G) \leq \deg(QR) - \deg(QS)$, c'est-à-dire $\deg(F+G) \leq \deg(F)$ ou $\deg(F+G) \leq \deg(G)$, finalement, $\deg(F+G) \leq \max(\deg(F), \deg(G))$. ■

Remarque 4.2.2

— *Une fraction rationnelle constante non nulle a un degré nul, mais la réciproque est fausse, par exemple :* $F = \dfrac{X}{X+1}$.

— *Si* $\deg(F) \neq \deg(G)$ *alors* $\deg(F+G) = \max(\deg(F), \deg(G))$.

— *Une fraction* F *est nulle si et seulement si son degré vaut* $-\infty$.

4.2.2 Pôles et racines

Définition. 4.2.2.

Soit $F \in \mathbb{K}(X)$ non nulle, et soit $\dfrac{P}{Q}$ un représentant irréductible de F. On dit que $a \in \mathbb{K}$ est racine de F de multiplicité $m \in \mathbb{N}^*$ lorsque a est racine du numérateur P de multiplicité m. On dit que $a \in \mathbb{K}$ est pôle de F de multiplicité $m \in \mathbb{N}^*$ lorsque a est racine du dénominateur Q de multiplicité m.

Remarque 4.2.3

— *Puisque* $\dfrac{P}{Q}$ *est irréductible, on voit qu'un scalaire* a *ne peut pas être à la fois pôle et racine de* F*, sinon* P *et* Q *seraient divisibles par* $X - a$.

— a *est un pôle de* F *de multiplicité* $m \in \mathbb{N}^*$ *revient à dire que* a *est racine de multiplicité* m *de* $\dfrac{1}{F}$.

— *Par exemple, la fraction* $F = \dfrac{X^3 - 1}{X^2 - 1}$ *possède deux racines complexes simples* j *et* j^2*, un pôle simple* -1*, mais pas de racine réelle.*

4.3 Fonctions rationnelles

Définition. 4.3.1.

Soit $F \in \mathbb{K}(X)$ et $\dfrac{P}{Q}$ un représentant irréductible de F. On pose

$$D_F = \mathbb{K} \setminus \{\text{pôles de } F\},$$

c'est-à-dire

$$D_F = \{x \in \mathbb{K} \mid Q(x) \neq 0\}.$$

On appelle **fonction rationnelle** de $\mathbb{K}$ dans $\mathbb{K}$ associée à la fraction F, la fonction notée $\tilde{F}$ de D_F vers $\mathbb{K}$ définie par

$$\tilde{F}(x) = \frac{P(x)}{Q(x)}.$$

Remarque 4.3.1 *Avant d'étudier une fonction rationnelle, il faut la mettre sous forme irréductible.*

Théorème. 4.3.1.

Soient $F, G \in \mathbb{K}(X)$, si les fonctions rationnelles $\tilde{F}$ et $\tilde{G}$ sont égales sur une partie infinie I de $D_F \cap D_G$, alors les fractions rationnelles sont égales, i.e. $F = G$.

Preuve. Le corps $\mathbb{K}$ est infini, l'ensemble des pôles de F et celui de G sont finis, donc $D_F \cap D_G$ est un ensemble infini.
Posons $F = \dfrac{P}{Q}$ et $G = \dfrac{R}{S}$ irréductibles. Alors $\forall x \in I$, on a

$$P(x)S(x) - R(x)Q(x) = 0,$$

donc le polynôme $PS - QR$ est nul (infinité de racines), ce qui signifie exactement que $F = G$.
■

4.4 Dérivation d'une fraction rationnelle

Soit $F \in \mathbb{K}(X)$ une fraction rationnelle et $\dfrac{P}{Q} = \dfrac{R}{S}$ deux représentants de F. On a $PS = QR$, d'où

$$(P'Q - PQ')S^2 = P'QS^2 - PQ'S^2 = P'QS^2 - Q'QRS,$$

mais en dérivant la relation polynomiale $PS = QR$, on obtient

$$P'S + PS' = Q'R + QR',$$

d'où

$$(P'Q - PQ')S^2 = QS(QR' - PS') = Q^2SR' - QPSQ' = Q^2SR' - Q^2RS' = Q^2(SR' - RS'),$$

ce qui traduit l'égalité des fractions :

$$\frac{P'Q - PQ'}{Q^2} = \frac{R'S - RS'}{S^2}.$$

Définition. 4.4.1.

