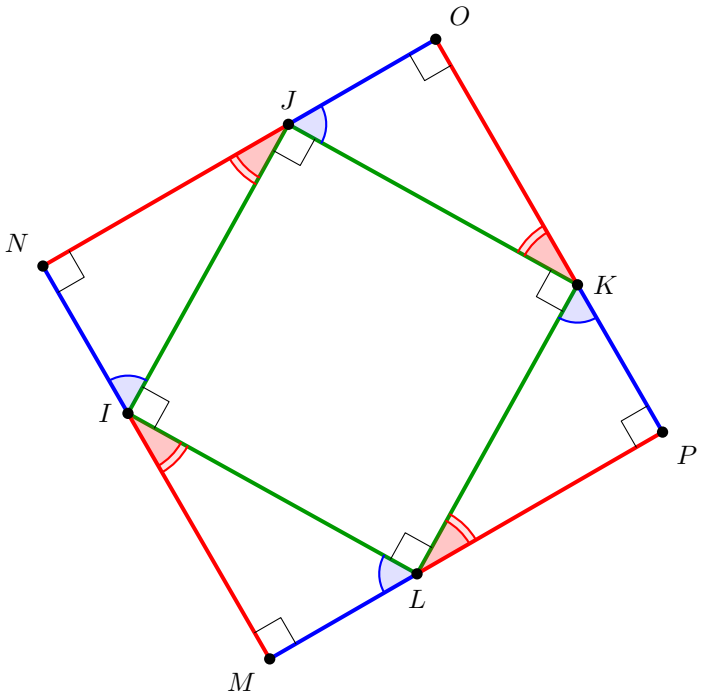
MAT1150

Arithmétique et géométrie classique

Deuxième édition



Christophe Hohlweg

Auteur de l'édition originale

André-Pierre Lamarche

Contribution à la deuxième édition

8 septembre 2026

Université du Québec à Montréal

Table des matières

À propos de cette édition

Le présent manuel constitue une réécriture et une nouvelle édition des notes de cours ***MAT1006 — Arithmétique et géométrie classique***, rédigées par Christophe Hohlweg et diffusées dans leur version du 13 mai 2013 [Hohlweg 2013].

Le contenu original a été réorganisé, reformulé et enrichi de nouvelles figures ainsi que d'explications pédagogiques supplémentaires.

Introduction

La géométrie et l'arithmétique classiques restent, encore à ce jour, incontournables dans une formation mathématique. Premièrement, parce que beaucoup des idées développées depuis la Grèce antique sont toujours d'actualité, mais aussi parce que l'un des meilleurs moyens de s'initier au langage et au raisonnement mathématiques, ainsi qu'à l'algèbre et à la géométrie modernes, consiste à suivre l'évolution des idées mathématiques, depuis la géométrie de l'école pythagoricienne jusqu'au début du XIX^{e} siècle.

Pour couvrir la matière et les notions abordées dans le cours ***MAT1150 - Arithmétique et géométrie classique*** de l'UQAM, il fallait se référer à plusieurs ouvrages de niveau secondaire ou collégial, en français ou en anglais. J'ai ressenti le besoin de fournir aux étudiants de ce cours un seul texte regroupant cours et exercices. C'est ainsi qu'est né ce texte.

Je tiens à remercier tout particulièrement et très chaleureusement Marie-Hélène Descary qui, au mois de mai 2011, a accepté de transcrire en LaTeX les notes et les dessins manuscrits qui constituaient les deux premiers chapitres de ces notes de cours. La présentation des idées de ce manuscrit a été grandement améliorée grâce à ses suggestions et à ses commentaires.

Je tiens aussi à remercier très chaleureusement Catherine Bourbeau, qui a accepté de retravailler et de réviser ce texte durant l'été 2012 afin de rendre cet ouvrage aussi clair et accessible que possible.

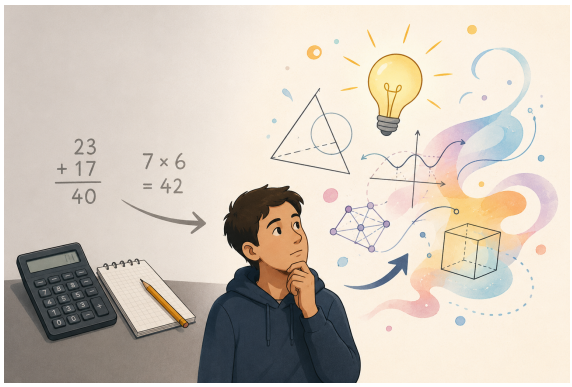
En ce qui concerne la partie arithmétique de ce livre, je suis très reconnaissant à Jacques Labelle et à Christophe Reutenauer de m'avoir autorisé à travailler à partir de leurs notes de cours : ***MAT1000 - Algèbre 1, UQAM (1994)***. Je remercie également très chaleureusement Luc Bélair, Eve Paquette et Christophe Reutenauer d'avoir bien voulu lire très attentivement ce chapitre et de m'avoir suggéré des modifications qui en ont grandement amélioré le contenu.

Christophe Hohlweg, Montréal, étés 2011 et 2012

Chapitre 0

Les bases du raisonnement mathématique

0.1 Pourquoi formaliser la pensée mathématique ?



Pour bien des gens, les mathématiques sont souvent synonymes de calculs ou de chiffres. Nous connaissons tous quelqu'un qui, lorsqu'il faut convertir des degrés Celsius en Fahrenheit, ou encore calculer le rabais d'un article en solde ou estimer la quantité de peinture nécessaire pour repeindre le salon, s'exclame : « Je n'ai jamais été bon en maths ! ».

Ces situations m'ont toujours fait sourire. Il faut bien mal connaître les mathématiques pour les réduire à de simples opérations arithmétiques apprises à la petite école. En réalité, les additions et les multiplications sont aux mathématiques ce que l'orthographe est à la littérature : indispensables, certes, mais bien loin d'en constituer l'essence. Une orthographe impeccable ne suffit pas à écrire un best-seller ; de même, savoir calculer ne suffit pas à « faire des mathématiques ».

Les mathématiques forment avant tout un langage, un outil de communication et un mode de pensée rigoureux. Comme toute langue, elles possèdent leur vocabulaire, leur grammaire et leurs règles de composition. Ce chapitre a pour objectif de présenter les bases de cette communication mathématique : comment formuler une définition, comprendre un théorème, distinguer un lemme d'un corollaire, et surtout, comment enchaîner ces idées dans un raisonnement cohérent.

En apprenant à lire et à écrire dans ce langage, on découvre que la rigueur n'est pas une contrainte, mais un moyen d'exprimer la beauté et la logique cachées derrière les formes les plus simples.

0.1.1 Intuition et démonstration

Bien avant d'être un ensemble de règles et de formules, les mathématiques naissent souvent d'une intuition : une idée que l'on sent vraie, une régularité observée, un motif qui se répète. Par exemple, après avoir remarqué que $2 + 2 = 4$, que $3 + 3 = 6$ et que $4 + 4 = 8$, on est naturellement porté à conclure que « doubler un nombre, c'est toujours le

multiplier par deux ». Cette conclusion intuitive est correcte — mais elle le devient réellement à partir du moment où on peut la justifier pour tous les nombres par un raisonnement logique, et non seulement par quelques exemples.

C'est là toute la différence entre penser que c'est vrai et savoir que c'est vrai. L'intuition, c'est la première étincelle qui éclaire le chemin. La démonstration, c'est la lampe qui nous empêche de nous égarer.

Les grands mathématiciens eux-mêmes s'appuient sur leur intuition — mais ils savent qu'elle peut tromper, et qu'elle doit être validée par un raisonnement rigoureux.

0.1.2 Pourquoi la rigueur est essentielle

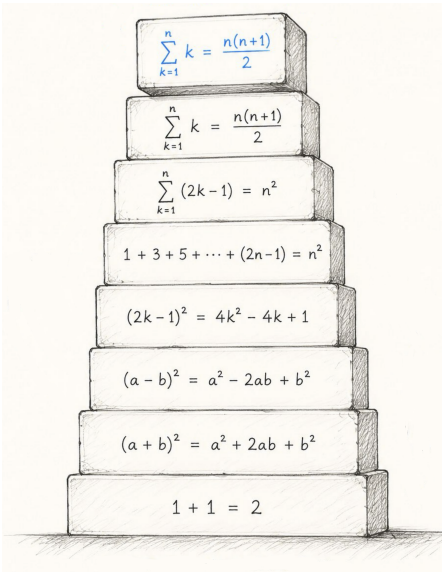
La rigueur n'est pas un luxe réservé aux puristes ; c'est la condition même qui permet aux mathématiques d'exister comme science universelle. Dans la vie courante, une idée peut « sembler vraie » et être acceptée sans preuve. En mathématiques, rien n'est vrai tant qu'on ne l'a pas démontré à partir de définitions et de principes admis.

Cette exigence de rigueur a deux vertus :

- Elle garantit la fiabilité des résultats : un théorème démontré est vrai partout, toujours, pour quiconque raisonne correctement à partir des mêmes hypothèses ;
- Elle permet la construction d'un savoir cumulatif : chaque résultat repose sur les précédents, comme des briques dans un édifice.

Ainsi, la rigueur permet de transformer des idées en connaissances transmissibles. Elle fait des mathématiques une langue commune, où chaque mot et chaque symbole ont un sens précis.

Quand on écrit une démonstration, on ne cherche pas seulement à convaincre autrui : on s'assure que la vérité du résultat ne dépend plus de personne ni d'aucune intuition personnelle.



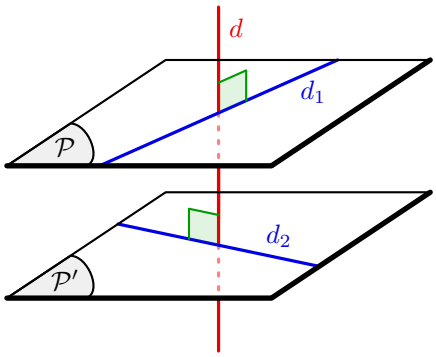
0.1.3 Quand l'intuition se trompe

Considérons l'affirmation suivante :

« Deux droites perpendiculaires à une même droite sont parallèles. »

Dans le **plan**, cette phrase est vraie : si l'on trace une droite d, puis deux droites d_1 et d_2 perpendiculaires à d, alors d_1 et d_2 sont parallèles. En revanche, dès que l'on passe à la **géométrie de l'espace**, l'énoncé devient faux.

Pour s'en convaincre, imaginons une droite d. Plaçons maintenant deux droites dans l'espace, chacune ***perpendiculaire*** à d, mais situées à des « hauteurs » différentes et orientées différemment : on obtient deux droites d_1 et d_2 qui sont toutes deux perpendiculaires à d, sans être parallèles ni sécantes entre elles. On dit alors que d_1 et d_2 sont **gauches**.



Cet exemple illustre que notre intuition, souvent formée dans le plan, ne se transpose pas toujours à l'espace. En géométrie, on ne peut pas se contenter de « ce qui se voit » : il faut s'appuyer sur des définitions précises et des enchaînements logiques.

C'est pour pouvoir exprimer ces idées avec précision que les mathématiques ont développé un langage particulier — fait de définitions, de propositions et de démonstrations. Avant de pouvoir en user, il faut en comprendre la grammaire. C'est ce que nous allons explorer maintenant.

