Algèbre 1 - Premier semestre 2023 - 2024

Responsable CM : Nicolas Arancibia Robert
Bureau : Site St Martin, Bâtiment E, cinquième étage, Bureau 552
e-mail : nat@cy-tech.fr - nicolas.arancibia-robert@cyu.fr

Évaluation :

- **DS 1 :** Semaine du 23/10/2023 (25%)
- **DS 2 :** Semaine du 27/11/2023 (25%)
- **Examen :** Semaine du 22/01/2023 (40%)
- **Note TD :** (10%)

Modalités d'Évaluation

Vous aurez 4 notes :

- 2 contrôles continus : $DS1$ et $DS2$, durée 1h, en séance de TD,
  - Algèbre 1 : Semaines du 23 Octobre et du 27 Novembre.
  - Analyse 1 : Semaines du 13 Novembre et du 11 Décembre.
- 1 Examen de fin de semestre : E, durée 2h, semaine du 22 Janvier.
- 1 note de TD : TD, donnée par l'enseignant.

On calcule alors une moyenne (pondérée) M

$$M = 0.25 \times (DS1 + DS2) + 0.4 \times E + 0.1 \times TD$$

Votre note finale $\boldsymbol{NF}$ est le max entre la moyenne M et la note de l'examen E

$$\boldsymbol{NF} = \max(M, E).$$

Exemples

$$\text{Moyenne : } M = 0.25 \times (DS1 + DS2) + 0.4 \times E + 0.1 \times TD$$

- Exemple 1

$DS1 = 8$	$DS2 = 17$	$E = 9$	$TD = 19$

On calcule la moyenne :

$$M = 0.25 \times (8 + 17) + 0.4 \times 9 + 0.1 \times 19 = 11.75$$

La note finale est le max entre M et E donc $\boldsymbol{NF = 11.75}$

- Exemple 2

$DS1 = 15$	$DS2 = 2$	$E = 13$	$TD = 12$

On calcule la moyenne :

$$M = 0.25 \times (15 + 2) + 0.4 \times 13 + 0.1 \times 12 = 10.65$$

La note finale est le max entre M et E donc $\boldsymbol{NF = 13}$.

Rattrapage pour Absence

En cas d'absence (justifiée ou injustifiée) la note correspondante dans la formule de la moyenne sera 0.
Il y aura à la fin de semestre une épreuve de rattrapage pour les absences.

Attention ! C'est un rattrapage pour les absences uniquement, indépendante des notes que vous avez obtenues.

Si vous êtes absent.e à l'examen vous devez **obligatoirement** passer l'épreuve de rattrapage.
Si vous êtes absent.e à DS1 ou DS2 vous pouvez passer l'épreuve de rattrapage si vous le souhaitez.
$\Rightarrow$ Remarque : il y aura une unique épreuve de rattrapage qui durera 2h et portera sur l'ensemble du semestre, même si vous la passez pour une absence au DS1 ou DS2.

La note R obtenue au rattrapage remplacera le 0 dans le calcul de la note finale.

Exemples

- Exemple 1 | $DS1 = 11$ | $DS2 = 15$ | $E =$ABS | $TD = 16$ |

  Rattrapage OBLIGATOIRE. Vous obtenez $R = 12$ qui remplace E

  $$M = 0.25 \times (11 + 15) + 0.4 \times \mathbf{12} + 0.1 \times 16 = 12.9$$

  La note finale est le max entre M et $E = R = 12$ donc $\boldsymbol{NF = 12.9}$

- Exemple 2 | $DS1 = 12$ | $DS2 =$ ABS | $E = 13$ | $TD = 15$ |

  On peut calculer la moyenne :

  $$M = 0.25 \times (12 + \mathbf{0}) + 0.4 \times 13 + 0.1 \times 15 = 9.7$$

  La note finale est le max entre M et E donc a priori $\boldsymbol{NF = 13}$.
  Rattrapage optionnel. Vous décidez de passer le rattrapage et obtenez $R = 14$, on recalcule alors

  $$M' = 0.25 \times (12 + \mathbf{14}) + 0.4 \times 13 + 0.1 \times 15 = 13.2$$

  La note finale est le max entre M' et E donc $\boldsymbol{NF = 13.2}$.

Thèmes

- Logique et raisonnement
- Ensembles
- Relations binaires
- Applications
- Nombres complexes
- Polynômes
- Fractions rationnelles

Logique et raisonnement

Ce chapitre regroupe les différents points de vocabulaire, notations et raisonnement nécessaires pour la conception et la rédaction efficace d'une démonstration mathématique. Nous allons donc apprendre à bien écrire et à bien argumenter en mathématiques.

Thèmes détaillès

- Rudiments de Logique
  - Propositions.
  - Quantificateurs.
  - Implication, contraposition, équivalence.
- Modes de Raisonement
  - Contraposition
  - Par l'absurde
  - Par analyse-synthèse
  - Récurrence

Définition (Proposition)

On appelle **proposition (ou assertion)** *toute phrase P dont on peut dire si elle est* vraie (V) *ou* fausse (F).

Autrement dit, on appelle proposition toute phrase P au sujet de laquelle on peut poser la question :

$$\ll \textbf{ P est-elle vraie ? } \gg$$

Exemples :

- « $3 \times 3 = 9$ » est une proposition vraie.
- « 7 est pair » est une proposition fausse.
- « l'entier 49 est un carré » est une proposition vraie ($7^2 = 49$).
- « Les zéros non triviaux de la fonction zêta de Riemann ont tous une partie réelle égale à $1/2$ » (Hypothèse de Riemann) est une proposition dont on ne sait pas s'il est vraie ou fausse. (Conjecture)

Remarque : La plupart des phrases grammaticalement correctes sont des propositions, mais par exemple :

- « Dis-le-moi ! »,
- « Bonjour »,
- « Quelle heure est-il ? », ou
- « Comment vas-tu ? »

n'en sont pas, la question :

« Est-il vrai que bonjour ? » **n'a aucun sens.**

Rudiments de Logique

Remarque : Dans un cours de mathématiques, lorsqu'on énonce une propostion, c'est pour affirmer qu'elle est vraie, et qu'on va la démontrer.

On a plusiers types de propositions.

Définition

- *Un* **Axiome** *est une proposition qui n'est pas démontrable mais que l'on considère vraie et que ce sera l'un de nos points de départ pour faire des mathématiques.*
  Exemple : *Axiomes d'Euclide, axiomes de Péano.*
- *Un* **Théorème** *est une proposition vraie particulièrement important.*
  Exemple : *Théoreme Pythagore, Théoreme de Fermat(-Wiles).*
- *Un* **Lemme** *est une proposition vraie, utile à la démonstration d'une proposition plus important.*
  Exemple : *Lemme de Zorn, Lemme de Schwarz.*
- *Un* **Corollaire** *est une proposition vraie, conséquence immediate d'une autre proposition vraie.*
- *Une* **Conjecture** *est une proposition qu'on pense généralement vraie, sans en avoir la preuve.*
  Exemple : *Conjecture de Riemann, Conjecture de Goldbach.*

Rudiments de Logique

Remarque : Dans un cours de mathématiques, lorsqu'on énonce une propostion, c'est pour affirmer qu'elle est vraie, et qu'on va la démontrer.

On a plusiers types de propositions.

Définition

- *Un* **Axiome** *est une proposition qui n'est pas démontrable mais que l'on considère vraie et que ce sera l'un de nos points de départ pour faire des mathématiques.*
  Exemple : *Axiomes d'Euclide, axiomes de Péano.*
- *Un* **Théorème** *est une proposition vraie particulièrement important.*
  Exemple : *Théoreme Pythagore, Théoreme de Fermat(-Wiles).*
- *Un* **Lemme** *est une proposition vraie, utile à la démonstration d'une proposition plus important.*
  Exemple : *Lemme de Zorn, Lemme de Schwarz.*
- *Un* **Corollaire** *est une proposition vraie, conséquence immediate d'une autre proposition vraie.*
- *Une* **Conjecture** *est une proposition qu'on pense généralement vraie, sans en avoir la preuve.*
  Exemple : *Conjecture de Riemann, Conjecture de Goldbach.*

Théorème de Fermat-Wiles :

Il n'existe pas de nombres entiers strictement positifs x, y et z tels que :
$x^n + y^n = z^n$ pour $n \in \mathbb{N}$, $n \geq 2$

Lemme de Zorn :

si un ensemble ordonné est tel que toute chaîne (sous-ensemble totalement ordonné) possède un majorant, alors il possède un élément maximal.

Conjecture de Goldbach :

Tout nombre entier pair supérieur à 3 peut s'écrire comme la somme de deux nombres premiers.

Rudiments de Logique

Notation : Lorsque une proposition dépend d'une variable x appartenant à un ensemble E, on pourra la noter $P(x)$. L'ensemble E sera pour la plupart donné par $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, ou d'un sous-ensemble de l'un de ces ensembles.

Exemples :

- Si on pose $P(x) : x \geq 1$, alors

$$\begin{aligned} P(2) &\quad \text{est vraie} \\ P(-1) &\quad \text{est fausse.} \end{aligned}$$

- On rappelle qu'un nombre premier est un entier naturel $p \geq 2$ qui n'est divisible que par 1 et par lui même.

  Si on pose

$$P(n) : \ \ll \text{n est un nombre premier} \gg$$

  alors

$$\begin{aligned} P(7) &\quad \text{est vraie} \\ P(8) &\quad \text{est fausse} \\ P(6700417) &\quad \text{est vraie} \quad \text{(Prouvé par L. Euler (1732)).} \end{aligned}$$

Rudiments de Logique

Nous disposons de deux types d'outils pour fabriquer des nouvelles propositions :

- **les opérations sur les propositions :**
  - Équivalence ($\Longleftrightarrow$)
  - Négation (non)
  - Conjonction (et)
  - Disjonction (ou)
  - Implication ($\Longrightarrow$)

  et **les quantificateurs :**
  - Pour tout ($\forall$)
  - Existe ($\exists$)

La première opération sur les propositions que nous allons étudier est l'equivalence.

Définition (Équivalence)

Soient P et Q deux propositions. On définit la proposition P est **équivalent** *à Q, notée*

$$P \iff Q,$$

comme la proposition étant vraie si P et Q ont la même valeur de vérité, et fausse sinon.

Ce qui peut être résumé par le tableau suivant, appelé **table de vérité**

P	Q	$P \iff Q$
V	V	V
V	F	F
F	V	F
F	F	V

Vocabulaire : Lorsque P et Q sont équivalentes, on dit que

P est vraie **si et seulement si** Q est vraie.

Exemples :

- Si x est un nombre réel, les énoncés

$$\ll\ x \in [-8,5]\ \gg \qquad \text{et} \qquad \ll\ (x+8)(x-5) \leq 0\ \gg$$

  sont équivalents.

- L'affirmation

$$\ll\ x = 3 \iff x+2 = 5\ \gg$$

  est une affirmation vraie pour tout réel x.

- L'affirmation

$$\ll\ x = 1 \iff x^2 = 1\ \gg$$

  est une affirmation qui n'est pas vraie pour tout réel x.

Remarque : Deux propositions P et Q sont équivalentes si elles ont **les mêmes tables de vérités**. En comparant les tables de vérités nous pourrons donc vérifier la véracité d'une proposition.

La deuxième opération sur les propositions est la négation.

Définition (Négation)

La proposition contraire de P, notée (non P), et appelée **négation** *de P, est la proposition définie comme étant vraie lorsque P est fausse et fausse lorsque P est vrai.*

On résumé ceci par la table de vérité suivante

P	non P
V	F
F	V

Exemple :

- La négation de « mon chat est noir » est « mon chat n'est pas noir ».
- La négation de « tous les chats sont noirs » est « il existe un chat qui n'est pas noir ».
- La negation de « $x \leq 0$ » est « $x > 0$ » (et non pas « $x \geq 0$ »).
- La negation de « f est la fonction nulle » est « f n'est pas la fonction nulle » ou encore « f ne s'annule pas en au moins un point »

Exemple : La négation de « dans tous les pays, tous les musiciens sont mortels » est « il existe au moins un pays dans lequel on peut trouver au moins un musicien immortel » (et non « il existe un pays où tous les musiciens sont immortels »).

Remarque : Nous allons voir un peu plus tard que les deux propositions suivantes sont contraires l'une de l'autre

- « Quel que soit x, $P(x)$ est vraie. » et « Il existe un x tel que $P(x)$ est faux ».

La négation vérifie la propriété suivant.

Théorème (Double négation)

Pour tout proposition P, on a l'équivalence

$$P \iff \text{non (non } P).$$

Démonstration.

On écrit les tables de vérité :

P	(non P)	non (non P)
V	F	V
V	F	V
F	V	F
F	V	F

Puisque la table de vérite de P est la même que celle de « non (non P) », on conclut que les deux affirmations sont équivalents. □

Passons à étudier maintenant la conjonction et la disjonction de deux propositions.

Définition (Conjonction (et))

A deux propositions P et Q, on peut associer la **conjonction** *de P et Q, notée*

$$\ll P \text{ et } Q \gg \quad (ou\ P \wedge Q)$$

qui est

- *vraie si les deux propositions P et Q sont vraies ;*
- *fausse si l'une au moins des deux propositions P ou Q est fausse.*

On résume ceci par la table de vérité suivante

P	Q	P et Q
V	V	V
V	F	F
F	V	F
F	F	F

Exemples :

- Soit $ABCD$ un rectangle. La proposition

  « L'angle $\widehat{ABC}$ est droit et les diagonales $[AC]$ et $[BD]$ se coupent en leur milieu »

  est vraie ou fausse ? Elle est vraie. En effet

  - « L'angle $\widehat{ABC}$ est droit » est une proposition vraie.
  - « Les diagonales $[AC]$ et $[BD]$ se coupent en leur milieu » est une proposition vraie.

- Soit ABC un triangle. La proposition

  $$\ll [AB] > [AC] + [CB] \quad \text{et} \quad \widehat{ABC} + \widehat{CAB} + \widehat{BCA} = \pi \gg$$

  est vraie ou fausse ? Elle est fausse. En effet

  - « $[AB] > [AC] + [CB]$ » est une proposition fausse.
  - « $\widehat{ABC} + \widehat{CAB} + \widehat{BCA} = \pi$ » est une proposition vraie.

Définition (Disjonction (ou))

A deux propositions P et Q, on peut associer la **disjonction** *de P et Q, notée*

$$\ll P \text{ ou } Q \gg \quad (\text{ou } P \vee Q)$$

qui est

- *vraie lorsque l'une au moins des deux propositions P ou Q est vraie ;*
- *fausse si les deux propositions P et Q sont fausses.*

On résume ceci par la table de vérité suivante

P	Q	P ou Q
V	V	V
V	F	V
F	V	V
F	F	F

Exemple : Soit ABC un triangle. La proposition

$$\ll [AB] > [AC] + [CB] \quad \textbf{ou} \quad \widehat{ABC} + \widehat{CAB} + \widehat{BCA} = \pi \gg$$

est Vraie.

Remarque : On prendra garde au fait que le « ou » logique est un ou **inclusif**, contrairement au « ou » du langage courant qui lui est (en général) **exclusif**.

Distinguer :

1. le « ou » **exclusif** de la langue française : «Fromage ou Dessert».
   On ne peut pas avoir les deux.

2. le « ou » **logique ou inclusif** : «On recrute un enseignant qui sait parler l'allemand ou l'espagnol» ou «On recrute un informaticien qui sait coder en C++ ou en Python».
   On peut avoir les deux.

Étudions comme la négation modifie les conjonction et les disjonctions.

Théorème (Lois de Morgan)

Soit P et Q deux énoncés. Alors

- **Conjonction :** $\text{non } (P \text{ et } Q) \iff (\text{non } P) \text{ ou } (\text{non } Q)$.
- **Disjonction :** $\text{non } (P \text{ ou } Q) \iff (\text{non } P) \text{ et } (\text{non } Q)$.

Démonstration.

Negation d'une conjonction : On écrit les tables de vérité :

P	(non P)	Q	(non Q)	P et Q	non (P et Q)	(non P) ou (non Q)
V	F	V	F	V	F	F
V	F	F	V	F	V	V
F	V	V	F	F	V	V
F	V	F	V	F	V	V

Puisque la table de vérite de « $\text{non } (P \text{ et } Q)$ » est la même que celle de « $(\text{non } P)$ ou $(\text{non } Q)$ », on conclut que les deux affirmations sont équivalents.

Negation d'une disjonction : Même méthode, voir TD pour les détails. □

Définition (Implication)

Étant données deux propositions logiques P et Q, on définit la proposition P **implique** *Q, notée*

$$P \implies Q$$

comme la proposition étant fausse dans le seul cas où P est vraie et Q fausse. On appelle P son **antécédent** *et Q son* **conséquent**.

On résume ceci par la table de vérité suivante

P	Q	$P \implies Q$
V	V	V
V	F	F
F	V	V
F	F	V

Remarque : Contrairement à (P ou Q) et (P et Q), la table de vérité de $P \Longrightarrow Q$ n'est pas totalement intuitive. En effet, si P est fausse, alors l'implication est nécessairement vraie. C'est-à-dire

$$\ll \text{Faux implique n'importe quoi } \gg .$$

En particulier, **faux implique faux** est considéré comme vraie en mathématique. Ce choix est en fait raisonnable. Imaginons par exemple l'assertion suivante :

$P \Longrightarrow Q$: **J'ai eu une discussion avec mon chien implique mon chien parle**.

Bien entendu, cette implication est juste, mais ni

$$P : \textbf{J'ai eu une discussion avec mon chien}$$

ni

$$Q : \textbf{mon chien parle}$$

ne le sont.

Exemples :

- « n est pair » $\Longrightarrow$ « n est divisible par 2 » est une proposition vraie.
- Soient a et b deux réels. Alors
  - $a = b \Longrightarrow a^2 = b^2$ est vraie, mais
  - $a^2 = b^2 \Longrightarrow a = b$ est fausse en général. En effet

$$\underbrace{\underbrace{a^2 = (-a)^2}_{\text{Vrai}} \quad \Longrightarrow \quad \underbrace{a = -a}_{\text{Faux}}}_{\text{Faux}}$$

  - $|a| = |b| \Longrightarrow a = b$ est fausse en général. En effet

$$\underbrace{\underbrace{|a| = |-a|}_{\text{Vrai}} \quad \Longrightarrow \quad \underbrace{a = -a}_{\text{Faux}}}_{\text{Faux}}$$

Vocabulaire : Nous utiliserons souvent le vocabulaire suivant, si $P \Longrightarrow Q$ est **vraie**, nous dirons :

si P alors Q.

La assertion P est alors appelée

une **condition suffisante** de Q.

Pour que Q soit vraie, **il suffit** que P soit vraie. Autrement dit, savoir que P est vraie permet de conclure que Q est vraie. En même temps, la assertion Q est appelée

une **condition nécessaire** de P.

Pour que P soit vraie, **il faut** que Q soit vraie. Autrement dit, si Q n'est pas vraie, alors P ne peut pas être vraie.

Distinguer :

1. Pour aller visiter la Tour Eiffel,
   - Il faut que je prenne le Métro et que je marche.
     Faux : je peux prendre le bus.
   - Il suffit que je prenne le Métro et que je marche.
     Vrai
2. Pour montrer que 231 n'est pas premier
   - Il suffit que je le décompose en produit de nombres premiers.
     Vrai : $231 = 3 \times 7 \times 11$ suffit pour montrer que 231 n'est pas premier.
   - Il faut que je le décompose en produit de nombres premiers.
     Faux : je peux aussi écrire $231 = 3 \times 77$.

Définition (Réciproque, contraposée)

- *On appelle* **réciproque** *de l'implication :* $P \Longrightarrow Q$*, la proposition :*

$$Q \Longrightarrow P.$$

- *On appelle* **contraposée** *de l'implication :* $P \Longrightarrow Q$*, la proposition :*

$$(non\ Q) \Longrightarrow (non\ P).$$

Exemple : Considérons la proposition

P : La nuit, tous les chats sont gris

- Sa réciproque est : Si tous les chats sont gris, alors il fait nuit.
- Sa contraposée est : Si au moins un chat n'est pas gris, alors il fait jour.

Remarque : Si une implication est vraie, sa réciproque n'est pas forcément vraie.

Par contre toute implication est équivalente à sa contraposée.

Théorème

Soit P et Q deux propositions. Alors

$$\Big(P \Longrightarrow Q\Big) \iff \Big((\text{non } Q) \implies (\text{non } P)\Big).$$

Démonstration.

On écrit la table de vérité de la proposition $(\text{non } Q) \Longrightarrow (\text{non } P)$.

P	$(\text{non } P)$	Q	$(\text{non } Q)$	$(\text{non } Q) \Longrightarrow (\text{non } P)$	$P \Longrightarrow Q$
V	F	V	F	V	V
V	F	F	V	F	F
F	V	V	F	V	V
F	V	F	V	V	V

On retrouve la même table de vérité que la proposition « $P \Longrightarrow Q$ ». La proposition « $P \implies Q$ » et la proposition « $\text{non } Q \Longrightarrow \text{non } P$ » sont donc équivalentes. □

L'implication nous offre une autre manière d'exprimer une equivalence : Toute équivalence est une double implication.

Théorème (Équivalence et double implication)

Soit P et Q deux propositions. Alors

$$(P \iff Q) \iff (P \implies Q) \text{ et } (Q \implies P)$$

Démonstration.

On écrit la table de vérité de la proposition $(P \implies Q)$ et $(Q \implies P)$.

P	Q	$P \implies Q$	$Q \implies P$	$(P \implies Q)$ et $(Q \implies P)$	$P \iff Q$
V	V	V	V	V	V
V	F	F	V	F	F
F	V	V	F	F	F
F	F	V	V	V	V

On retrouve la même table de vérité que la proposition « $P \iff Q$ ». Les deux propositions sont donc équivalentes. □

Remarque - Vocabulaire : Nous avons vu que, si $P \implies Q$ est vraie, alors l'assertion P est appelée

une **condition suffisante** de Q

et la assertion Q est appelée

une **condition nécessaire** de P.

Dans le cas où $P \iff Q$, nous avons à la fois

$$P \implies Q \quad \text{et} \quad Q \implies P.$$

Autrement dit, nous pouvons dire que P est une condition **nécessaire et suffisante de** Q. Ou encore que pour que Q soit vraie, **il faut et il suffit** que P soit vraie.

La proposition suivant nous donne une autre carectérisation de l'implication et nous indique comme l'implication est modifiée par la négation.

Proposition

Soit P et Q deux propositions. Alors

$$(P \Longrightarrow Q) \iff (\text{non } P) \text{ ou } Q,$$

De plus par négation, on obtient

$$\text{non } (P \Longrightarrow Q) \iff P \text{ et } (\text{non } Q).$$

Démonstration.

Voir TD pour les détails. □

Quantificateurs

Un autre outil pour définir des nouvelles propositions est la notion de quantificateur.

Définition (Quantificateur universel $\forall$)

*Le symbole $\forall$ placé devant une variable x signifie « **pour tout** x », « **quelque soit** x ». Ainsi la proposition :*

$$\forall x \in E,\ P(x),$$

se lit

Pour tout x appartenant à l'ensemble E on a $P(x)$.

La proposition : $\forall x \in E$, $P(x)$ est donc

- **vraie** *si tout objet dans E a la propriété P, et*
- **fausse** *sinon, c'est-à-dire si au moins un objet dans E n'a pas la propriété P.*

Quantificateurs

Exemples :

- $\forall x \in \mathbb{R},\ x^2 \neq -1$ est une proposition vraie, car le carré d'un réel est toujours positif.
- $\forall x \in \mathbb{R}, \sin x \leq 1$ est une proposition vraie.
- $\forall x \in \mathbb{R},\ (x-1)(x-3) \geq 0$, est une proposition fausse, puisque, par exemple, pour $x = 2$, on a $(x-1)(x-3) < 0$.

Définition (Quantificateur existentiel $\exists$)

*Le symbole $\exists$ placé devant une variable x signifie « **il existe (au moins) un** x ».*
La proposition

$$\exists x \in E,\ P(x)$$

se lit donc

Il existe un élément x de E tel que $P(x)$.

La proposition : $\exists x \in E,\ P(x)$ est donc

- **vraie** *si au moins un objet dans E a la propriété P, et*
- **fausse** *sinon, c'est-à-dire si aucun objet dans E a la propriété P.*

Finalement, Le symbole $\exists!$ placé devant une variable x signifie

il existe un unique x.

Quantificateurs

Exemples :

- « $\exists z \in \mathbb{C},\ z^2 = -1$ » est une proposition vraie car par example $i^2 = -1$.
- $\exists x \in \mathbb{R},\ (x-1)(x-3) \geq 0$, est une proposition vraie, puisque pour $x = 4$, l'inégalité est vérifiée.
- « $\forall r \in \mathbb{Q},\ \exists p \in \mathbb{N},\ pr \in \mathbb{Z}$ » est une proposition vraie.
- « $\exists n \in \{2, 3, 4, \cdots\},\ n \neq 23$ et $(23/n) \in \mathbb{N}$ » est une proposition fausse.
- « $\exists! n \in \mathbb{N},\ 1 \leq 2n \leq 3$ » est une proposition vraie. En effet 1 est le seul entier satisfaisant la proposition.

Quantificateurs

Remarque : L'ordre des quantificateurs est important. Il permet notamment de déterminer quelles variables « **peuvent dépendre des autres** ».

On peut le constater en comparant par exemple les propositions :

- $\forall x \in \mathbb{R},\ \exists y \in \mathbb{R}_+,\ x^2 = y$, est une proposition vraie, car le carré de tout nombre réel est un réel positif.

- $\exists y \in \mathbb{R}_+,\ \forall x \in \mathbb{R},\ x^2 = y$, est une proposition fausse. En effet, s'il existait un réel y vérifiant $\forall x \in \mathbb{R},\ x^2 = y$ alors on pourrait appliquer cette affirmation avec

  $$x = 0 \quad \text{et} \quad x = 1,$$

  et on obtiendrait

  $$0^2 = 1^2,$$

  ce qui est impossible.

Théorème (Négation des quantificateurs)

- *La négation de :* $\forall x \in E, P(x)$ *est*

$$\exists x \in E, \ \textit{non}\ P(x).$$

- *La négation de :* $\exists x \in E, \ P(x)$ *est*

$$\forall x \in E, \ \textit{non}\ P(x).$$

Remarque : C'est-à dire, pour nier une proposition contenant des quantificateurs, on change les $\forall$ en $\exists$ et réciproquement, puis on nie la conclusion. La négation de

$$\forall x, \exists y, \ P(x, y)$$

est

$$\exists x, \ \forall y, \ \text{non}\ P(x, y).$$

Exemples : Écrire les négation des propositions suivantes :

- $\forall x \in \mathbb{R},\ \sin x^2 + \cos x^2 = 1.$

  Solution : $\exists x \in \mathbb{R},\ \sin x^2 + \cos x^2 \neq 1.$

- $\exists x \in \mathbb{R},\ x^2 + x - 2 = 0.$

  Solution : $\forall x \in \mathbb{R},\ x^2 + x - 2 \neq 0.$

- $\exists M \in \mathbb{R}^+, \forall x \in \mathbb{R}, f(x) \leq M.$

  Solution : $\forall M \in \mathbb{R}^+, \exists x \in \mathbb{R}, f(x) > M$

Écriture : Mentionnons que, l'usage des symboles $\exists$ et $\forall$ est restreint aux assertions mathématiques. Ces symboles sont des quantificateurs, ils n'ont leur place qu'à l'intérieur d'une assertion. Dans une phrase en français, nous préférerons l'usage de **pour tout** et **il existe**. De même, nous n'utiliserons pas $\Longrightarrow$ mais les termes **alors** ou **donc**.