Soit $F = \dfrac{P}{Q} \in \mathbb{K}(X)$, on appelle **fraction dérivée** de F la fraction notée F' (ou $\dfrac{dF}{dX}$) définie par :

$$F' = \frac{P'Q - PQ'}{Q^2}.$$

Le résultat ne dépend pas du représentant de F choisi.
On définit également les **dérivées successives** de F en posant $F^{(0)} = F$ et pour tout $n \in \mathbb{N}$,

$$F^{(n+1)} = \left(F^{(n)}\right)'.$$

Remarque 4.4.1

— *Soit P un polynôme, la dérivée de P en tant que fraction rationnelle est*

$$\left(\frac{P}{1}\right)' = \frac{P' \cdot 1 - P \cdot 0}{1^2} = P',$$

on retrouve bien la dérivée de P en tant que polynôme.

— *Contrairement aux polynômes, le degré de F' n'est pas toujours égal à $\deg(F)-1$. Par exemple : $F = \dfrac{X}{X+1}$, on a $\deg(F) = 0$ et*

$$F' = \frac{1}{(X+1)^2},$$

donc $\deg(F') = -2$. Par contre, on a toujours $\deg(F') \leq \deg(F) - 1$.

On retrouve les propriétés usuelles de la dérivation avec les formules suivantes :

Propriétés 4.4.1

Soit $F, G \in \mathbb{K}(X)$,

1. $(F+G)' = F' + G'$;
2. $(F \times G)' = F' \times G + F \times G'$;
3. $(\lambda \cdot F)' = \lambda \cdot F'$;
4. $\left(\dfrac{1}{F}\right)' = -\dfrac{F'}{F^2}$;
5. *Formule de Leibniz :*

$$\forall n \in \mathbb{N}, (F \times G)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} F^{(k)} \cdot G^{(n-k)}.$$

Preuve. Laissée en exercice. ■

Définition. 4.4.2.

Soit F une fraction non nulle, la dérivée logarithmique de F est la fraction $\dfrac{F'}{F}$.

Théorème. 4.4.1.

Si F est une fraction non nulle qui se factorise en $F = F_1 \times \cdots \times F_n$ dans $\mathbb{K}(X)$ avec $n \in \mathbb{N}^*$, alors :

$$\frac{F'}{F} = \frac{F_1'}{F_1} + \cdots + \frac{F_n'}{F_n}$$

Preuve. Par récurrence sur n en commençant par le cas $n = 2$. Si $F = F_1F_2$, alors :

$$F' = F_1'F_2 + F_1F_2',$$

d'où :

$$\frac{F'}{F} = \frac{F_1'}{F_2} + \frac{F_1F_2'}{F_1F_2} = \frac{F_1'}{F_1} + \frac{F_2'}{F_2}.$$

Le passage du rang n au rang $n+1$ se ramène au cas $n = 2$. ■

4.5 Décomposition d'une fraction rationnelle

4.5.1 Partie entière

Théorème. 4.5.1. et définition

Soit $F \in \mathbb{K}(X)$. Alors il existe un unique polynôme E et une unique fraction rationnelle G tels que $F = E + G$ et $\deg(G) < 0$. E est appelé *la partie entière* de F.

Preuve.

Soit $F = \dfrac{A}{B}$ une fraction, on effectue la division euclidienne de A par B : $A = BQ + R$ avec $\deg(R) < \deg(B)$. On a alors :

$$F = Q + \frac{R}{B},$$

avec $\deg\left(\dfrac{R}{B}\right) < 0$ et $Q \in \mathbb{K}[X]$.

Supposons qu'il existe un autre polynôme S et une fraction G tels que $F = S + G$ avec $\deg(G) < 0$, alors $\deg(Q - S) = \deg\left(G - \dfrac{R}{B}\right) < 0$, donc $Q = S$ car ce sont des polynômes, et $G = \dfrac{R}{B}$.

■

Remarque 4.5.1 — *La partie entière de F est l'un unique polynôme E tel que $\deg(F - E) < 0$,*

— *La partie entière de F, c'est le quotient dans la division euclidienne du numérateur de F par le dénominateur,*

— *Si $\deg(F) < 0$, alors la partie entière de F est nulle.*

4.5.2 Éléments simples

Définition. 4.5.1.

Un élément simple de $\mathbb{K}(X)$ est une fraction du type $\dfrac{A}{B^n}$, où B est un polynôme irréductible unitaire (c'est-à-dire $B \in I_{\mathbb{K}}[X]$), $\deg(A) < \deg(B)$, et $n > 1$.