0.2 Énoncés et langage logique

Le but premier d'un langage est de permettre la communication entre individus. Le langage mathématique n'échappe pas à cette règle. Nous allons passer en revue dans cette partie les bases du langage et du raisonnement mathématique. Nous allons illustrer nos propos à l'aide de trois « devinettes » tirées du livre fascinant de R. Smullyan : ***Le livre qui rend fou*** [Smullyan 1997].

Devinette 1

Vous payez 20$ une bouteille de Shiraz. Le vin coûte 19$ de plus que la bouteille. Combien vaut la bouteille ?

Dans un texte mathématique, on structurera généralement la réponse comme suit :

Réponse : La bouteille vaut 50¢.

Afin d'accepter la réponse comme étant vraie, on doit la justifier à l'aide d'une démonstration (aussi appelée preuve) :

Démonstration Le vin coûte 19$ plus le prix de la bouteille (c'est une des hypothèses de départ).

Si on y ajoute le prix de la bouteille, on obtient le prix de la bouteille de Shiraz, soit 20$ (seconde hypothèse de départ réécrite).

Donc le prix total, soit 20$, est composé de 19$ et de deux fois le prix de la bouteille (déduction logique par « implication »). D'où la bouteille vaut la moitié de 1$, soit 50¢ (dernière implication et conclusion).

■

Ainsi, pour répondre correctement à une question (mathématique ou non d'ailleurs), on a besoin d'énoncer clairement la question, puis sa réponse : c'est ***l'introduction*** ; puis on rédige clairement la preuve de ce que l'on vient d'affirmer : ***c'est le plan et le développement du plan***. C'est dans cette dernière partie que l'on utilise un ***raisonnement*** (qui dans l'exemple se compose d'***implications***).

En mathématiques, on travaille avec des propositions — aussi appelées assertions, ou énoncés — qui sont les phrases mathématiques, le tout structuré dans un texte que l'on appelle la preuve ou l'argument. Le tout est lié par le raisonnement. On distinguera dans les pages qui suivent les différents types d'énoncés, puis les différents moyens de montrer une proposition par un raisonnement.

Notre exposé se veut le plus informel possible. L'étude formelle du langage mathématique est l'objet du cours de logique.

0.2.1 Énoncés

Une phrase ayant pour but de définir des objets mathématiques, d'en affirmer les propriétés ou de les introduire s'appelle un ***énoncé***.

Il y a trois types d'énoncés : les ***définitions***, les ***notations*** et les ***propositions***.

0.2.1.1 Définitions

Une ***définition*** introduit un nouveau concept ou précise le sens d'un mot déjà connu. Elle n'affirme rien sur le monde : elle fixe le vocabulaire que l'on utilisera pour raisonner.

Une définition doit être :

- Claire, sans ambiguïté.
- Nécessaire, c'est-à-dire qu'elle introduit une idée qui ne peut être exprimée autrement.
- Utilisable, c'est-à-dire formulée de manière à pouvoir être invoquée dans une démonstration.

Par exemple :

Définition 0.1: (valeur absolue)

Soit x un nombre réel. Le plus grand des nombres x et $-x$ se nomme la ***valeur absolue de*** x.

Ici, on ne démontre rien : on établit simplement une convention de langage.

Une bonne définition doit pouvoir être utilisée sans équivoque dans tout énoncé ultérieur. Voici un exemple d'utilisation de cette définition :

Exemple

Montrons que, pour tout nombre réel x, on a

$$x \leqslant |x|.$$

Par définition, $|x|$ est le plus grand des deux nombres x et $-x$. Il est donc supérieur ou égal à chacun d'eux, en particulier à x. Ainsi, $x \leqslant |x|$.

⚠ **Remarque** Une définition ne peut pas être « vraie » ou « fausse » : elle est adoptée. Ce sont les propositions et théorèmes qui, ensuite, en tireront des conséquences vraies ou fausses.

0.2.1.2 Notations

Un énoncé qui désigne un objet par un symbole est une ***notation***.

Exemple

- Notons $|x|$ la valeur absolue du réel x ;
- Notons $\sqrt{x}$ la racine carrée de x ;
- Notons AB la distance entre les points A et B.

0.2.1.3 Propositions

Un énoncé qui affirme une propriété est une ***proposition***.

Exemple

La valeur absolue d'un nombre réel est toujours positive.

On en arrive à la règle qui va guider tout raisonnement mathématique :

Règle

Une proposition est soit fausse, soit vraie, ***mais pas les deux en même temps !***

Exemple

La proposition $0 < -1$ est fausse, tandis que la proposition $0 > -1$ est vraie.

En mathématiques, on énonce généralement des propositions vraies. Ainsi, si une proposition est fausse, on énonce plutôt sa ***négation***.

0.2.2 Négation, conjonction et disjonction

0.2.2.1 Négation

Pour développer notre intuition, nous allons considérer aussi des énoncés en langage usuel, comme : tous les hommes sont mortels. Ceci posé, la négation de cette proposition est « il existe au moins un homme qui est immortel ».

Notation

Si P est une proposition, on note sa ***négation*** de l'une des façons suivantes :

- non(P)
- $\neg P$

En vertu de la règle énoncée précédemment, il est clair que $\neg(\neg P) = P$.

⚠ **Remarque** la négation, ou contraire, de « ce tableau est noir » est « ce tableau n'est pas noir ». Ce n'est pas « ce tableau est blanc ».

0.2.2.2 Conjonction et disjonction

Étant données deux propositions P et Q, il est souvent nécessaire de les combiner pour former de nouveaux énoncés. Selon le contexte, on peut vouloir que les deux propositions soient vraies simultanément, ou encore qu'il suffise que l'une d'elles soit vraie. Les opérations logiques « et » et « ou » permettent précisément de formaliser ces situations.

Définition 0.2: (conjonction)

Soient P et Q deux propositions. La ***conjonction*** de P et Q, notée $P \wedge Q$ et lue « P et Q », est la proposition qui est vraie si et seulement si P et Q sont toutes deux vraies.

Définition 0.3: (disjonction)

Soient P et Q deux propositions. La ***disjonction*** de P et Q, notée $P \vee Q$ et lue « P ou Q », est la proposition qui est vraie si et seulement si au moins l'une des propositions P et Q est vraie, c'est-à-dire lorsque P est vraie, lorsque Q est vraie, ou lorsque les deux le sont simultanément. Autrement dit, si la proposition $P \vee Q$ est vraie, les propositions P et Q ne peuvent pas être toutes les deux fausses.

0.2.3 Les quantificateurs « pour tout » et « il existe »

Une expression comme « $x^2 \geqslant 0$ » dépend de la valeur attribuée à x. Pour en faire une proposition complète, il faut préciser l'ensemble dans lequel varie x et indiquer si l'affirmation concerne tous ses éléments ou seulement certains d'entre eux.

Définition 0.4: (propositions universelle et existentielle)

Soient E un ensemble et $P(x)$ une propriété qui dépend d'un élément x de E.
Une ***proposition universelle*** affirme que $P(x)$ est vraie pour tout élément x de E. On l'écrit

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

où $\forall$ est le quantificateur universel et se lit « pour tout » ou « quel que soit ».
Une ***proposition existentielle*** affirme qu'au moins un élément x de E possède la propriété $P(x)$. On l'écrit

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

où $\exists$ est le quantificateur existentiel et se lit « il existe ».
Enfin, l'écriture

$$\exists! x \in E, \quad P(x).$$

se lit « il existe un unique x dans E tel que $P(x)$ » et affirme à la fois l'existence et l'unicité de cet élément.

Exemple

La proposition

$$\forall n \in \mathbb{Z}, \quad n^2 \geqslant 0$$

affirme que le carré de tout entier est positif.
La proposition

$$\exists n \in \mathbb{Z}, \quad n^2 = 4$$

affirme qu'il existe au moins un entier dont le carré vaut 4.

Règle

La négation d'une proposition universelle est une proposition existentielle :

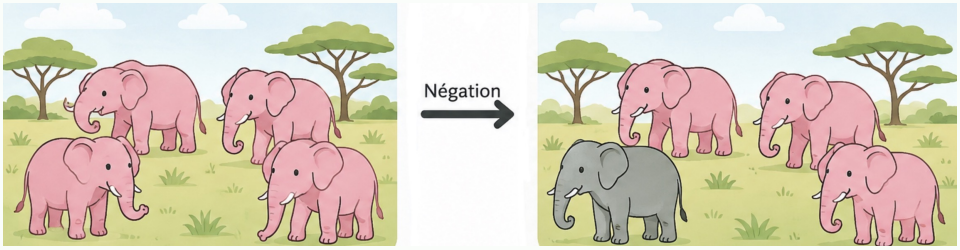
$$\neg\big(\forall x \in E,\ P(x)\big) \quad \Longleftrightarrow \quad \exists x \in E,\ \neg P(x).$$

La négation d'une proposition existentielle est une proposition universelle :

$$\neg\big(\exists x \in E,\ P(x)\big) \quad \Longleftrightarrow \quad \forall x \in E,\ \neg P(x).$$

Exemple

La négation de « tous les éléphants sont roses » est « il existe au moins un éléphant qui n'est pas rose ».



Ainsi, pour réfuter une proposition universelle, il suffit de trouver un seul objet qui ne possède pas la propriété annoncée : cet objet est un ***contre-exemple***.

0.2.4 Implication, réciproque et équivalence

Soient P et Q deux propositions.

Définition 0.5: (implication)

La nouvelle proposition « si P, alors Q » exprime que si P est vraie alors Q est vraie. C'est ***l'implication***, notée par le symbole $\Longrightarrow$.

Définition 0.6: (réciproque)

La ***réciproque*** de l'implication $P \implies Q$ est l'implication $Q \implies P$. Elle s'énonce donc « si Q, alors P ».

Exemple

Soit x un nombre réel. Alors l'implication suivante est vraie :

$$x > 0 \quad \implies \quad x \geqslant 0.$$

⚠ **Remarque** Sa réciproque ($x \geqslant 0 \implies x > 0$) n'est pas vraie, car x peut prendre la valeur 0.

Il arrive parfois qu'une implication soit vraie dans les deux sens. On parle alors d'une ***équivalence*** :

Définition 0.7: (équivalence)

La nouvelle proposition « P si et seulement si Q » exprime que P est vraie si et seulement si Q est vraie. C'est ***l'équivalence***, notée par le symbole $\iff$.

Exemple

Une proposition P est vraie si et seulement si sa négation $\neg P$ est fausse :

$$P \quad \iff \quad \neg(\neg P).$$

Dans la pratique, pour montrer $P \iff Q$, on montre $P \implies Q$ et $Q \implies P$.

0.2.4.1 Réécriture de la preuve de la devinette 1

On va illustrer ce que l'on vient de voir en reprenant la preuve de la première devinette. On commence tout d'abord par deux énoncés (notations), et on continue ensuite avec une succession d'implications pour confirmer notre réponse. On rappelle que la réponse était 50¢.

Démonstration (Devinette 1)

Soit b le prix de la bouteille, et soit v le prix du vin.

Par hypothèse on a :

$$\begin{aligned} (20 = b + v) \ \wedge \ (v = 19 + b) \quad &\implies \quad 20 = b + 19 + b \\ &\implies \quad b = 0{,}5 \end{aligned}$$

D'où la bouteille vaut 50¢.

■

Le langage mathématique nous permet ainsi de rédiger clairement, et surtout universellement, un argumentaire mathématique écrit dans le langage usuel. En général, ceci facilite la lecture et donc la compréhension.

⚠ **Remarque** Mettre trop de texte ou trop de justifications alourdit une preuve ! Il faut donc se limiter à l'essentiel en ne mettant que les justifications nécessaires.