Modes de raisonnement

Nous avons introduis la notion de proposition et donné une liste d'outils pour, à partir de propositions simples, construire des propositions plus complexes. Mais il demeure une question important, comme on fait pour vérifier la véracité d'une proposition ? Pour cela nous allons à présent :

- Introduire différents modes de raisonnement que vont nous permettre de montrer ou, au moins, de rendre plus facile la preuve de une assertion.

Modes de raisonnement : Implication

Pour montrer une **implication :**

$$P \implies Q,$$

plusieurs types de raisonnement peuvent être mis en oeuvre, donnons trois :

• **Raisonnement direct :** On montre que si la proposition P est vraie alors la proposition Q est vraie. Quand on procède ainsi pour montrer que $P \implies Q$, on écrit **sans réfléchir :**

Supposons P vraie. Montrons que Q est vraie.

$\left.\begin{array}{l}\vdots\\ \end{array}\right\}$ Preuve de Q.

Modes de raisonnement : Implication

Exemple : Montrer que si n est un entier pair, alors n^2 est pair.

Preuve : Soit $n \in \mathbb{N}$. On suppose que n est un entier pair. Montrons que n^2 est pair. Comme n est un entier pair, il existe $k \in \mathbb{N}$ tel que

$$n = 2k.$$

Donc

$$n^2 \ = \ 4k^2 = \ 2(2k^2).$$

C'est-à-dire n^2 est pair.

Modes de raisonnement : Implication

• **Raisonnement par contraposition :** (non Q) $\Longrightarrow$ (non P). Rappelons que si la proposition

$$(\text{non } Q) \Longrightarrow (\text{non } P) \quad \text{est vraie,}$$

alors la proposition

$$P \Longrightarrow Q \quad \text{est vraie.}$$

C'est-à-dire, pour montrer $P \Longrightarrow Q$ il suffit de montrer

$$(\text{non } Q) \Longrightarrow (\text{non } P).$$

Pour cela on écrit sans réfléchir :

Supposons (non Q) vraie. Montrons que (non P) est vraie.

$$\left.\begin{array}{l} \vdots \\ \end{array}\right\} \text{Preuve de (non}P\text{).}$$

Modes de raisonnnement : Implication

Exemple : Montrer par un raisonnement par contraposition que, si n^2 est pair, alors n est pair.

Preuve : Nous devons montrer la proposition

si n n'est pas pair, alors n^2 n'est pas pair.

C'est-à-dire, nous devons montrer la proposition

si n est impair, alors n^2 est impair.

Comme n est un entier impair, il existe $k \in \mathbb{Z}$ tel que

$$n = 2k + 1.$$

Donc

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

C'est-à-dire n^2 est impair.

Modes de raisonnement : Implication

• Un type de raisonnement qui va se montrer très utile dans la suite est le **raisonnement par l'absurde.** Pour pouvoir l'introduire, appelons d'abord **contradiction** toute proposition de la forme :

$$Q \text{ et } (\text{non } Q).$$

Le principe du raisonnement par l'absurde s'énonce alors ainsi :

Si d'une proposition on arrive à tirer une contradiction, c'est qu'elle est FAUSSE.

Donc, quand on veut montrer qu'une proposition P est vraie, on peut raisonner par l'absurde de la manière suivante :

Faisons l'hypothèse que P est **fausse**(ou que (non P) est **vraie**).

$$\left.\begin{array}{c}\vdots\\ \\ \end{array}\right\} \text{Obtention d'une contradiction.}$$

Si on obtient une contradiction, c'est donc parce que l'hypothèse de départ était fausse. Par conséquent P est vraie.

Exemple : **On sait que π est irrationnel**. Montrer que « $\frac{\pi}{3}$ est irrationnel. »

Preuve : Supposons par l'absurde que $\frac{\pi}{3}$ est rationnel. Ecrivons-le donc sous forme

$$\frac{\pi}{3} = \frac{p}{q}$$

avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$. Ainsi

$$\pi = \frac{3p}{q}.$$

Par conséquent, π est rationnel. C'est absurde donc « $\frac{\pi}{3}$ est irrationnel ».

Modes de raisonnement : Implication

Exemple :Montrer que $\sqrt{2}$ est irrationnel.

Preuve : Supposons par l'absurde que $\sqrt{2}$ est rationnel et écrivons-le donc sous forme **irréductible** :

$$\sqrt{2} = \frac{p}{q}$$

avec $p, q \in \mathbb{N}^\times$ et p et q premiers entre eux (n'ont pas de diviseur commun). L'égalité :

$$p^2 = (\sqrt{2}q)^2 = 2q^2$$

montre que p^2 est pair, et donc que p est pair d'après l'exemple précedent. Ainsi

$$p = 2p', \quad \text{pour un certain } p' \in \mathbb{Z}.$$

Par conséquent

$$q^2 = \left(\frac{p}{\sqrt{2}}\right)^2 = \left(\frac{2p'}{\sqrt{2}}\right)^2 = \frac{4(p')^2}{2} = 2(p')^2.$$

Ceci montre que q^2 est pair et donc que q est pair. Disons

$$q = 2q', \text{ pour un certain } q' \in \mathbb{Z}.$$

Modes de raisonnement : Implication

Nous avions supposé la fraction $\frac{p}{q}$ irréductible, mais finalement nous l'avons réduite

$$\frac{p}{q} = \frac{2p'}{2q'} = \frac{p'}{q'}.$$

Contradiction ! Donc la hypothèse de depart est fausse. Comme voulu, $\sqrt{2}$ est irrationnel.

Modes de raisonnement

Remarque : Le raisonnement par l'absurde nous donne une autre façon de montrer l'implication

$$P \Longrightarrow Q.$$

En effet, comme $P \Longrightarrow Q$ est équivalent à la proposition

$$\text{(non P) ou Q,}$$

on en déduit que si la proposition

$$\text{P et (non Q)} \quad \Big(= \text{non } \Big(\text{(non P) ou Q}\Big)\Big)$$

conduit à une contradiction, alors $P \Longrightarrow Q$ est vraie.

Modes de raisonnement : Implication

Exercice : Démontrer, en raisonnant par l'absurde, que si $n \in \mathbb{N}^{\times}$, alors $n^2 + 1$ n'est pas le carré d'un entier naturel.

Indication : Supposer que n est un **entier positif strictement positif** et que $n^2 + 1$ est le **carré d'un entier naturel** a. Trouver une contradiction.

Modes de raisonnement : Équivalence

Pour montrer une **équivalence :**

$$P \iff Q,$$

deux stratégies sont possibles :

- **Double Implication :** Soit on raisonne par double implication et on montre séparément les propositions

$$P \implies Q \quad \text{et} \quad Q \implies P.$$

C'est-à-dire, on écrit

Supposons P vraie. Montrons que Q est vraie.

$$\left.\begin{array}{c}\vdots\end{array}\right\} \text{Preuve de } Q.$$

Réciproquement

Supposons Q vraie. Montrons que P est vraie.

$$\left.\begin{array}{c}\vdots\end{array}\right\} \text{Preuve de } P.$$

Modes de raisonnement : Équivalence

Exemple : On a vu que :

- Si n est un entier pair, alors n^2 est pair.
- Si n^2 est pair, alors n est pair.

Donc n est pair **si et seulement si** n^2 est pair.

Modes de raisonnement : Équivalence

Exemple : Montrer que

$$\forall x,\ y \in \mathbb{R}, \quad x^2 + y^2 = 0 \Longleftrightarrow x = y = 0.$$

Preuve : Soient $x, y \in \mathbb{R}$. L'implication

$$x^2 + y^2 = 0 \ \Longleftarrow \ x = y = 0$$

est triviale, car si $x = y = 0$ alors

$$x^2 = y^2 = 0 \quad \text{et donc} \quad x^2 + y^2 = 0.$$

Pour la implication réciproque,

$$x^2 + y^2 = 0 \Longrightarrow x = y = 0;$$

si $x^2 + y^2 = 0$, alors :

$$\underset{\geq 0}{x^2} = \underset{\leq 0}{-y^2},$$

donc

$$x^2 = -y^2 = 0$$

et enfin : $x = y = 0$.

Modes de raisonnement : Équivalence

• **De manière directe** : Soit on raisonne directement par équivalence en changeant peu à peu P en Q :

$$P \iff \cdots \iff \cdots \iff Q.$$

Attention :

- Cette stratégie n'est pas toujours disponible et lorsqu'elle est utilisable il faut le faire avec précaution. En effet, dans une chaîne d'équivalences, **toute l'information doit être préservée d'une étape à l'autre**, il faut donc le faire soigneusement.
- Dans la plupart de case c'est mieux de montrer des implications plutôt que des équivalences. Le raisonnement par équivalence est souvent inutile et générateur d'erreurs logiques.

Modes de raisonnement : Équivalence

Remarque : Le raisonnement par équivalence permet de montrer qu'une proposition est vraie en montrant qu'elle est équivalente à une proposition dont on sait déjà qu'elle est vraie.

Donnos un exemple de cette dernière remarque.

Exemple : Montrer que pour tout $(x, y) \in \mathbb{R}^2$, $xy \leq \frac{1}{2}(x^2 + y^2)$.

Preuve : Soit $(x, y) \in \mathbb{R}^2$, on a

$$\begin{aligned} xy \leq \frac{1}{2}(x^2 + y^2) &\iff 2xy \leq x^2 + y^2 \\ &\iff 0 \leq x^2 - 2xy + y^2 \\ &\iff 0 \leq (x - y)^2. \end{aligned}$$

La dernière proposition étant vraie, la première l'est également.

Modes de raisonnement : Quantificateur universel $\forall$

Pour démontrer qu'une propriété

$$\forall x \in E,\ P(x) \quad \text{est vraie,}$$

on doit étudier les différentes situations selon les valeurs de x. On procède toujours comme suit : on écrit **sans réfléchir** :

$$\left.\begin{array}{l} \text{Soit } x \in E. \text{ Montrons que } P(x) \\ \vdots \end{array}\right\} \text{ Preuve de } P(x).$$

Exemple : Montrer que $\forall x \in \mathbb{R},\ \frac{x}{1+x^2} \leq \frac{1}{2}$.

Preuve : Soit $x \in \mathbb{R}$. Montrons que $\frac{x}{1+x^2} \leq \frac{1}{2}$. On a

$$0 \leq (x-1)^2 = x^2 - 2x + 1.$$

Donc

$$2x \leq x^2 + 1 \quad \Longrightarrow \quad \frac{2x}{x^2+1} \leq 1 \quad \Longrightarrow \quad \frac{x}{x^2+1} \leq \frac{1}{2}.$$

Modes de raisonnement : Quantificateur universel $\forall$

Remarque : Pour montrer qu'une assertion du type

$$\forall x \in E, \quad P(x),$$

est **fausse**, on peut donner un **contre-exemple**, c'est-à-dire un exemple de x pour lequel $P(x)$ n'est pas vérifiée.

Modes de raisonnement : Quantificateur universel $\exists$

Quand on veut montrer que

$$\exists x \in E,\ P(x)$$

et qu'on a déjà en tête un exemple d'objet $x \in E$ qui a la propriété P, on écrit **sans réfléchir** :

$$\text{Posons } x = \cdots \quad \text{(l'exemple qu'on a en tête.)}$$

Vérifions que $P(x)$.

$$\left.\begin{array}{l} \vdots \\ \end{array}\right\} \text{Vérifications que } x \text{ satisfait } P(x).$$

Exemple : Montrer que $\forall x \in \mathbb{R},\ \forall y \in \mathbb{R}, \exists z \in \mathbb{R},\ z > x + y$.

Preuve : Soient $x \in \mathbb{R},\ y \in \mathbb{R}$. Après réflexion, posons :

$$z = x + y + 1.$$

Alors comme voulu : $z > x + y$.

Modes de raisonnement : Quantificateur universel $\exists$

La difficulté, bien sûr, ne consiste souvent pas à vérifier que x a la propriété P, mais **à avoir l'idée d'un exemple de tel objet x.** Il n'existe hélas pas de règle générale pour avoir des idées. Donnons tout de même une méthode qui peut s'avérer utile pour trouver x.

Pour déterminer les solutions d'un problème, ou plus précisément l'ensemble des éléments d'un ensemble E qui satisfont une propriété P, on raisonne souvent par **analyse-synthèse**.

Modes de raisonnement : Analyse - Synthèse

- **Analyse** : On suppose que le problème est résolu et on en déduit des conditions nécessaires que la solution doit satisfaire. Pour cela on écrit : Soit $x \in E$. Faisons l'hypothèse que $P(x)$ est vraie.

  $\left.\begin{array}{c}\vdots\\ \\ \end{array}\right\}$ On part naïvement d'un élément x de propriété P et on essaie de le faire parler pour savoir qui il est. **Quelles sont les possible valeurs de x ?**

- **Synthèse** : On montre que ces conditions obtenues sont suffisantes, et on résout le problème. Pour cela, on pose

  $x = \cdots$ **Ici, les possibles valeurs de x trouvées dans l'analyse.**

  On doit vérifier que $x \in E$ et que $P(x)$ est vraie :

  $\left.\begin{array}{c}\vdots\\ \\ \end{array}\right\}$ **Vérification que x appartient à E et satisfait la propriété P.**

Modes de raisonnement : Analyse - Synthèse

En Résumé :

- Dans l'analyse, on restraint le nombre des solutions possibles.
- Dans la synthèse, on vérifie que les possibilités obtenues dans l'analyse sont en fait des solutions.

Modes de raisonnement : Analyse - Synthèse

Exemple : Déterminer les solutions réelles de l'équation

$$\sqrt{x+6} = x.$$

Solution :

- **Analyse** : Supposons que x est solution de cette équation. Alors

$$\sqrt{x+6} = x \implies x+6 = x^2 \implies x^2 - x - 6 = 0.$$

Donc

$$x = 3 \quad \text{ou} \quad x = -2.$$

Nous avons ainsi montré que si x est solution de $\sqrt{x+6} = x$, alors nécessairement $x = 3$ ou $x = -2$.

- **Synthèse** : On teste à présent les valeurs obtenues : -2 ne convient pas puisque

$$\sqrt{-2+6} = 2 \neq -2,$$

mais 3 convient car on a bien

$$\sqrt{3+6} = 3.$$

Nous avons ainsi montré que l'équation $\sqrt{x+6} = x$ admet une unique solution $x = 3$.

Raisonnement par récurrence

On connait très bien

$$\mathbb{N} = \{0,\ 1,\ 2,\ 3,\ \cdots\}$$

l'addition, la multiplication sur $\mathbb{N}$, ainsi que les relations

$$<,\ \leq \ \text{et} \ \geq .$$

Dans cette section on s'interesse a une autre propriété de l'ensemble $\mathbb{N}$, qui est essentielle : **toute partie non vide A de l'ensemble $\mathbb{N}$ a un plus petit élément m.** Ceci signifie :

- d'une part que m est un élément de $A \subset \mathbb{N}$,
- d'autre part que m est inférieur ou égal à tout élément de A, c'est à dire

$$\forall x \in A, \quad m \leq x.$$

Cette propriété est la base du **Raisonnement par Récurrence**.

Raisonnement par récurrence

Proposition (Récurrence Simple)

On considère une propriété $\mathscr{P}(n)$ dépendant de l'entier $n \in \mathbb{N}$, et on suppose que :

- **Initialisation** *: $\mathscr{P}(0)$ est vraie,*
- **Hérédité** *: pour tout $n \in \mathbb{N}$, si $\mathscr{P}(n)$ est vraie, alors $\mathscr{P}(n+1)$ est vraie.*

Alors la propriété $\mathscr{P}(n)$ est vraie pour tout $n \in \mathbb{N}$.

Remarque : L'initialisation peut commencer à un entier $k_0 \in \mathbb{N}$ arbitraire (pas necessairement 0) et dans ce cas la propriété n'est démontrée vraie qu'à partir du rang k_0 : Si

- $\mathscr{P}(k_0)$ est vraie,
- Pour tout entier n supérieur ou égal à k_0, $\mathscr{P}(n)$ est vraie, alors $\mathscr{P}(n+1)$ est vraie.

Alors la propriété $\mathscr{P}(n)$ est vraie pour tout entier supérieur ou égal à k_0.

Démonstration.

Soit

$$A = \{n \in \mathbb{N} : \mathscr{P}(n) \text{ est vraie}\}.$$

Pour montrer que $A = \mathbb{N}$, on raisonne par l'absurde. Supposons donc $A \neq \mathbb{N}$, dans ce cas, le complémentaire A^c de la partie A dans $\mathbb{N}$ est non vide. Elle admet donc un plus petit élément que l'on note p. Puisque $0 \in A$, on a

$$p \geq 1.$$

De plus, comme p est le plus petit élémént de A^c, on déduit que

$$p - 1 \geq 0$$

ne peut appartenir au complémentaire de A. On a donc $p - 1 \in A$. Ainsi $\mathscr{P}(p-1)$ est vraie, ce qui implique que $\mathscr{P}(p)$ est vraie, et donc que p appartient à A. Finalement,

$$p \in A \quad \text{et} \quad p \in A^c.$$

Contradiction ! ! Par conséquent, $A = \mathbb{N}$, est la proposition est vraie pour tout $n \in \mathbb{N}$. □

Raisonnement par récurrence

Quand on veut montrer par récurrence que

$$\forall n \in \mathbb{N},\ \mathscr{P}(n),$$

on rédige ainsi :

- **Initialisation :** Vérification que $\mathscr{P}(0)$ est vraie (où plus généralement $\mathscr{P}(k_0)$ si l'initialisation commence à k_0).
- **Hérédité :** Soit $n \in \mathbb{N}$. Supposons $\mathscr{P}(n)$ vraie. Montrons que $\mathscr{P}(n+1)$ est vraie :

$$\left.\begin{array}{l} \vdots \\ \end{array}\right\} \text{Preuve que } \mathscr{P}(n+1) \text{ est vraie.}$$

Raisonnement par récurrence

Exemple : Montrer que pour tout entier naturel n, $2^n > n$.

Initialisation : On a $2^0 = 1 > 0$, donc $\mathscr{P}(0)$ est vraie.

Hérédité : Soit $n \in \mathbb{N}$. Supposons $\mathscr{P}(n)$ vraie, c'est-à-dire,

$$2^n > n.$$

Montrons que $2^{n+1} > n+1$ est vraie. On a

$$2^{n+1} = 2 \cdot 2^n = 2^n + 2^n.$$

Ainsi, par hypothèse de récurrence, on en déduit

$$2^{n+1} = 2^n + 2^n > n + 2^n.$$

Maintenant, pour tout $n \in \mathbb{N}$ on a

$$2^n \geq 1.$$

Par conséquent

$$2^{n+1} > n + 2^n \geq n + 1.$$

C'est-à-dire $2^{n+1} > n+1$. Fin de la récurrence. Par conséquent pour tout entier naturel n, $2^n > n$.

Raisonnement par récurrence

Exemple : Montrer que pour tout entier naturel n, $3^n - 1$ est pair.

Initialisation : On a $3^0 - 1 = 1 - 1 = 0$, donc $\mathscr{P}(0)$ est vraie.

Hérédité : Soit $n \in \mathbb{N}$. Supposons $\mathscr{P}(n)$ vraie, c'est-à-dire

$$\begin{aligned} 3^n - 1 \text{ est pair} \quad &\Longrightarrow \quad 3^n - 1 = 2k, \quad k \in \mathbb{Z} \\ &\Longrightarrow \quad 3^n = 2k + 1. \end{aligned}$$

Montrons que $3^{n+1} - 1$ est pair. On a

$$3^{n+1} - 1 = 3 \cdot 3^n - 1 = 3(2k + 1) - 1 = 6k + 3 - 1 = 2(3k + 1).$$

C'est-à-dire $3^{n+1} - 1$ est pair. Fin de la recurrence. Par conséquent, pour tout entier naturel n, $3^n - 1$ est pair.

Raisonnement par récurrence

Il arrive parfois qu'on ne sache pas déduire $\mathscr{P}(n+1)$ de $\mathscr{P}(n)$, mais

$$\textbf{seulement} \quad \mathscr{P}(n+2) \quad \textit{de} \quad \mathscr{P}(n) \quad \textbf{et} \quad \mathscr{P}(n+1).$$

Le principe du raisonnement par récurrence prend dans ce cas la forme suivante.

Proposition (Récurrence Double)

On considère une propriété $\mathscr{P}(n)$ dépendant de l'entier $n \in \mathbb{N}$, et on suppose que :

- *$\mathscr{P}(0)$ et $\mathscr{P}(1)$ sont vrais,*
- *pour tout $n \in \mathbb{N}$, si $\mathscr{P}(n)$ et $\mathscr{P}(n+1)$ sont vrais, alors $\mathscr{P}(n+2)$ est vraie.*

Alors la propriété $\mathscr{P}(n)$ est vraie pour tout $n \in \mathbb{N}$.

Remarque : Les récurrences classiques sont dites simples et il existe bien entendu des récurrences triples, etc.

Raisonnement par récurrence

Quand on veut montrer par récurrence **double** que

$$\forall n \in \mathbb{N},\ \mathscr{P}(n),$$

on rédige ainsi :

- **Initialisation :** Vérification que $\mathscr{P}(0)$ et $\mathscr{P}(1)$ sont vrais.
- **Hérédité :** Soit $n \in \mathbb{N}$. Supposons $\mathscr{P}(n)$ et $\mathscr{P}(n+1)$ sont vrais.Montrons que $\mathscr{P}(n+2)$ est vraie.

$$\left.\begin{array}{l} \vdots \\ \end{array}\right\} \text{Preuve que } \mathscr{P}(n+2) \text{ est vraie.}$$

Théorème (Récurrence forte)

On considère une propriété $\mathscr{P}(n)$ dépendant de l'entier $n \in \mathbb{N}$, et on suppose que :

- *$\mathscr{P}(0)$ est vraie,*
- *pour tout $n \in \mathbb{N}$, si $\mathscr{P}(k)$ est vraie pour $k \leq n$, alors $\mathscr{P}(n+1)$ est vraie.*

Alors la propriété $\mathscr{P}(n)$ est vraie pour tout $n \in \mathbb{N}$.

Exemple : Montrer que tout entier $n \geq 2$ se décompose en produit de nombres premiers.

Ensembles

- Introduction à la théorie des ensembles :
  - Définition et exemples.
  - Inclusion, Égalité.
  - Ensemble des parties
- Opération sur les ensembles :
  - Intersection, Union.
  - Différence, Complémentaire.
  - Partition d'un ensemble.
  - Produit Cartésien.

Ensembles

Définition (Ensemble)

Un **ensemble** *E est une* **collection** *ou un groupement d'objets distincts. Les objets x de E s'appellent* **les éléments** *de E.*

- *Si E est un ensemble et si x est un élément de E, on dit que x* **appartient** *à E ou que x est dans E et on écrit*

$$x \in E.$$

- *Dans le cas contraire, si x n'est pas un élément de E, on dit que x* **n'appartient pas** *à E ou que x n'est pas dans E et on écrit*

$$x \notin E.$$

Remarque :

- Il existe un unique ensemble ne contenant aucun élément. C'est **l'ensemble vide** noté $\emptyset$.
- Un ensemble qui ne contient qu'un seul élément est appelé **singleton**.

Ensembles

Pour définir un ensemble, on peut le décrire :

- **Par extension** : en donnant la liste complète explicite de tous ses éléments. On note cette liste entre accolades, l'ordre des éléments listés n'ayant aucune importance.

  Exemple :

  - $\{1\}$, $\{1,4\}$, $\{1,4,9\}$ et

    $$\{1,4,9,11\} = \{9,4,11,1\}.$$

  - $2\mathbb{N} = \{0,2,4,\cdots\}$: L'ensemble des entiers naturels pairs.
  - $2\mathbb{N}+1 = \{1,3,5,\cdots\}$: L'ensemble des entiers naturels impairs.

- **Par compréhension** : en donnant une propriété P que ses éléments vérifient et sont seuls à vérifier. On note

$$\{x \in E \ : \ P(x)\} \quad \text{ou} \quad \{x \in E \mid P(x)\}$$

l'ensemble des éléments de E qui vérifient P.

Exemple :

- $2\mathbb{N} = \{n \in \mathbb{N} : \exists k \in \mathbb{N}, n = 2k\}$: L'ensemble des entiers naturels pairs.
- $2\mathbb{N} + 1 = \{n \in \mathbb{N} : \exists k \in \mathbb{N}, n = 2k + 1\}$: L'ensemble des entiers naturels impairs.
- $\mathbb{Q} = \left\{ x \in \mathbb{R} : \exists p \in \mathbb{Z}, \exists q \in \mathbb{N}^*, x = \frac{p}{q} \right\}$: L'ensemble des rationnels.
- $[a, b[= \{x \in \mathbb{R} \ : \ a \leq x < b\}$: l'intervalle semi-ouverte à droite.

Définition (Inclusion)

Soient E et F deux ensembles. On dit que E est **inclus** *dans F , ou que F contient E, ou que E est une partie de F, ce qu'on note*

$$E \subset F$$

si tout élément de E est élément de F, c'est-à-dire

$$\forall x, \quad (x \in E \implies x \in F).$$

Exemple :

- On a la suite d'inclusions
$$\{1\} \subset \{1,4\} \subset \{1,4,9\} \subset \{1,4,9,11\}.$$
- On a
$$2\mathbb{N} \subset \mathbb{N} \quad \text{et} \quad 2\mathbb{N}+1 \subset \mathbb{N}.$$
- On a la suite d'inclusions
$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$
- On a
$$[a,b[\quad \subset \quad \mathbb{R}.$$

Ensembles

Attention ! : Ne pas confondre appartenance et inclusion.

- On a bien
$$0 \in \mathbb{N}$$
mais
$$0 \notin \mathbb{N}.$$
Néanmoins
$$\{0\} \subset \mathbb{N}.$$
Un élément appartient à un ensemble.
Par rapport à $\mathbb{N}$, 0 est donc une bille dans un sac et non un sac dans un sac.

- On a bien
$$\mathbb{N} \subset \mathbb{Z}$$
mais
$$\mathbb{N} \notin \mathbb{Z}.$$
Un ensemble est contenu dans un ensemble.
Par rapport à $\mathbb{Z}$, $\mathbb{N}$ est donc un sac dans un sac et non une bille dans un sac.

Ensembles

Quand on veut montrer une inclusion :

$$E \subset F,$$

on écrit **sans réfléchir :**

$$\left.\begin{array}{l} \text{Soit } x \in E. \text{ Montrons que } x \in F \text{ est vraie.} \\ \vdots \end{array}\right\} \text{ Preuve que } x \in F.$$

Exemple : Montrer que

$$\{x \in \mathbb{R} : \exists y \in \mathbb{R}_+,\ x \geq y\} \subset \mathbb{R}_+.$$

Preuve : Soit $x \in \mathbb{R}$. On suppose qu'il existe $y \in \mathbb{R}_+$ tel que $x \geq y$. Montrons que $x \in \mathbb{R}_+$. Or $y \geq 0$ par hypothèse et $x \geq y$, donc

$$x \geq 0.$$

Ainsi, $\{x \in \mathbb{R} : \exists y \in \mathbb{R}_+,\ x \geq y\} \subset \mathbb{R}_+$.