— **Éléments simples dans $C(X)$** : On sait que $I_C[X] = \{X - a \mid a \in \mathbb{C}\}$, donc les éléments simples de $C(X)$ sont des fractions du type :

$$\frac{\alpha}{(X-a)^n},$$

avec $\alpha, a \in \mathbb{C}$ et $n > 1$.

— **Éléments simples de $R(X)$** : On sait que $I_R[X] = \{X - a \mid a \in \mathbb{R}\} \cup \{X^2 + pX + q \mid p, q \in \mathbb{R}, p^2 - 4q < 0\}$, donc les éléments simples de $R(X)$ sont de deux types :

— **Éléments simples de première espèce** :

$$\frac{\alpha}{(X-a)^n},$$

avec $\alpha, a \in \mathbb{R}$ et $n > 1$.

— **Éléments simples de seconde espèce** :

$$\frac{aX+b}{(X^2+pX+q)^n},$$

avec $a, b, p, q \in \mathbb{R}$, $p^2 - 4q < 0$, et $n > 1$.

4.5.3 Décomposition en éléments simples

Lemme 4.5.1 *Si T, S sont deux polynômes premiers entre eux et si $\deg\left(\frac{A}{TS}\right) < 0$, alors il existe deux polynômes U et V tels que :*

$$\frac{A}{TS} = \frac{U}{T} + \frac{V}{S}$$

avec $\deg(U) < \deg(T)$ et $\deg(V) < \deg(S)$.

Preuve. Il existe deux polynômes U_0 et V_0 tels que $U_0S + V_0T = 1$ (théorème de Bézout). On a alors :

$$\frac{A}{TS} = \frac{AU_0}{T} + \frac{AV_0}{S},$$

soit E_1 la partie entière de $\frac{AU_0}{T}$ et E_2 celle de $\frac{AV_0}{S}$. Il existe deux polynômes U et V tels que :

$$\frac{AU_0}{T} = E_1 + \frac{U}{T} \quad \text{avec} \quad \deg(U) < \deg(T),$$

et

$$\frac{AV_0}{S} = E_2 + \frac{V}{S} \quad \text{avec} \quad \deg(V) < \deg(S),$$

d'où :

$$\frac{A}{TS} = E_1 + E_2 + \frac{U}{T} + \frac{V}{S}.$$

Mais $\deg\left(\frac{U}{T} + \frac{V}{S}\right) < 0$, donc $E_1 + E_2$ est la partie entière de $\frac{A}{TS}$. Or celle-ci est nulle, donc $E_1 + E_2 = 0$, ce qui donne le résultat. ■

[. Conséquence] Par récurrence, on en déduit que si $B_1, \ldots, B_n$ sont premiers entre eux deux à deux et si $\deg\left(\frac{A}{B_1 \times \cdots \times B_n}\right) < 0$, alors il existe des polynômes $U_1, \ldots, U_n$ tels que :

$$\frac{A}{B_1 \times \cdots \times B_n} = \sum_{i=1}^{n} \frac{U_i}{B_i}$$

avec $\deg(U_i) < \deg(B_i)$.

En appliquant ceci à notre fraction F, on peut affirmer qu'il existe des polynômes $(U_i)_{1 \le i \le r}$ tels que :

$$F = E + \sum_{i=1}^{r} \frac{U_i}{P_i^{m_i}},$$

avec $\deg(U_i) < \deg(P_i^{m_i})$.

Lemme 4.5.2 *Si T est un polynôme irréductible unitaire et si $\deg\left(\frac{A}{T^n}\right) < 0$ (avec $n > 1$), alors il existe des polynômes $V_1, \ldots, V_n$ tels que :*

$$\frac{A}{T^n} = \sum_{k=1}^{n} \frac{V_k}{T^k}$$

avec $\deg(V_k) < \deg(T)$.

Preuve. Par récurrence sur n : pour $n = 1$ il n'y a rien à faire. Si le théorème est vrai au rang n et si $\deg\left(\frac{A}{T^{n+1}}\right) < 0$, alors on effectue la division euclidienne de A par T : $A = QT + V_{n+1}$ avec $\deg(V_{n+1}) < \deg(T)$, ce qui donne :

$$\frac{A}{T^{n+1}} = \frac{Q}{T^n} + \frac{V_{n+1}}{T^{n+1}}.$$

Il est facile de voir que $\deg\left(\frac{Q}{T^n}\right) < 0$, on peut donc appliquer l'hypothèse de récurrence, ce qui donne le résultat.