Nous savons maintenant formuler et relier des propositions. Pour parler des objets auxquels elles s'appliquent, il nous faut un second vocabulaire fondamental : celui des ensembles.

0.3 Le langage des ensembles

Sans développer complètement la théorie des ensembles, nous donnons les principaux éléments de ce langage et les notations utilisées. La notion d'ensemble est fondamentale en mathématiques. Les termes « groupement », « famille » ou « collection » donnent une intuition de cette notion.

En arithmétique, on regroupe les nombres en ensembles tels que $\mathbb{N}$, $\mathbb{Z}$ ou $\mathbb{R}$. En géométrie, une droite, un plan ou une figure peuvent être considérés comme des ensembles de points. Le langage des ensembles permet de décrire ces objets et les relations qui les unissent avec précision.

0.3.1 Ensembles, éléments et appartenance

Définition 0.8: (ensemble et élément)

Un ***ensemble*** est une collection d'objets. Les objets qui le composent sont appelés ses ***éléments***.
Si x est un élément de l'ensemble E, on écrit $x \in E$ et on lit « x appartient à E » ou « x est élément de E ». Dans le cas contraire, on écrit $x \notin E$.

Un ensemble est entièrement déterminé par ses éléments. Leur ordre n'a aucune importance et un même élément n'est jamais compté deux fois. Ainsi,

$$\{1, 2, 3\} = \{3, 2, 1\} = \{1, 1, 2, 3\}.$$

L'ensemble qui ne contient aucun élément est appelé ***ensemble vide*** et est noté $\emptyset$. On distingue notamment l'ensemble vide $\emptyset$ de l'ensemble $\{\emptyset\}$, qui contient un élément : l'ensemble vide.

⚠ **Remarque** Il a été historiquement bien établi que l'imprécision de la définition d'un ensemble peut engendrer des paradoxes (voir par exemple le ***paradoxe de Russell*** dans tout bon livre de logique). Pour éviter cela, nous ne travaillerons qu'avec un petit nombre d'ensembles bien étudiés et stables. Toutes nos constructions découlerons en fait de l'ensemble vide et d'axiomes.

Notation: (ensembles de nombres)

Nous utiliserons fréquemment les ensembles suivants :

- $\mathbb{N}$, l'ensemble des entiers naturels (c-à-d $0, 1, 2, 3, \dots$) ;
- $\mathbb{Z}$, l'ensemble des entiers relatifs (c-à-d $0, -1, 1, -2, 2, -3, 3, \dots$) ;
- $\mathbb{Q}$, l'ensemble des nombres rationnels (On rappelle qu'un nombre rationnel s'écrit a/b ou encore $\frac{a}{b}$, où a est un entier relatif et b un entier naturel différent de 0.) ;

- $\mathbb{R}$, l'ensemble des nombres réels (par exemple, π, $\sqrt{2}$, les nombres rationnels) ;
- $\mathbb{C}$, l'ensemble des nombres complexes (par exemple, les nombres réels, les nombres imaginaires).

Ils vérifient

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}.$$

Il existe une construction formelle pour chacun de ces ensembles (qui n'est pas l'objet de ce cours mais celui des cours de théorie des ensembles, d'algèbre, d'analyse et/ou de topologie).

0.3.2 Décrire un ensemble

On peut décrire un ensemble en donnant la liste de ses éléments. On dit alors que l'ensemble est décrit ***en extension***. Par exemple,

$$E = \{2, 4, 6, 8\}.$$

Lorsqu'une liste serait trop longue, ou même infinie, on peut plutôt donner une propriété qui caractérise les éléments de l'ensemble. On dit alors que l'ensemble est décrit ***en compréhension*** :

$$A = \big\{x \in E \mid P(x)\big\}.$$

Cette notation se lit « l'ensemble des éléments x de E tels que la propriété $P(x)$ est vraie ». Ainsi, on aura pour tout élément x de E : $x \in A \iff P(x)$. Autrement dit, si l'on veut montrer qu'un élément x de E est en fait dans A, il suffit de montrer que x répond à la propriété $P(x)$. Réciproquement, si $x \in E$ répond à la propriété $P(x)$, il est dans A.

Exemple

- L'ensemble des entiers pairs est : $2\mathbb{Z} = \{n \in \mathbb{Z} \mid \exists k \in \mathbb{Z}, n = 2k\}$;
- $\mathbb{N} = \{x \in \mathbb{Z} \,|\, x \geqslant 0\}$;
- $\mathbb{Q} = \left\{\frac{a}{b} \,|\, a \in \mathbb{Z}, b \in \mathbb{N}, b \neq 0\right\}$.

La description en compréhension fait donc intervenir à la fois le langage des ensembles et celui des propositions étudié précédemment.

0.3.3 Ensemble fini et infini

Définition 0.9

Un ensemble E est ***fini*** si on peut écrire $E = \{x_1, \ldots, x_n\}$, avec $n \in \mathbb{N}$ fixé, tel que les éléments x_i soient tous distincts. Dans ce cas, on appelle le nombre n le ***cardinal*** ou la ***cardinalité*** de E et on le note : $n = |E|$.

Par convention $|\emptyset| = 0$.

Un ensemble E est ***infini*** s'il n'est pas fini.

Exemple

$\{1, 3, 6, 7, 8, 9, 10, 34\} = \{x_1, x_2, \ldots, x_8\}$ est fini, mais $\mathbb{N}$ est infini.

0.3.4 Inclusion et égalité

Définition 0.10: (inclusion)

Soient A et B deux ensembles. On dit que A est un ***sous-ensemble*** de B lorsque tout élément de A appartient aussi à B. On écrit alors $A \subseteq B$. Autrement dit,

$$A \subseteq B \quad \iff \quad \big(\forall x, \quad x \in A \Longrightarrow x \in B\big).$$

Si A n'est pas un sous-ensemble de B, on écrit $A \nsubseteq B$.

⚠ **Remarque** On trouvera dans la littérature d'autres manières classiques de se référer à un sous-ensemble. Soit B un ensemble et soit A un sous-ensemble de B. On peut dire que A est ***inclus*** ou ***contenu*** dans B ou encore que A est ***une partie*** de B. On peut également écrire $B \supseteq A$, ce qui se lit « B ***contient*** A ».

Attention : la notation $A \subset E$ peut avoir deux sens selon les auteurs : elle peut signifier soit $A \subseteq E$, soit $A \subseteq E$ avec $A \neq E$. Dans ce cours, nous préciserons toujours explicitement lorsque $A \neq E$.

Il importe de distinguer l'***appartenance*** de l'***inclusion***. Si x est un élément de E, on écrit $x \in E$. En revanche, $\{x\}$ est un ensemble contenu dans E, donc $\{x\} \subseteq E$.

⚠ **Remarque** L'ensemble vide est inclus dans tout ensemble. De plus, tout ensemble est inclus dans lui-même : $\emptyset \subseteq E$ et $E \subseteq E$.

0.3.4.1 Démontrer une inclusion ou une égalité d'ensembles

Pour démontrer qu'un ensemble A est inclus dans un ensemble B, on considère un élément quelconque $x \in A$, puis on montre que cet élément appartient nécessairement à B. Autrement dit, on démontre l'implication

$$x \in A \Longrightarrow x \in B.$$

Deux ensembles sont égaux lorsqu'ils possèdent exactement les mêmes éléments. Pour démontrer que $A = B$, on procède généralement par ***double inclusion*** :

$$A = B \quad \iff \quad (A \subseteq B) \wedge (B \subseteq A).$$

On peut aussi montrer directement que, pour tout objet x,

$$x \in A \quad \iff \quad x \in B.$$

0.3.4.2 L'ensemble des sous-ensembles

Définition 0.11: (ensemble des parties)

Soit E un ensemble. L'ensemble formé de tous les sous-ensembles de E est appelé l'***ensemble des parties*** de E et est noté $\mathcal{P}(E)$:

$$\mathcal{P}(E) = \{A \mid A \subseteq E\}.$$

Exemple

Si $E = \{1, 2, 3\}$, alors

$$\mathcal{P}(E) = \big\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, E\big\}.$$

⚠ **Remarque** Si E est un ensemble fini de cardinalité $|E| = n$, alors

$$|\mathcal{P}(E)| = 2^n.$$

Nous admettrons ce résultat, dont la démonstration relève du dénombrement.

0.3.5 Union, intersection et différence

Soient A et B deux sous-ensembles d'un même ensemble E.

Définition 0.12: (union et intersection)

L'***union*** de A et B, notée $A \cup B$, contient les éléments qui appartiennent à A, à B ou aux deux (figure 1a) :

$$A \cup B = \big\{x \in E \mid (x \in A) \vee (x \in B)\big\}.$$

L'***intersection*** de A et B, notée $A \cap B$, contient les éléments qui appartiennent à la fois à A et à B (figure 1b) :

$$A \cap B = \big\{x \in E \mid (x \in A) \wedge (x \in B)\big\}.$$

Lorsque $A \cap B = \emptyset$, on dit que A et B sont ***disjoints*** : ils ne possèdent aucun élément en commun.

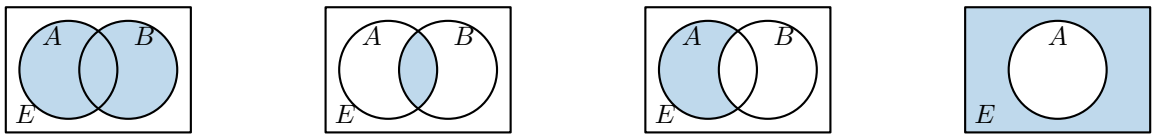
Définition 0.13: (différence et complémentaire)

La ***différence*** de A et B, notée $A \setminus B$, est l'ensemble des éléments de A qui n'appartiennent pas à B (figure 1c) :

$$A \setminus B = \{x \in A \mid x \notin B\}.$$

Le ***complémentaire*** de A dans E, noté A^c, est l'ensemble $E \setminus A$ (figure 1d). Ainsi,

$$A^c = \{x \in E \mid x \notin A\}.$$



(a) $A \cup B$ (b) $A \cap B$ (c) $A \setminus B$ (d) A^c

FIGURE 1 – Représentation des opérations ensemblistes par des diagrammes de Venn. Les régions bleues représentent les ensembles considérés.

Ces opérations traduisent exactement les connecteurs logiques :

$$x \in A \cup B \iff (x \in A) \vee (x \in B),$$
$$x \in A \cap B \iff (x \in A) \wedge (x \in B),$$
$$x \in A^c \iff \neg(x \in A).$$

EXEMPLE

Soit $P = 2\mathbb{Z}$ l'ensemble des entiers pairs et soit $I = \{2k+1 \mid k \in \mathbb{Z}\}$ l'ensemble des entiers impairs. Alors

$$P \cap I = \emptyset \qquad \text{et} \qquad P \cup I = \mathbb{Z}.$$

Les ensembles P et I sont donc disjoints et, ensemble, ils contiennent tous les entiers.

0.3.6 Produit cartésien

DÉFINITION 0.14: (COUPLE)

Un ***couple*** (a, b) est formé d'un premier élément a et d'un second élément b. L'ordre des éléments est important : en général, $(a, b) \neq (b, a)$.