Exemple : Montrer que

$$E = \{k(k+1) : k \in \mathbb{N}\} \subset 2\mathbb{N}.$$

Preuve : Soit $n \in E$, alors

$$n = k(k+1) \quad \text{pour un certain } k \in \mathbb{N}.$$

Montrons que $n \in 2\mathbb{N}$. On peut affirmer que k est pair ou impair, et si k est impair alors $k+1$ est pair. Dans tous les cas

$$k \quad \text{ou} \quad k+1 \quad \text{est pair.}$$

Par produit, $n = k(k+1)$ l'est aussi, donc $n \in 2\mathbb{N}$. Par conséquent, $E \subset 2\mathbb{N}$.

À faire chez soi :

- Soit E l'ensemble des entiers naturels multiples de 6 et F l'ensemble des entiers naturels pairs. Montrer que $E \subset F$.
- Soit $E = [2, 3]$ et $F = \{x \in \mathbb{R} : x^2 - 3x - 10 \leq 0\}$. Montrer que $E \subset F$.

Définition (Égalité)

Soient E et F deux ensembles. Les ensembles E et F sont **égaux** *s'ils ont exactement les mêmes éléments, i.e. si :*

$$\forall x, \quad (x \in E \iff x \in F).$$

Exemples :

- Nous avons
$$\{x \in \mathbb{R} : x^2 - 3x - 10 < 0\} =]-2, 5[.$$
- Nous avons
$$\{0, 1\} = \{n \in \mathbb{N} : n^2 = n\}.$$

Théorème

Soient E et F deux ensembles. Alors :

$$E = F \quad \text{si et seulement si} \quad E \subset F \text{ et } F \subset E.$$

Ensembles

Pour montrer une égalité d'ensembles :

$$E = F,$$

deux stratégies sont possibles :

- Soit on raisonne par double inclusion : **En montrant d'abord** $E \subset F$:

  Soit $x \in E$. Montrons que $x \in F$ est vraie.

  $\left.\begin{array}{l} \vdots \\ \end{array}\right\}$ Preuve que $x \in F$.

  Puis, en montrant $F \subset E$:

  Soit $x \in F$. Montrons que $x \in E$ est vraie.

  $\left.\begin{array}{l} \vdots \\ \end{array}\right\}$ Preuve que $x \in E$.

- Soit on raisonne directement par équivalence :

$$\forall x : \quad x \in E \iff \cdots \iff \cdots \iff x \in F.$$

Exemple : Montrer que

$$\mathbb{R}_- = \{x \in \mathbb{R} : \forall y \in \mathbb{R}_+ \quad x \leq y\}.$$

Preuve : On raisonne par double inclusion

- Montrons
$$\mathbb{R}_- \subset \{x \in \mathbb{R} : \forall y \in \mathbb{R}_+ \quad x \leq y\}.$$
Soit $x \in \mathbb{R}_-$. Nous devons montrer que $\forall y \in \mathbb{R}_+$, $x \leq y$, mais par hypothèse $x \leq 0$. Donc
$$x \leq 0 \leq y.$$
- Montrons
$$\{x \in \mathbb{R} : \forall y \in \mathbb{R}_+ \quad x \leq y\} \subset \mathbb{R}_-.$$
Soit $x \in \mathbb{R}$ tel que $\forall y \in \mathbb{R}_+,\ x \leq y$. Alors en particulier, pour $y = 0$ on a $x \leq 0$. C'est-à-dire $x \in \mathbb{R}_-$.

Définition (Ensemble des parties d'un ensemble)

Soit E un ensemble. On note $\mathscr{P}(E)$ l'ensemble des parties de E

$$\mathscr{P}(E) = \{A : A \subset E\}.$$

Remarque : Pour tout ensemble A :

- $A \in \mathscr{P}(E) \iff A \subset E$, i.e. la notation $A \subset E$ a la même signification que la notation $A \in P(E)$.
- $a \in E \iff \{a\} \subset E \iff \{a\} \in \mathscr{P}(E)$.
- $\emptyset \in \mathscr{P}(E)$ et $E \in \mathscr{P}(E)$.

Exemple : Déterminer l'ensemble des parties de E lorsque :

- $E = \{a, b\}$:
$$\mathscr{P}(E) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}.$$
- $E = \{a, b, c\}$:
$$\mathscr{P}(E) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}.$$

Opérations sur les ensembles

Étudions certaines opérations sur les ensembles.

Définition (Intersection)

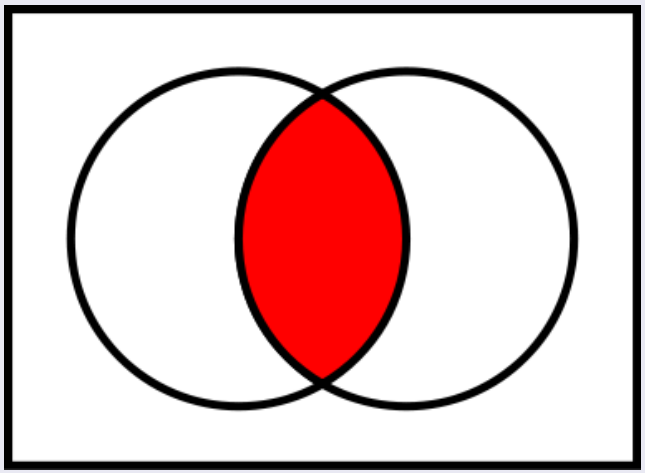
Soit E un ensemble, et soient A et B deux sous-ensembles de E.

- **L'intersection** *de A et B est l'ensemble, noté $A \cap B$, défini par :*

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

En d'autres termes, l'intersection de A et de B est l'ensemble des éléments qui sont à la fois dans A et dans B.

Diagramme de Venn :



Opérations sur les ensembles

Exemple :

- $\{1,4,7\} \cap \{3,5,7,11\} = \{7\}$.
- $\mathbb{Z} \cap \mathbb{Q} = \mathbb{Z}$.
- $$([-1,5] \cap]0,7[) \cap]4,9[\ =]0,5] \cap]4,9[\ =]4,5].$$
- On a

$$\{(x,y) \in \mathbb{R}^2 : x^2 + y^2 = 1\} \cap \{(x,y) \in \mathbb{R}^2 : x = y\}$$
$$= \left\{ \left(-\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2} \right), \left(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2} \right) \right\}.$$

- $\mathbb{R}_+ \cap \mathbb{R}_- = \{0\}$.
- $2\mathbb{N} \cap (2\mathbb{N}+1) = \emptyset$.

Opérations sur les ensembles

Définition (Ensembles disjoints)

Soient A et B deux ensembles. On dit que A et B sont **disjoints** *si*

$$A \cap B = \emptyset.$$

Autrement dit si A et B n'ont aucun élément commun.

Opérations sur les ensembles

Définition (Union)

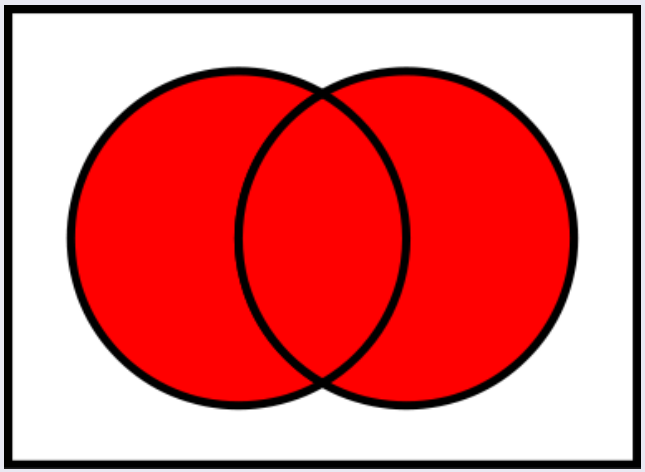
Soit E un ensemble, et soient A et B deux sous-ensembles de E.

- **L'union** *de A et B est l'ensemble, noté $A \cup B$, défini par :*

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

En d'autres termes, l'union de A et de B est l'ensemble des éléments qui appartiennent à A ou à B. Le « ou » utilisé ici est inclusif : x **est un élément de A ou un élément de B ou un élément de A et de B.**

Diagramme de Venn :



Opérations sur les ensembles

Exemple :

- $\{3,4,7,9\} \cup \{2,7,9,10,21,84\} = \{2,3,4,7,9,10,21,84\}$.
- $\mathbb{R}_+ \cup \mathbb{R}_- = \mathbb{R}$.
- $\mathbb{Q} \cup \mathbb{I} = \mathbb{R}$.
- $\{1,-1\} \cup]1,-1[= [-1,1]$.

Remarque :

- Si $A \subset B$. Alors

$$A \cap B = A \quad \text{et} \quad A \cup B = B.$$

- Soient A et B deux ensembles. Alors on a toujours les inclusions suivantes :

$$A \cap B \subset A \subset A \cup B \quad \text{et} \quad A \cap B \subset B \subset A \cup B.$$

Opérations sur les ensembles

L'union et l'intersection se généralisent facilement au cas de plus de deux ensembles.

Définition

Soit E un ensemble et n un entier supérieur ou égale à 2. Supposons donnés n sous-ensembles

$$A_1,\ A_2,\ \cdots,\ A_n,$$

de E.

- **Union :**

$$A_1 \cup A_2 \cup \cdots \cup A_n \ = \bigcup_{i\in\{1,2,\cdots,n\}} A_i \ = \ \{x \in E : \exists i \in \{1,2,\cdots,n\},\ x \in A_i\}.$$

i.e. l'ensemble des objets qui appartiennent à l'un des A_i.

- **Intersection :**

$$A_1 \cap A_2 \cap \cdots \cap A_n \ = \bigcap_{i\in\{1,2,\cdots,n\}} A_i \ = \ \{x \in E : \forall i \in \{1,2,\cdots,n\},\ x \in A_i\}.$$

i.e. l'ensemble des objets qui appartiennent à tous les A_i.

Opérations sur les ensembles

L'union et l'intersection satisfont les propriétés suivants.

Théorème

Soit E un ensemble, et considérons trois sous-ensembles A, B, C de E.

- *L'intersection et l'union sont* **commutatives** *:*

$$A \cap B = B \cap A \quad et \quad A \cup B = B \cup A.$$

- *L'intersection et l'union sont* **associatives** *:*

$$A \cap (B \cap C) = (A \cap B) \cap C = A \cap B \cap C,$$
$$A \cup (B \cup C) = (A \cup B) \cup C = A \cup B \cup C.$$

- *Pour tout sous-ensemble A de E on a*

$$A \cap E = A.$$

- *Pour tout sous-ensemble A de E on a*

$$A \cup \emptyset = A.$$

Opérations sur les ensembles

Théorème

Soit E un ensemble, et considérons trois sous-ensembles A, B, C de E.

- *L'intersection et la réunion sont* **distributives** *l'une par rapport à l'autre :*

$$\begin{aligned} A \cap (B \cup C) &= (A \cap B) \cup (A \cap C), \\ A \cup (B \cap C) &= (A \cup B) \cap (A \cup C). \end{aligned}$$

Démonstration.

Voir TD. □

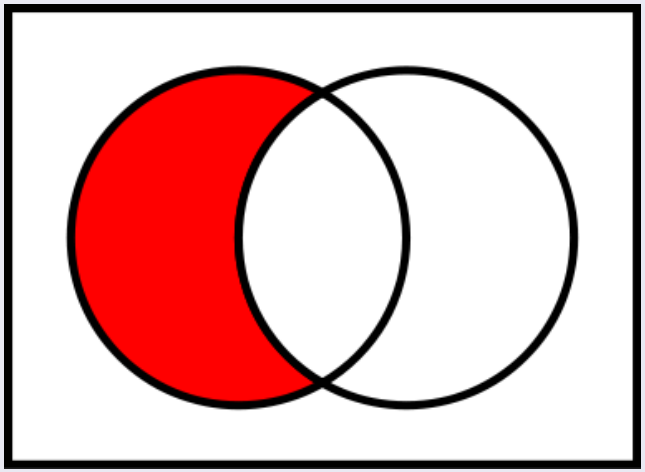
Définition (Différence)

Soit E un ensemble, et soient A et B deux sous-ensembles de E.

- *La* **différence** *de A avec B, noté $A \setminus B$, est l'ensemble de tous les éléments de A qui ne sont pas dans B, i.e.*

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

Diagramme de Venn *:*



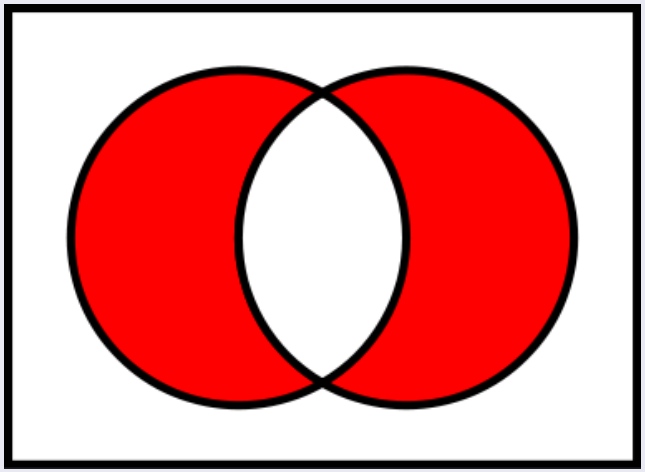
Définition (Différence Symétrique)

Soit E un ensemble, et soient A et B deux sous-ensembles de E.

- *La* **différence symétrique** *de A avec B, noté $A\Delta B$, est l'ensemble des élements qui sont dans un et un seul des deux ensembles A et B, i.e.*

$$A\Delta B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A).$$

Diagramme de Venn *:*



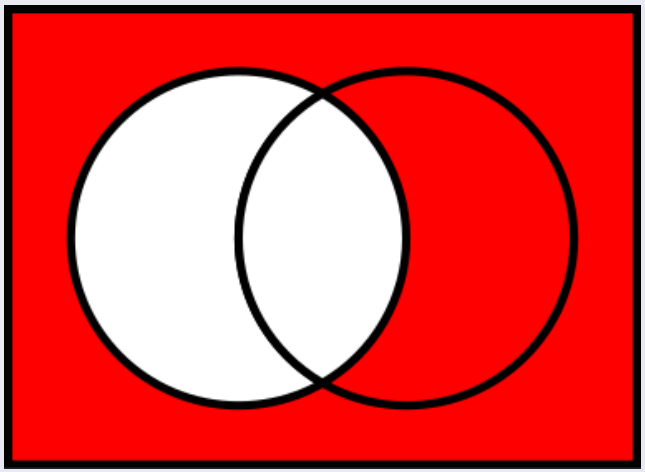
Définition (Complément)

Soient E un ensemble et A une partie de E.

- *Le* **complémentaire** *de A dans E est l'ensemble, noté C_A^E, de tous les éléments de E qui ne sont pas dans A,i.e.*

$$C_A^E = \{x : x \in E \text{ et } x \notin A\} = E \setminus A.$$

Diagramme de Venn :



Remarque : S'il n'y a pas d'ambigüité sur l'ensemble E, on privilégiera la notation A^c pour C_A^E.

Opérations sur les ensembles

Le passage au complémentaire satisfait les propriétés suivantes.

Théorème

Soient A et B deux parties de E.

1. $(A^c)^c = A \quad$ *et* $\quad \emptyset^c = E \quad$ *et* $\quad E^c = \emptyset$.
2. *Si $A \subset B$, alors*
$$B^c \subset A^c.$$
3. **Lois de Morgan :**
$$(A \cap B)^c = A^c \cup B^c \quad \text{et} \quad (A \cup B)^c = A^c \cap B^c.$$

Démonstration.

Voir TD. □

Partition d'un ensemble

Définition (Partition)

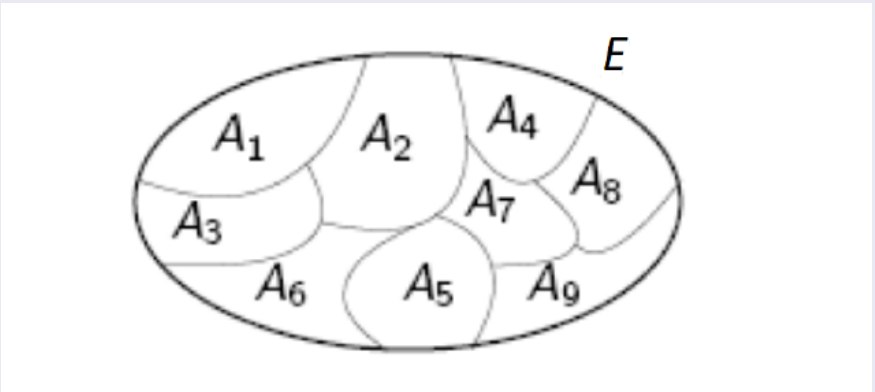
Une **partition d'un ensemble** E *est un ensemble*

$$\{A_1, A_2, \cdots, A_n\}$$

constitué de parties de E *vérifiant :*

- *Pour tout* $k \in \{1, \cdots, n\}$, $A_k \neq \emptyset$, *i.e.* **aucun** A_k **ne doit être vide**.
- $\bigcup_{k=1}^{n} A_k = E$, *i.e.* **la réunion des** A_k **est égale à** E.
- *Pour tout couple* A_i, A_j *avec* $A_i \neq A_j$ *on a* $A_i \cap A_j = \emptyset$, *i.e. les* A_i *sont* **deux à deux disjoints**.

Diagramme de Venn :



Partition d'un ensemble

Exemples :

- L'ensemble $\{2\mathbb{N}, 2\mathbb{N}+1\}$ définit une partition de $\mathbb{N}$.
- L'ensemble $\{\mathbb{Q}, \mathbb{I}\}$ définit une partition de $\mathbb{R}$.
- L'ensemble $\left\{\left[0, \frac{1}{2}\right], \left]\frac{1}{2}, \frac{3}{2}\right], \left]\frac{3}{2}, 2\right]\right\}$ définit une partition de $[0, 2]$.

Exercice : Donner toutes les partitions de l'ensemble

$$E = \{a, b, c\}.$$

Solution :

- $P_0 = \{E\} = \{\{a, b, c\}\}$.
- $P_1 = \{\{a\}, \{b\}, \{c\}\}$.
- $P_2 = \{\{a\}, \{b, c\}\}$ et $P_2' = \{\{b\}, \{a, c\}\}$ et $P_2'' = \{\{a, b\}, \{c\}\}$.

Produit Cartésien

On finit ce chapitre en rappelant la définition du produit cartésien.

Définition (Produit Cartésien)

Soient A et B deux parties de E. Le **produit cartésien** *de A et B est l'ensemble, noté*

$$A \times B,$$

constitué de tous les couples (x, y) où

$$x \in A \quad et \quad y \in B.$$

On a donc :

$$A \times B = \big\{(x, y) : x \in A \ \ et \ \ y \in B\big\}.$$

Exemple : Soit $A = \{a, b\}$ et $B = \{1, 2\}$, alors

$$A \times B \ = \ \{(a, 1), (a, 2), (b, 1), (b, 2)\}.$$

Produit Cartésien

Exemple : Avec

$$C = \{1, 2\} \qquad \text{et} \qquad D = \{1, 2, 3\}$$

on a

$$C \times D = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3)\}.$$

Remarque : On ne confond pas les couples (a, b) et (b, a) qui désignent **deux objets différents**, alors que $\{a, b\}$ et $\{b, a\}$ désignent le **même ensemble**.

L'exemple montre que le premier et le deuxième terme du couple n'appartiennent pas au même ensemble.

Produit Cartésien

Le produit cartésien se généralise au cas de plus de deux ensembles.

Définition (Produit cartésien d'une famille finie d'ensembles)

Soit n un entier supérieur ou égale à 2. Supposons donnés n ensembles

$$A_1,\ A_2,\ \cdots,\ A_n.$$

Alors le **produit cartésien** *de $A_1,\ A_2,\ \cdots,\ A_n$ est l'ensemble défini par*

$$\begin{aligned} A_1 \times A_2 \times \cdots \times A_n &= \left\{(x_1, x_2, \cdots, x_n) :\ x_1 \in A_1,\ x_2 \in A_2,\ \cdots, x_n \in A_n\right\} \\ &= \left\{(x_1, x_2, \cdots, x_n) :\ \forall i \in \{1, \cdots, n\},\ x_i \in A_i\right\}. \end{aligned}$$

L'élément $(x_1, x_2,\ \cdots\ , x_n)$ est appelé un n-tuple de composants $x_1,\ x_2,\ \cdots,\ x_n$.

Remarque :

- Lorsque $A = B$, on note
$$A \times A = A^2.$$
et on généralise cette notation pour l'ensemble
$$A^n = A \times A \times \cdots \times A.$$
(produit cartésien de n facteurs égaux à A).
- La diagonale de A^2 est l'ensemble $\Delta = \{(x, x), x \in A\}$.

Produit Cartésien

Le produit cartésien satisfait les propriétés suivantes.

Proposition

Soient A, B, C, D des parties d'un ensemble E.

- $(A \times C) \cup (A \times D) = A \times (C \cup D)$.
- $(A \times C) \cap (B \times D) = (A \cap B) \times (C \cap D)$.

Démonstration.

Voir TD. □

Relations Binaires

- Relation d'équivalence :
  - Classes d'équivalence.
  - Partition d'un ensemble par une relation d'équivalence.
- Relation d'ordre :
  - Relation d'ordre partiel, totale.
  - Relation d'ordre stricte.
  - Minimum, maximum, borne inférieure, borne supérieure.

Définition

Soient E et F deux ensembles. On appelle **relation** $\mathscr{R}$ *de E sur F la donnée d'une partie*

$$R \subset E \times F.$$

- *La partie R est appelé le graphe de la relation $\mathscr{R}$.*
- *On dit qu'un élément $x \in E$ est* **en relation avec** *un élément $y \in F$ si*

$$(x, y) \in R.$$

- *On exprime cette situation en écrivant $x\mathscr{R}y$. C'est-à-dire*

$$x\mathscr{R}y \iff (x, y) \in R.$$

Finalement, si $E = F$ la relation $\mathscr{R}$ est appelée **relation binaire**.

Exemple : Soit $E = \{1, 2, 3, 4\}$ et $\mathscr{R}$ la relation binaire sur E dont le graphe est donné par

$$R = \{(1,1), (1,3), (2,2), (2,4), (3,1), (3,3), (4,2), (4,4)\}.$$

C'est-à-dire

$$a \mathscr{R} b \iff (a, b) \in R.$$

Ainsi, par exemple

$$1 \mathscr{R} 1 \quad \text{et} \quad 1 \mathscr{R} 3,$$

mais

1 n'est pas en relation avec 2 et **1 n'est pas en relation avec 4**.

Relations Binaires

Exemple :

- La relation d'inclusion dans l'ensemble des parties de E

$$A\mathscr{R}B \iff A \subset B.$$

Ici donc

$$R = \{(A, B) \in \mathscr{P}(E) \times \mathscr{P}(E) \ : \ A \subset B\}.$$

- La relation de divisibilité sur les entiers relatifs

$$m\mathscr{R}n \iff m|n \quad (m \text{ divise } n).$$

Ici donc

$$R = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \ : \ m|n \in \mathbb{Z}\}.$$

- Sur tout ensemble E, on peut définir la relation égalité

$$x\mathscr{R}y \iff x = y.$$

Ici donc

$$R = \{(a, b) \in E \times E \ : \ a = b\}.$$

- Les relations $\leq$ et $<$ sur $\mathbb{R}$, sont aussi des relations binaires.

Remarque : Parce que le couple (x, y) n'est pas egal au couple (y, x), la relation $x\mathscr{R}y$ peut être vraie sans que la relation $y\mathscr{R}x$ le soit. Par exemple, si on considère la relation d'inclusion sur $\mathbb{R}$, nous avons

$$[0, 2[\mathscr{R}[0, 2] \quad \text{car} \quad [0, 2[\subset [0, 2],$$

mais $[0, 2]$ n'est pas inclus dans $[0, 2[$, donc

$$[0, 2] \quad \text{n'est pas en relation avec} \quad [0, 2[.$$

Relations Binaires

Etudions certaines propriétés éventuelles des relations binaires.

Définition

Soit $\mathscr{R}$ une relation binaire sur E.

- *On dit que $\mathscr{R}$ est* **réflexive** *si :*

$$\forall x \in E, \quad x \mathscr{R} x$$

- *On dit que $\mathscr{R}$ est* **transitive** *si :*

$$\forall x \in E,\ \forall y \in E,\ \forall z \in E, \quad x \mathscr{R} y \ \text{ et } \ y \mathscr{R} z \quad \Longrightarrow \quad x \mathscr{R} z$$

- *On dit que $\mathscr{R}$ est* **symétrique** *si :*

$$\forall x \in E,\ \forall y \in E, \quad x \mathscr{R} y \implies y \mathscr{R} x$$

- *On dit que $\mathscr{R}$ est* **antisymétrique** *si :*

$$\forall x \in E,\ \forall y \in E, \quad x \mathscr{R} y \ \text{ et } \ y \mathscr{R} x \quad \Longrightarrow \quad x = y.$$

Remarque : L'antisymetrie n'est pas le contraire de la symétrie. Par exemple, la relation **égalité** possède les deux propriétés.

Exemples :

- Soit $E = \{1, 2, 3, 4\}$. Alors la relation binaire $\mathscr{R}$ sur E dont le graphe est donné par

$$R = \{(1,1), (1,3), (2,2), (2,4), (3,1), (3,3), (4,2), (4,4)\},$$

  est réflexive, symétrique et transitive.

- La relation d'égalité " $=$ " sur E est réflexive, transitive, symétrique et antisymétrique.

- La relation d'inclusion $\subset$ sur $\mathscr{P}(E)$ est réflexive, transitive et antisymétrique.

Exemples :

- La relation $\leq$ sur $\mathbb{R}$ est réflexive, transitive et antisymétrique. Elle n'est pas symétrique car par exemple : $2 \leq 5$ mais : $5 \not\leq 2$.
- La relation $<$ sur $\mathbb{R}$ est transitive et antisymétrique, mais elle n'est ni réflexive, ni symétrique.
- La relation $|$ de divisibilité sur $\mathbb{Z}$ est réflexive et transitive, mais elle n'est pas antisymétrique car par exemple : $5|-5$ et $-5|5$ mais $5 \neq -5$.

Relation d'équivalence

Nous allons étudier deux importants types des relations binaires : **Les relations d'equivalence** et **les relations d'ordre**. Commencons par étudier les relations d'equivalence.

Définition

On dit qu'une relation binaire $\mathscr{R}$ sur E est une relation **d'équivalence** *si $\mathscr{R}$ est à la fois réflexive, transitive et symétrique.*

Pour $a \in E$, l'ensemble des éléments $x \in E$ en relation avec a est appelé la **classe d'équivalence** *de a, notée*

$$cl(a) \quad ou \quad [a] \quad ou \quad \overline{a}.$$

C'est-à-dire

$$cl(a) = \{x \in E : \ a\mathscr{R}x\}.$$

Exemple : Soit n un entier naturel. La relation sur $\mathbb{Z}$ définie par

$$a\mathscr{R}b \quad \Longleftrightarrow \quad n \ \text{ divise } \ a-b$$

est une relation d'équivalence. Si $a\mathscr{R}b$ on dit que a et b sont **congrus modulo** n.