On peut appliquer ce théorème à chacune des fractions $\frac{U_i}{P_i^{m_i}}$: il existe des polynômes $V_{1,i}, \ldots, V_{m_i,i}$ tels que :

$$\frac{U_i}{P_i^{m_i}} = \sum_{j=1}^{m_i} \frac{V_{j,i}}{P_i^j},$$

avec $\deg(V_{j,i}) < \deg(P_i)$.

Ce qui donne pour F :

$$F = E + \sum_{i=1}^{r} \left(\sum_{j=1}^{m_i} \frac{V_{j,i}}{P_i^j} \right).$$

C'est une décomposition de F en éléments simples. ■

Théorème. 4.5.2.

Toute fraction rationnelle se décompose, de manière unique, comme somme de sa partie entière et d'éléments simples.

Preuve. On démontre seulement l'existence. Soit F une fraction non nulle et non polynomiale : $F = \frac{A}{B}$ (forme irréductible), on calcule sa partie entière E, on a alors :

$$F = E + \frac{R}{B}$$

avec $\deg\left(\frac{R}{B}\right) < 0$, on est alors amené à décomposer une fraction de degré strictement négatif en éléments simples.

On factorise le dénominateur B en produit de polynômes irréductibles unitaires :

$$B = \prod_{i=1}^{r} P_i^{m_i} \quad \text{(où } B \text{ est unitaire)},$$

et on applique les lemmes précédents. ■

Remarque 4.5.2 *Décomposer une fraction rationnelle F non nulle, c'est l'écrire comme somme de sa partie entière et de ses éléments simples.*

Exemples 4.5.1

— *$F = \frac{X^3}{X^2+1}$, sa partie entière est X, et on a $F = X + \frac{-X}{X^2+1}$: c'est la décomposition de F en éléments simples dans $\mathbb{R}(X)$, mais pas dans $\mathbb{C}(X)$.*

— *Dans $\mathbb{C}(X)$ on a : $F = X + \frac{-1/2}{X+i} + \frac{-1/2}{X-i}$.*

Théorème. 4.5.3.

Soit P un polynôme non nul et $P = \lambda P_1^{m_1} \times \cdots \times P_n^{m_n}$ sa décomposition en facteurs irréductibles unitaires, alors

$$\frac{P'}{P} = \sum_{i=1}^{n} m_i \frac{P_i'}{P_i}.$$

Preuve. Preuve : Découle de la propriété de la dérivée logarithmique. ■

4.5.4 Décomposition dans $\mathbb{C}(X)$

Forme de la décomposition

Soit $F = \dfrac{A}{B} \in \mathbb{C}(X)$, sous forme irréductible, soit E sa partie entière et soit

$$B = \prod_{k=1}^{r} (X - a_k)^{m_k}$$

la factorisation du dénominateur. Les complexes a_k sont les pôles de F, et les entiers $m_k > 1$ sont les multiplicités respectives.

D'après l'étude générale, la forme de la décomposition de F sera :

$$F = E + \sum_{k=1}^{r} \sum_{j=1}^{m_k} b_{j,k} \frac{1}{(X - a_k)^j}.$$

Chaque pôle de F va donc générer des éléments simples qui lui correspondent : ce sont les $b_{j,k} \dfrac{1}{(X - a_k)^j}$ pour $j \in \{1, \ldots, m_k\}$.

La somme des éléments simples relatifs au pôle a_k est appelée *partie polaire* de F relative au pôle a_k, elle est notée $PF(a_k)$.

Définition. 4.5.2. partie polaire

On a donc $PF(a_k) = \sum_{j=1}^{m_k} b_{j,k} \dfrac{1}{(X - a_k)^j}$, et la forme de la décomposition de F est :

$$F = E + PF(a_1) + \cdots + PF(a_r).$$

C'est-à-dire : partie entière plus les parties polaires relatives aux pôles de F. La décomposition dans $\mathbb{C}(X)$ consiste donc à calculer des parties polaires.

Calcul d'une partie polaire

Soit $F = \dfrac{A}{B} \in \mathbb{C}(X)$ (sous forme irréductible) et soit $a \in \mathbb{C}$ un pôle de F de multiplicité $m > 1$.