DÉFINITION 0.15: (PRODUIT CARTÉSIEN)

Soient A et B deux ensembles. Le ***produit cartésien*** de A et B, noté $A \times B$ et lu « A croix B », est l'ensemble des couples dont le premier élément appartient à A et le second à B :

$$A \times B = \{(a, b) \mid a \in A \ \wedge \ b \in B\}.$$

EXEMPLE: (UN JEU DE CARTES)

Soient

$$V = \{A, K, Q, J, 10, 9, 8, 7, 6, 5, 4, 3, 2\} \qquad \text{et} \qquad C = \{\spadesuit, \heartsuit, \diamondsuit, \clubsuit\}$$

Le produit $V \times C$ représente alors les 52 cartes du jeu. Par exemple, $(A, \spadesuit)$ représente l'as de pique et $(10, \heartsuit)$ le dix de cœur.

Définition 0.16: (n-uplet)

Soit E un ensemble et soit $n \in \mathbb{N}^*$. Le produit cartésien de E avec lui-même n fois est noté

$$E^n \quad = \quad \underbrace{E \times E \times \cdots \times E}_{n \text{ fois}}.$$

Ses éléments, de la forme $(x_1, x_2, \ldots, x_n)$, sont appelés des ***n-uplets***.

Exemple

Le plan muni de coordonnées s'identifie à $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$: chacun de ses points est représenté par un couple (x, y). De même, les points de l'espace sont représentés par des triplets $(x, y, z) \in \mathbb{R}^3$.

Remarque

- Pour tout ensemble E, $\emptyset \times E = E \times \emptyset = \emptyset$.
- En général, $A \times B \neq B \times A$. Par exemple,

  $$\{0, 1\} \times \{1\} = \{(0, 1), (1, 1)\},$$

  tandis que

  $$\{1\} \times \{0, 1\} = \{(1, 0), (1, 1)\}.$$

- Il faut distinguer le couple (a, b) de la paire $\{a, b\}$. L'ordre compte dans un couple, mais pas dans un ensemble :

  $$(a, b) \neq (b, a) \qquad \text{en général, tandis que} \qquad \{a, b\} = \{b, a\}.$$

- Si A et B sont finis, alors $|A \times B| = |A| \cdot |B|$.

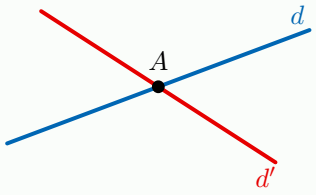
0.3.7 Le langage des ensembles en géométrie

En géométrie, les points sont les éléments fondamentaux, tandis que les droites, les plans et les figures sont considérés comme des ensembles de points. Les notations ensemblistes prennent alors un sens géométrique immédiat :

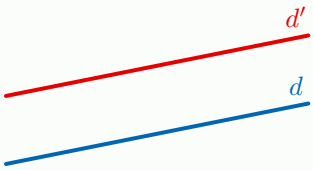
- $A \in d$ signifie que le point A appartient à la droite d ;
- $d \subseteq \mathcal{P}$ signifie que tous les points de la droite d appartiennent au plan $\mathcal{P}$;
- $[AB] \subseteq (AB)$ signifie que le segment $[AB]$ est contenu dans la droite (AB) ;
- $d \cap d'$ désigne l'ensemble des points communs aux droites d et d'.

Exemple: (Intersection de deux droites)

Si deux droites distinctes d et d' se coupent en un unique point A, alors $d \cap d' = \{A\}$. Si elles n'ont aucun point commun, alors $d \cap d' = \emptyset$. Ces deux situations sont illustrées ci-dessous.



$d \cap d' = \{A\}$.



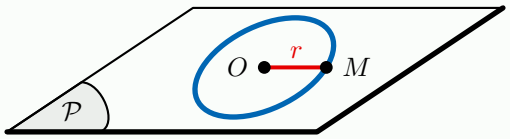
$d \cap d' = \emptyset$.

On peut également décrire une figure par une propriété.

Exemple: (Le cercle comme ensemble de points)

En anticipant légèrement sur le vocabulaire géométrique, nous noterons OM la distance entre les points O et M. Le cercle de centre O et de rayon r dans un plan $\mathcal{P}$ est alors l'ensemble

$$\mathcal{C}(O, r) = \{M \in \mathcal{P} \mid OM = r\}.$$



Ainsi, un point M appartient au cercle si et seulement si sa distance au centre O est égale à r.

Le langage des ensembles nous permettra donc de traduire les relations géométriques en propositions précises. Nous possédons maintenant le vocabulaire nécessaire pour comprendre comment les résultats mathématiques sont formulés, organisés et utilisés.

0.4 Les résultats mathématiques : organisation, lecture et utilisation

0.4.1 Propositions et théorèmes

Dans la section 0.2.1, le mot ***proposition*** désignait, au sens logique, tout énoncé auquel on peut attribuer une valeur de vérité : une proposition peut donc être vraie ou fausse.

Nous adoptons maintenant le point de vue de l'exposé mathématique. Lorsqu'un ouvrage présente ses résultats, il met en évidence certaines propositions vraies, établies par démonstration, et leur attribue différents rôles selon leur importance et leur place dans le développement de la théorie. Elles sont alors présentées comme des ***propositions***, des ***lemmes***, des ***théorèmes*** ou des ***corollaires***.

Dans ce contexte, une ***proposition*** et un ***théorème*** sont tous deux des résultats mathématiques établis par démonstration, à partir de définitions, d'axiomes et de résultats déjà admis. Ces deux termes désignent donc la même nature d'objet : un résultat vrai, établi par un raisonnement rigoureux. Ce qui les distingue n'est pas la rigueur de leur démonstration, mais leur importance et leur fonction dans l'organisation de l'exposé.

En général :

- on réserve le mot théorème aux résultats majeurs ou centraux d'une théorie ;
- on emploie le mot proposition pour des résultats plus techniques ou intermédiaires, nécessaires à la progression du raisonnement mais de portée plus locale.

Ainsi, une proposition peut jouer le rôle d'une étape, d'une clarification ou d'un outil, tandis qu'un théorème marque souvent une conclusion ou un tournant significatif.

Pour illustrer la manière dont un ouvrage présente un théorème, considérons l'énoncé fictif suivant. Nous lui donnerons provisoirement le statut de théorème, puis nous examinerons plus loin si ce statut est réellement justifié.

Théorème 0.17: (théorème du parapluie)

Si l'on sort sans parapluie sous la pluie, **alors** on finira mouillé.

Cette phrase possède la structure d'un théorème : une condition (les hypothèses, que l'on distingue ici par le mot-clé ***si***), une conséquence (la conclusion, dénotée par le mot-clé ***alors***), et une logique claire reliant les deux. En mathématiques, un théorème fonctionne de la même façon — la différence est simplement que les notions y sont définies avec plus de précision et démontrées à l'aide de règles logiques universelles.

Pour utiliser un théorème, on doit d'abord s'assurer que toutes ses hypothèses sont satisfaites, après quoi on peut tenir sa conclusion pour vraie dans la suite du raisonnement. Par exemple :

Exemple

J'ai oublié mon parapluie à la maison ce matin. Il pleuvait lors de ma marche pour me rendre au travail. Me suis-je fait mouiller ?

Réponse : Remarquons qu'en oubliant mon parapluie à la maison, je suis forcément sorti sans parapluie. Et puisqu'il pleuvait, le théorème du parapluie me confirme que je me suis bien fait mouiller.

On voit ici qu'avant de sauter à la conclusion que je me suis fait mouiller, j'ai d'abord dû énumérer les deux hypothèses du théorème.

⚠ **Remarque** Bien que les hypothèses d'un théorème soient ***suffisantes*** pour affirmer sa conclusion, elles ne sont en général pas ***nécessaires***. En d'autres termes, si les hypothèses du théorème ne sont pas toutes satisfaites, on ne peut pas confirmer que la conclusion soit fausse. Dans notre exemple, si une personne sort sous la pluie ***avec*** son parapluie, on ne peut pas confirmer qu'elle est restée au sec. En effet, il ne suffit pas d'avoir un parapluie sous la pluie pour ne pas se mouiller : encore faut-il l'ouvrir pour se couvrir de la pluie ! Ainsi, il est tout à fait possible de se faire mouiller par la pluie même en ayant emporté son parapluie.

Avant de terminer, voici une réécriture du théorème du parapluie :

Théorème 0.18

Une personne qui sort sous la pluie sans parapluie finit inévitablement mouillée.

Remarquons qu'un théorème ne porte pas toujours un nom. Dans ce cas-ci, pour faire référence à ce théorème plus tard dans le texte, je pourrai évoquer le THÉORÈME 0.18. Il faut bien comprendre que cette numérotation est propre à cet ouvrage et que son emploi dans un autre contexte n'aurait aucun sens. Dans le cadre de ce cours, lors de la rédaction des devoirs et des examens, il ne sera pas nécessaire de mentionner explicitement le théorème évoqué lorsque celui-ci n'a pas de nom. Il suffira de vérifier chacune de ses hypothèses, puis d'affirmer qu'elles impliquent sa conclusion.

Remarquons également que cette réécriture du THÉORÈME DU PARAPLUIE laisse tomber les mots-clés ***si*** et ***alors***. Bien que ce ne soit pas explicite, il suffit d'une courte réflexion pour reconnaître que les hypothèses et la conclusion restent inchangées.

Dans un théorème, la distinction entre les hypothèses et la conclusion est essentielle : les hypothèses précisent le contexte dans lequel le résultat est garanti, et la conclusion indique ce qu'on peut en déduire avec certitude.

0.4.2 Lemmes et corollaires

Les théorèmes et propositions ne vivent pas isolés : ils s'appuient les uns sur les autres.

De moindre envergure qu'un théorème, un ***lemme*** est un résultat intermédiaire, souvent d'apparence modeste, mais indispensable pour démontrer un théorème plus important. Par exemple :

LEMME 0.19

La pluie mouille tout ce qu'elle touche.

Bien qu'il ne s'agisse pas d'un résultat très intéressant, on peut imaginer que ce lemme a été utile pour démontrer la véracité du THÉORÈME DU PARAPLUIE.

On peut voir le lemme comme un précurseur à un théorème. À l'autre bout du spectre, le ***corollaire*** est quant à lui une conséquence immédiate d'un théorème. Par exemple, le THÉORÈME DU PARAPLUIE mène au corollaire suivant :

COROLLAIRE 0.20

Sous la pluie, une personne sans parapluie n'est jamais plus sèche qu'une personne munie d'un parapluie.

On peut voir un raisonnement mathématique comme un édifice : les lemmes en sont les fondations, les théorèmes les murs porteurs, et les corollaires les fenêtres qui laissent voir plus loin. Chacun contribue à la solidité de l'ensemble.

Nous examinerons bientôt comment ces briques s'assemblent dans une démonstration complète.

0.4.3 Conjectures et contre-exemples

Les mathématiques, comme toute science, avancent par essais et erreurs. Avant d'être démontré, un résultat n'est parfois qu'une idée plausible, fondée sur l'observation ou l'intuition : une ***conjecture***.

Définition 0.21

On appelle ***conjecture*** une affirmation que l'on suppose vraie, mais dont aucune démonstration rigoureuse n'a encore été établie.

Les conjectures jouent un rôle essentiel : elles guident la recherche, orientent les raisonnements et posent les questions que les démonstrations devront confirmer ou infirmer.

Exemple: (Conjecture du parapluie)

Après quelques promenades pluvieuses, j'ai cru remarquer que chaque fois que je sortais sous la pluie sans parapluie, je finissais mouillé. J'ai donc formulé la conjecture suivante :

« Si l'on sort sous la pluie sans parapluie, alors on finit mouillé. »

Convaincu par son évidence, je l'ai même élevée au rang de théorème du parapluie.

Cependant, une conjecture — même très crédible — peut s'avérer fausse. Il suffit d'un seul contre-exemple pour la réfuter.