Relation d'équivalence

Exemple : Soit $E = \{1, 2, 3, 4\}$. Nous avons vu que la relation binaire $\mathscr{R}$ sur E dont le graphe est donné par

$$R = \{(1,1), (1,3), (2,2), (2,4), (3,1), (3,3), (4,2), (4,4)\},$$

est réflexive, symétrique et transitive. C'est-à-dire, $\mathscr{R}$ est une relation d'équivalence. De plus, nous avons

$$\begin{array}{ccccc} cl(1) & = & \{1,3\} & = & cl(3), \\ cl(2) & = & \{2,4\} & = & cl(4). \end{array}$$

Relation d'équivalence

L'ensemble des classes d'équivalence nous donnent une partition de l'ensemble E.

Proposition (Partition d'un ensemble en classes d'équivalence)

Soit $\mathscr{R}$ une relation d'équivalence sur un ensemble E. Alors les classes d'équivalences forment une **partition de** *E, c'est-à-dire*

- *toute classe d'équivalence est non vide :*

$$\forall x \in E, \quad cl(x) \neq \emptyset,$$

- *deux classes d'équivalence sont soit disjointes soit égales :*

$$\forall x, y \in E \quad \textit{tel que} \quad cl(x) \neq cl(y) \quad \textit{on a} \quad cl(x) \cap cl(y) = \emptyset,$$

- *la réunion des classes d'équivalence est égale à E :*

$$E = \bigcup_{x \in E} cl(x).$$

Relation d'ordre

Passons à étudier les relations d'ordre.

Définition

On dit qu'une relation binaire $\mathscr{R}$ sur E est une **relation d'ordre** *si $\mathscr{R}$ est à la fois réflexive, transitive et antisymétrique.*

- *Les relations d'ordre sont généralement notées $\leq$ ou $\preccurlyeq$ ou $\lesssim$ ou $\preceq$.*
- *Soit $\preccurlyeq$ une relation d'ordre sur E, on dit alors que $(E, \preccurlyeq)$ est un ensemble ordonné.*

Définition (Ordre total ou ordre partiel)

Soit $\preccurlyeq$ une relation d'ordre sur E.

- *Deux éléménts x et y de E sont dits comparables (pour $\preccurlyeq$) si*

$$x \preccurlyeq y \quad ou \quad y \preccurlyeq x.$$

- *Si deux éléments quelconques sont toujours comparables, on dit que $\preccurlyeq$ est une relation d'***ordre total***. E est dit totalement ordonné par $\preccurlyeq$.*
- *Sinon, on dit que $\preccurlyeq$ est une relation d'***ordre partiel***. E est dit* **partiellement ordonné** *par $\preccurlyeq$.*

Relation d'ordre

Exemple :

- Sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$ on a une relation d'ordre total, notée $\leq$ (Voir cours d'analyse).
- Sur $\mathscr{P}(E)$, la relation
$$A \preccurlyeq B \iff A \subset B$$
c'est une relation d'ordre partiel (sauf si $E = \emptyset$ ou $E = \{a\}$). En effet, si $a \in E$, $b \in E$, $\{a\}$ et $\{b\}$ non comparables.
- Sur $\mathbb{R}^2$
$$(x, y) \preccurlyeq (x', y') \iff (x \leq x') \quad \text{et} \quad (y \leq y')$$
est un ordre partiel. Par exemple $(1, 2)$ et $(4, 0)$ non comparables.

Relation d'ordre

Définition (Relation stricte associée à une relation d'ordre)

Soit $\preccurlyeq$ une relation d'ordre sur E. On définit alors une nouvelle relation sur E par

$$\forall x, y \in E, \quad x \prec y \quad \Longleftrightarrow \quad x \preccurlyeq y \quad \text{et} \quad x \neq y.$$

La relation $\prec$ on l'appelle la **relation stricte** *associée à $\preccurlyeq$.*

Exemple : Naturellement, la relation usuelle $<$ sur $\mathbb{R}$ est la relation stricte de la relation $\leq$.

Attention ! : La relation stricte n'est pas une relation d'ordre car elle n'est pas reflexive : On ne peut pas avoir

$$x \preccurlyeq x \quad \text{et} \quad x \neq x.$$

Proposition

La relation $\prec$ est transitive et antisymétrique.

Définition (Majorant - Minorant)

Soit A une partie d'un ensemble E muni d'une relation d'ordre $\preceq$.

- *A est* **majorée** *s'il existe $M \in E$ tel que pour tout $x \in A$ nous avons*

$$x \preceq M.$$

  On dit alors que M est un **majorant** *de A.*

- *A est* **minorée** *s'il existe $m \in E$ tel que pour tout $x \in A$ nous avons*

$$m \preceq x.$$

  On dit alors que m est un **minorant** *de A.*

- *A est* **bornée** *lorsque A est à la fois majorée et minorée. C'est-à-dire, s'il existe $m \in E$ et $M \in E$ tel que pour tout $x \in A$ nous avons*

$$m \preceq x \preceq M.$$

Relation d'ordre

Remarque : On ne parle jamais « **du** » majorant d'une partie majorée de E mais bien toujours d'**UN** majorant car une telle peut possèder plein. Même chose à dire sur les minorants.

Exemple :

- L'ensemble $\{8, 10, 12\}$ est minoré par 2 et majoré par 120 pour la relation de divisibilité $\mid$ sur $\mathbb{N}$.
- $\mathscr{P}(E)$ est minoré par $\emptyset$ et majoré par E pour la relation d'inclusion $\subset$.
- Tout réel inférieur ou égal à 0 est un minorant de l'intervalle $]0, 1[$ par rapport à la relation d'ordre usuelle sur $\mathbb{R}$. Tout réel supérieur ou égal à 1 est un majorant de l'intervalle $]0, 1[$ par rapport à la relation d'ordre usuelle sur $\mathbb{R}$.

Relation d'ordre

Un majorant ou minorant de une partie A de E, n'appartient pas necéssairement à A. Quand il appartient à l'ensemble on dit :

Définition (Maximum - Minimum)

Soit A une partie d'un ensemble E muni d'une relation d'ordre.

- **Plus grand élément** *: On appelle* **plus grand élément** *de A ou* **maximum** *de A tout élément de A qui majore A. C'est-à-dire, tout majorant de A qui est dans A.*
- **Plus petit élément** *: On appelle* **plus petit élément** *de A ou* **minimum** *de A tout élément de A qui minore A. C'est-à-dire, tout minorant de A qui est dans A.*

Exemple : On travaille dans cette série d'exemples avec l'ordre usuel sur $\mathbb{R}$.

- 0 est le plus petit élémént de $\mathbb{R}_+$ et le plus grand élément de $\mathbb{R}_-$.
- $]0,1[$ ne possède ni plus petit élément ni plus grand élément.
- 0 est le plus petit élémént de $[0,1]$, et 1 est le plus grand élémént de $[0,1]$.

Relation d'ordre

Exemple : On travaille dans cette série d'exemples avec la relation de divisibilité $|$ sur $\mathbb{N}$.

- L'ensemble $\{2, 3, 6\}$ possède un plus grand élément, c'est 6, mais pas de plus petit élément.
- 0 est le plus grand élément de $\mathbb{N}$ et 1 est son plus petit élément.
- L'ensemble $\mathbb{N} \setminus \{0, 1\}$ ne possède ni plus petit élément ni plus grand élément.

Théorème (Unicité)

Soit $\preccurlyeq$ une relation d'ordre et A une partie de E. Si A possède un plus grand (resp. petit) élément, celui-ci est **UNIQUE**. *On peut donc l'appeler* **LE** *plus grand (resp. petit) élément de A et le noter*

$$\max A \quad (\textit{resp.} \quad \min A).$$

Relation d'ordre

L'intervalle

$$[a, b[$$

pour **la relation d'ordre usuel** n'a pas de plus grand élément, pourtant sa borne b est quelque chose de cet ordre — mais quoi ? Comment décrire conceptuellement ce réel qui n'est pas dans $[a, b[$ mais qui n'est pas n'importe qui pour $[a, b[$?

Ce qui rend le majorant b si particulier pour $[a, b[$, c'est qu'il est le meilleur majorant qu'on pouvait espérer :

LE PLUS PETIT POSSIBLE.

Nous allons donc le donner un nom au plus petit majorant (et au plus grand minorant).

Définition

Soit A une partie de un ensemble E muni d'une relation d'ordre.

- *Si l'ensemble des minorants de A admet un plus grand élément, on l'appelle* **borne inférieure** *de A et on le note*

$$\inf A.$$

- *Si l'ensemble des majorants de A admet un plus petit élément, on l'appelle* **borne supérieure** *de A et on le note*

$$\sup A.$$

Relation d'ordre

Remarque : La différence essentielle entre les plus grands éléments et les bornes supérieures d'une partie A, c'est que les bornes supérieures n'appartiennent pas forcément à A.

Exemple : Avec l'ordre usuel sur $\mathbb{R}$, les intervalles $[a, b]$, $]a, b[$, $[a, b[$ et $]a, b]$ ont a pour borne inférieur et b pour borne supérieur.

Théorème (Lien entre les notions de plus grand/petit élément et borne supérieure/inférieure)

Soit $\preccurlyeq$ une relation d'ordre et A une partie de E. Si A possède un plus grand (resp. petit) élément, alors A possède une borne supérieure (resp. inférieure) et :

$$\sup(A) = \max(A) \quad (\textit{resp.}\ \inf(A) = \min(A)).$$

Exemple : Avec l'ordre usuel sur $\mathbb{R}$ on a :

$$\inf[a, b] = \min[a, b] = a \quad \text{et} \quad \sup[a, b] = \max[a, b] = b.$$

Applications

Définition (Application)

Soient E et F deux ensembles. Une **application** *f de E vers F est le moyen d'associer, à chaque élément x de E un* **unique** *élément y de F. Plus formellement, on appelle* **application** *(ou* **fonction***) de E dans F toute relation dont le graphe $\Gamma \subset E \times F$ est tel que :*

$$\forall x \in E,\ \exists! y \in F, \quad (x, y) \in \Gamma.$$

On note

$$y = f(x),$$

*et on dit que $y = f(x)$ est l'***image** *de x par f. E est l'***ensemble de départ** *de f et F est l'***ensemble d'arrivée** *de f. On note*

$$\begin{aligned} f : E &\longrightarrow F \\ x &\longmapsto y = f(x). \end{aligned}$$

Si y est un élément de F, on dit que x est un **antécédent** *de y par f lorsque $y = f(x)$.*

Applications

Définition (Ensemble d'applications)

L'ensemble des applications de E dans F est noté $\mathscr{F}(E,F)$ ou F^E.

Applications

Exemples :

- **Application identité** : On appelle application identité d'un ensemble E, et on note Id_E, l'application de E dans E définie par

$$\begin{aligned} \mathrm{Id}_E : E &\longrightarrow E \\ x &\longmapsto x. \end{aligned}$$

- **Application constante** : Une application $f : E \to F$ est dite constante s'il existe $\alpha \in F$ tel que $\forall\, x \in E,\ f(x) = \alpha$. C'est-à-dire

$$\begin{aligned} f : E &\longrightarrow F \\ x &\longmapsto \alpha. \end{aligned}$$

- **Fonction indicatrice d'une partie d'un ensemble** : Soit E un ensemble et A une partie de E. On appelle fonction indicatrice de A et on note $\mathbb{1}_A$ la fonction de E dans $\{0,1\}$ définie par :

$$\begin{aligned} \mathbb{1}_A : E &\longrightarrow \{0,1\} \\ x &\longmapsto \mathbb{1}_A(x) = \begin{cases} 1 & \text{si } x \in A, \\ 0 & \text{si } x \notin A. \end{cases} \end{aligned}$$

Applications

Exemple :

- **Famille d'éléments** : Soit E un ensemble et I un ensemble (le plus souvent fini ou dénombrable), généralement

$$I = \{1, \cdots, n\} \quad \text{ou} \quad I = \mathbb{N} \quad \text{ou} \quad I = \mathbb{Z}.$$

On appelle famille d'éléments de E indéxée par I toute application de I dans E

$$\begin{aligned} f : I &\longrightarrow E \\ i &\longmapsto f(i) \end{aligned}$$

On note

$$f(i) = x_i \quad (\in E).$$

On represente un telle famille par

$$(x_i)_{i \in I}.$$

Remarque : Une suite numérique est une famille d'éléments de $\mathbb{R}$ indéxée par $\mathbb{N}$:

$$(u_n)_{n \in \mathbb{N}}.$$

Remarque : Une fonction est définie par des couples. Si l'ensemble des couples est modifié, on n'a pas le même graphe et on ne définit plus la même fonction :

$$f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2 \end{array} \quad \text{et} \quad g : \begin{array}{ccc} [0,2] & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2 \end{array}$$

ne sont pas les mêmes fonctions.

Définition (Égalité entre fonctions)

Deux applications f et g sont égales si :

- *elles ont le même ensemble de départ E et le même ensemble d'arrivée, et*
- *si pour tout $x \in E$, on a*

$$f(x) = g(x).$$

Image directe, Image reciproque

Définition (Image directe d'une partie, image d'une application)

Soit $f : E \to F$ une application.

- *Pour toute partie A de E, on appelle* **image (directe)** *de A par f, notée $f(A)$, l'ensemble :*

$$\begin{aligned} f(A) &= \{y \in F : \exists a \in A,\ y = f(a)\} \\ &= \{f(a) : a \in A\}. \end{aligned}$$

- *L'image de E tout entier est simplement appelée l'***image de** *f et est notée généralement*

$$\mathrm{Im} f \quad \textit{plutôt que} \quad f(E).$$

Image directe, Image reciproque

Exemple :

- L'image de $\mathbb{R}$ par la fonction
$$x \mapsto x^2$$
est $\mathbb{R}_+$. L'image de $[0, 3[$ par cette même fonction est $[0, 9[$.
- Considérons la fonction
$$x \mapsto \sin x.$$
Alors :
  - l'image de
$$\pi\mathbb{Z} := \{\cdots\ ,\ -2\pi\ ,\ -\pi\ ,\ 0\ ,\ \pi\ ,\ 2\pi\ ,\ \cdots\}$$
par la fonction sinus est le singleton $\{0\}$.
  - l'image de $[0, \pi]$ par la fonction sinus est $[0, 1]$.
  - l'image de $[-\pi/2, \pi/2]$ par la fonction sinus est $[-1, 1]$.

Image directe, Image reciproque

Définition (Expression « à valeurs dans $\cdots$ »)

Soient $f : E \to F$ une application et B une partie de F. On dit que f est **à valeurs dans** *B si toute valeur de f est élément de B, i.e. si*

$$\forall x \in E,\ f(x) \in B,$$

ou encore si

$$\mathrm{Im} f \subset B.$$

Remarque : En général, $\mathrm{Im} f$ est plus petit que F

$$\mathrm{Im} f \ \subset \ F.$$

Exemple : Les fonctions

$$\begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2 \end{array} \quad \text{et} \quad \begin{array}{rccc} \exp : & [0,2] & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \exp(x). \end{array}$$

sont deux fonctions à valeurs dans $\mathbb{R}_+$.

Image directe, Image reciproque

Étudions comme l'image directe se comporte par rapport à certaines opérations sur les ensembles.

Proposition

Soit $f : E \to F$. Soit A et B deux parties quelconques de E. On a

- $$A \subset B \Longrightarrow f(A) \subset f(B).$$
- $$f(A \cup B) = f(A) \cup f(B).$$
- $$f(A \cap B) \subset f(A) \cap f(B).$$
- $$f(\emptyset) = \emptyset \quad \text{et} \quad f(\{a\}) = \{f(a)\}.$$

Démonstration.

Voir TD. □

Image directe, Image reciproque

Attention : Notons que nous avons seulement

$$f(A \cap B) \subset f(A) \cap f(B).$$

En effet, $f(A \cap B)$ et $f(A) \cap f(B)$ ne sont en général pas egaux, comme l'on peut voir dans le diagramme :

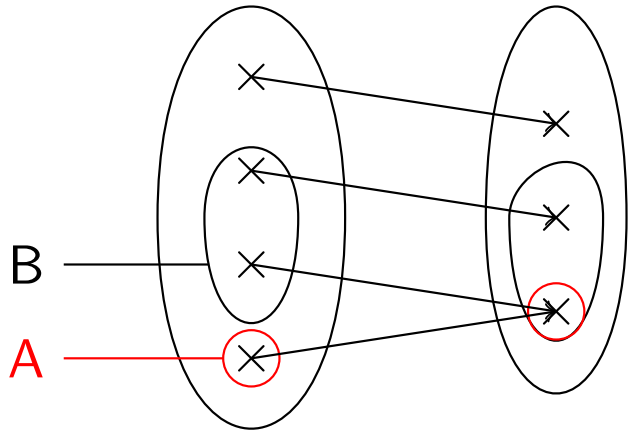


Image directe, Image reciproque

Définition (Image réciproque d'une partie)

Soient $f : E \to F$ une application et B une partie de F.

*L'***image réciproque** *de B par f, notée $f^{-1}(B)$ est l'ensemble des éléments de E dont l'image est dans B :*

$$f^{-1}(B) = \{x \in E,\ f(x) \in B\}.$$

C'est la partie de E **formée par les antécédents des éléments de** *B.*

Remarque :

- On peut écrire
$$x \in f^{-1}(B) \quad \Longleftrightarrow \quad f(x) \in B.$$
- On a
$$f^{-1}(\emptyset) = \emptyset \quad \text{et} \quad f^{-1}(F) = E.$$
Pour tout $b \in F$
$$f^{-1}(\{b\}) = \{x \in E : f(x) = b\}.$$
Par conséquent, si $b \notin \mathrm{Im} f$ on a $f^{-1}(\{b\}) = \emptyset$.

Image directe, Image reciproque

Exemples :

- L'image réciproque de $\mathbb{R}_+$ par la fonction exponentielle est $\mathbb{R}$ tout entier :

$$\exp^{-1}(\mathbb{R}_+) = \mathbb{R}.$$

- L'image réciproque de $[9, 25[$ par la fonction carrée est :

$$f^{-1}([9, 25[) =]-5, -3] \cup [3, 5[.$$

- L'image réciproque de $\{0\}$ par la fonction sinus est

$$\sin^{-1}(\{0\}) = \pi\mathbb{Z} = \{k\pi : k \in \mathbb{Z}\}.$$

L'image reciproque de $[4, 6]$ par le même fonction est :

$$\sin^{-1}([4, 6]) = \emptyset.$$

Image directe, Image reciproque

Étudions maintenant comme l'image reciproque se comporte par rapport à certaines opérations sur les ensembles.

Proposition

Soit $f : E \to F$. Soit $A \subset F$ et $B \subset F$. On a

- $$f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B).$$
- $$f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B).$$
- $$f^{-1}(A^c) = \left(f^{-1}(A)\right)^c.$$

Démonstration.

Voir TD. □

Opérations sur les applications

Introduisons certaines opérations qui vont nous permettre de fabriquer de nouvelles applications.

Définition (Composition)

Soient E, F et G trois ensembles, f une application de E dans F et g une application de F dans G. La **composée de f par g** *est l'application de E dans G, notée $g \circ f$ et définie pour tout $x \in E$ par*

$$(g \circ f)(x) = g(f(x)).$$

c'est-à-dire

$$\begin{array}{rccccc} g \circ f : & E & \xrightarrow{f} & F & \xrightarrow{g} & G \\ & x & \longmapsto & f(x) & \longmapsto & g(f(x)). \end{array}$$

Remarque : La composition, en général, n'est possible que dans un seul sens, et quand elle est possible dans les deux, on n'a aucune raison d'avoir :

$$f \circ g = g \circ f.$$

Opérations sur les applications

La composition satisfait les propriétés suivantes.

Proposition

Soient E, F, G, H des ensembles.

- **Neutralité de l'identité** *: Pour tout $f \in \mathscr{F}(E,F)$, on a : $f \circ \mathrm{Id}_E = f$:*

$$\begin{array}{rccc} f \circ \mathrm{Id}_E : & E & \xrightarrow{\mathrm{Id}_E} & E \xrightarrow{f} F \\ & x & \longmapsto & x \longmapsto f(x). \end{array}$$

- **Neutralité de l'identité** *: Pour tout $f \in \mathscr{F}(E,F)$, on a : $\mathrm{Id}_F \circ f = f$:*

$$\begin{array}{rccc} \mathrm{Id}_F \circ f : & E & \xrightarrow{f} & F \xrightarrow{\mathrm{Id}_F} F \\ & x & \longmapsto & f(x) \longmapsto f(x). \end{array}$$

- *La composition est* **associative** *: $\forall f \in \mathscr{F}(E,F)$, $\forall g \in \mathscr{F}(F,G)$, $\forall h \in \mathscr{F}(G,H)$, on a :*

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

Démonstration.

Montrons que la composition est **associative** :

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

Pour tout $x \in E$ on a

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

Ainsi, $(h \circ g) \circ f = h \circ (g \circ f)$. □

Opérations sur les applications

Soit $f \in \mathscr{F}(E, F)$. On peut aussi créer de nouvelles applications en ne modifiant que l'ensemble de depart ou l'ensemble d'arrivée de f.

Définition

Soit A une partie de E.

- *Soit $f : E \to F$ une application. On appelle* **restriction** *de f à A l'application notée*

$$f|_A : A \to F$$

définie par

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

- *Soit $f : A \to F$ une application. On appelle* **prolongement** *de f à E toute application g de E dans F telle que :*

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

C'est-à-dire f est la restriction de g à A ($g|_A = f$).

Opérations sur les applications

Remarque :

- Restreindre/prolonger une application, c'est diminuer/augmenter la taille de son ensemble de définition.
- Parce que il existe en général beaucoup de prolongements d'une application donnée, on parle d'**un** prolongement et non **du** prolongement. Par exemple, si f est l'identite de $\mathbb{R}_+$:

$$\begin{aligned} \mathrm{Id}_{\mathbb{R}_+} : \mathbb{R}_+ &\longrightarrow \mathbb{R}_+ \\ x &\longmapsto x, \end{aligned}$$

elle possède une infinité de prolongements à $\mathbb{R}$ tout entier, parmi lesquels

- L'application **identité** de $\mathbb{R}$.
- L'application **valeur absolue** de $\mathbb{R}$.
- L'application

$$\begin{aligned} h : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto \frac{1}{2}(|x| + x). \end{aligned}$$

Notons que h est identiquement nulle sur $\mathbb{R}_-$ (i.e. $h(x) = 0$ pour tout $x \leq 0$).

Définition (Injection)

Soit $f : E \to F$ une application. On dit que f est **injective** *sur E ou que c'est une* **injection** *sur E si :*

$$\forall x \in E,\ \forall x' \in E, \quad f(x) = f(x') \quad \Longrightarrow \quad x = x'.$$

Autrement dit, f est injective si toute élément y de F possède **au plus un** *antécédent par f.*

Exemples :

- La application identité d'un ensemble E, est injective.
- Soit $a \in \mathbb{R}^\times$. Alors toute application affine sur $\mathbb{R}$ de la forme :

$$f(x) = ax + b$$

est injective.

- L'application $f : \mathbb{R} \to \mathbb{R}$ définie par

$$f(x) = x^3$$

est injective.

- L'application exponentielle $f(x) = e^x,\ x \in \mathbb{R}$, est injective.

Remarques

- Une définition equivalente de l'injectivité est

$$\forall x \in E,\ \forall x' \in E, \quad x \neq x' \quad \Longrightarrow \quad f(x) \neq f(x').$$

Notons que la proposition précédente est la contraposition de

$$\forall x \in E,\ \forall x' \in E, \quad f(x) = f(x') \quad \Longrightarrow \quad x = x'.$$

- Le changement de l'ensemble de départ d'une application peut modifier la propriété d'être injective. Par exemple :
  - La fonction carré n'est pas injective sur $\mathbb{R}$, mais elle l'est sur $\mathbb{R}_+$.
  - La restriction de cos : $\mathbb{R} \to \mathbb{R}$ à l'intervalle $[0, \pi]$ est injective.

Injections-Surjections-Bijections

Étudions certaines propriétés des fonctions injectives.

Proposition

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

- *Si f et g sont injectives, alors $g \circ f$ est injective.*
- *Si $g \circ f$ est injective, alors f est injective.*

Démonstration.

- Soient $x, y \in E$. Supposons $g \circ f(x) = g \circ f(y)$. Nous voulons montrer que : $x = y$. Or

$$g(f(x)) = g(f(y)) \underbrace{\Longrightarrow}_{g \text{ injective}} f(x) = f(y) \underbrace{\Longrightarrow}_{f \text{ injective}} x = y.$$

- Soient $x, y \in E$. Supposons $f(x) = f(y)$. Nous voulons montrer que : $x = y$. Or

$$f(x) = f(y) \quad \Longrightarrow \quad g \circ f(x) = g \circ f(y) \underbrace{\Longrightarrow}_{g \circ f \text{ injective}} x = y.$$

Définition (Surjection)

Soit $f : E \to F$ une application. On dit que f est une application **surjective** *de E sur F ou que c'est une* **surjection** *de E sur F si :*

$$\forall y \in F, \quad \exists x \in E, \quad y = f(x).$$

Cela revient à dire que :

$$\mathrm{Im} f = F.$$

Autrement dit, f est surjective de E sur F si et seulement si tout élément de F possède **au moins un antécédent** *dans E par f.*

Exemples :

- L'application $|\cdot| : \mathbb{Z} \to \mathbb{N}$ définie par

  $$n \mapsto |n|$$

  est surjective.
- L'application $f : \mathbb{R}^3 \to \mathbb{R}^2$ définie par

  $$(x, y, z) \mapsto (x, y)$$

  est surjective.

Remarques :

- Pour montrer qu'une application $f : E \to F$ est surjective, on se donne un élément quelconque y de F et on montre qu'il a au moins un antécédent dans E, c'est-à-dire on montre qu'il existe $x \in E$, avec

$$f(x) = y.$$

- Toute application est surjective de son ensemble de définition **sur son image**.
- Le changement de l'ensembles d'arrivée d'une application peut modifier la propriété d'être surjective. Par exemple :
  - L'application f de $\mathbb{R}$ dans $\mathbb{R}_+$ définie par $f(x) = x^2$ **est** surjective.
  - L'application f de $\mathbb{R}$ dans $\mathbb{R}$ définie par $f(x) = x^2$ **n'est pas** surjective.

Injections-Surjections-Bijections

Étudions certaines propriétés des fonctions surjectives.

Proposition

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

- *Si f et g sont surjectives, alors $g \circ f$ est surjective.*
- *Si $g \circ f$ est surjective, alors g est surjective.*

Démonstration.

- **Montrons que $g \circ f$ est surjective**. Soit $y \in G$. Nous voulons montrer qu'il existe $x \in E$ tel que $y = g \circ f(x)$. Or g **est surjective**, donc il exist $t \in F$ tel que

$$y = g(t).$$

Mais f est aussi surjective, donc : $t = f(x)$ pour un certain $x \in E$. Finalement, comme voulu :

$$y = g(t) = g(f(x)) = g \circ f(x).$$

□

Démonstration.