— **Cas d'un pôle simple** : on prend $m = 1$. On peut écrire $B = (X - a)Q$ avec $Q(a) \neq 0$. Comme $m = 1$, la partie polaire de F relative à a est $PF(a) = \dfrac{c}{X - a}$, en regroupant les parties polaires relatives aux autres pôles, on peut écrire :

$$F = E + \frac{c}{X - a} + \frac{U}{V}$$

avec E la partie entière et $\deg\left(\frac{U}{V}\right) < 0$. En multipliant par $X - a$, on obtient :

$$AQ = (X-a)E + c + (X-a)\frac{U}{V},$$

mais comme a n'est pas un pôle de $\frac{U}{V}$, on peut évaluer en a, ce qui donne :

$$c = \frac{A(a)}{Q(a)}.$$

Comme $B = (X-a)Q$, il est facile de voir que $Q(a) = B'(a)$, en conclusion : Si a est un pôle simple de $F = \frac{A}{B}$, alors la partie polaire de F relative à a est $PF(a) = \frac{c}{X-a}$, avec $c = \frac{A(a)}{B'(a)} = \frac{A(a)}{Q(a)}$, o Q est tel que $B = (X-a)Q$.

Exemple 4.5.1 *Soit $F = \frac{1}{X^{n-1}}$ avec $n > 1$. On a $\deg(F) < 0$, donc la partie entière est nulle. Les pôles de F sont les racines n-ièmes de l'unité : $a_k = \exp\left(\frac{2ik\pi}{n}\right)$ avec $k \in \{0, 1, \ldots, n-1\}$, et ce sont des pôles simples. La partie polaire de F relative à a_k est $c_k \frac{1}{X - a_k}$ avec $c_k = \frac{1}{n a_k^{n-1}} = \frac{a_k}{n}$. La décomposition de F est :*

$$\frac{1}{X^{n-1}} = \sum_{k=0}^{n-1} \frac{a_k}{n(X-a_k)}.$$

— **Cas d'un pôle double**

Soit $m = 2$, on peut écrire $B = (X-a)^2 Q$ avec $Q(a) \neq 0$. La partie polaire de F relative à a est

$$PF(a) = \frac{\alpha}{X-a} + \frac{\beta}{(X-a)^2},$$

en regroupant les parties polaires relatives aux autres pôles, on obtient :

$$F = E + \frac{\alpha}{X-a} + \frac{\beta}{(X-a)^2} + \frac{U}{V}$$

avec $\deg\left(\frac{U}{V}\right) < 0$.

Si on multiplie le tout par $(X-a)^2$ et que l'on évalue en a (puisque a n'est pas un pôle de $\frac{U}{V}$), on obtient

$$\beta = \frac{A(a)}{Q(a)}.$$

Pour obtenir α, on peut poser $G = F - \frac{\beta}{(X-a)^2}$, on a alors

$$G = E + \frac{\alpha}{X-a} + \frac{U}{V},$$

donc a est un pôle simple de G, ce qui nous ramène au cas précédent.

Autre méthode : On pose $H = (X-a)^2 \times F = \dfrac{A}{Q}$, on a en fait

$$H = (X-a)^2 E + \alpha(X-a) + \beta + (X-a)^2 \frac{U}{V}.$$

En évaluant en a, on trouve $\beta = H(a)$, et en évaluant la dérivée en a, on trouve $\alpha = H'(a)$. En conclusion :

Si a est un pôle double de $F = \dfrac{A}{B}$, alors la partie polaire de F relative à a est :

$$PF(a) = \frac{\alpha}{X-a} + \frac{\beta}{(X-a)^2},$$

avec $\beta = H(a)$ et $\alpha = H'(a)$, en posant $H = (X-a)^2 \times F$.

Remarque 4.5.3 *Cette deuxième méthode se généralise au cas d'un pôle a de multiplicité $m > 3$ en posant $H = (X-a)^m \times F$.*

Exemple 4.5.2 *Soit $F = \dfrac{X^6}{(X-1)^2(X^3+1)}$. La fraction est irréductible et son degré vaut 1, il y a donc une partie entière non nulle, on trouve $E = X+2$ (le dénominateur est égal à $X^5 - 2X^4 + X^3 + X^2 - 2X + 1$). La fraction possède 4 pôles :*