Définition 0.22

On appelle ***contre-exemple*** un exemple particulier qui contredit une affirmation universelle.

Exemple: (Contre-exemple au théorème du parapluie)

Un matin pluvieux, je suis sorti sans parapluie, un journal à la main. Je l'ai tenu au-dessus de ma tête, créant un abri de fortune. En arrivant à destination, j'étais toujours sec. Cet exemple contredit directement le théorème du parapluie : il est donc faux !

Le contre-exemple montre que nous avons attribué trop rapidement à cet énoncé le statut de théorème. Puisqu'il est faux, il ne s'agissait en réalité que d'une conjecture. Pour en faire un résultat valide, il faudrait préciser davantage ses hypothèses, notamment en excluant les autres formes de protection contre la pluie.

⚠ **Remarque** Un seul contre-exemple suffit à invalider une conjecture, mais aucun nombre d'exemples favorables ne suffit à la prouver. C'est toute la différence entre l'observation empirique et la démonstration mathématique.

En mathématiques comme ailleurs, il ne suffit donc pas qu'une idée semble vraie pour qu'elle le soit : il faut en préciser soigneusement les conditions, puis en apporter la preuve.

Nous allons maintenant examiner plus précisément la structure de ces énoncés, afin d'apprendre à en reconnaître les hypothèses et la conclusion.

0.4.4 Hypothèses et conclusion

Les résultats mathématiques présentés sous forme de propositions, de lemmes ou de théorèmes possèdent généralement une structure logique commune : ils relient des hypothèses à une conclusion.

Comme nous l'avons vu à la SECTION 0.2.4, de nombreux résultats mathématiques relient des conditions à une conséquence selon la forme

$$A \Longrightarrow B.$$

Dans la formulation d'un théorème, d'un lemme ou d'une proposition, la condition A est appelée ***hypothèse***, tandis que la propriété B est appelée ***conclusion***. On peut lire l'énoncé comme une promesse :

Si les hypothèses sont satisfaites, alors la conclusion est garantie.

Reprenons notre THÉORÈME DU PARAPLUIE :

Si l'on sort sous la pluie sans parapluie, alors on finit mouillé.

Dans cet énoncé :

- L'hypothèse est « on sort sous la pluie sans parapluie » ;
- La conclusion est « on finit mouillé ».

Le rôle de la démonstration est précisément de justifier que la conclusion découle nécessairement des hypothèses, sans supposer quoi que ce soit d'autre.

⚠ REMARQUE Beaucoup d'erreurs de raisonnement viennent d'une confusion entre les hypothèses et la conclusion, ou d'une hypothèse implicite passée sous silence. Le contre-exemple du journal, par exemple, montrait que l'hypothèse « sans parapluie » ne couvrait pas tous les cas possibles d'abri contre la pluie.

Nous savons maintenant comment se structurent les énoncés mathématiques. Voyons comment repérer concrètement leurs différentes composantes lorsqu'on les rencontre dans un texte.

0.4.5 Comment lire un énoncé

Lire un énoncé mathématique ne consiste pas seulement à en parcourir les mots, mais à en décoder la structure logique. Tout énoncé — qu'il s'agisse d'un théorème, d'un lemme ou d'une simple proposition — doit être lu avec l'idée qu'il relie des hypothèses à une conclusion.

Si les hypothèses sont vérifiées, alors la conclusion est garantie.

Ainsi, lorsqu'on rencontre un nouvel énoncé, il faut adopter une démarche systématique :

1. **Identifier les hypothèses.** Que suppose-t-on vrai au départ ? Ces hypothèses peuvent concerner des conditions numériques (par exemple $x > 0$), des propriétés géométriques (comme « les trois points sont alignés ») ou des objets bien définis (« soit f une fonction continue »).
2. **Repérer la conclusion.** Que promet l'énoncé si toutes les hypothèses sont respectées ? C'est la partie que la démonstration viendra justifier.
3. **Clarifier le vocabulaire.** Chaque mot a un sens précis : « parallèle », « orthogonal », « premier », « connexe »… Avant même de tenter de comprendre la logique, il faut être certain de comprendre le langage.
4. **Évaluer la portée de l'énoncé.** S'applique-t-il à tous les cas possibles, ou seulement à une situation particulière ? Les mathématiques s'appuient sur la généralité : un seul contre-exemple suffit à invalider une affirmation universelle.

⚠ REMARQUE Lire un énoncé mathématique, c'est comme lire un contrat : il ne faut pas se fier à l'apparente évidence de la promesse, mais vérifier les conditions qui la rendent valide.

Cette attitude de lecture — attentive, analytique et critique — est au cœur de la rigueur mathématique. Elle permet non seulement de comprendre les théorèmes, mais aussi de les utiliser correctement dans un raisonnement.

EXEMPLE

Supposons qu'un théorème affirme : ***« Si un triangle est équilatéral, alors ses trois angles sont égaux. »*** Pour l'appliquer à une situation donnée, il ne suffit pas d'aimer la conclusion : il faut d'abord vérifier que les hypothèses sont satisfaites, c'est-à-dire que le triangle est effectivement équilatéral.

En résumé, lire un énoncé, c'est **comprendre ce qu'il affirme, ce qu'il suppose et ce qu'il ne dit pas**. C'est à cette condition qu'on peut ensuite l'utiliser avec confiance dans une démonstration.

Une fois la structure d'un énoncé bien comprise, il reste à savoir reconnaître les situations dans lesquelles on peut l'utiliser.

0.4.6 Comment utiliser un énoncé

Une fois un énoncé démontré, il devient un ***outil de raisonnement*** : il peut être invoqué sans devoir être redémontré. Autrement dit, un théorème prouvé devient une ***règle de confiance*** : on peut l'appliquer chaque fois que ses hypothèses sont satisfaites. Utiliser un énoncé, c'est reconnaître dans une situation donnée que les ***hypothèses*** de cet énoncé sont vérifiées, et en déduire directement la ***conclusion***.

Cette démarche comporte deux étapes essentielles :

1. **Identifier** les hypothèses de l'énoncé et vérifier qu'elles sont toutes remplies dans le contexte étudié.
2. **Appliquer** la conclusion, sans refaire la démonstration, car sa validité est déjà établie.

⚠ REMARQUE Lorsqu'on invoque un théorème, il est essentiel de vérifier que **toutes** ses hypothèses sont respectées. Si une seule d'entre elles échoue, on ne peut pas conclure — même si le résultat semble intuitivement vrai. C'est souvent là que se cachent les erreurs logiques les plus subtiles.

En pratique, l'application d'un théorème s'accompagne souvent d'une citation explicite, surtout dans les textes formels :

EXEMPLE

D'après le THÉORÈME DU PARAPLUIE, toute personne sortant sous la pluie sans parapluie finit mouillée. Or, Paul est sorti sous la pluie sans parapluie. Donc, **par application du théorème du parapluie**, Paul est mouillé.

⚠ REMARQUE Dans un contexte d'examen ou de devoir, il n'est pas toujours nécessaire de nommer explicitement le théorème utilisé, tant que le raisonnement montre clairement quelles hypothèses ont été vérifiées et quelle conclusion en découle.

En résumé, ***utiliser un énoncé***, c'est savoir reconnaître le moment où il s'applique. Cette compétence est au cœur du raisonnement mathématique : elle transforme la théorie en pratique, et la connaissance en outil.

Jusqu'ici, nous avons appris à lire et à employer des résultats déjà établis. Voyons maintenant comment démontrer un nouveau résultat à partir des hypothèses et des connaissances dont on dispose.

0.5 Démontrer un résultat

De nombreux résultats mathématiques prennent la forme d'une implication $P \implies Q$: on suppose que les hypothèses P sont vraies et l'on doit établir la conclusion Q. Plusieurs méthodes de raisonnement permettent d'y parvenir.

0.5.1 Le raisonnement direct

La plupart du temps, on fait comme suit : on suppose comme hypothèse de départ que la proposition P est vraie ; puis, par une suite d'arguments, une suite d'implications, qui dépendent du problème particulier (et pour lesquels il est impossible de donner une recette générale), on montre que la proposition Q est vraie.

Exemple: (Raisonnement direct)

Montrons par un raisonnement direct que la somme de deux entiers pairs est paire. L'implication à démontrer est

$$m \text{ et } n \text{ sont pairs} \quad \implies \quad m+n \text{ est pair.}$$

Démonstration Supposons que m et n sont pairs. Il existe alors des entiers k et ℓ tels que

$$m = 2k \qquad \text{et} \qquad n = 2\ell.$$

Par conséquent,

$$m+n \quad = \quad 2k+2\ell \quad = \quad 2(k+\ell).$$

Comme $k+\ell$ est un entier, cette dernière égalité montre que $m+n$ est pair, ce qui est précisément la conclusion recherchée.

■

0.5.2 Le raisonnement par contraposée (ou indirect)

On peut aussi démontrer sa contraposée :

Définition 0.23: (contraposée)

La ***contraposée*** de la proposition $(P \implies Q)$ est la proposition $(\neg Q \implies \neg P)$, que l'on exprime aussi parfois $(\neg P \impliedby \neg Q)$.

Une implication et sa contraposée sont toujours équivalentes ; démontrer l'une revient à démontrer l'autre, et vice-versa.

Exemple: (Raisonnement indirect)

On considère P la proposition « x est pair » et Q la proposition « x n'est pas le carré d'un entier impair ». Pour montrer $P \implies Q$, c'est-à-dire

$$x \text{ est pair} \quad \implies \quad x \text{ n'est pas le carré d'un entier impair},$$

on montrera $\neg Q \implies \neg P$, c'est-à-dire :

$$(x = n^2) \wedge (n \text{ est un entier impair}) \quad \implies \quad x \text{ est impair.}$$

Démonstration Supposons que $x = n^2$, où n est un entier impair. Il existe alors un entier k tel que $n = 2k + 1$. Par conséquent,

$$x \quad = \quad n^2 \quad = \quad (2k+1)^2 \quad = \quad 2(2k^2 + 2k) + 1.$$

Puisque $2k^2 + 2k$ est un entier, cette égalité montre que x est impair ; en particulier, x n'est pas pair. Nous avons donc démontré $\neg Q \implies \neg P$, et par conséquent $P \implies Q$.

■

0.5.3 Le raisonnement par l'absurde (aussi appelé raisonnement par contradiction)

Ce type de raisonnement consiste à supposer qu'une proposition P est fausse, c'est-à-dire que $\neg P$ est vraie, puis à montrer par une suite d'implications logiques que cette hypothèse est absurde. Puisque $\neg P$ est alors fausse, P est vraie.

Notons que $\neg(P \implies Q)$ équivaut à $P \wedge (\neg Q)$. Ainsi, pour montrer que la proposition $P \implies Q$ est vraie, on fait l'hypothèse absurde que P et $\neg Q$ sont toutes les deux vraies. Par une suite d'implications logiques, on montre ensuite que $\neg P$ l'est forcément aussi. On obtient alors que P et $\neg P$ sont toutes les deux vraies, ce qui est absurde en vertu de notre règle qui dit que soit P est vraie, soit $\neg P$ est vraie, mais pas les deux en même temps. On en conclut que l'hypothèse de départ était bien absurde ($P \wedge (\neg Q)$ est donc fausse), ce qui implique finalement que $P \implies Q$ est vraie.

Voici un exemple de ce raisonnement :

Devinette 2: ([Smullyan 1997])

Cent hommes politiques se réunissent pour fonder un nouveau parti.

Chacun d'eux est soit honnête, soit malhonnête.