- Montrons que g est surjective. Soit $y \in G$. Nous voulons montrer qu'il existe $x \in F$ tel que $y = g(x)$. Or $g \circ f$ **est surjective**, donc :

$$y = g \circ f(t)$$

pour un certain $t \in E$. Il suffit dès lors de poser :

$$x = f(t) \text{ pour avoir } y = g(x).$$

Définition (Bijection)

Soit $f : E \to F$ une application. On dit que f est une application **bijective** *(ou encore une* **bijection***) si*

$$\forall y \in F, \quad \exists! x \in E, \quad y = f(x).$$

Autrement dit, f est bijective de E sur F si et seulement si tout élément de F possède **un et un seul antécédent** *dans E par f.*

Proposition

Soit f une application d'un ensemble E dans un ensemble F. Alors

$$f \text{ est } \textbf{bijective} \iff f \text{ est } \textbf{injective} \text{ et } \textbf{surjective}$$

Remarque : Pour montrer qu'une application $f : E \to F$ est bijective, on pourra raisonner en deux étapes en montrant l'injectivité et la surjectivité de f.

Exemples :

- Soit $m \in \mathbb{R}^{\times}$. Alors toute application affine de la forme

$$x \longmapsto mx + n$$

est bijective.

- L'application

$$x \longmapsto x^3$$

est bijective.

- On sait que l'application

$$f : \mathbb{R} \to \mathbb{R}$$
$$x \mapsto x^2$$

n'est ni injective, ni surjective. Or si on restreint l'ensemble de depart de f à $\mathbb{R}_+$, et on modifie l'ensemble d'arrivée de $\mathbb{R}$ à $\mathbb{R}_+$, on obtient que la fonction

$$g : \mathbb{R}_+ \to \mathbb{R}_+$$
$$x \mapsto x^2$$

est bijective. **Le changement de l'ensembles de départ et d'arrivée d'une application peut modifier la propriété d'être bijective.**

Définition (Bijection Réciproque)

Soit $f : E \to F$ une application. On appelle **réciproque** *de f toute application $g : F \to E$ pour laquelle*

$$g \circ f = Id_E \quad \text{et} \quad f \circ g = Id_F.$$

Remarque : Les identités : $\forall x \in E,\ g \circ f(x) = x$ et $\forall y \in F,\ f \circ g(y) = y$ expriment l'idée que g défait le travail que f opère et vice versa.

Théorème

Soit $f : E \to F$ une application. Alors

f est bijective de E sur F si et seulement si f possède une réciproque.

Une telle réciproque est alors **unique**, *appelée* **la réciproque de** *f et notée f^{-1}. Pour tous $x \in E$ et $y \in F$ on a*

$$f^{-1}(y) = x \quad \Longleftrightarrow \quad y = f(x).$$

Remarque : Si $f : E \to F$ est une application bijective. Alors son application réciproque f^{-1} est l'unique application de F dans E, qui à tout élément de F associe son unique antécédent par f. C'est-à-dire

$$\begin{array}{rccl} f^{-1} : F & \longrightarrow & E & \\ y & \longmapsto & f^{-1}(y) & = \text{ l'unique antécédent de } y \text{ par } f. \end{array}$$

Exemples :

- L'application Id_E est bijective de E sur E de réciproque elle-même. En effet
$$\mathrm{Id}_E \circ \mathrm{Id}_E = \mathrm{Id}_E.$$
- Soient $a \in \mathbb{R}^*$ et $b \in \mathbb{R}$. La fonction
$$x \mapsto ax + b$$
est bijective. Pour trouver sa réciproque, notons que
$$y = ax + b \quad \Longleftrightarrow \quad \frac{y-b}{a} = x.$$
Par conséquent, la réciproque de $ax + b$ est la fonction définie par
$$y \longmapsto \frac{y-b}{a}.$$

Injections-Surjections-Bijections

Étudions certaines propriétés des fonctions bijectives.

Proposition

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

- *Si $g \circ f$ est bijective, alors f est injective et g est surjective.*
- *Si f et g sont bijectives, alors $g \circ f$ est bijective et on a*

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

- *Si f est une bijection de E dans F, alors sa bijection réciproque f^{-1} est aussi bijective et :*

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

Injections-Surjections-Bijections

En pratique, comment montrer concrètement qu'une application $f : E \to F$ est bijective ? Le tableau suivant, résume la marche à suivre.

Priorité	Ce qu'on fait	Ce qu'on obtient
1	Si on connaît spontanément une expression explicite de f^{-1}, on appelle g la fonction en question et on vérifie simplement que : $$g \circ f = \mathrm{Id}_E \quad \text{et} \quad f \circ g = \mathrm{Id}_F.$$	Bijectivité + Réciproque
2	Si on ne connaît pas spontanément f^{-1}, on peut essayer d'en trouver une expression explicite via l'équivalence : $$y = f(x) \iff x = f^{-1}(y).$$	Bijectivité + Réciproque
3	Si on ne se sent pas capable de trouver une expression explicite de f^{-1}, on montre en deux temps que f est à la fois injective et surjective.	Bijective

Injections-Surjections-Bijections

Soit f une application de E sur F. C'est important de ne pas confondre l'application réciproque avec l'image réciproque

$$f^{-1} : \mathscr{P}(F) \longrightarrow \mathscr{P}(E)$$

qui existe même lorsque f n'est pas bijective. Quand l'application est bijective, nous avons la relation suivante entre l'image reciproque de f et l'image directe de f^{-1}.

Proposition

Soit f une bijection de E sur F et B une partie de F. Alors

$$f^{-1}(B) = f^{-1}(B)$$

où

- $f^{-1}(B)$ *à gauche correspond à l'image* **réciproque** *de B par f.*
- $f^{-1}(B)$ *à droite correspond à l'image* **directe** *de B par f^{-1}.*

Les Nombres Complexes

Introduction :

- L'equation
$$x + 2 = 1$$
n'as pas de solution dans $\mathbb{N}$, mais elle en a dans $\mathbb{Z}$, $\ll$ un ensemble plus grand que $\mathbb{N} \gg$.
- L'equation
$$3x = 1$$
n'as pas de solution dans $\mathbb{Z}$, mais elle en a dans $\mathbb{Q}$.
- L'equation
$$x^2 = -1$$
n'a pas de solution dans $\mathbb{R}$.

On va donc construire un ensemble plus grand que $\mathbb{R}$ dans lequel cette équation possède des solutions. On appellera cet ensemble $\mathbb{C}$:

l'ensemble des nombres complexes.

Les Nombres Complexes

On définit un élément particulier de $\mathbb{C}$, note i qui n'est pas réel, tel que

$$i^2 = -1.$$

L'equation $x^2 + 1 = 0$ possède alors 2 solutions

$$\begin{aligned} x^2 + 1 = 0 &\iff x^2 - i^2 = 0 \\ &\iff (x - i)(x + i) = 0 \\ &\iff x = \pm i. \end{aligned}$$

Donnons la définition de l'ensemble des nombres complexes.

Définition

On appelle ensemble des **nombres complexes** *et on note* $\mathbb{C}$*, l'ensemble des nombres de la forme*

$$a + ib \quad \text{où } a \text{ et } b \text{ sont des réels},$$

et où i *est un élément qui vérifie*

$$i^2 = -1.$$

Les Nombres Complexes

Étudions quelques propriétés de l'ensemble des nombres complexes.

Proposition

Soit $z \in \mathbb{C}$. Alors il existe un unique couple $(a, b) \in \mathbb{R}^2$ tel que

$$z = a + ib.$$

Démonstration.

En effet, si (a, b) et (a', b') sont tels que

$$a + ib = z = a' + ib' \quad \Longrightarrow \quad (a - a') = i(b' - b).$$

En élevant au carré, on obtient

$$(a - a')^2 = -(b' - b)^2 \quad \Longrightarrow \quad a = a' \text{ et } b = b'.$$

□

La proposition précédente nous amène à définir.

Définition

Soit $z = a + ib \in \mathbb{C}$. On dit que z a pour **écriture algébrique** *$a + ib$ et on définit :*

- *a sa* **partie réelle** *qu'on notera*
$$\mathrm{Re}(z) = a,$$
- *b sa* **partie imaginaire** *qu'on notera*
$$\mathrm{Im}(z) = b.$$

Remarques :

- Les réels sont exactement les nombres complexes de partie imaginaire nulle, c'est-à-dire
$$\mathbb{R} = \{z \in \mathbb{C} : \ \mathrm{Im}(z) = 0\} \ = \ \{a + 0i : \ a \in \mathbb{R}\} \subset \mathbb{C}.$$
- Un nombre complexe de partie réelle nul est appelé un **imaginaire pur**. L'ensemble des imaginaires pures sera noté $i\mathbb{R}$. C'est-à-dire
$$i\mathbb{R} = \{z \in \mathbb{C} : \ \mathrm{Re}(z) = 0\} \ = \ \{0 + ib : \ b \in \mathbb{R}\} \subset \mathbb{C}.$$

Définition (Égalité entre nombres complexes)

Deux nombres complexes

$$z = a + bi \quad \text{et} \quad z' = a' + ib'$$

sont **égaux** *si et seulement si ils ont* **même partie réelle** *et* **même partie imaginaire** *:*

$$a + ib = a' + ib' \iff \begin{cases} a = a' \\ b = b'. \end{cases}$$

<u>En résumé</u> :

UNE égalité de nombres complexes = DEUX égalités de nombres réels

L'ensemble $\mathbb{C}$ est muni de deux opérations : d'addition et de multiplication qui généralisent celles que nous connaissons sur $\mathbb{R}$.

Définition (Addition sur $\mathbb{C}$)

Pour tous

$$z = a + ib \in \mathbb{C} \quad et \quad z' = a' + ib' \in \mathbb{C},$$

on définit

$$z + z' = (a + a') + i(b + b').$$

Ce qui signifie que

$$\begin{aligned} \mathrm{Re}(z + z') &= \mathrm{Re}(z) + \mathrm{Re}(z') \\ \mathrm{Im}(z + z') &= \mathrm{Im}(z) + \mathrm{Im}(z'). \end{aligned}$$

Définition (Multiplication sur $\mathbb{C}$)

Pour tous

$$z = a + ib \in \mathbb{C} \quad et \quad z' = a' + ib' \in \mathbb{C},$$

on définit

$$z \cdot z' = (aa' - bb') + i\,(ab' + a'b.)\,.$$

Ce qui signifie que

$$\begin{aligned} \mathrm{Re}(zz') &= \mathrm{Re}(z)\mathrm{Re}(z') - \mathrm{Im}(z)\mathrm{Im}(z') \\ \mathrm{Im}(zz') &= \mathrm{Re}(z)\mathrm{Im}(z') + \mathrm{Im}(z)\mathrm{Re}(z'). \end{aligned}$$

Remarque :

- En général :

$$\mathrm{Re}(zz') \neq \mathrm{Re}(z)\mathrm{Re}(z') \quad \text{et} \quad \mathrm{Im}(zz') \neq \mathrm{Im}(z)\mathrm{Im}(z')$$

- En particulier :

$$\mathrm{Re}(z^2) \neq \mathrm{Re}(z)^2 \quad \text{et} \quad \mathrm{Im}(z^2) \neq \mathrm{Im}(z)^2.$$

Définition (Quotient)

Enfin, pour tout $z = x + iy \in \mathbb{C}^\times$ on a

$$\frac{1}{z} = \frac{1}{x+iy} = \frac{x-iy}{x^2+y^2}.$$

Les Nombres Complexes

Donnons un point de vu géometrique à la définition des nombres complexes.

Proposition

L'application

$$\begin{aligned} f : \mathbb{R}^2 &\longrightarrow \mathbb{C} \\ (a, b) &\longmapsto z = a + ib \end{aligned}$$

réalise une bijection de $\mathbb{R}^2$ *sur* $\mathbb{C}$.

Interprétation géométrique de $\mathbb{C}$: Si l'on a fixé un repère permettant de décrire les points du plan par deux coordonnées **cartésiennes**, alors la bijection

$$f : (a, b) \longmapsto z = a + ib,$$

nous permet d'identifier tout nombre complexe z à un point du plan.

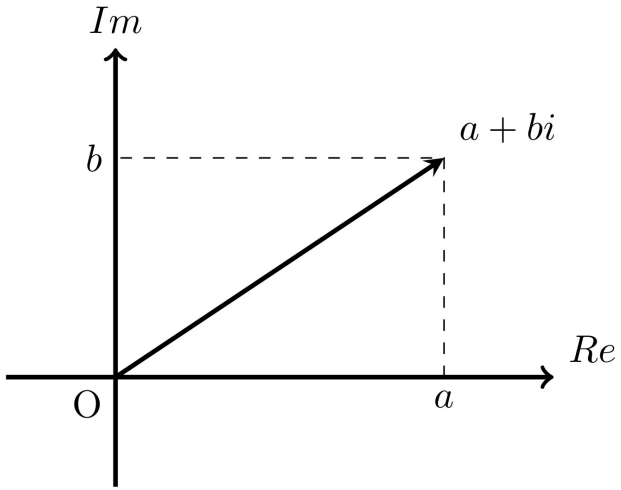
En effet, si z est un nombre complexe et si $z = a + ib$ est son écriture sous forme algébrique, alors le couple $(a, b) \in \mathbb{R}^2$ fournit un moyen de représenter z par un point du plan : on représente z par le point

$$M(z) \text{ d'}\underline{\textbf{abscisse}}\ a \text{ et d'}\underline{\textbf{ordonnée}}\ b.$$

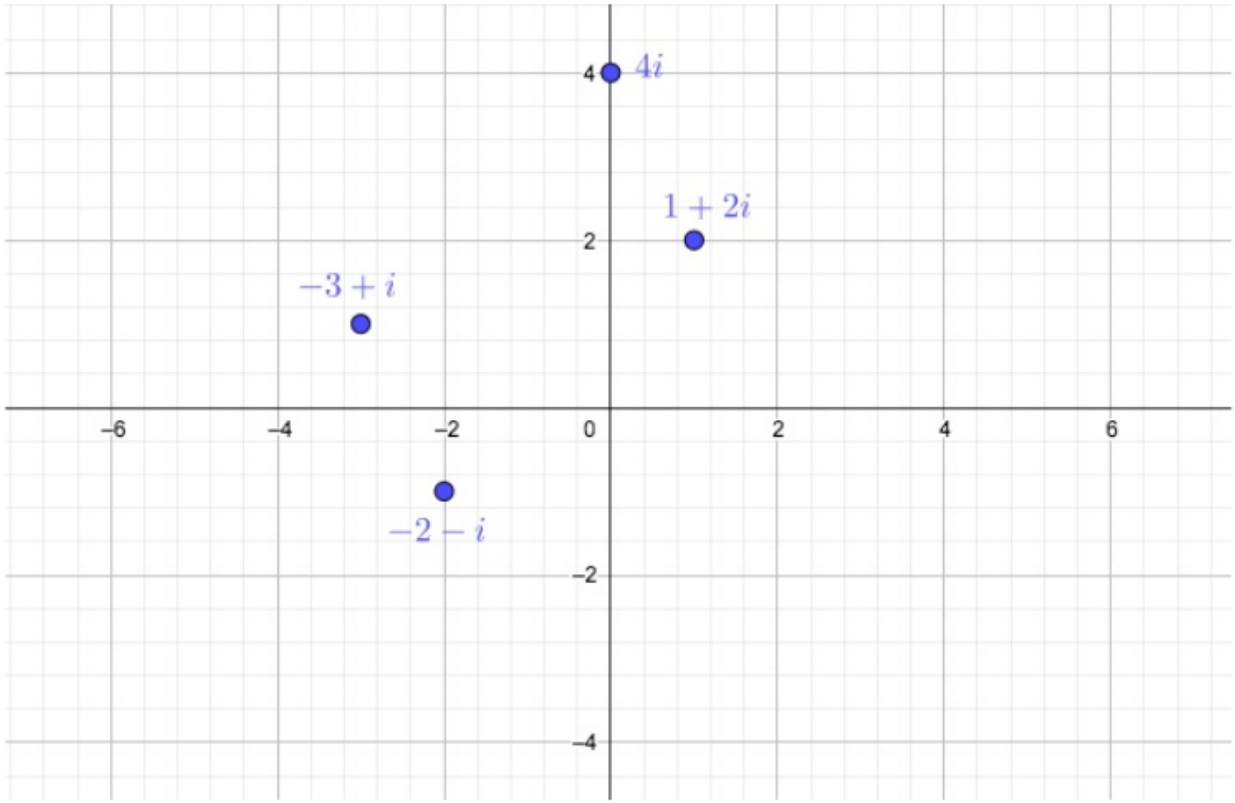
Réciproquement, si M est un point du plan et si (a, b) est le couple de nombres réels donnant son abscisse et son ordonnée dans le repère donné, alors le nombre complexe

$$z = a + ib \text{ est appelé } \underline{\textbf{l'affixe}} \text{ de } M.$$

Graphiquement nous avons :

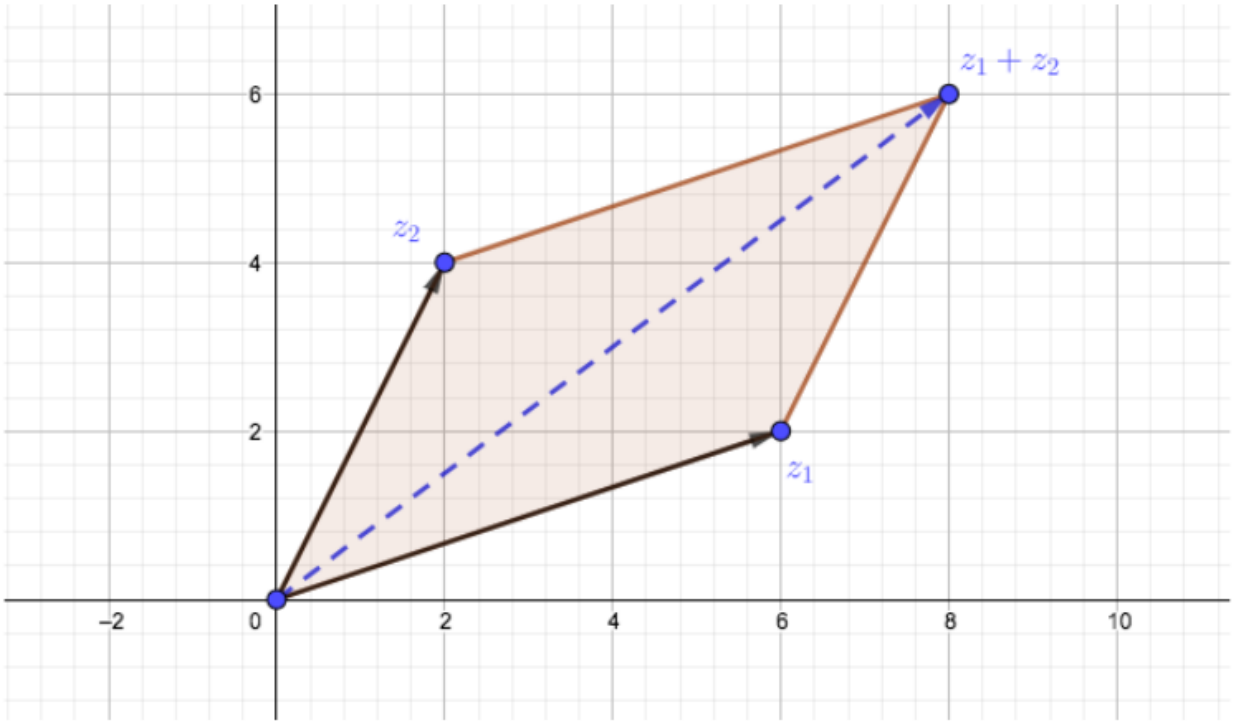


Exemple :



Si $z = a + ib$ est un nombre complexe, on peut le représenter par le point du plan dont les coordonnées cartésiennes sont données par le couple $(a, b) \in \mathbb{R}^2$.

L'addition des nombres complexes admet une interprétation géométrique simple : si z_1 et z_2 sont deux nombres complexes et si l'on note O, M_1, M_2 les points du plan d'affixes respectifs 0, z_1 et z_2, alors le point d'affixe $z_1 + z_2$ se trouve au quatrième sommet du parallélogramme dont les autres sommets sont O, M_1 et M_2.



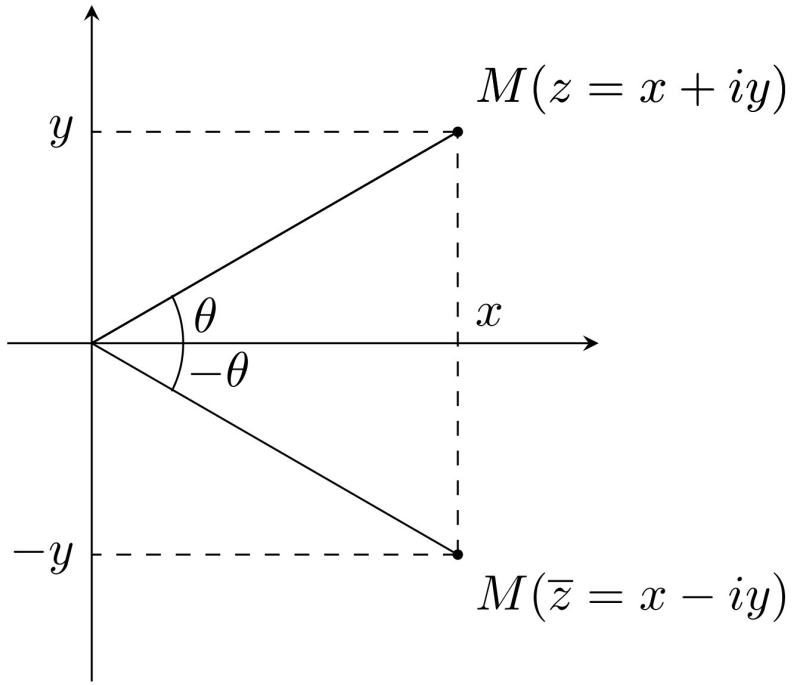
A tout nombre complexe on peut attacher deux notions importants.

Définition (Conjugué)

Soit $z = x + iy \in \mathbb{C}$. On appelle **conjugué** *de z le nombre complexe $\overline{z}$, défini par*

$$\overline{z} = x - iy \quad (i.e. \quad \overline{z} = \mathrm{Re}(z) - i\mathrm{Im}(z)).$$

Remarque : Notons que $\overline{z}$ est l'affixe du vecteur du plan de coordonnées $(x, -y)$:

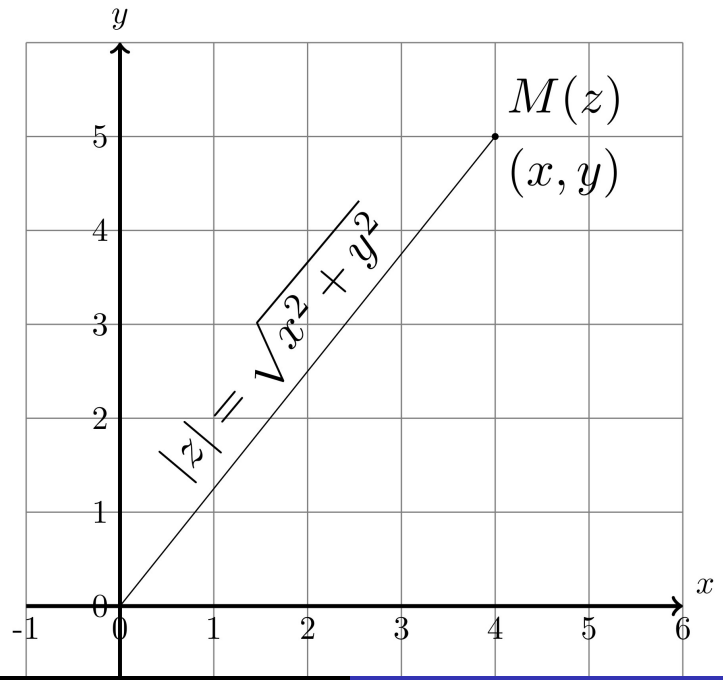


Définition (Module)

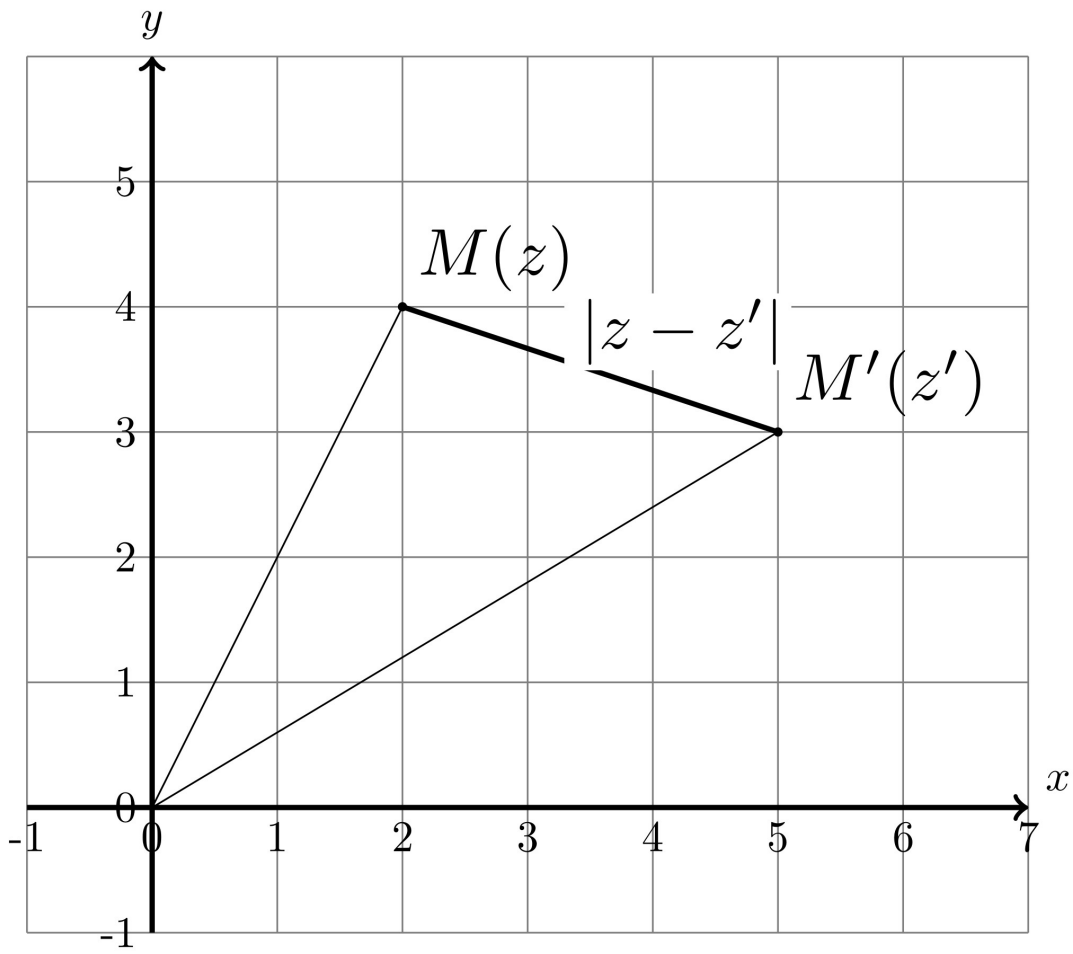
Soit $z = x + iy \in \mathbb{C}$. On appelle **module** *de z le nombre réel positif noté $|z|$ et défini par*

$$|z| = \sqrt{x^2 + y^2} \quad \left(i.e. \quad |z| = \sqrt{\mathrm{Re}^2(z) + \mathrm{Im}^2(z)} \right)$$

Remarque : Le module $|z|$ est égal à la norme du vecteur d'affixe z :



Remarque : Pour tous z, $z' \in \mathbb{C}$ d'images M, M' dans le plan, le module $|z - z'|$ est la distance MM' :



Il en découle que pour tout $R > 0$, nous avons :

- **Le cercle** de centre $a \in \mathbb{C}$ et rayon R est

$$\{z \in \mathbb{C} : |z - a| = R\}.$$

- Le **disque ouvert** de centre $a \in \mathbb{C}$ et rayon R est

$$\{z \in \mathbb{C} : |z - a| < R\}.$$

- Le **disque fermé** de centre $a \in \mathbb{C}$ et rayon R est

$$\{z \in \mathbb{C} : |z - a| \leq R\}.$$

Étudions quelques propriétés du conjugé d'un nombre complexe.