- *1 : c'est un pôle double, on pose $H = (X-1)^2 \times F = \dfrac{X^3}{X^3+1}$, la partie polaire relative à 1 est :*

$$PF(1) = \frac{9}{4}\frac{1}{X-1} + \frac{1}{2}\frac{1}{(X-1)^2}.$$

  Car $H(1) = \dfrac{1}{2}$ et $H'(1) = \dfrac{9}{4}$.
- *-1 : c'est un pôle simple, la partie polaire de F relative à -1 est :*

$$PF(-1) = \frac{1}{12}\frac{1}{X+1}.$$

- *$-j$: c'est un pôle simple, la partie polaire relative à $-j$ est :*

$$PF(-j) = \frac{1}{3}\frac{1}{X+j}.$$

- *$-j^2$: c'est un pôle simple, la partie polaire relative à $-j^2$ est :*

$$PF(-j^2) = \frac{1}{3}\frac{1}{X+j^2}.$$

Finalement, la décomposition de F en éléments simples dans $C(X)$ est :

$$F = X + 2 + \frac{9}{4}\frac{1}{X-1} + \frac{1}{2}\frac{1}{(X-1)^2} + \frac{1}{12}\frac{1}{X+1} + \frac{1}{3}\frac{1}{X+j} + \frac{1}{3}\frac{1}{X+j^2}.$$

Proposition. 4.5.1.

Si F est à coefficients réels, alors les parties polaires relatives aux pôles conjugués, sont conjuguées.

Preuve. Si a est un pôle complexe non réel de F de multiplicité m, alors on sait que a est un pôle de F de même multiplicité car $F \in \mathbb{R}(X)$, en regroupant les parties polaires relatives aux pôles autres que a, on obtient :

$$F = E + PF(a) + \frac{U}{V},$$

où $E \in \mathbb{R}[X]$ est la partie entière, si on conjugue l'expression, alors on obtient :

$$F = E + PF(a) + \frac{U}{V}.$$

Si on pose $PF(a) = \sum_{k=1}^{m} c_k \frac{1}{(X-a)^k}$, alors

$$PF(a) = \sum_{k=1}^{m} c_k \frac{1}{(X-a)^k},$$

et donc

$$F = E + \sum_{k=1}^{m} c_k \frac{1}{(X-a)^k} + \frac{U}{V},$$

mais a n'est pas un pôle de $\frac{U}{V}$, donc $PF(a)$ est la partie polaire de F relative à a, c'est-à-dire $PF(a) = PF(a)$. ■

Exemple 4.5.3 1. *Soit* $F = \frac{1}{(X^2+X+1)^2}$, $\deg(F) < 0$ *donc sa partie entière est nulle.* F *possède deux pôles doubles* j *et* j^2. *La partie polaire relative au pôle* j *est :*

$$PF(j) = \frac{H'(j)}{X-j} + \frac{H(j)}{(X-j)^2}$$

En posant $H = (X-j)^2 \times F = \frac{1}{(X-j^2)^2}$, *on obtient* $H(j) = -\frac{1}{3}$ *et* $H'(j) = -\frac{2i}{\sqrt{3}} \cdot \frac{9}{3}$.

F *étant à coefficients réels, la partie polaire relative à* j^2 *est la conjuguée de celle relative à* j. *La décomposition de* F *est donc :*

$$F = \frac{-1}{3(X-j)^2} - \frac{2i}{\sqrt{3}} \cdot \frac{9}{(X-j)} + \frac{-1}{3(X-j)^2} + \frac{2i}{\sqrt{3}} \cdot \frac{9}{(X-j)}.$$

2. *Soit* $F = \frac{X^4+1}{X(X^2-1)^2}$. $\deg(F) < 0$ *donc la partie entière est nulle. La fraction est irréductible, impaire, et possède un pôle simple* 0, *et deux pôles doubles* 1 *et* -1. *La forme générale de la décomposition de* F *est :*

$$F = \frac{a}{X} + \frac{b}{X-1} + \frac{c}{(X-1)^2} + \frac{d}{X+1} + \frac{e}{(X+1)^2}.$$

F *étant impaire, on a* $F(X) = -F(-X)$, *ce qui donne :*

$$F = \frac{a}{X} + \frac{b}{X+1} - \frac{c}{(X+1)^2} + \frac{d}{X-1} - \frac{e}{(X-1)^2}.$$