Sachant que parmi eux il y a au moins un homme honnête (**proposition** P_1) et que, si l'on en prend deux au hasard, il y en a toujours au moins un malhonnête (**proposition** P_2), pouvez-vous dire combien d'hommes politiques honnêtes il y a ?

Réponse : Il y a un homme politique honnête et 99 malhonnêtes.

Démonstration

Ici, la proposition Q sera : il y a un seul homme politique honnête. Sa négation sera donc :

$$\neg Q \quad : \quad \text{soit il n'y a aucun homme politique honnête, soit il y en a au moins deux.}$$

Procédons par contradiction. Supposons que Q est fausse, c'est-à-dire que $\neg Q$ est vraie.

On a alors que :

$$P_1 \wedge (\neg Q) \qquad \Longrightarrow \qquad \text{il y a au moins deux hommes politiques honnêtes.}$$

Il existe alors au moins une paire d'hommes politiques honnêtes. Donc P_2 est fausse, contredisant l'une des hypothèses de départ.

Ainsi, $\neg Q$ est fausse. Autrement dit, Q est vraie.

■

0.5.4 Le raisonnement *cas par cas*

Ce type de raisonnement se définit mieux par l'exemple :

Exemple

[Smullyan 1997, Chapitre 3]

« À la suite de certaines rumeurs, on envoya d'urgence l'inspecteur Craig afin d'enquêter dans onze asiles d'aliénés où avaient cours, disait-on, des pratiques curieuses.

Dans chacun d'eux ne logeaient que des médecins et leurs patients, mais les médecins, tout comme les patients, étaient parfaitement sains d'esprit, ou complètement fous.

On distinguait les individus sains d'esprit à ce qu'ils raisonnaient fort bien et faisaient parfaitement la différence entre le vrai et le faux.

Les fous aussi étaient faciles à reconnaître : ils croyaient systématiquement fausse toute affirmation vraie, et toute affirmation fausse leur semblait vraie.

Je dois ajouter que ce petit monde était sincère, car chacun n'affirmait que ce qui lui semblait être vrai. »

Devinette 3: (Le premier asile)

« Dans le premier asile Craig n'interrogea que deux personnes.

– Dites-moi, Durand, fit-il à la première, que savez-vous de Dupont ?

– Le docteur Dupont, rectifia l'autre, c'est l'un de nos médecins.

Ensuite Craig rencontra Dupont à qui il demanda :

– D'après vous, Durand est-il un patient ou un médecin ?

– Un patient, je suis formel !

L'inspecteur Craig réfléchit un moment et arriva à la conclusion qu'il y avait en effet quelque chose d'anormal dans cet asile, car il abritait un patient sain d'esprit ou un médecin fou !
Comment est-il parvenu à cette conclusion ? »

Il nous faut donc montrer qu'il y a un médecin fou ou un patient sain d'esprit.

 DÉMONSTRATION On va procéder par un raisonnement ***cas par cas***. Il y a quatre cas possibles pour la condition de Durand : il est un médecin fou, un médecin sain d'esprit, un patient fou ou un patient sain d'esprit. Si Durand est un médecin fou ou un patient sain d'esprit, on a automatiquement notre réponse. Il ne nous reste donc que deux cas :

1- **Durand est un médecin sain d'esprit.** Il dit donc la vérité, d'où Dupont est un médecin. Mais comme Dupont dit que Durand est un patient, l'affirmation de Dupont est fausse. Dupont est donc un médecin fou. On a bien dans ce cas un médecin fou ou un patient sain d'esprit !

2- **Durand est un patient fou.** Son affirmation est donc fausse : Dupont est donc un patient. Mais Dupont dit que Durand est un patient, ce qui est vrai, donc Dupont est un patient sain d'esprit. On a donc encore un patient sain d'esprit ou un médecin fou.

■

0.5.5 Organiser et rédiger une démonstration

Il n'existe pas de recette générale permettant de trouver une démonstration. On peut néanmoins organiser sa démarche de la façon suivante :

1. **Identifier les hypothèses.** Quelles informations peut-on supposer vraies au départ ?
2. **Identifier la conclusion.** Que doit-on précisément démontrer ?
3. **Choisir une stratégie.** Peut-on procéder directement, par contraposée, par l'absurde ou par une étude de cas ?
4. **Enchaîner des déductions justifiées.** Chaque affirmation doit découler des hypothèses, d'une définition ou d'un résultat déjà établi.
5. **Conclure explicitement.** La dernière phrase doit indiquer clairement que la conclusion recherchée a été obtenue.

 REMARQUE Cette méthode aide à organiser et à rédiger une preuve ; elle ne garantit pas que l'idée décisive sera facile à trouver. Cette idée vient souvent de l'expérience, de l'intuition et de plusieurs essais.

Nous disposons maintenant d'un langage commun pour lire, utiliser et démontrer les résultats mathématiques. Dans la suite de cet ouvrage, qu'il soit question de géométrie ou d'arithmétique, nous chercherons toujours à identifier clairement les hypothèses, à justifier chaque déduction et à formuler explicitement la conclusion obtenue.

0.6 Écrire les mathématiques : MEMENTO

Ce texte est une traduction libre de la section « A Mathematical Writing Checklist » du document ***A Guide to Writing Mathematics*** de Kevin P. Lee [Lee].

Vous trouverez ci-dessous une liste de consignes à suivre lorsque vous rédigez un texte mathématique.

- ☐ **Avez-vous bien lu et relu votre texte ?**
- ☐ **Avez-vous écrit une introduction ?**

  Soyez sûr que vous avez expliqué le problème au lecteur. Supposez que le lecteur n'est pas familié avec le problème en question.

- ☐ **Avez-vous bien précisé toutes vos hypothèses ?**

  écrivez toutes les hypothèses que vous faites. (Avez-vous supposé que la fonction est continue ? Linéaire ? Que x est un nombre réel ?)

- ☐ **Est-ce que la grammaire, l'orthographe et la ponctuation sont correctes ? Est-ce que votre écriture est claire, fluide et facile à comprendre ?**

  Faite attention qu'il n'y ait pas de phrase incomplète. Les formules et équations ont aussi besoin de faire partie de phrase complète, et n'échappent pas aux règles de ponctuation. Assurez-vous que votre texte se lise facilement.

- ☐ **Avez-vous bien défini toutes les variables ?**

  Assurez-vous d'introduire toutes les variables que vous utilisez.

- ☐ **Utilisez-vous bien les symboles mathématiques ?**

  N'utilisez-pas un symbole " $=$ " en dehors d'une formule. Assurez-vous que vous utilisez adéquatement les symboles dans votre texte. Assurez-vous d'utiliser équations et formules de façon appropriée.

- ☐ **Utilisez-vous les mots dans le bon contexte ?**

  Si vous n'êtes pas certains de la définition précise du mot que vous voulez utiliser, assurez-vous en dans un dictionnaire.

- ☐ **Est-ce que les mathématiques sont correctes ?**
- ☐ **Avez-vous résolu le problème ? Avez-vous une conclusion ?**

  Parfois, dans l'empressement général, on oublie de répondre à la question. Assurez-vous d'y répondre, en français si possible.

0.7 Exercices

Exercice 0.1 (Négation en langage courant) Parmi les énoncés suivants :

- il y a un éléphant rose ;
- il existe un éléphant gris ;
- tous les éléphants sont roses ;
- il y a un éléphant qui n'est pas rose.

(a) lequel est la négation de « les éléphants ne sont pas tous roses » ?

(b) lequel lui est équivalent ? Pourquoi ?

Exercice 0.2 (Négation d'inégalités) Écrire la négation des propositions suivantes, où $x, y \in \mathbb{R}$.

(a) $x > y$;

(b) $x \geqslant y$;

(c) $x > y$ ou $x < y$;

(d) $x \neq y$.

Réponse : (a) $x \leqslant y$; (b) $x < y$; (c) $x = y$; (d) $x = y$.

Exercice 0.3 (Quantificateurs) Traduire chacun des énoncés suivants à l'aide des symboles $\forall$, $\exists$ ou $\exists!$.

(a) Le carré de tout entier est positif.

(b) Il existe un entier dont le carré vaut 2.

(c) Il existe un unique réel x tel que $2x = 6$.

Écrire ensuite la négation des énoncés ***(a)*** et ***(b)***, d'abord avec des symboles, puis en français.

Exercice 0.4 (Implications et Coupe Stanley) Ce soir aura lieu la 6$^{\text{e}}$ partie de la série finale de la Coupe Stanley, qui oppose les Canadiens de Montréal aux Stars de Dallas. Le score actuel dans la série est de trois parties à deux en faveur des Canadiens. On considère les propositions suivantes :

A : Les Canadiens remportent la 6$^{\text{e}}$ partie.

B : Les Canadiens remportent la Coupe Stanley.

Que peut-on dire des quatre propositions suivantes :

(a) $B \Longrightarrow A$;

(b) $A \Longrightarrow B$;

(c) $\neg B \Longrightarrow \neg A$;

(d) $\neg A \Longrightarrow \neg B$.

On rappelle que le vainqueur de la Coupe est la première équipe qui remporte quatre parties de la série finale et qu'il n'y a pas de parties nulles.

Réponse : (a) Faux ; (b) Vrai ; (c) Vrai ; (d) Faux.

EXERCICE 0.5 (Appartenance, inclusion et ensemble vide) Déterminer si chacun des énoncés suivants est vrai ou faux, puis justifier la réponse.

(a) $\{4,1,2,3\} \subseteq \{1,2,3,4,3,2,1\}$;
(b) $\{4,1,2,3\} \neq \{1,2,3,4,3,2,1\}$;
(c) $\big\{\{4,5\},\{1,2\}\big\} \subseteq \{1,2,4,5\}$;
(d) $\emptyset \in \{a,b\}$;
(e) $\emptyset \subseteq \{a,b,f,g\}$;
(f) $\emptyset \in \big\{\emptyset,\{\emptyset\}\big\}$;
(g) $\emptyset \subseteq \emptyset$;
(h) $\{\emptyset\} \in \big\{\emptyset,\{\emptyset\}\big\}$;
(i) $\{\emptyset\} \subseteq \big\{\emptyset,\{\emptyset\}\big\}$;
(j) $\big\{\emptyset,\{1\},\{2,3\}\big\} \subseteq \big\{\{1\},\{2,3\}\big\}$;
(k) $\big\{\{4\}\big\} \in \big\{3,\{4\}\big\}$;
(l) $\big\{\{\emptyset\}\big\} \in \big\{\emptyset,\{\emptyset\}\big\}$;
(m) $\big\{\{1,2\}\big\} \subseteq \big\{\emptyset,\{1,2\}\big\}$;
(n) $\big\{\{\emptyset\}\big\} \subseteq \big\{\emptyset,\{\emptyset\}\big\}$.

Réponse : (a) Vrai ; (b) Faux ; (c) Faux ; (d) Faux ; (e) Vrai ; (f) Vrai ; (g) Vrai ; (h) Vrai ; (i) Vrai ; (j) Faux ; (k) Faux ; (l) Faux ; (m) Vrai ; (n) Vrai.

EXERCICE 0.6 (Calculs sur les ensembles) Soient

$$A = \{1,2,3\}, \qquad B = \{4,5\} \qquad \text{et} \qquad C = \{2,3,4,5\}.$$

Écrire explicitement chacun des ensembles suivants.

(a) $\mathcal{P}(A)$;
(b) $\mathcal{P}\big(\mathcal{P}(B)\big)$;
(c) $A \setminus B$;
(d) $B \setminus A$;
(e) le complémentaire de B dans C ;
(f) $C \setminus A$;
(g) $C \setminus B$;
(h) $A \setminus C$;
(i) $B \setminus C$.