Proposition

Soit $z \in \mathbb{C}$. Alors

- $$\overline{\overline{z}} = z.$$
- $$\mathrm{Re}(z) = \frac{z + \overline{z}}{2}.$$
- $$\mathrm{Im}(z) = \frac{z - \overline{z}}{2i}.$$
- $$z \in \mathbb{R} \iff \overline{z} = z.$$
- $$z \in i\mathbb{R} \iff \overline{z} = -z.$$

Étudions comme le conjugé se comporte par rapport à la somme et le produit de complexes.

Proposition

Pour tous $z, z' \in \mathbb{C}$, nous avons

$$\begin{aligned} \overline{z + z'} &= \overline{z} + \overline{z'} \\ \overline{z \cdot z'} &= \overline{z} \cdot \overline{z'}. \end{aligned}$$

En particulier, si $z' \neq 0$, alors

$$\overline{\left(\frac{z}{z'}\right)} = \frac{\overline{z}}{\overline{z'}},$$

et pour tout $\alpha \in \mathbb{R}$

$$\overline{\alpha z} = \alpha \overline{z}.$$

.

Donnons maintenant certaines propriétes du module.

Proposition

Soient $z, z' \in \mathbb{C}$.

Propriétés algébriques *:*

- $|\overline{z}| = |z|$
- $|zz'| = |z|\,|z'|$, *et si* $z' \neq 0$ *alors*

$$\left|\frac{z}{z'}\right| = \frac{|z|}{|z'|}.$$

Propriétés géométriques *:*

- $|z| = 0 \iff z = 0.$
- $|\mathrm{Re}(z)| \leq |z| \quad$ *et* $\quad |\mathrm{Im}(z)| \leq |z|.$

Remarques :

- Pour tout $z \in \mathbb{C}$ nous avons

$$\begin{aligned} z\overline{z} &= \mathrm{Re}^2(z) + \mathrm{Im}^2(z) \\ &= |z|^2. \end{aligned}$$

- L'inverse de $z = x + iy \in \mathbb{C}^\times$ se calcule donc grâce à la formule

$$z\overline{z} = |z|^2.$$

En effet

$$z\overline{z} = |z|^2 \quad \Longrightarrow \quad \frac{1}{z} = \frac{\overline{z}}{|z|^2} = \frac{x - iy}{x^2 + y^2}.$$

Étudions comme le module se comporte par rapport à la somme et la diffèrence.

Proposition

Soient $z, z' \in \mathbb{C}$.

Inégalité triangulaire :

$$|z + z'| \leq |z| + |z'|.$$

Inégalité triangulaire generalisée (1) :

$$\Big||z| - |z'|\Big| \leq |z + z'| \leq |z| + |z'|.$$

Inégalité triangulaire generalisée (2) :

$$\Big||z| - |z'|\Big| \leq |z - z'| \leq |z| + |z'|.$$

Nombres complexes de module 1

Passons à étudier un important sous-ensemble de $\mathbb{C}$: l'ensemble de nombres complexes de module 1.

Définition

On appelle **cercle trigonométrique** *et on note* $\mathbb{U}$ *l'ensemble des nombres complexes de module* 1 *:*

$$\mathbb{U} = \{z \in \mathbb{C} : \ |z| = 1\}.$$

Remarque : Géometriquement, $\mathbb{U}$ est le circle de centre 0 et rayon 1. En effet,

$$x + iy \in \mathbb{U} \quad \Longleftrightarrow \quad |z| = \sqrt{x^2 + y^2} = 1 \quad \Longleftrightarrow \quad x^2 + y^2 = 1.$$

Nous allons exprimer les éléménts du cercle trigonométrique à l'aide des fonctions cosinus et sinus. Pour cela définissons.

Définition

Soit $\theta \in \mathbb{R}$*, on appelle* **exponetielle** $i\theta$ *le nombre complexe défini par*

$$e^{i\theta} = \cos\theta + i\sin\theta.$$

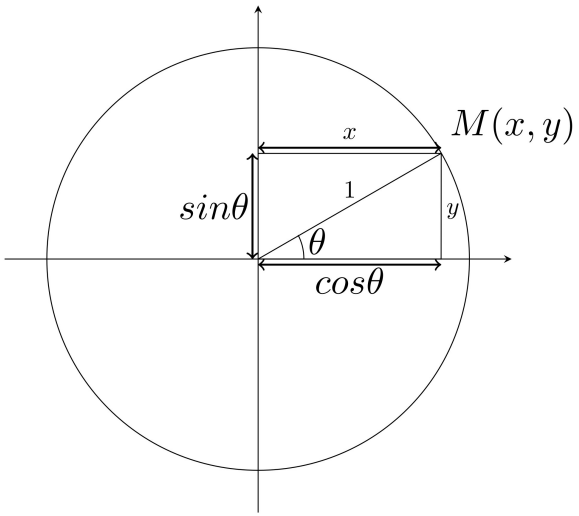
Nombres complexes de module 1

Remarques : Notons que pour tout $\theta \in \mathbb{R}$ on a :

- $$\left|e^{i\theta}\right| = |\cos(\theta) + i\sin\theta| = \sqrt{\cos^2(\theta) + \sin^2(\theta)} = 1.$$

  C'est-à-dire, $\forall \theta \in \mathbb{R},\ e^{i\theta} \in \mathbb{U}$.

- Nous savons que tout point du cercle de **centre** 0 et de **rayon** 1 a des coordonnées de la forme $(\cos(\theta), \sin(\theta)),\ \theta \in \mathbb{R}$. En effet, nous avons



Ainsi, comme pour tout $z = x + iy \in \mathbb{U}$, nous avons $x^2 + y^2 = 1$, nous pouvons écrire

$$\cos(\theta) = x \quad \text{et} \quad \sin(\theta) = y \quad \Longrightarrow \quad z = \cos(\theta) + i\sin(\theta) = e^{i\theta}.$$

Nombres complexes de module 1

Les remarques précédentes nous permettent d'énoncer le résultat suivant.

Théorème

- *Pour tout* $z \in \mathbb{C}$

$$z \in \mathbb{U} \iff \exists\, \theta \in \mathbb{R},\ z = e^{i\theta}.$$

En résumé

$$\mathbb{U} = \{e^{i\theta},\ \theta \in \mathbb{R}\}.$$

- *Pour tous* $\theta \in \mathbb{R},\ \theta' \in \mathbb{R}$ *on a*

$$e^{i\theta} = e^{i\theta'} \iff \left\{ \begin{array}{rcl} \cos(\theta) & = & \cos(\theta') \\ \sin(\theta) & = & \sin(\theta') \end{array} \right\} \iff \theta = \theta' \mod (2\pi).$$

Nombres complexes de module 1

Étudions quelques propriétés de l'exponentielle $i\theta$.

Théorème

Soient $\theta, \theta' \in \mathbb{R}$ et $n \in \mathbb{N}$.

- **Conjugaison :**

$$\overline{e^{i\theta}} = e^{-i\theta} = \frac{1}{e^{i\theta}}$$

- **Formule d'Euler :**

$$\cos(\theta) = \frac{e^{i\theta} + e^{-i\theta}}{2} \quad et \quad \sin(\theta) = \frac{e^{i\theta} - e^{-i\theta}}{2i}.$$

- **Transformation des sommes en produits :**

$$e^{i(\theta+\theta')} = e^{i\theta} \cdot e^{i\theta'}.$$

- **Formule de De Moivre :**

$$(\cos(\theta) + i\sin(\theta))^n = \cos(n\theta) + i\sin(n\theta).$$

Nombres complexes de module 1

Démonstration.

- **Conjugaison :** Pour tout réel $\theta \in \mathbb{R}$, on a

$$\begin{aligned}\overline{e^{i\theta}} = \overline{\cos(\theta) + i\sin(\theta)} &= \cos(\theta) - i\sin(\theta) \\ &= \cos(-\theta) + i\sin(-\theta) \\ &= e^{-i\theta}\end{aligned}$$

- **Formule d'Euler :** Ces formules sont évidentes à partir de la définition de $e^{i\theta}$.

- **Transformation des sommes en produits :** Soit $\theta \in \mathbb{R}$ et $\theta' \in \mathbb{R}$. Alors

$$\begin{aligned}e^{i\theta} \cdot e^{i\theta'} &= (\cos(\theta) + i\sin(\theta))(\cos(\theta') + i\sin(\theta')) \\ &= (\cos(\theta)\cos(\theta') - \sin(\theta)\sin(\theta') + i(\cos(\theta)\sin(\theta') + \sin(\theta)\cos(\theta')) \\ &= \cos(\theta + \theta') + i\sin(\theta + \theta') \\ &= e^{i(\theta+\theta')}.\end{aligned}$$

Démonstration.

- **Formule de De Moivre :** Soit $\theta \in \mathbb{R}$. Alors le point précédent nous permet, grâce à une recurrence simple, de conclure

$$\left(e^{i\theta}\right)^n = e^{in\theta} \implies \begin{aligned} (\cos(\theta) + i\sin(\theta))^n &= (e^{i\theta})^n \\ &= e^{in\theta} \\ &= \cos(n\theta) + i\sin(n\theta). \end{aligned}$$

Applications à la trigonométrie

Étudions quelques applications de l'exponentiele $i\theta$ à la trigonométrie.

Linéarisation des puissances de cosinus et sinus : Linéariser une expression polynomiale de la forme

$$\cos^k(x) \cdot \sin^\ell(x)$$

en $\sin(x)$ et $\cos(x)$, c'est l'exprimer comme une **combinaison lineaire** de

$$\cos(x),\ \cos(2x),\ \cos(3x), \cdots \quad \text{et} \quad \sin(x),\ \sin(2x),\ \sin(3x), \cdots$$

en supprimant toute puissance et tout produit.

Applications à la trigonométrie

Décrivons la méthode avec un exemple : Linéariser $\cos^4(x)\sin^2(x)$. On procède comme suit :

(1) On utilise les formules d'Euler pour changer $\cos(x)$ et $\sin(x)$ en e^{ix} et e^{-ix}.

$$\cos^4(x)\sin^2(x) = \left(\frac{e^{ix}+e^{-ix}}{2}\right)^4 \left(\frac{e^{ix}-e^{-ix}}{2i}\right)^2$$

(2) On développe complètement, avec le binôme de Newton.

$$\begin{aligned}\cos^4(x)\sin^2(x) &= -\frac{1}{64}\left(e^{4ix}+4e^{2ix}+6+4e^{-2ix}+e^{-4ix}\right) \\ &\qquad \cdot \left(e^{2ix}-2+e^{-2ix}\right) \\ &= -\frac{1}{64}\left(e^{6ix}+2e^{4ix}-e^{2ix}-4-e^{-2ix}+2e^{-4ix}+e^{-6ix}\right).\end{aligned}$$

(3) On regroupe les termes deux à deux conjugués pour reconnaître des $\cos(\alpha x)$ ou $\sin(\beta x)$ grâce à la formule d'Euler.

$$\begin{aligned}
\cos^4(x)\sin^2(x) &= -\frac{1}{64}\left(\left(e^{6ix}+e^{-6ix}\right)+2\left(e^{4ix}+e^{-4ix}\right)-\left(e^{2ix}+e^{-2ix}\right)-4\right)\\
&= \frac{1}{32}\left(-\left(\frac{e^{6ix}+e^{-6ix}}{2}\right)-2\left(\frac{e^{4ix}+e^{-4ix}}{2}\right)+\left(\frac{e^{2ix}+e^{-2ix}}{2}\right)\right.\\
&\qquad\qquad\left.+2\right)\\
&= \frac{1}{32}\left(-\cos(6x)-2\cos(4x)+\cos(2x)+2\right).
\end{aligned}$$

Applications à la trigonométrie

Technique de l'angle moitié : Pour factoriser une expression du type

$$e^{ix} + e^{iy} \quad \text{et} \quad e^{ix} - e^{iy}.$$

On procede comme suit :

1. On commence par noter que

$$x = \frac{x+y}{2} + \frac{x-y}{2} \quad \text{et} \quad y = \frac{x+y}{2} - \frac{x-y}{2}.$$

2. Donc

$$\begin{aligned} e^{ix} + e^{iy} &= \left(e^{\frac{i(x+y)}{2}} \cdot e^{\frac{i(x-y)}{2}} + e^{\frac{i(x+y)}{2}} \cdot e^{-\frac{i(x-y)}{2}} \right) \\ &= e^{\frac{i(x+y)}{2}} \left(e^{\frac{i(x-y)}{2}} + e^{-\frac{i(x-y)}{2}} \right) \\ &= 2e^{\frac{i(x+y)}{2}} \cos\left(\frac{x-y}{2} \right). \end{aligned}$$

De même

$$e^{ix} - e^{iy} = e^{\frac{i(x+y)}{2}} \left(e^{\frac{i(x-y)}{2}} - e^{-\frac{i(x-y)}{2}} \right) = 2e^{\frac{i(x+y)}{2}} i \sin\left(\frac{x-y}{2} \right).$$

Applications à la trigonométrie

La **technique de l'angle de l'angle moitié** nous permet de calculer facilement les expressions suivantes :

Proposition

Pour tous $x, y \in \mathbb{R}$

$$\begin{aligned}
\cos(x)+\cos(y) &= 2\cos\left(\frac{x+y}{2}\right)\cos\left(\frac{x-y}{2}\right)\\
\cos(x)-\cos(y) &= -2\sin\left(\frac{x+y}{2}\right)\sin\left(\frac{x-y}{2}\right)\\
\sin(x)+\sin(y) &= 2\sin\left(\frac{x+y}{2}\right)\cos\left(\frac{x-y}{2}\right)\\
\sin(x)-\sin(y) &= 2\cos\left(\frac{x+y}{2}\right)\sin\left(\frac{x-y}{2}\right).
\end{aligned}$$

Applications à la trigonométrie

Exemple : En utilisant que

$$\sin(x) \;=\; \mathrm{Im}(\cos(x) + i\sin(x)) \;=\; \mathrm{Im}(e^{ix})$$

et

$$\sin(y) \;=\; \mathrm{Im}(\cos(y) + i\sin(y)) \;=\; \mathrm{Im}(e^{iy}),$$

on déduit

$$\begin{aligned}\sin(x)+\sin(y) = \mathrm{Im}\left(e^{ix}+e^{iy}\right) &= \mathrm{Im}\left(2e^{\frac{i(x+y)}{2}}\cos\left(\frac{x-y}{2}\right)\right)\\ &= 2\sin\left(\frac{x+y}{2}\right)\cos\left(\frac{x-y}{2}\right).\end{aligned}$$

Applications à la trigonométrie

Comme l'on vient de voir dans la proposition précédente, l'une des avantages de la forme exponentielle est qu'elle permet de faire très facilement des calculs de trigonométrie. Ainsi vous pouvez très facilement démontrer les formules suivantes.

Théorème

1. $\cos(x+y) = \cos(x)\cos(y) - \sin(x)\sin(y)$.
2. $\sin(x+y) = \sin(x)\cos(y) + \cos(x)\sin(y)$.
3. $\tan(x+y) = \frac{\tan(x)+\tan(y)}{1-tan(x)tan(y)}$.
4. $\cos(x) = \frac{1-\tan^2\left(\frac{x}{2}\right)}{1+\tan^2\left(\frac{x}{2}\right)}$.
5. $\sin(x) = \frac{2\tan^2\left(\frac{x}{2}\right)}{1+\tan^2\left(\frac{x}{2}\right)}$.
6. $\tan(x) = \frac{2\tan^2\left(\frac{x}{2}\right)}{1-\tan^2\left(\frac{x}{2}\right)}$.

Forme Trigonométrique d'un nombre complexe

L'exponentielle $i\theta$ nous offre une autre manière d'exprimer tout nombre complexe. Soit $z \in \mathbb{C}$ avec $z \neq 0$. Notons que si on compute le module de $\frac{z}{|z|}$ on obtient

$$\left|\frac{z}{|z|}\right| = \left|z \cdot \frac{1}{|z|}\right| = |z| \cdot \left|\frac{1}{|z|}\right| = |z| \cdot \frac{1}{|z|} = \frac{|z|}{|z|} = 1.$$

Donc pour tout $z \in \mathbb{C}$ avec $z \neq 0$, nous avons

$$\frac{z}{|z|} \in \mathbb{U} \quad \Longrightarrow \quad \exists \theta \in \mathbb{R},\ \frac{z}{|z|} = e^{i\theta}.$$

Par conséquent, tout nombre complexe peut être écrit sous la forme

$$z = |z| \cdot e^{i\theta}.$$

Forme Trigonométrique d'un nombre complexe

Résumons ce que vient d'être dite dans le théorème suivant :

Théorème

Tout nombre complexe **non nul** *peut être écrit sous la forme :*

$$z = re^{i\theta} \quad \text{avec} \quad r \in \mathbb{R}_+^* \quad \text{et} \quad \theta \in \mathbb{R}.$$

Cette forme est dite **trigonométrique**.

- *Le réel r est unique car : $r = |z|$. En effet*

$$|z| = |re^{i\theta}| = |r| \cdot |e^{i\theta}| = |r|.$$

- *Mais θ, appelé* **UN argument** *de z, et note $\arg(z)$, est* **seulement unique à 2π près**. *En revanche, il existe un et un seul argument de z dans $]-\pi, \pi]$, et celui ci est appelé l'***argument principal** *de z.*

- *Le couple (r, θ) est aussi appelé* **UN** *couple de* **coordonnées polaires** *du point d'image z.*

Forme Trigonométrique d'un nombre complexe

Remarques :

- Zéro n'a pas de forme trigonométrique, donc pas d'arguments. Un peu plus de détails, l'égalité
$$0 = |0|e^{i\theta}$$
est vérifiée par tous les nombres réels θ ; il n'est donc pas raisonnable de parler d'argument du nombre complexe 0 (sinon, la cohérence imposerait que tout nombre réel soit un argument de 0).

- Un nombre complexe non nul admet toujours une infinité d'arguments différents.

- Pour tout $z \in \mathbb{C}^*$, $z' \in \mathbb{C}^*$, nous avons
$$z = z' \iff \begin{cases} |z| = |z|' \\ \arg(z) = \arg(z') \mod (2\pi). \end{cases}$$

Forme Trigonométrique d'un nombre complexe

Exemple : Les formes trigonométriques des réels et des imaginaires pur sont :

- **Cas des réels :** Pour tout $x \in \mathbb{R}^*$, nous avons

$$x = \begin{cases} xe^{i0} & \text{si } x > 0, \\ (-x)e^{i\pi} & \text{si } x < 0. \end{cases}$$

- **Cas des imaginaires purs :** Pour tout $y \in \mathbb{R}^*$, nous avons

$$iy = \begin{cases} ye^{i\frac{\pi}{2}} & \text{si } y > 0, \\ (-y)e^{-i\frac{\pi}{2}} & \text{si } y < 0. \end{cases}$$

Forme Trigonométrique d'un nombre complexe

Étudions quelques propriétés des arguments.

Proposition (Propriétés des arguments)

Pour tous $z \in \mathbb{C}^*$, $z' \in \mathbb{C}^*$, nous avons

- $$\arg(zz') = \arg(z) + \arg(z') \mod(2\pi).$$
- $$\arg(\overline{z}) = -\arg(z) \mod(2\pi).$$
- $$\arg\left(\frac{1}{z}\right) = -\arg(z) \mod(2\pi).$$

Démonstration.

- $\arg(zz') = \arg(z) + \arg(z') \mod(2\pi)$: Nous avons

$$zz' = |z| \cdot e^{i \arg(z)} |z'| \cdot e^{i \arg(z')} = |zz'| \cdot e^{i(\arg(z)+\arg(z'))}.$$

D'où on conclut que $\arg(zz') = \arg(z) + \arg(z') \mod (2\pi)$.

- $\arg(\overline{z}) = -\arg(z) \mod(2\pi)$: Nous avons

$$\overline{z} = \overline{|z| \cdot e^{i \arg(z)}} = \overline{|z|} \cdot \overline{e^{i \arg(z)}} = |z| \cdot e^{-i \arg(z)} = |\overline{z}| \cdot e^{-i \arg(z)}.$$

D'où on conclut que $\arg(\overline{z}) = -\arg(z) \mod (2\pi)$.

- $\arg\left(\frac{1}{z}\right) = -\arg(z) \mod(2\pi)$: Nous avons

$$\frac{1}{z} = \frac{1}{|z| \cdot e^{i \arg(z)}} = \frac{1}{|z|} \cdot e^{-i \arg(z)}.$$

D'où on conclut que $\arg\left(\frac{1}{z}\right) = -\arg(z) \mod (2\pi)$.

Forme Trigonométrique d'un nombre complexe

Soit $z \in \mathbb{C}$. Nous avons deux façon d'exprimer z :

- **Forme Algébrique** : $z = x + iy$.
- **Forme Trigonométrique** : $z = re^{i\theta}$.

Étudions le lien qui existe entre ces deux écritures.

Théorème (Lien entre la forme algébrique et les formes trigonométriques)

Soit $z \in \mathbb{C}^*$ de

forme algébrique : $z = x + iy$ *et de* **forme trigonométrique :** $z = re^{i\theta}$.

1. *Forme algébrique en fonction d'une forme trigonométrique :*

$$x = r\cos(\theta) \quad et \quad y = r\sin(\theta).$$

2. *Forme trigonométrique en fonction d'une forme algébrique :*

$$r = \sqrt{x^2 + y^2} \quad et \quad \theta = \begin{cases} \arctan\left(\frac{y}{x}\right) & \mod(2\pi) \quad si\ x > 0, \\ \arctan\left(\frac{y}{x}\right) + \pi & \mod(2\pi) \quad si\ x < 0. \end{cases}$$

Équations du second degré à coefficients complexes

Passons maintenant à étudier quelques équations polynomiales dans $\mathbb{C}$. Commençons par étudier les **equations de degré deux**. Notre objectif est de montrer que toute équation de la forme

$$az^2 + bz + c = 0, \quad a \in \mathbb{C}^\times,\ b,\ c \in \mathbb{C}$$

possède des solutions sur $\mathbb{C}$.

Définition (Racines carrées d'un nombre complexe)

On appelle racine carrée d'un nombre complexe z tout nombre complexe ω vérifiant

$$\omega^2 = z.$$

Théorème

Pour tout $z \in \mathbb{C}^*$, l'équation d'inconnu $\omega \in \mathbb{C}$:

$$\omega^2 = z,$$

possède exactement **deux solutions opposées**.

Démonstration.

On commence par écrire z sous forme trigonométrique

$$z = re^{i\theta},\ r \in \mathbb{R}_+,\ \theta \in \mathbb{R}.$$

Posons

$$\zeta = \sqrt{r}e^{\frac{i\theta}{2}} \quad \Longrightarrow \quad \zeta^2 = z.$$

Nous disposons ainsi d'**un exemple** de racine carrée de z, et grâce à lui, nous allons trouver toutes les solutions de l'équation

$$\omega^2 = z.$$

□

Démonstration.

Nous avons

$$\begin{aligned}
\omega^2 = z &\iff \omega^2 = \zeta^2 \\
&\iff \omega^2 - \zeta^2 = 0 \\
&\iff (\omega - \zeta)(\omega + \zeta) = 0 \\
&\iff \omega = \zeta \quad \text{ou} \quad \omega = -\zeta \\
&\iff \omega = \sqrt{r}e^{i\frac{\theta}{2}} \quad \text{ou} \quad \omega = -\sqrt{r}e^{i\frac{\theta}{2}} \\
&\iff \omega = \sqrt{r}e^{i\frac{\theta}{2}} \quad \text{ou} \quad \omega = \sqrt{r}e^{i\left(\frac{\theta}{2}+\pi\right)}.
\end{aligned}$$

On a donc le résultat voulu. □

Équations du second degré à coefficients complexes

Attention :

- $\sqrt{x}$ est une notation **autorisée** si $x \in \mathbb{R}_+$.
- $\sqrt{z}$ est une notation **interdite** si $z \in \mathbb{C} \setminus \mathbb{R}_+$.

Pourquoi cet interdit ? Parce que nous ne savons pas choisir, tout nombre complexe non nul possède

deux racines carrées distinctes

qui se valent, l'une l'autre. Il n'y a que dans le cas des réels positifs qu'on sait choisir, car les racines carrées d'un réel positif x sont toutes les deux réelles, l'une positive, l'autre négative, et on choisit de noter $\sqrt{x}$ la première.

Équations du second degré à coefficients complexes

De la preuve du théorème précédent, on sait que si la forme trigonométrique de z est

$$z = re^{i\theta},$$

alors les deux racines carrés de z, sont

$$\sqrt{r}e^{i\frac{\theta}{2}} \quad \text{et} \quad \sqrt{r}e^{i\left(\frac{\theta}{2}+\pi\right)}.$$

Le problème c'est que, très souvent il est très difficil de déterminer la forme trigonométrique d'un complexe. Dans ce cas, pour trouver les racines carrés il nous faut travailler avec l'écriture **algebrique** du nombre complexe.

Équations du second degré à coefficients complexes

Pour déterminer l'écriture algébrique des racines carrées, on procèdera comme suit : **Décrivons la méthode avec un exemple : Calculer les racines carrés de**

$$24 + 10i.$$

(1) On cherche les racines de $z = a + ib$, sous la forme

$$w = x + iy.$$

L'équation $w^2 = z$ donne le système

$$w^2 = z \iff (x^2 - y^2) + i(2xy) = a + ib \iff \begin{cases} x^2 - y^2 = a, \\ 2xy = b. \end{cases}$$

en identifiant parties réelle et imaginaire. **Dans notre exemple** :

$$w^2 = 24+10i \iff (x^2-y^2) + i(2xy) = 24+i10 \iff \begin{cases} x^2 - y^2 = 24, \\ 2xy = 10. \end{cases}$$

Équations du second degré à coefficients complexes

(2) On pensera systématiquement à ajouter l'équation

$$|w|^2 = |z| \quad \Longleftrightarrow \quad x^2 + y^2 = \sqrt{a^2 + b^2}$$

pour trouver les valeurs de x^2 et y^2. **Dans notre exemple** :

$$|w|^2 = |24 + 10i| \quad \Longleftrightarrow \quad x^2 + y^2 = \sqrt{24^2 + 10^2} = 26.$$

Nous avons donc trois equations :

$$\begin{cases} x^2 + y^2 = 26, \\ x^2 - y^2 = 24, \\ 2xy = 10. \end{cases} \quad \Longrightarrow \quad \begin{cases} x^2 = 25, \\ y^2 = 1, \\ xy = 5. \end{cases}$$

(3) On prend ensuite les racines carrées, en faisant attention aux signes relatifs de x et y, donné par l'équation $2xy = b$.
Dans notre exemple nous avons donc les solutions :

$$(x, y) = (5, 1) \quad \text{ou} \quad (x, y) = (-5, -1) \quad \Longleftrightarrow \quad w = 5+i \quad \text{ou } w = -5-i.$$

Équations du second degré à coefficients complexes

Maintenant que on a montré que tout nombre complexe possède exactement deux racines carrées, nous pouvons donner la preuve de que toute équation de degré 2 possède des solutions dans $\mathbb{C}$.