L'unicité de la décomposition nous donne les relations $d = b$ et $e = -c$, ce qui fait deux coefficients en moins à calculer. La partie polaire relative à 0 est $PF(0) = \frac{1}{X}$ (pôle simple). En substituant 1 à X dans $(X-1)^2 \times F$, on obtient $c = \frac{1}{2}$, et en faisant tendre x vers $+\infty$ dans la fonction rationnelle $x \mapsto xF(x)$, on obtient la relation $1 = a + b + d$, i.e., $2b = 0$, d'où $b = 0$. Finalement, la décomposition de F est :

$$F = \frac{1}{X} + \frac{1}{2(X-1)^2} - \frac{1}{2(X+1)^2}.$$

4.5.5 Décomposition dans $\mathbb{R}(X)$

Forme de la décomposition

Soit $F = \frac{A}{B} \in \mathbb{R}(X)$ (sous forme irréductible), soit E sa partie entière et soit :

$$B = \prod_{k=1}^{n} (X - a_k)^{m_k} \times \prod_{k=1}^{r} (X^2 + p_k X + q_k)^{\alpha_k}$$

la factorisation de B en produit de facteurs irréductibles unitaires ($p_k^2 - 4q_k < 0$). D'après l'étude générale, la forme de la décomposition de F est :

$$F = E + \sum_{k=1}^{n} \sum_{j=1}^{m_k} \frac{b_{j,k}}{(X-a_k)^j} + \sum_{k=1}^{r} \sum_{j=1}^{\alpha_k} \frac{c_{j,k}X + d_{j,k}}{(X^2 + p_k X + q_k)^j}.$$

La première somme est en fait la somme des parties polaires de F relatives aux pôles réels de F. Les techniques de calcul sont les mêmes dans le cas complexe. La seconde somme est la somme des éléments simples de seconde espèce.

Calcul des éléments simples de seconde espèce

On se limitera au cas où $X^2 + pX + q$ est un diviseur irréductible de B de multiplicité 1. En regroupant les autres éléments simples, on obtient :

$$F = E + \frac{aX + b}{X^2 + pX + q} + \frac{U}{V}.$$

Soient c et $\overline{c}$ les deux racines complexes (non réelles) de $X^2 + pX + q$, alors c et $\overline{c}$ ne sont pas des pôles de $\frac{U}{V}$, et c et $\overline{c}$ sont des pôles simples de F. On peut calculer la partie polaire de F relative à c dans $\mathbb{C}(X)$:

$$PF(c) = \frac{\alpha}{X - c}.$$

Comme $F \in \mathbb{R}(X)$, on a $PF(c) = \frac{\alpha}{X - c}$, la somme de ces deux parties polaires donne :

$$PF(c) + PF(\overline{c}) = \frac{2\Re(\alpha)}{X - 2\Re(\alpha c)} \cdot \frac{X^2 + pX + q}{.}$$

C'est un élément simple de $\mathbb{R}(X)$. Comme la décomposition dans $\mathbb{R}(X)$ est unique, il en résulte que :

$$\frac{aX+b}{X^2+pX+q} = \frac{2\Re(\alpha)}{X-2\Re(\alpha c)} \cdot \frac{X^2+pX+q}{.}$$

Autre méthode : soit $H = (X^2+pX+q)\cdot F$, on a :

$$H = (X^2+pX+q)\cdot E + \frac{aX+b}{X^2+pX+q} + \frac{(X^2+pX+q)\cdot U}{V}.$$

On obtient alors le système :

$$\begin{cases} H(c) = ac+b \\ H'(c) = ac+b \end{cases}$$

En résolvant, on trouve a et b.

Exemple 4.5.4 *Soit $F = \dfrac{X^4}{X^3-1}$. On a $\deg(F) = 1$, il y a donc une partie entière non nulle, celle-ci vaut X. D'autre part, on a $X^3-1 = (X-1)(X^2+X+1)$, d'où la forme de la décomposition :*

$$F = X + \frac{a}{X-1} + \frac{bX+c}{X^2+X+1}.$$

La partie polaire relative à 1 est $PF(1) = \dfrac{1}{3(X-1)}$. Dans $\mathbb{C}(X)$, la partie polaire relative à j est $PF(j) = \dfrac{j}{3(X-j)}$, et la partie polaire relative à j^2 est la conjuguée, i.e. $PF(j^2) = \dfrac{j}{3(X-j^2)}$, la somme de ces deux parties polaires donne :

$$\frac{-X+1}{3(X^2+X+1)},$$

la décomposition de F est donc :

$$F = X + \frac{1}{3(X-1)} + \frac{-X+1}{3(X^2+X+1)}.$$

Remarque 4.5.4 *En évaluant en 0, on obtient $c-a=0$, d'où $c=a=\dfrac{1}{3}$. En faisant tendre x vers $+\infty$ dans $x(F(x)-x) = \dfrac{x^2}{x^3-1}$, on obtient $a+b=0$, d'où $b=-a=-\dfrac{1}{3}$.*