EXERCICE 0.7 (Complémentaire et inclusion) Soient A et B deux ensembles tels que $A \subseteq B$, et soit $A^c = B \setminus A$ le complémentaire de A dans B.

(a) Démontrer les égalités suivantes :

(i) $A \cup A^c = B$;

(ii) $A^c \cap A = \emptyset$;

(iii) $\emptyset^c = B$;

(iv) $B^c = \emptyset$.

(b) Démontrer ensuite que, pour deux ensembles quelconques A et B,

$$A \subseteq B \iff A \cap B = A.$$

Exercice 0.8 (Lois de De Morgan) Soient A et B deux sous-ensembles d'un même ensemble E. Démontrer que :

(a) $(A^c)^c = A$;

(b) $(A \cup B)^c = A^c \cap B^c$;

(c) $(A \cap B)^c = A^c \cup B^c$.

Dans cet exercice, tous les complémentaires sont pris dans E.

Exercice 0.9 (Propriétés de l'union et de l'intersection) Soient A, B et C trois ensembles. Démontrer les propriétés suivantes :

(a) **Idempotence :** $A \cap A = A$ et $A \cup A = A$.

(b) **Commutativité :** $A \cup B = B \cup A$ et $A \cap B = B \cap A$.

(c) **Ensemble vide :** $A \cup \emptyset = A$ et $A \cap \emptyset = \emptyset$.

(d) **Inclusion :** si $A \subseteq B$, alors $A \cup B = B$ et $A \cap B = A$.

Exercice 0.10 (Analyser un énoncé) Considérons la phrase suivante :

> « Si un triangle est équilatéral, alors ses trois angles sont égaux. »

(a) Indiquez quelles sont les hypothèses et quelle est la conclusion.

(b) Écrivez la réciproque et la contraposée de cet énoncé.

(c) Parmi ces trois énoncés, lesquels sont vrais ?

Exercice 0.11 (Conjecture et contre-exemple) Un ami vous affirme :

> « Tous les nombres premiers sont impairs. »

(a) Reformulez cette affirmation sous forme de conjecture.

(b) Trouvez un contre-exemple qui la réfute.

(c) Reformulez l'énoncé corrigé pour qu'il soit vrai.

Exercice 0.12 (Raisonnement direct) Trouver mon âge sachant que dans 20 ans, j'aurai le double de l'âge que j'avais il y a 10 ans. Il faut évidemment justifier votre réponse !

Réponse : J'ai 40 ans.

Exercice 0.13 (Raisonnement par contraposée) Écrire la contraposée des implications suivantes :

(a) $P \Longrightarrow Q$;

(b) $P \Longrightarrow \neg Q$;

(c) $\neg P \Longrightarrow Q$;

(d) tous les chats sont gris ;

(e) chaque sport est bon pour la santé ;

(f) aucune hirondelle ne fait le printemps.

Exercice 0.14 (Raisonnement ***cas par cas***) Démontrer que, pour tout entier n, le produit $n(n+1)$ est pair.

Indice : Distinguer le cas où n est pair de celui où n est impair. On pourra écrire respectivement $n = 2k$ et $n = 2k+1$, où $k \in \mathbb{Z}$.

Chapitre 1

Géométrie élémentaire du plan et de l'espace

L'objectif de ce chapitre est multiple. Tout d'abord, nous allons essayer de donner une idée au lecteur du rôle des mathématiques en tant qu'outil de création pour la société. Les modèles mathématiques actuels sont beaucoup trop nombreux et souvent trop complexes pour être abordés dans un seul cours de premier niveau universitaire. Cependant, le développement des outils mathématiques utilisés en construction remonte à l'Antiquité et particulièrement au temps de la Grèce Antique[1] : ce modèle est la ***géométrie euclidienne du plan et de l'espace***. Il fut et est encore utilisé en architecture. Le second objectif est de développer chez le lecteur un sens de la création en mathématique, ce qu'on appelle entre mathématiciens « l'intuition mathématique ». Le troisième objectif est de montrer ce que sont le langage et le raisonnement mathématique ainsi que l'importance de bien apprendre à les manier précisément. Enfin, nous espérons réussir à amener le lecteur à saisir la différence entre une vérité mathématique, qui est absolue en tant que création dans un univers imaginaire et autoréférentiel, et une vérité réelle, qui n'est pas absolue et est sujette aux interprétations quant aux choix arbitraires des modèles mathématiques utilisés pour en décrire la réalité.

Les notions élémentaires de géométrie supposées connues sont rassemblées dans l'ANNEXE A, intitulée « Rappels de géométrie ». Le lecteur pourra s'y référer au besoin tout au long de ce chapitre pour revoir une définition, une notation ou une propriété.

La plupart des résultats présentés dans ce chapitre sont sans doute connus du lecteur. L'accent est mis sur la démonstration de ces résultats, le «pourquoi c'est vrai», la raison pour laquelle les prédictions mathématiques s'avèrent d'une redoutable précision. Finissons par citer un physicien bien connu :

> Comment se fait-il que les mathématiques, qui sont un produit de la pensée humaine et indépendante de toute expérience, s'adaptent d'une manière si admirable aux objets de la réalité ? – Einstein, Albert

1.1 Introduction

Commençons par un problème qui n'est peut-être pas si loin de la réalité historique que l'on pense.

> Il y a bien longtemps, au tout début de l'existence de la ville, un riche citoyen d'Athènes convoqua le plus habile architecte de la ville pour lui demander de lui construire une propriété aux formes parfaites.

1. Les mathématiques en tant que domaine de savoir sont nées du temps de l'école pythagoricienne et la somme des connaissances acquises nous a été transmise grâce aux Élément d'Euclide, voir par exemple [Rittaud 2000]

Il souhaitait que sa demeure soit un carré de 7 mètres[2] de côté ; que les murs soient aussi des carrés et enfin que le toit soit une pyramide parfaite (c'est-à-dire que les faces soient des triangles équilatéraux). De plus, il souhaitait que sa nouvelle demeure soit entourée d'une clôture en forme de carré, avec des côtés parallèles aux murs de la maison. Il désirait aussi que la longueur de chaque côté de la clôture soit égale à la hauteur de la pyramide formant le toit multipliée par la diagonale d'un mur.

Le riche citoyen en question informa aussi l'architecte qu'il avait soumis ce projet à deux autres architectes et qu'il donnerait le contrat à celui qui prouverait qu'il réaliserait la construction de la plus parfaite manière.

L'architecte, qui n'avait à sa disposition en ce temps là qu'une corde et un bout de bois d'un mètre de longueur pour tout outil de mesure et de tracé, dut se gratter la tête longtemps afin de développer les techniques qui lui seraient utiles pour contenter ce riche citoyen et le convaincre de la perfection de sa solution. Comment vous y prendriez-vous ? (N'oubliez pas que si un autre concurrent arrive avec un meilleure réponse, vous ne remportez pas le contrat.)

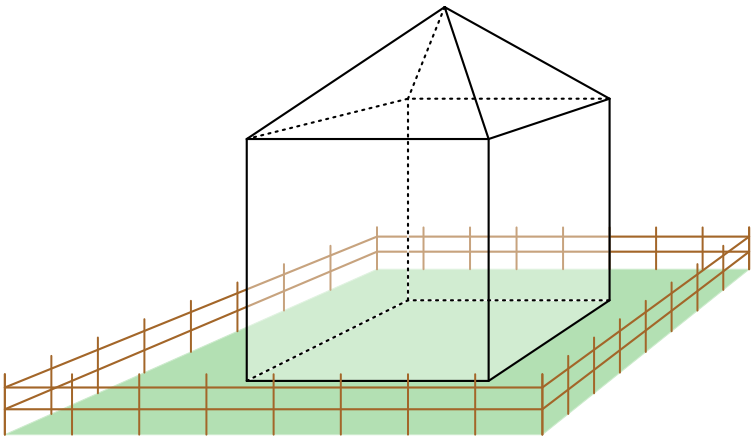
Nous allons nous servir de ce problème, auquel nous répondrons dans ce chapitre, pour illustrer nos propos. En face d'un tel problème, le mathématicien décompose les différents problèmes en sous-problèmes. Il faut tout d'abord se débarrasser des bruits de fond en se donnant des hypothèses de travail.

Hypothèses au sujet de la mise en œuvre de la solution.

On suppose que l'architecte dispose :

- d'une équipe compétente de maçons, charpentiers, tailleurs de pierres, etc. ;
- de tous les matériaux bruts qu'il souhaite ;
- du bâton de bois comme unité de mesure (le mètre) ;
- d'une corde pour tracer des lignes droites entre deux points : il suffit de planter deux piquets et de tendre la corde entre ces deux piquets ;
- de la même corde pour tracer des cercles : il suffit de planter un piquet, d'y attacher la corde, de choisir une longueur de corde puis de tourner autour du piquet.

L'architecte ne dispose pas d'équerre ni de règle graduée, instruments trop imprécis pour construire une maison de cette taille. Son travail est maintenant de donner aux artisans une recette précise pour la construction. Nous sommes prêts à ce point à sortir du monde réel et à entrer dans celui des mathématiques afin d'imaginer ce fameux plan de construction.



2. Il n'y avait évidement pas d'unité de mesure tel que le mètre dans ce temps là ; nous l'utilisons ici par commodité.

Mathématisation du problème.
Résumons ce dont nous avons besoin : nous devons savoir construire des carrés, des triangles équilatéraux, des cubes et des pyramides, rapporter des longueurs et les multiplier (pour la clôture) et tracer des parallèles. Le tout avec le moins d'approximation possible.

> En d'autres termes, sachant que l'on sait tracer des droites et des cercles, il faut trouver une solution parfaite et convaincante pour reporter des longueurs, les multiplier, construire un angle droit, construire des triangles équilatéraux et tracer des parallèles.

Pour répondre à cette question, nous allons tout d'abord nous en éloigner un petit peu — une habitude des mathématiciens — afin de mieux comprendre le contexte dans lequel se passe notre étude : on appelle cela ***l'abstraction***.

1.1.1 Préliminaires et notations

Nous nous contenterons de l'idée intuitive d'objets tels que les points, les droites, les segments, les angles, les perpendiculaires, les droites parallèles, les plans, l'espace, les longueurs, les distances et l'aire. Ce faisant, nous suivrons l'évolution historique du domaine de la géométrie. Certains de ces objets seront néanmoins décrits comme des ensembles de points à l'aide du langage mathématique moderne. Le langage et les symboles nécessaires ont été présentés au CHAPITRE 0, auquel le lecteur pourra se référer au besoin.