Théorème

Soient a, b et c trois nombres complexes avec $a \neq 0$. Alors les solutions de l'equation d'inconnu $z \in \mathbb{C}$:

$$az^2 + bz + c = 0$$

sont

$$\frac{-b+\delta}{2a} \quad \text{et} \quad \frac{-b-\delta}{2a},$$

où δ est l'une quelconque des deux racines carrées du discriminant

$$\Delta = b^2 - 4ac.$$

Démonstration.

Nous avons

$$\begin{aligned} az^2+bz+c &= a\left(z^2+\frac{b}{a}z+\frac{c}{a}\right) \\ &= a\left(\left(z+\frac{b}{2a}\right)^2-\frac{b^2-4ac}{4a^2}\right). \end{aligned}$$

Soit δ l'une de deux racines carrés de b^2-4ac. Alors

$$\frac{b^2-4ac}{4a^2}=\left(\frac{\delta}{2a}\right)^2.$$

Ce qui nous permet d'écrire

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

Démonstration.

Ainsi

$$\begin{aligned} az^2+bz+c &= a\left(\left(z+\frac{b}{2a}\right)^2-\left(\frac{\delta}{2a}\right)^2\right) \quad \left(x^2-y^2=(x+y)(x-y)\right) \\ &= a\left(\left(z+\frac{b}{2a}\right)+\frac{\delta}{2a}\right)\cdot\left(\left(z+\frac{b}{2a}\right)-\frac{\delta}{2a}\right) \\ &= a\left(z-\left(\frac{-b-\delta}{2a}\right)\right)\cdot\left(z-\left(\frac{-b+\delta}{2a}\right)\right). \end{aligned}$$

Les racines de az^2+bz+c sont donc

$$\frac{-b-\delta}{2a} \quad \text{et} \quad \frac{-b+\delta}{2a}$$

Équations du second degré à coefficients complexes

En lien avec ce qui précède, la relation triviale :

$$(z-x)(z-y) \quad = \quad z^2-(x+y)z+xy$$

nous permet de calculer x et y quand on connaît leur somme $x+y$ et leur produit xy.

Théorème (Systèmes somme-produit)

Soient b, $c \in \mathbb{C}$.Les solutions du système somme-produit d'inconnues $x, y \in \mathbb{C}$

$$\begin{cases} x+y=b \\ xy=c \end{cases}$$

sont les deux racines du polynôme z^2-bz+c (éventuellement égales).

Remarque : La somme des solutions de az^2+bz+c vaut $\frac{-b}{a}$ et leur produit $\frac{c}{a}$.

Racine n-ième

Nous avons décrit les racines carrées de tout complexe non nul z. Faisons le même avec les racines de degré n. Pour tout $z \in \mathbb{C}$ et $n \in \mathbb{N}^{\times}$, nous allons donc étudier l'equation :

$$\zeta^n = z.$$

Commençons avec le cas $z = 1$.

Définition (Racines n-ièmes de l'unité)

Soit $n \in \mathbb{N}^*$. On appelle **racines n-ièmes de l'unité** *tout nombre complexe ζ tel que*

$$1 = \zeta^n.$$

On noté $\mathbb{U}_n$ l'ensemble de **racines n-ièmes de l'unité**.

Le résultat suivant nous donne une déscription de l'ensemble de **racines n-ièmes de l'unité**.

Théorème

Soit $n \in \mathbb{N}^*$. Alors il existe exactement n racines n-ièmes de l'unité, qui sont

$$\mathbb{U}_n = \left\{ e^{\frac{2ik\pi}{n}} : \quad 0 \leq k \leq n-1 \right\}.$$

Racine n-ième

Démonstration.

Soit $\zeta \in \mathbb{C}^\times$. Posons

$$r = |\zeta|$$

et notons θ l'unique argument de ζ dans l'intervalle $[0, 2\pi[$. Par identification de formes trigonométriques, on déduit

$$\begin{aligned}
\zeta^n = 1 \quad &\iff \quad r^n \cdot e^{in\theta} = 1 \cdot e^{i\cdot 0} \\
&\iff \quad r^n = 1 \quad \text{et} \quad n\theta = 0 \mod (2\pi) \\
&\underbrace{\iff}_{r>0} \quad r = 1 \quad \text{et} \quad \exists k \in \mathbb{Z},\ n\theta = 2k\pi \\
&\iff \quad r = 1 \quad \text{et} \quad \exists k \in \mathbb{Z},\ \theta = (2k\pi)/n \\
&\underbrace{\iff}_{\theta \in [0,2\pi[} \quad r = 1 \quad \text{et} \quad \exists k \in \mathbb{Z},\ 0 \leq k \leq n-1,\ \theta = (2k\pi)/n.
\end{aligned}$$

Ainsi, ζ est une **racine n-ième de l'unité** si et seulement si

$$\exists k \in \mathbb{Z},\ 0 \leq k \leq n-1, \text{ tel que } \zeta = e^{\frac{2ik\pi}{n}}$$

.

Démonstration.

Ceci nous fait bien un total de n racines distinctes, car les nombres

$$0,\ \frac{2\pi}{n},\ \frac{4\pi}{n},\ \frac{6\pi}{n},\cdots,\ \frac{2(n-1)\pi}{n}$$

sont distincts et éléments de $[0, 2\pi[$, donc les nombres complexes

$$1,\ e^{\frac{2i\pi}{n}},\ e^{\frac{4i\pi}{n}},\ e^{\frac{6i\pi}{n}},\cdots,\ e^{\frac{2(n-1)i\pi}{n}}$$

sont distincts aussi. □

Racines n-ième

Les racines de l'unité satisfont la propriété suivante.

Proposition

Soit n un entier naturel supérieur ou égal à 2. La somme des racines n-ième de l'unité est égale è 0. Autrement dit, sot ζ une racine n-ième de l'unité différente de 1, alors

$$1 + \zeta + \zeta^2 + \cdots + \zeta^{n-1} = 0.$$

Un exemple important, est celui de l'ensemble des racines cubiques de l'unité.

Définition (Le nombre j)

On note j la **racine cubique de l'unité**

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

Quelques relations à connaître

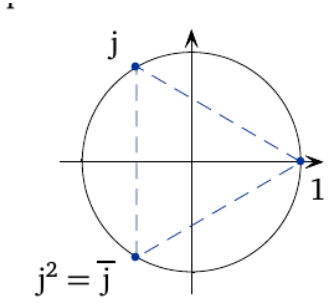
$$j^3 = 1, \quad \overline{j} = j^2, \quad 1 + j + j^2 = 0,$$

et pour tout $z \in \mathbb{C}$

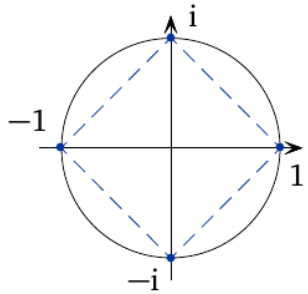
$$z^2 + z + 1 = (z - j)(z - \overline{j}).$$

Racines n-ième

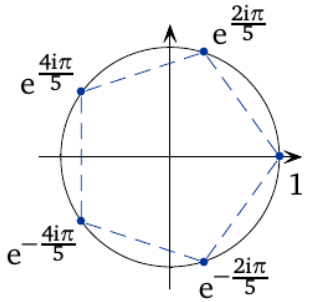
Visualisation géométrique des racines de la unité : Soit $n \geq 3$. Les éléménts dans $\mathbb{U}_n$ définissent les sommets d'un polygone régulier à n côtés.



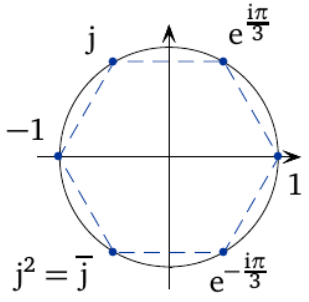
$\mathbb{U}_3$ est l'ensemble des sommets d'un triangle équilatéral.



$\mathbb{U}_4$ est l'ensemble des sommets d'un carré.



$\mathbb{U}_5$ est l'ensemble des sommets d'un pentagone régulier.



$\mathbb{U}_6$ est l'ensemble des sommets d'un hexagone régulier.

Racines n-ième

Étudions maintenant les racines n-ième de tout nombre complexe non nul.

Définition (Racines n-ièmes)

Soit $n \in \mathbb{N}^\times$ et $z \in \mathbb{C}$ non nul. On appelle **racine n-ième** *de z tout nombre complexe ζ tel que*

$$z = \zeta^n.$$

L'ensemble de **racines n-ièmes** de z sont décrit dans le résultat suivant.

Théorème

Soit $n \in \mathbb{N}^\times$.

1. *La seule racine n-ième de 0 est 0. (En effet, $\zeta^n = 0 \iff \zeta = 0$.)*
2. *Tout nombre complexe $z = re^{i\theta} \in \mathbb{C}^*$ avec $r > 0$ et $\theta \in \mathbb{R}$ possède exactement n racines n-ièmes, à savoir :*

$$\sqrt[n]{r} \cdot e^{\frac{i\theta}{n} + \frac{2ik\pi}{n}} \quad 0 \leq k \leq n-1$$

Racines n-ième

Démonstration.

Soit $z = re^{i\theta} \in \mathbb{C}^*$ avec $r > 0$ et $\theta \in \mathbb{R}$. Posons

$$\zeta = \sqrt[n]{r} e^{\frac{i\theta}{n}} \quad \Longrightarrow \quad \zeta^n = z.$$

Nous disposons ainsi d'**un exemple** de racine n-ème de z, et grâce à lui, nous allons les trouver toutes. Pour tout $\omega \in \mathbb{C}$:

$$\begin{aligned}
\omega^n = z \quad &\Longleftrightarrow \quad \omega^n = \zeta^n \\
&\Longleftrightarrow \quad \left(\frac{\omega}{\zeta}\right)^n = 1 \\
&\Longleftrightarrow \quad \exists k \in \mathbb{Z},\ 0 \leq k \leq n-1,\ \text{tel que } \frac{\omega}{\zeta} = e^{\frac{2ik\pi}{n}} \\
&\Longleftrightarrow \quad \exists k \in \mathbb{Z},\ 0 \leq k \leq n-1,\ \text{tel que } \omega = \zeta \cdot e^{\frac{2ik\pi}{n}}.
\end{aligned}$$

Ainsi, $\omega^n = z$ si et seulement si

$$\exists k \in \mathbb{Z},\ 0 \leq k \leq n-1,\ \text{tel que } \omega = \sqrt[n]{r} \cdot e^{\frac{i\theta}{n} + \frac{2ik\pi}{n}}.$$

Ce qui montre le résultat. □

Exponentielle complexe

Nous avons défini la fonction exponentielle sur les nombres complexes de la forme $i\theta,\ \theta \in \mathbb{R}$. Étendons sa définition à tout nombre complexe.

Définition

Pour tout $z \in \mathbb{C}$, on appelle **exponentielle complexe** *de z le nombre complexe défini sous forme trigonométrique*

$$e^z = e^{\mathrm{Re}(z)} \cdot e^{i\mathrm{Im}(z)}.$$

En d'autres termes

$$|e^z| = e^{\mathrm{Re}(z)}$$

et

$$\arg(e^z) = \mathrm{Im}(z) \mod 2\pi.$$

Exponentielle complexe

Donnons quelques propriétés de la fonction exponentielle.

Proposition

1. **Périodicité :** *L'exponentielle complexe est $2i\pi$-périodique, i.e. pour tout $z \in \mathbb{C}$*

$$e^z = e^{z'} \iff z = z' \mod 2i\pi.$$

2. **Transformation des sommes en produits :** *Pour tous $z \in \mathbb{C}^*$, $z' \in \mathbb{C}^*$ nous avons*

$$e^{z+z'} = e^z \cdot e^{z'}.$$

Remarque : Faites attention au « i » dans l'equation

$$e^z = e^{z'} \iff z = z' \ \mathbf{mod}\ \ 2\mathrm{i}\pi.$$

Démonstration.

1. **Périodicité :** Simple identification de formes trigonométriques :

$$\begin{aligned}
e^z = e^{z'} &\iff e^{\mathrm{Re}(z)} \cdot e^{i\mathrm{Im}(z)} = e^{\mathrm{Re}(z')} \cdot e^{i\mathrm{Im}(z')} \\
&\iff e^{\mathrm{Re}(z)} = e^{\mathrm{Re}(z')} \quad \text{et} \quad e^{i\mathrm{Im}(z)} = e^{i\mathrm{Im}(z')} \\
&\iff \mathrm{Re}(z) = \mathrm{Re}(z') \quad \text{et} \quad \mathrm{Im}(z) = \mathrm{Im}(z') \mod (2\pi) \\
&\iff z = z' \mod (2i\pi).
\end{aligned}$$

2. **Transformation des sommes en produits :** Nous avons

$$\begin{aligned}
e^{z+z'} &= e^{\mathrm{Re}(z+z')} \cdot e^{i\mathrm{Im}(z+z')} \\
&= e^{\mathrm{Re}(z)+\mathrm{Re}(z')} \cdot e^{i\mathrm{Im}(z)+i\mathrm{Im}(z')} \\
&= e^{\mathrm{Re}(z)} \cdot e^{\mathrm{Re}(z')} \cdot e^{i\mathrm{Im}(z)} \cdot e^{i\mathrm{Im}(z')} \\
&= e^{\mathrm{Re}(z)} \cdot e^{i\mathrm{Im}(z')} \cdot e^{\mathrm{Re}(z')} \cdot e^{i\mathrm{Im}(z)} \\
&= e^z \cdot e^{z'}.
\end{aligned}$$

Une dernière remarque géométrique

Finissons cet chapitre avec quelques remarques supplementaires sur la géometrie du plan complexe.

- L'**addition** de deux nombres complexes s'interprète géométriquement en termes de **translation** : En effet soit $u \in \mathbb{C}$. Alors la application

$$\begin{aligned} t_u : \mathbb{C} &\longrightarrow \mathbb{C} \\ z &\longmapsto z + u. \end{aligned}$$

  correspond géométriquement à la **translation** de vecteur $\vec{u}$.

Une dernière remarque géométrique

- La application

$$\begin{aligned} S_O : \mathbb{C} &\longrightarrow \mathbb{C} \\ z &\longmapsto -z. \end{aligned}$$

  correspond, géométriquement, à la **symétrie** de centre O.
- La application

$$\begin{aligned} S_x : \mathbb{C} &\longrightarrow \mathbb{C} \\ z &\longmapsto \overline{z}. \end{aligned}$$

  correspond, géométriquement, à la **symétrie** d'axe O_x.
- La application

$$\begin{aligned} S_y : \mathbb{C} &\longrightarrow \mathbb{C} \\ z &\longmapsto -\overline{z}. \end{aligned}$$

  correspond, géométriquement, à la **symétrie** d'axe O_y.

Une dernière remarque géométrique

Le **produit** de deux nombres complexes s'interprète géométriquement en termes d'**homothétie** et de **rotation**. En effet :

- Soit $\lambda \in \mathbb{R}$. Alors la application

$$H_\lambda : \mathbb{C} \longrightarrow \mathbb{C}$$
$$z \longmapsto \lambda z.$$

  correspond, géométriquement, à l'**homothétie** de centre O et de rapport λ.

- Soit $\theta \in \mathbb{R}$. Alors la application

$$R_\theta : \mathbb{C} \longrightarrow \mathbb{C}$$
$$z \longmapsto e^{i\theta} z.$$

  correspond, géométriquement, à la **rotation** de centre O et d'angle θ.

- Soit $\omega = \rho e^{i\theta}$. Alors la application

$$HR_\omega : \mathbb{C} \longrightarrow \mathbb{C}$$
$$z \longmapsto \rho e^{i\theta} z.$$

  correspond, géométriquement, à la composée d'une **rotation** de centre O et d'angle θ avec une **homothétie** de centre O et de rapport ρ.

Polynômes

- **Polynômes**
  - Définition.
  - Opérations sur les polynômes.
  - Degré d'un polynôme.
  - Divisibilité dans l'ensemble des polynômes.
- **Racines d'un polynôme**
  - Evaluation polynômiale
  - Racines d'un polynôme
- **Décomposition en facteurs irréductibles**

Note : Dans ce chapitre nous travaillerons à la fois sur $\mathbb{R}$ et sur $\mathbb{C}$. Afin d'alléger l'écriture, nous utiliserons la lettre $\mathbb{K}$ pour désigner $\mathbb{R}$ ou $\mathbb{C}$. Ainsi une propriété ou une définition qui est valable à la fois sur $\mathbb{R}$ et sur $\mathbb{C}$ sera énoncée sur $\mathbb{K}$.

Définition (Scalaire)

On appelle **scalaire** *un élément de* $\mathbb{K}$.

Définition (Polynôme)

On appelle **polynôme** *P d'indéterminée X* **à coefficients dans** $\mathbb{K}$ *toute expression de la forme*

$$\begin{aligned} P(X) &= a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \\ &= \sum_{k=0}^{n} a_k X^k. \end{aligned}$$

où

- $n \in \mathbb{N}$, *et*
- $a_0, a_1, \cdots, a_n$ *sont des éléments de* $\mathbb{K}$. *On les appelle les* **coefficients du polynôme** P.

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

Remarque : X **N'EST PAS UN NOMBRE !** L'objet X est un objet mathématique bien précis que l'on appelle indéterminée. Ce n'est ni une valeur ni une variable.

Polynômes

Donnons quelques exemples de polynômes.

Définition

On appelle :

- **Polynôme constant :** *Tout polynôme de la forme* $P(X) = a_0$ *avec* $a_0 \in \mathbb{K}$.
- **Polynôme unité** *: Le polynôme* $P(X) = 1$.
- **Polynôme nul** *: Le polynôme* $P(X) = 0$.
- **Monôme :** *Tout polynôme de la forme*

$$P(X) = a_k X^k, \ a_k \in \mathbb{K}.$$

Théorème (Égalité entre polynômes)

Deux polynômes sont **égaux** *si et seulement si leurs coefficients sont égaux. C'est-à-dire*

$$\sum_{k=0}^{n} a_k X^k = \sum_{k=0}^{m} b_k X^k \quad \Longleftrightarrow \quad m = n \ \text{ et } \ a_k = b_k, \ \forall k \in \mathbb{N}, \ 0 \leq k \leq n.$$

En particulier, un polynôme est nul si et seulement si tous ses coefficients sont nuls.

Remarque : Notons que, si

$$P = \sum_{k=0}^{n} a_k X^k,$$

alors pour tout $m > n$, on convient d'écrire

$$P = \sum_{k=0}^{m} a_k X^k,$$

en posant $a_k = 0$ pour $k = n+1, \ n+2, \ \cdots \ , \ m$.

Polynômes

Sur l'ensemble de polynômes nous pouvons définir une **addition** et une **multiplication**.

Définition (Addition-Multiplication)

Soient

$$P(X) = \sum_{k=0}^{n} a_k X^k \quad et \quad Q(X) = \sum_{k=0}^{m} b_k X^k$$

deux polynômes à coefficients dans $\mathbb{K}$.

- **Somme :** *On définit le polynome* $P + Q$ *par*

$$(P+Q)(X) = \sum_{k=0}^{\max(m,n)} (a_k + b_k) X^k.$$

en convenant que $a_k = 0$ *si* $k > n$ *et* $b_k = 0$ *si* $k > m$.

- **Produit :** *On définit le polynome* $P \cdot Q$ *par*

$$(P \cdot Q)(X) = \sum_{k=0}^{m+n} c_k X^k \quad où \quad c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

en convenant que $a_k = 0$ *si* $k > n$ *et* $b_k = 0$ *si* $k > m$.

Définition (Multiplication par un scalaire)

Soit

$$P(X) = \sum_{k=0}^{n} a_k X^k$$

un polynôme à coefficients dans $\mathbb{K}$ *et* $\lambda \in \mathbb{K}$.

- **Multiplication par** λ *: On définit le polynome* λP *par*

$$(\lambda P)(X) \ = \ \sum_{k=0}^{n} \lambda a_k X^k.$$

Exemple : Considérons les polynômes

$$P(X) = 1 - 2X - X^3 \quad \text{et} \quad Q(X) = 1 + X^2.$$

Alors

$$\begin{aligned} (P+Q)(X) &= 2 - 2X + X^2 - X^3. \\ (P \cdot Q)(X) &= 1 - 2X + X^2 - 3X^3 - X^5. \\ \forall \lambda \in \mathbb{K},\ \lambda P(x) &= \lambda - 2\lambda X - \lambda X^3. \end{aligned}$$

Sur l'ensemble de pôlynomes nous pouvons définir aussi la composition.

Définition (Composition)

Soient

$$P(X) = \sum_{k=0}^{n} a_k X^k \quad et \quad Q(X) = \sum_{k=0}^{m} b_k X^k$$

deux polynômes à coefficients dans $\mathbb{K}$.

- **Composée de deux polynômes :** *On définit le polynôme composé* $P \circ Q$ *par*

$$(P \circ Q)(X) = \sum_{k=0}^{n} a_k Q(X)^k.$$

Exemple :

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

Polynômes

Étudions quelques propriétés de l'addition :

Théorème

L'addition dans $\mathbb{K}[X]$ *est :*

- **associative** *: Pour tout polynôme* $P, Q, R \in \mathbb{K}[X]$*, nous avons*

$$(P + Q) + R = P + (Q + R);$$

- **commutative** *: Pour tout polynôme* $P, Q \in \mathbb{K}[X]$*, nous avons*

$$P + Q = Q + P;$$

- **admet pour élément neutre le polynôme nul** *: Pour tout polynôme* $P \in \mathbb{K}[X]$*, nous avons*

$$0 + P = P + 0 = P.$$

Démonstration.

À vous de vérifier. □

Polynômes

Étudions quelques propriétés du produit :

Théorème

Le produit dans $\mathbb{K}[X]$ *est :*

- **associative** *: Pour tout polynôme* $P, Q, R \in \mathbb{K}[X]$

$$(P \cdot Q) \cdot R \;=\; P \cdot (Q \cdot R);$$

- **commutative** *: Pour tout polynôme* $P, Q \in \mathbb{K}[X]$

$$P \cdot Q \;=\; Q \cdot P;$$

- **admet pour élément neutre le polynôme unité** *: Pour tout polynôme* $P \in \mathbb{K}[X]$

$$1 \cdot P \;=\; P \cdot 1 \;=\; P.$$

Démonstration.

À vous de vérifier. □

Degré d'un polynôme

Attaché à chaque polynôme on a l'important notion de degré.

Définition (Degré d'un polynôme)

Soit

$$P = \sum_{k=0}^{n} a_k X^k$$

un polynôme non nul de $\mathbb{K}[X]$. *On appelle* **degré du polynôme** P *le plus grand entier* k *tel que*

$$a_k \neq 0.$$

On note cet entier $\deg(P)$ *et on dit que :*

- a_k *est le* **coefficient dominant** *de* P. *Autrement dit, le* **coefficient dominant**, *est le coefficient du monôme de plus haut degré de* $P(X)$.
- P *est* **unitaire** *(ou normalisé) si son* **coefficient dominant** *est égal à 1.*

Remarque : Par convention, le polynôme nul est de degré $-\infty$:

$$deg(0) = -\infty.$$

Degré d'un polynôme

Exemple :

- $X^{1515} - 1$ est un polynome unitaire, de degré 1515.
- $3X^5 + 2X^4 - 2x + 1$ est un polynome de degré 5 , de coefficient dominant 3.
- $5 + 17X + 30X^4 + 6X^7$ est un polynome de degré 7, de coefficient dominant 6.

Le degré d'un polynôme satisfait les propriétés suivants.

Théorème

Soient $P(X)$ et $Q(X)$ deux polynômes à coefficients dans $\mathbb{K}$. Alors

- $\deg(P + Q) \leq \max(\deg(P); \deg(Q))$.
- $\deg(P \cdot Q) = deg(P) + deg(Q)$.
- *Pour tout* $\lambda \in \mathbb{K}^*$, $deg(\lambda P) = deg(P)$.
- *Si* $\deg(Q) \geq 1$, $deg(P \circ Q) = \deg(P) \cdot \deg(Q)$.

Démonstration.

Soient

$$P(X) = \sum_{k=0}^{n} a_k X^k \quad \text{et} \quad Q(X) = \sum_{k=0}^{m} b_k X^k$$

avec $a_n \neq 0$ et $b_m \neq 0$. Alors

$$\deg P = n \quad \text{et} \quad \deg Q = m$$

(on vérifiera sans difficulté que toutes ses propriétés restent vrais dans le cas où l'un des 2 polynomes est nul).

- $\deg(\mathrm{P} + \mathrm{Q}) \leq \max(\deg(\mathrm{P}), \deg(\mathrm{Q}))$: Pour tout $k > \max(m, n)$, on a

$$a_k = b_k = 0 \quad \Longrightarrow \quad a_k + b_k = 0.$$

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

Démonstration.

- $\deg(\mathrm{P} \cdot \mathrm{Q}) = \deg(\mathrm{P}) + \deg(\mathrm{Q})$: Le terme de plus haut degré de $P \cdot Q$ est

$$(a_n \cdot b_m)X^{n+m}.$$

Ainsi $\deg(P \cdot Q) = m + n$.

- Si $\deg(\mathrm{Q}) \geq 1$, $\deg(\mathrm{P} \circ \mathrm{Q}) = \deg(\mathrm{P}) \cdot \deg(\mathrm{Q})$: Supposons $\deg(Q) \geq 1$. On a par définition

$$P \circ Q(X) = a_0 + a_1 Q(X) + \cdots + a_n Q(X)^n.$$

Maintenant, le point précédent nous permet de conclure que pour tout $0 \leq k \leq n$, on a

$$\deg(Q^k) \ = \ k \deg(Q).$$

Ainsi, le terme de plus haut degré de $P \circ Q$ est $a_n Q(X)^n$. D'où on conclut

$$\deg(P \circ Q) \ = \ \deg(a_n Q(X)^n) \ = \ n \cdot deg(Q) \ = \ \deg(P) \cdot \deg(Q).$$

Degré d'un polynôme

Exemple où $\deg(P+Q) < \max(\deg P, \deg Q)$: Soit

$$P = X^3 - X + 2 \quad \text{et} \quad Q = -X^3 + X^2.$$

Alors

$$(P+Q)(X) = X^2 - X + 2 \implies \begin{aligned} \deg(P+Q) &= 2 \\ &< 3 = \max(\deg P, \deg Q). \end{aligned}$$

Remarque : Si $\deg(P) \neq \deg(Q)$, alors

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

Degré d'un polynôme

En utilisant les propriétés du degré, on peut facilement montrer la proposition suivant.

Proposition

Le produit de deux polynomes non nuls est non nul. Autrement dit :

$$\forall\ P, Q \in \mathbb{K}[X], \quad P \cdot Q = 0 \implies P = 0 \quad \textit{ou} \quad Q = 0.$$

Démonstration.

$$\begin{aligned} P \cdot Q = 0 &\implies \deg P + \deg Q = \deg(P \cdot Q) = -\infty \\ &\implies \deg P = -\infty \ \text{ ou } \ \deg Q = -\infty \\ &\implies P = 0 \ \text{ ou } \ Q = 0. \end{aligned}$$

□

Dérivation de Polynômes

Une autre opération que on peut définir sur l'ensemble des polynomes, c'est la dérivation.