4.6 Applications de la décomposition

4.6.1 Calcul de la dérivée n-ième d'une fraction

Exemple 4.6.1 *Soit $f(x) = \dfrac{1}{x^2+1}$, calculons $f^{(n)}(x)$. Dans $\mathbb{C}(X)$, on a :*

$$\frac{1}{X^2+1} = \frac{1}{2i(X-i)} - \frac{1}{2i(X+i)},$$

d'où :

$$f^{(n)}(x) = \frac{1}{2i}\left((-1)^n n! \frac{1}{(x-i)^{n+1}} - (-1)^n n! \frac{1}{(x+i)^{n+1}}\right).$$

Ce qui donne :

$$f^{(n)}(x) = (-1)^n n!\, Im\left(\frac{(x+i)^{n+1}}{(x^2+1)^{n+1}}\right) = (-1)^n n! \sum_{k=0}^{\lfloor \frac{n+1}{2} \rfloor} \binom{n+1}{2k+1} (-1)^k \frac{x^{n-2k}}{(x^2+1)^{n+1}}.$$

4.6.2 Primitives d'une fraction rationnelle

Soit $F \in \mathbb{R}(X)$, on décompose F en éléments simples dans $\mathbb{R}(X)$, on est donc ramené à calculer des primitives de trois types :

— La partie entière : c'est un polynôme.

— Les éléments simples de première espèce : $\dfrac{1}{(X-a)^n}$ avec $n > 1$, on sait les intégrer, car :

$$\int \frac{dt}{(t-a)^n} = \begin{cases} \ln(|t-a|), & \text{si } n = 1, \\ \dfrac{-1}{(n-1)(t-a)^{n-1}}, & \text{si } n > 1. \end{cases}$$

— Les éléments simples de seconde espèce :

Pour les éléments simples de seconde espèce $\dfrac{aX+b}{X^2+pX+q}$, la méthode est la suivante :

— On fait apparaître la dérivée du trinôme X^2+pX+q au numérateur et on compense les X en multipliant par un facteur adéquat, puis on compense les constantes en ajoutant ce qu'il faut, ce qui donne :

$$\frac{aX+b}{X^2+pX+q} = \frac{a}{2} \cdot \frac{2X+p}{X^2+pX+q} + \left(b - \frac{ap}{2}\right) \cdot \frac{1}{X^2+pX+q}.$$

La première de ces deux fractions est facile à intégrer (du type $\dfrac{u'}{u}$).

— Pour la deuxième fraction : on met le trinôme X^2+pX+q sous forme canonique afin de mettre la fraction sous la forme :

$$\frac{\alpha u'}{1+u^2},$$

où u est une fonction de x. Cette fraction s'intègre en $\alpha \arctan(u)$.

Exemple 4.6.2 *Calculons* $F(x) = \displaystyle\int \frac{x\,dt}{t^3+1}$ *sur* $]-1, +\infty[$ *:*

On décompose la fraction rationnelle $\dfrac{1}{X^3+1}$ *en éléments simples dans* $\mathbb{R}(X)$*, ce qui donne :*

$$\frac{1}{X^3+1} = \frac{1}{3(X+1)} - \frac{X-2}{3(X^2-X+1)}.$$

On a :

$$\frac{X-2}{X^2-X+1} = \frac{1}{2} \cdot \frac{2X-1}{X^2-X+1} - \frac{3}{2} \cdot \frac{1}{X^2-X+1},$$

et :

$$\frac{1}{X^2-X+1} = \frac{1}{(X-\frac{1}{2})^2+\frac{3}{4}} = \frac{2}{\sqrt{3}} \cdot \frac{1}{\left(\frac{2X-1}{\sqrt{3}}\right)^2+1}.$$

On en déduit alors :

$$F(x) = \frac{1}{3}\ln(x+1) - \frac{1}{6}\ln(x^2-x+1) + \frac{\sqrt{3}}{3}\arctan\left(\frac{2x-1}{\sqrt{3}}\right),$$

c'est-à-dire :

$$F(x) = \frac{1}{3}\ln\left(\frac{x+1}{\sqrt{x^2-x+1}}\right) + \frac{\sqrt{3}}{3}\arctan\left(\frac{2x-1}{\sqrt{3}}\right) + \textit{cte}.$$