Définition (Polynôme dérivé)

Soit

$$P = \sum_{k=0}^{n} a_k X^k$$

un polynôme dans $\mathbb{K}[X]$. *On appelle* **dérivée (formelle)** *du polynôme* P, *le polynôme* P' *défini par*

$$P'(X) = \begin{cases} 0 & \text{si } \deg(P) \leq 0 \\ \sum_{k=1}^{n} k a_k X^{k-1} = a_1 + 2a_2 X + \cdots + n a_n X^{n-1} & \text{si } \deg(P) > 0. \end{cases}$$

On définit par itération les polynômes dérivés successifs de P *par*

$$\begin{aligned} P^{(0)} &= P \\ P^{(k)} &= \left(P^{(k-1)}\right)' \text{ pour tout } k \geq 1. \end{aligned}$$

Dérivation de Polynômes

Exemple : Soit

$$P = 5X^3 + X^2 - 7X + 3.$$

Alors les dérivées succesives de P sont :

$$\begin{aligned} P^{(0)}(X) &= 5X^3 + X^2 - 7X + 3 \\ P^{(1)}(X) &= 15X^2 + 2X - 7 \\ P^{(2)}(X) &= 30X + 2 \\ P^{(3)}(X) &= 30 \\ P^{(k)}(X) &= 0, \quad \forall k \geq 4. \end{aligned}$$

Étudions quelques propriétés de la dérivation.

Proposition

Soit P un polynôme dans $\mathbb{K}[X]$. Alors, si $\deg(P) \geq 1$, on a

$$\deg(P') = \deg(P) - 1.$$

Démonstration.

Cela vient tout simplement de la définition de la dérivée. À vous de vérifier. □

Dérivation de Polynômes

Nous avons aussi le résultat suivant.

Théorème

Soient $P(X)$ et $Q(X)$ deux polynômes à coefficients dans $\mathbb{K}$.

- *On a $P' = 0 \iff P$ est constant.*
- $(P + Q)' = P' + Q'$.
- *Pour tout $\lambda \in \mathbb{K}$, $(\lambda P)' = \lambda P'$.*
- $(P \cdot Q)' = P' \cdot Q + P \cdot Q'$.
- $(P \circ Q)' = Q' \cdot (P' \circ Q)$.

Démonstration.

Cela vient aussi tout simplement des définitions des sommes et produits. À vous de vérifier. □

Dérivation de Polynômes

Un raissonement par récurrence, nous permet de traduire le théoòreme précédent au cas de dérivées d'ordre superieur.

Théorème

Soient $P(X)$ et $Q(X)$ deux polynômes à coefficients dans $\mathbb{K}$.

- *Si* $\deg(P) = n$, *alors*

$$P^{(k)} = 0$$

  pour tout $k > n$.

- *Pour tout* $\lambda,\ \mu \in \mathbb{K}$ *et* $n \in \mathbb{N}$, *nous avons*

$$(\lambda P + \mu Q)^{(k)} = \lambda P^{(k)} + \mu Q^{(k)}.$$

- **Formule de Leibniz** *: Pour tout* $n \in \mathbb{N}$, *nous avons*

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

Divisibilité dans $\mathbb{K}[X]$

L'ensemble des polynômes $\mathbb{K}[X]$ dispose des propriétés similaires de celles de l'ensemble des entiers relatif. Sur $\mathbb{K}[X]$ on peut parler de la notion de divisibilité.

Définition (Divisibilité)

Soient $A, B \in \mathbb{K}[X]$. On dit que A **divise** *B ou que B est un* **multiple** *de A, s'il existe $Q \in \mathbb{K}[X]$, tel que*

$$B = A \cdot Q.$$

Si A **divise** *B on note*

$$A|B.$$

Le polynôme A est appelé **diviseur** *de B et B un* **multiple** *de A.*

Divisibilité dans $\mathbb{K}[X]$

Remarques :

- Un polynôme $P(X)$ non nul est divisible par les polynômes λ et $\lambda P(X)$ avec $\lambda \in \mathbb{K}^*$. En effet, pour tout $\lambda \in \mathbb{K}^*$, nous avons

$$P(X) = \lambda \cdot (\lambda^{-1} P(X)) \quad \text{et} \quad P(X) = (\lambda P(X)) \cdot \lambda^{-1}.$$

- Réciproquement, un polynôme de degré 0 (i.e. polynôme constant et non nul) divise tous les polynômes. En effet, pour tout $\lambda \in \mathbb{K}^*$ et pour tout $P(X) \in \mathbb{K}[X]$, nous avons

$$P(X) = \lambda \cdot (\lambda^{-1} P(X)).$$

- Tout polynôme divise le polynôme nul. En effet, pour tout $P(X) \in \mathbb{K}[X]$, nous avons

$$0 = P(X) \cdot 0.$$

Divisibilité dans $\mathbb{K}[X]$

Étudions quelques propriétés de la division.

Proposition

Soit A, B, C et D des polynômes dans $\mathbb{K}[X]$. On a alors :

- $$D|A \text{ et } D|B \implies D|(P\cdot A + Q\cdot B), \quad \forall P, Q \in \mathbb{K}[X].$$
- $$A|B \text{ et } C|D \implies (A\cdot C)|(B\cdot D).$$
- $$\forall k \in \mathbb{N}, \quad A|B \implies A^k|B^k.$$

Démonstration.

À vous de vérifier. □

Divisibilité dans $\mathbb{K}[X]$

Proposition

Soient $A, B \in \mathbb{K}[X]$ deux polynômes non nuls. Alors :

$$A|B \quad et \quad B|A \quad \Longleftrightarrow \quad \exists \lambda \in \mathbb{K}^*, \quad A = \lambda B$$

On dit alors que A et B sont des **polynômes associés**.

Démonstration.

- $\Longleftarrow$: Immediat
- $\Longrightarrow$: Si $A|B$ et $B|A$, alors il existe $C, D \in \mathbb{K}[X]$ tels que

$$B = A \cdot C \quad \text{et} \quad A = B \cdot D.$$

Ainsi

$$\deg B = \deg A + \deg C \geq \deg A \quad \text{et} \quad \deg A = \deg B + \deg D \geq \deg B.$$

Démonstration.

D'où on conclut

$$\deg A = \deg B \quad \Longrightarrow \quad \deg D = \deg C = 0.$$

Par conséquent, D est un polynome constante et non nul. C'est-à-dire

$$D = \lambda \in \mathbb{K}^*$$

et

$$A = \lambda B.$$

□

Divisibilité dans $\mathbb{K}[X]$

Proposition

Soient $P(X)$ et $Q(X)$ deux polynômes à coefficients dans $\mathbb{K}$. Alors

$$P \cdot Q = 1$$

si et seulement si P et Q sont des constantes inverses l'une de l'autre.

Démonstration.

- $\Longleftarrow$: Immediat.
- $\Longrightarrow$: Si $P \cdot Q = 1$, alors

$$0 = \deg(P \cdot Q) = \deg(P) + \deg(Q) \quad \Longrightarrow \quad \deg(P) = \deg(Q) = 0.$$

D'où on conclut que

$$P = \lambda \quad \text{et} \quad Q = \lambda'.$$

Or $\lambda \cdot \lambda' = 1$. Ce qui implique $\lambda' = \lambda^{-1}$.

Divisibilité dans $\mathbb{K}[X]$

Remarque : Cela veut dire qu'un polynôme non nul n'est pas forcément inversible. Les seuls polynômes inversibles sont les constantes non nulles.

Une autre propriété partagé entre l'ensemble des polynômes et l'ensemble des entiers relatif, est la **division euclidienne**.

Théorème (Division euclidienne)

Soient $A,\ B \in \mathbb{K}[X]$ *tels que* $B \neq 0$. *Alors, il existe un unique couple de polynômes* $(Q, R) \in (\mathbb{K}[X])^2$ *tel que :*

$$A = BQ + R, \quad \deg(R) < \deg(B).$$

Les polynômes Q *et* R *seront alors appelés le* **quotient** *et le* **reste** *dans la division euclidienne de* A *par* B.

Divisibilité dans $\mathbb{K}[X]$

Exemple : Faisons la division euclidienne de $A = 2X^4 - X^3 - 2X^2 + 3X - 1$ par $B = X^2 - X + 1$. Notons que on pose une division de polynômes comme on pose une division euclidienne de deux entiers. En effet

$$
\begin{array}{rrrrrrrrrrr|l}
 & 2X^4 & - & X^3 & - & 2X^2 & + & 3X & - & 1 & X^2 - X + 1 \\
\cline{11-11}
- & 2X^4 & - & 2X^3 & + & 2X^2 & & & & & 2X^2 + X - 3 \\
\cline{1-9}
 & & & X^3 & - & 4X^2 & + & 3X & - & 1 & \\
 & & - & X^3 & - & X^2 & + & X & & & \\
\cline{3-9}
 & & & & & -3X^2 & + & 2X & - & 1 & \\
 & & & & - & -3X^2 & + & 3X & - & 3 & \\
\cline{5-9}
 & & & & & & & -X & + & 2 &
\end{array}
$$

Alors on trouve

$$Q = 2X^2 + X - 3 \text{ (**Quotient**)} \quad \text{et} \quad R = -X + 2 \text{ (**Reste**)}.$$

On n'oublie pas de vérifier qu'effectivement $A = BQ + R$.

Divisibilité dans $\mathbb{K}[X]$

Proposition

Soient $A,\ B \in \mathbb{K}[X]$. *On a*

$$A \text{ divise } B \iff \text{le reste de la division euclidienne de } A \text{ par } B \text{ est nul.}$$

Démonstration.

- $\Longrightarrow$: Si $A|B$, alors il existe Q tel que $B = AQ$. Alors le couple $(Q, 0)$ satisfait la définition de la division euclidienne. Par unicité du reste de la division euclidienne pour les polynômes, on en déduit que ce reste est nul.
- $\Longleftarrow$: Si le reste de la division euclidienne de A par B est nul, on obtient qu'il existe $Q \in \mathbb{K}[X]$ tel que

$$B = AQ + 0 = AQ.$$

Donc on a bien $A|B$.

□

Évaluation polynomiale

Définition (Fonction polynomiale)

Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ *et* $\lambda \in \mathbb{K}$. *Alors on définit*

$$P(\lambda) = \sum_{k=0}^{n} a_k \lambda^k \qquad \text{(on evalue P en } \lambda\text{)}.$$

La fonction

$$\begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{K} \\ x & \longmapsto & P(x), \end{array}$$

est appelée **fonction polynomiale** *associée au polynome* P.

Évaluation polynomiale

L'évaluation polynomiale nous permet d'exprimer les coefficients d'un polynôme à l'aide des dérivées succesives.

Théorème (Formule de Taylor en 0)

Pour tout polynôme $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ *de degré* $n \in \mathbb{N}$, *on a*

$$P(X) = P(0) + P^{(1)}(0)X + \frac{P^{(2)}(0)}{2!}X^2 + \cdots + \frac{P^{(n)}(0)}{n!}X^n$$

Ce qui revient a

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

C'est-à-dire

$$a_k = \frac{P^{(k)}(0)}{k!}.$$

Évaluation polynomiale

Nous pouvons généraliser la formule de Taylor à tout $a \in \mathbb{K}$.

Théorème (Formule de Taylor en $a \in \mathbb{K}$)

Pour tout polynôme $P \in \mathbb{K}[X]$ de degré $n \in \mathbb{N}$ et $a \in \mathbb{K}$, nous avons :

$$P(X) = P(a) + P^{(1)}(a)(X-a) + \frac{P^{(2)}(a)}{2!}(X-a)^2 + \cdots + \frac{P^{(n)}(a)}{n!}(X-a)^n$$

Ce qui revient a

$$P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k.$$

Racines d'un polynôme

Étudions les points oú un polynôme s'annule.

Définition (Racines)

Soit $P \in \mathbb{K}[X]$. On dit que $a \in \mathbb{K}$ est une **racine** *(ou un* **zéro***) de P si*

$$P(a) = 0.$$

Remarques :

- Tout polynôme de degré 1 a une racine : la racine de

$$aX + b \quad \text{est} \quad -\frac{b}{a}.$$

  En effet

$$a \cdot \left(-\frac{b}{a}\right) + b = 0.$$

- L'existence de racines dépend de $\mathbb{K}$: par exemple $X^2 + 1$ n'a pas de racine dans $\mathbb{R}$, mais il a les racines $+i$ et $-i$ dans $\mathbb{C}$.

Racines d'un polynôme

Donnons une characterization des racines d'un polynôme.

Proposition

Soit $\alpha \in \mathbb{K}$ *et* $P \in K[X]$. *Alors*

$$\alpha \text{ est racine de } P \iff (X-\alpha)|P.$$

Démonstration.

On raissone par double implication :

- $\Longleftarrow$: Supposons que $(X-\alpha)|P$, alors il existe $Q \in \mathbb{K}[X]$ tel que

$$P = (X-\alpha)Q(X).$$

Ainsi

$$P(\alpha) = (\alpha-\alpha)Q(\alpha) = 0.$$

□

Démonstration.

- $\Longrightarrow$: Supposons que α soit racine de P, et écrivons la division euclidienne de P par $X - \alpha$:

  il existe $Q,\ R \in \mathbb{K}[X]$ tels que :

  $$P(X) = (X - \alpha)Q(X) + R(X), \qquad \deg(R) < \deg(X - a) = 1.$$

  Ainsi, $\deg(R) \leq 0$ et $R(X) = r \in \mathbb{K}$. On évalue alors l'égalité précédente en α :

  $$0 = P(\alpha) = (\alpha - \alpha)Q(\alpha) + r = r \quad \Longrightarrow \quad r = 0.$$

  Par conséquent, $P(X) = (X - \alpha)Q(X)$ et $(X - \alpha)$ divise P.

Racines d'un polynôme

Exemple : Considérons le polynôme $P = X^3 - X + 6$. On voit que -2 est racine de P :

$$(-2)^3 + 2 + 6 = 0$$

Par la proposition précédente, P se factorise par $(X + 2)$. Pour obtenir sa factorisation, on peut :

- soit écrire $P = (X + 2)(aX^2 + bX + c)$, développer :

$$\begin{aligned} aX^3 + (2a + b)X^2 + (2b + c)X + 2c &= P(X) \\ &= X^3 - X + 6 \end{aligned}$$

  et procéder par identification des coefficients

$$1 = a \quad ; \quad 0 = 2a + b \quad ; \quad -1 = 2b + c \quad ; \quad 6 = 2c$$

- soit faire la division euclidienne de P par $(X + 2)$: le quotient correspond à l'autre facteur de la factorisation.

Racines d'un polynôme

Définition (Ordre de multiplicité)

Soit $P(X) \in \mathbb{K}[X]$ un polynôme non nul et $\alpha \in \mathbb{K}$. On dit que α est une racine **d'ordre** *m (ou de* **multiplicité** *m) de P si :*

- *P* **est divisible** *par $(X-\alpha)^m$, et*
- *P* **n'est pas divisible** *par $(X-\alpha)^{m+1}$.*

Remarque : Puisque $(X-\alpha)^m$ divise $P(X)$ nous avons $m \leq deg(P)$. Donc

$$1 \leq m \leq \deg(P).$$

Racines d'un polynôme

Donnons une caractérisation de l'ordre de multiplicité à l'aide de la dérivation.

Proposition

Soient $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$. On a l'équivalence entre :

- $(X-\alpha)^m$ *divise* P,
- $P(\alpha) = P'(\alpha) = \cdots = P^{(m-1)}(\alpha) = 0$.

Si l'une de ces conditions est satisfaite, on dit alors que α est racine de P de **multiplicité au moins** *m.*

Démonstration.

C'est une conséquence directe de la formule de Taylor. À vous de vérifier. □

Exemple : Considérons $P = X^5 - 7X^4 + 19X^3 - 25X2 + 16X - 4$. On peut vérifier que

$$P(1) = P'(1) = P''(1) = 0.$$

Donc 1 est racine de P de multiplicité au moins 3. Ainsi

$$(X-1)^3 \quad \text{divise} \quad X^5 - 7X^4 + 19X^3 - 25X^2 + 16X - 4.$$

Racines d'un polynôme

Comme corollaire du résultat précédent on a :

Théorème

Soient $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$. Alors α est une racine **de multiplicité** *m de $P(X)$ si et seulement si*

$$P(\alpha) = P'(\alpha) = \cdots = P^{(m-1)}(\alpha) = 0 \quad \text{et} \quad P^{(m)}(\alpha) \neq 0.$$

Démonstration.

Cela découle tout simplement de la définition de la multiplicité d'une racine et de la proposition précédente. □

Vocabulaire :

- Lorsque $m \geq 2$, on parle de racine multiple.
- Les racines d'ordre 1, 2, 3 de P sont respectivement appelés racines simples, doubles, triples de P.

Racines d'un polynôme

Exemple : Considérons toujours $P = X^5 - 7X^4 + 19X^3 - 25X^2 + 16X - 4$. On a

$$P(1) = P'(1) = P''(1) = 0 \quad \text{et} \quad P^{(3)}(1) = 6.$$

Donc 1 est racine de P de multiplicité 3 exactement.

Étudions le nombre possible de racines d'un polynôme.

Proposition

Soit $P \in \mathbb{K}[X]$, et $\alpha_1,\ \alpha_2\ \cdots,\ \alpha_p$, p racines distincts de P. Alors

$$(X - \alpha_1) \cdot (X - \alpha_2) \cdot \ \cdots \ \cdot (X - \alpha_p) \quad \textit{divise} \quad P.$$

Racines d'un polynôme

Comme conséquence de cette proposition, on obtient les deux théorèmes suivants.

Théorème

Un polynôme de degré $n \in \mathbb{N}$ a au plus n racines distinctes.

Démonstration.

Soit P un polynôme et supposons que P admette p racines distinctes $\alpha_1, \cdots, \alpha_p$.

D'après la proposition précédente, il existe alors $Q \in \mathbb{K}[X]$ tel que :

$$P(X) = (X - \alpha_1) \cdot \cdots \cdot (X - \alpha_p) Q(X).$$

En prenant les degrés dans cette égalité, on en déduit que

$$\deg(P) = p + \deg(Q)$$

et donc

$$p \leq \deg(P) = n.$$

□

Racines d'un polynôme

Théorème

Le seul polynôme qui possède une **infinité de racines** *est le polynôme nulle.*

Démonstration.

C'est une conséquence directe de la proposition précédente : si P est non nul, il n'a qu'un nombre fini de racines. □

Racines d'un polynôme

Si on compte les racines avec leur multiplicité alors on a :

Théorème

Soit $P \in \mathbb{K}[X]$, et $\alpha_1, \alpha_2, \cdots, \alpha_p$, p racines distincts de P de multipicité respectives $m_1, m_2, \cdots, m_p$. Alors

$$(X-\alpha_1)^{m_1} \cdot (X-\alpha_2)^{m_2} \cdot \cdots \cdot (X-\alpha_p)^{m_p} \quad \textit{divise} \quad P.$$

Comme conséquence du théorème, on a le résultat suivante.

Corollaire

Un polynôme de degré n a au plus n racines comptées avec leurs ordres de multiplicité.

Décomposition en facteurs irréductibles

Étudions comme un polynome se décompose en produit de polynômes plus simples (i.e. de dégre inférieur)

Définition (Polynôme irréductible)

Soit $P(X) \in \mathbb{K}[X]$. On dit que $P(X)$ est **irréductible**, *s'il satisfait*

- $\deg P \geq 1$.
- *les seuls diviseurs de P sont les polynômes :*

$$\lambda \quad \text{et} \quad \lambda P(X), \quad \text{avec } \lambda \in \mathbb{K}^*.$$

C'est-à-dire, les polynômes constants non nuls et les polynômes associés à $P(X)$.

Autrement dit, $P(X)$ est **irréductible** *sur $\mathbb{K}$ s'il satisfait*

$$A,\ B \in \mathbb{K}[X],\ P(X) = A(X)B(X) \quad \Longrightarrow \quad \deg(A) = 0 \ \text{ ou } \ \deg(B) = 0.$$

Décomposition en facteurs irréductibles

Remarques

- Les polynômes de degré un sont irréductibles.
- Les polynômes irréductibles dans $\mathbb{K}[X]$ jouent le rôle des nombres premiers dans $\mathbb{N}$.

Rappelons que tout élément de $\mathbb{N}$ peut s'écrire comme un produit de nombres premiers, de manière analogue nous pouvons décomposer tout polynome en tant que produit de polynômes irréductibles.

Théorème

Tout polynôme de $\mathbb{K}[X]$ de degré supérieur ou égal à 1, se décompose de manière unique en produit d'une constante non nulle et de polynômes irréductibles unitaires à l'ordre des facteurs près.

Décomposition en facteurs irréductibles

Étudions plus en détail la décomposition d'un polynôme en facteurs irréductibles. Pour cela on définit.

Définition (Polynôme Scindé)

On dit qu'un polynôme $P \in \mathbb{K}[X]$ de degré supérieur ou égal à 1 est **scindé** *s'il peut être écrit comme un produit de polynômes de degré 1 de $\mathbb{K}[X]$.*

Remarque :

- Un polynôme $P \in \mathbb{K}[X]$ est scindé et irréductible sur $\mathbb{K}$ si et seulement si $\deg(P) = 1$.
- Le polynôme $X^2 + 1$ est irréductible sur $\mathbb{R}$ mais scindé sur $\mathbb{C}$ puisqu'il peut s'écrire :

$$X^2 + 1 = (X - i)(X + i).$$

La décomposition d'un polynôme dépend de $\mathbb{K}$. Nous allons donc distinguer les décompositions sur $\mathbb{C}[X]$ et sur $\mathbb{R}[X]$.

Décomposition dans $\mathbb{C}[X]$

Théorème (Théorème de d'Alembert-Gauss)

Tout polynôme non constant de $\mathbb{C}[X]$ possède au moins une racine dans $\mathbb{C}$.

On a la conséquence suivante de ce résultat.

Proposition

Tout polynôme non nul de $\mathbb{C}[X]$ est scindé.

Démonstration.

Montrons par récurrence la propriété :

$$\forall n \in \mathbb{N}^*,\ \mathscr{P}(n) :\ \text{tout polynôme de } \mathbb{C}[X] \text{ de degré } n \text{ est scindé.}$$

- **Initialisation** : Si $\deg P = 1$, alors P est scindé par définition, donc $\mathscr{P}(1)$ est vraie.

Décomposition dans $\mathbb{C}[X]$

Démonstration.

- **Hérédité** : Soit $n \in \mathbb{N}^*$ et supposons $\mathscr{P}(n)$ vraie. Soit P de degré $n+1$. D'après le **Théorème de d'Alembert Gauss**, P admet au moins une racine $\alpha \in \mathbb{C}$. Alors $(X-\alpha)$ divise P et il existe $Q \in \mathbb{K}[X]$, tel que

$$P(X) = (X-\alpha)Q(X).$$

Or $\deg(Q) = n$ et par hypothèse de récurrence, Q est scindé :

$$Q = \lambda(X-\alpha_1)\cdot\cdots\cdot(X-\alpha_n).$$

Ainsi

$$P = \lambda(X-\alpha)(X-\alpha_1)\cdot\cdots\cdot(X-\alpha_n)$$

est scindé, et $\mathscr{P}(n+1)$ est vraie. On conclut par principe de récurrence.

□

Décomposition dans $\mathbb{C}[X]$

Proposition

(1) *Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.*

(2) *Tout polynôme P de $\mathbb{C}[X]$ se factorise de façon unique (à l'ordre près des facteurs) en produit de polynômes irréductibles de $\mathbb{C}[X]$ sous la forme :*

$$P(X) = \lambda(X-\alpha_1)^{m_1} \cdot (X-\alpha_2)^{m_2} \cdot \ \cdots \ \cdot (X-\alpha_k)^{m_k}.$$

Démonstration.

(1) On a déjà vu que les polynômes de degré 1 sont irréductibles. Réciproquement, soit P un polynôme irréductible. Par le **Théorème de d'Alembert Gauss**, il existe α tel que $P(\alpha) = 0$. Ainsi

$$\exists Q \in \mathbb{K}[X], \quad P = (X-a)Q.$$

Comme de plus P est irréductible, on en déduit que $Q \in \mathbb{K}^*$ et que $\deg P = 1$.

(2) Soit P un polynôme de degré superieur ou égal à 1 de $\mathbb{C}[X]$. D'après la proposition précédente, P est **scindé** sur $\mathbb{C}[X]$, d'où l'existence d'une telle factorisation. □

Décomposition dans $\mathbb{R}[X]$

Passons maintenant à la décomposition dans $\mathbb{R}[X]$. Commençons par introduire le résultat suivant :

Lemma

Soit $P(X) \in \mathbb{R}[X]$. Si on considère $P(X)$ comme un polynôme de $\mathbb{C}[X]$ et que $\alpha \in \mathbb{C} \setminus \mathbb{R}$ est une racine de $P(X)$ alors $\overline{\alpha}$ est aussi une racine complexe de $P(X)$ avec même multiplicité.

Démonstration.

Soit $P(X) = \sum_{k=0}^{n} a_k X^k$. Supposons $\alpha \in \mathbb{C} \setminus \mathbb{R}$ est une racine de $P(X)$. Alors

$$0 = P(\alpha) \quad \Longrightarrow \quad 0 = \overline{P(\alpha)}.$$

Maintenant, puisque les coefficient de P sont réels, nous pouvons écrire

$$0 \;=\; \overline{\left(\sum_{k=0}^{n} a_k \alpha^k\right)} \;=\; \sum_{k=0}^{n} \overline{a_k} \cdot \overline{\alpha}^k \;=\; \sum_{k=0}^{n} a_k \overline{\alpha}^k \;=\; P(\overline{\alpha}).$$

Donc $\overline{\alpha}$ est une racine. □

Décomposition dans $\mathbb{R}[X]$

À l'aide du lemme précédent nous pouvons donner la décomposition dans $\mathbb{R}[X]$.

Théorème

1. *Les polynômes irréductibles de $\mathbb{R}[X]$ sont*
   - *les polynômes de degré 1 ;*
   - *les polynômes de degré 2 à* **discriminant strictement négatif**.
2. *Tout polynôme P de $\mathbb{R}[X]$ se factorise de façon unique (à l'ordre près des facteurs) en produit de polynômes irréductibles de $\mathbb{R}[X]$ sous la forme :*

$$P(X) = \lambda \left(\prod_{k=1}^{p} (X - \alpha_k)^{m_k} \right) \left(\prod_{k=1}^{q} (X^2 + \beta_k X + \gamma_k)^{n_k} \right).$$

Somme et produit des racines d'un polynôme

On finit le chapitre avec le résultat suivant.

Proposition (Somme et produit des racines d'un polynôme scindé)

Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ *un polynôme scindé,* $\alpha_1,\ \alpha_2\ \cdots,\ \alpha_n$, *ses racines (distinctes ou non). Alors*

$$\begin{aligned} \alpha_1 + \alpha_2 + \cdots + \alpha_n &= -\frac{a_{n-1}}{a_n}. \\ \alpha_1 \cdot \alpha_2 \cdot \ \cdots \ \cdot \alpha_n &= (-1)^n \frac{a_0}{a_n}. \end{aligned}$$

Remarque : En particulier, pour $n = 2$ et $P(X) = c + bX + aX^2$, nous avons :

$$\begin{aligned} \alpha_1 + \alpha_2 &= -\frac{b}{a} \\ \alpha_1 \cdot \alpha_2 &= \frac{c}{a} \end{aligned}$$