Les notations utilisées sont les suivantes :

NOTATIONS

(i) $\mathcal{P}$ désigne un ***plan*** (2 dimensions : longueur et largeur) ;

(ii) $\mathcal{E}$ désigne l'***espace*** (3 dimensions : longueur, largeur et épaisseur) ;

(iii) Si A est un point d'un plan $\mathcal{P}$, alors on notera : $A \in \mathcal{P}$ (le symbole « $\in$ » se lit « appartient à » ou « élément de ») ;

(iv) Pour deux points distincts $A, B \in \mathcal{P}$:

- (AB) désigne la ***droite*** passant par A et B ;
- $[AB]$ désigne le ***segment*** reliant A et B ;
- AB désigne la ***longueur*** du segment $[AB]$;

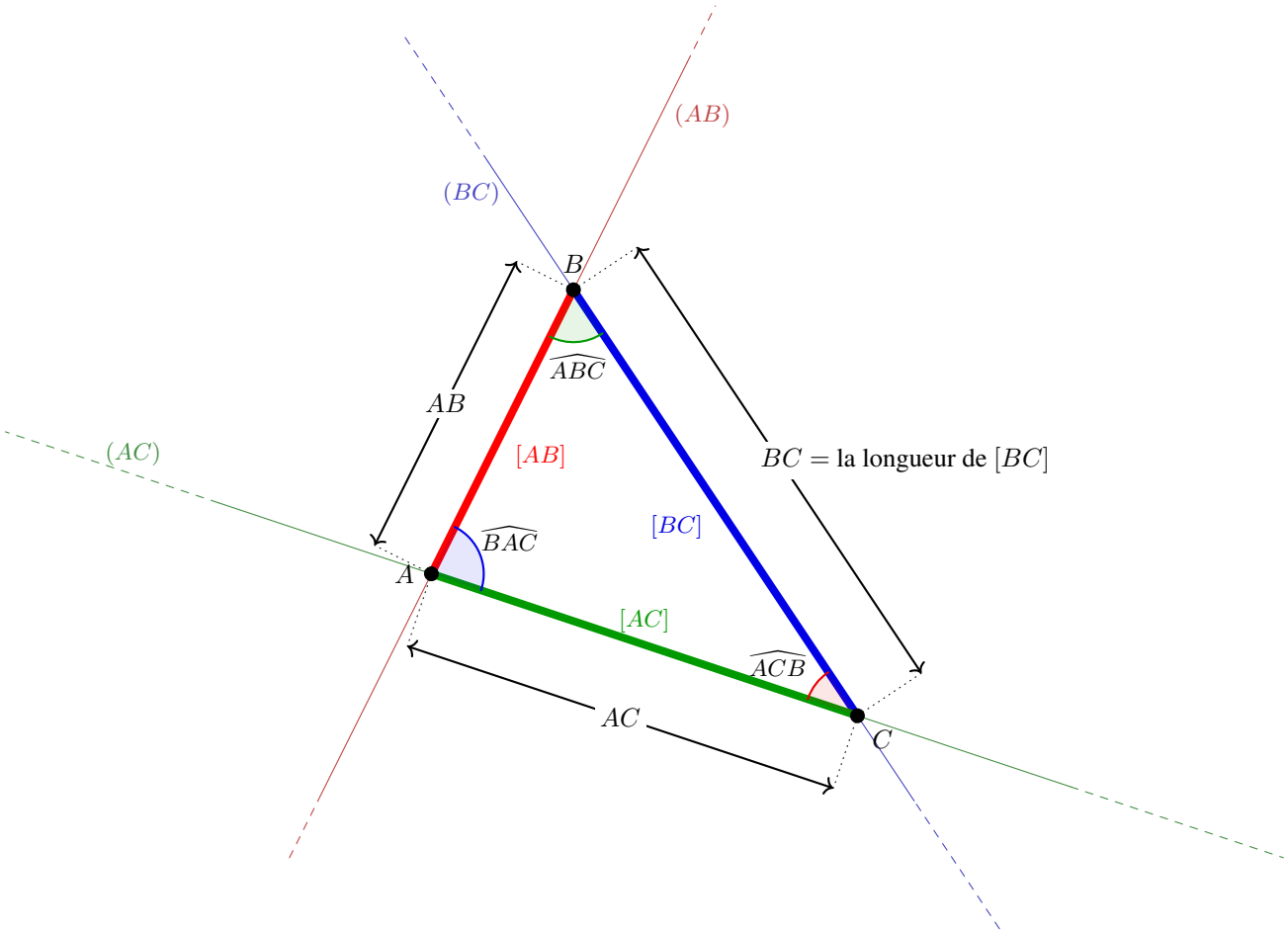
(v) ABC désigne un triangle dont :

- les ***sommets*** sont les points A, B et C ;
- les ***côtés*** sont $[AB]$, $[BC]$ et $[AC]$;
- les ***angles*** sont $\widehat{ABC} = \widehat{CBA}$, $\widehat{BAC} = \widehat{CAB}$ et $\widehat{ACB} = \widehat{BCA}$ (lorsque le contexte est sans ambiguïté, on notera ces angles $\widehat{A}$, $\widehat{B}$ et $\widehat{C}$) ;

(vi) Pour deux droites $d, d' \subset \mathcal{P}$:

- $d \perp d'$ signifie que d est ***perpendiculaire*** à d' ;
- $d \parallel d'$ signifie que d est ***parallèle*** à d'.

La figure qui suit illustre l'utilisation quelques unes de ces notations sur un triangle ABC.

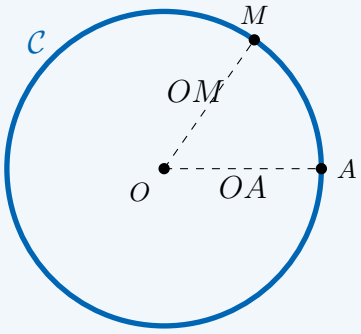


Pour donner une première idée de la façon dont nous allons présenter les mathématiques, nous rappelons ici la définition d'un cercle :

Définition 1.1

Soient $O, A \in \mathcal{P}$ deux points du plan. Le ***cercle $\mathcal{C}$ de centre O passant par A*** (ou encore de rayon OA) est l'ensemble de tous les points M du plan tel que $OM = OA$; autrement dit :

$$\mathcal{C} = \{M \in \mathcal{P} \,|\, OM = OA\}.$$



La phrase mathématique $\mathcal{C} = \{M \in \mathcal{P} \,|\, OM = OA\}$ se lit : « $\mathcal{C}$ est l'ensemble des points M du plan $\mathcal{P}$ tel que la longueur OM est égale à la longueur OA ».

1.2 Quelques résultats classiques

Nous allons revisiter ici deux résultats classiques bien connus et non sans lien avec le problème qui nous intéresse : la somme des angles d'un triangle est un angle plat (c'est à dire π) ainsi que la règle du parallélogramme.

La question principale qui va nous guider tout au long de cette visite est : ***pourquoi ces énoncés sont-ils vrais ?***

1.2.1 Somme des angles d'un triangle

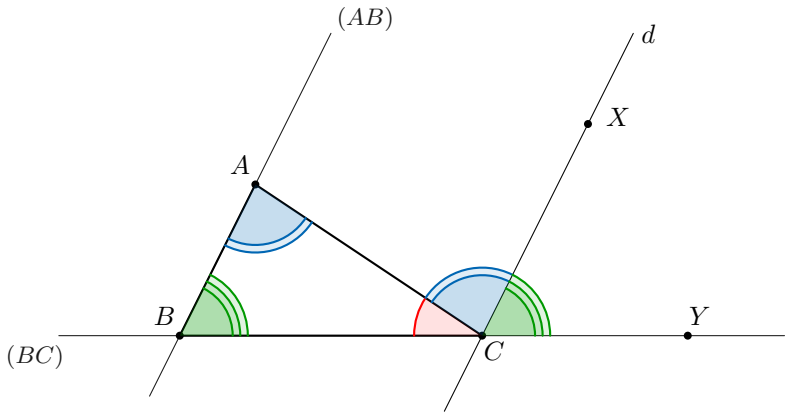
On considère l'énoncé suivant.

PROPOSITION 1.2

La somme des angles d'un triangle est un angle plat ($= \pi$).

Pourquoi cet énoncé est-il vrai ? Donnons en la démonstration.

DÉMONSTRATION Soit ABC un triangle et soit d la droite parallèle à (AB) passant par C. Plaçons le point X sur d, et le point Y sur (BC) comme l'illustre le dessin suivant :



En reportant les angles, on obtient :

$$\begin{aligned} \widehat{ABC} + \widehat{BAC} + \widehat{ACB} &= \widehat{XCY} + \widehat{ACX} + \widehat{ACB} \\ &= \widehat{BCY} \\ &= \pi. \end{aligned}$$

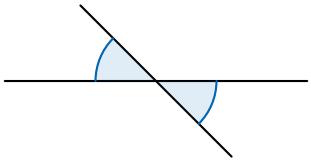
■

REMARQUE Si on analyse attentivement les arguments utilisés dans la preuve de cette proposition, on observe que la preuve est basé sur « le fait » suivant : on « reporte les angles » ou autrement dit :

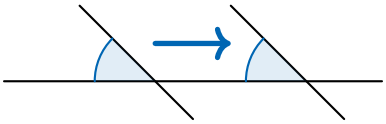
les angles sont invariants par translation et les angles opposés sont égaux.

On est alors en droit, on en a même le devoir, de poser à nouveau la question suivante : Pourquoi cet énoncé est-il vrai ? Avant de répondre à cette question, traduisons cet énoncé dans une forme mathématique plus concrète avec laquelle on pourra travailler.

Énoncé 1 : Soient d et d' deux droites sécantes. Alors les angles opposés par le point d'intersection sont égaux :



Énoncé 2 : Les angles sont invariants par translation :



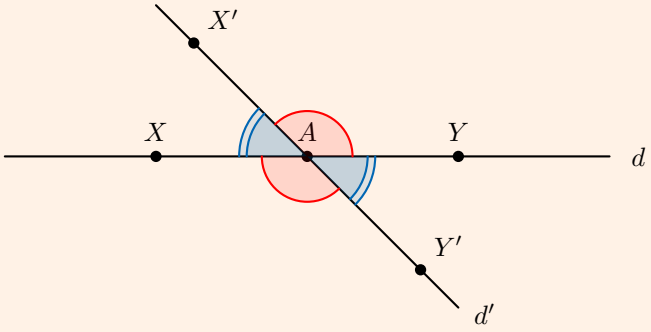
Que penser de ces énoncés ? Sont-ils vrais ? Peuvent-ils se démontrer ? Si oui, on est certain que la somme des angles d'un triangle est π ; sinon ... on n'est certain de rien. L'***énoncé 1*** peut se démontrer ; il s'agit d'une ***proposition***, que l'on énonce de la façon suivante :

Proposition 1.3

Soient d et d' deux droites sécantes. Alors les angles opposés par leur point d'intersection sont égaux.

Cet énoncé se « mathématise » de la façon suivante : en choisissant deux points $X, Y \in d$ et deux points $X', Y' \in d'$ tels que le point d'intersection $A \in d \cap d'$ soit entre X et Y et entre X' et Y', on peut alors écrire les égalités suivantes :

$$\widehat{XAY'} = \widehat{X'AY} \quad \text{et} \quad \widehat{YAY'} = \widehat{XAX'}.$$



Démonstration

$$\widehat{X'AY} + \widehat{YAY'} = \pi = \widehat{XAX'} + \widehat{X'AY} \implies \widehat{YAY'} = \widehat{XAX'}$$

Idem pour l'autre égalité.

■

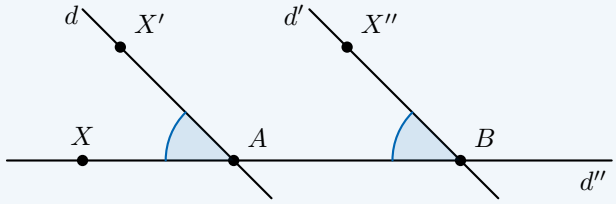
L'***énoncé 2*** ne peut quant à lui pas être démontré. Il s'agit d'un ***axiome***, que l'on accepte comme étant vrai sans preuve :

Axiome 1.4

Les angles sont invariants par translation.

Cette situation se « mathématise » de la façon suivante : soient d et d' deux droites parallèles et d'' une droite sécante à d et d'. En posant des points comme l'illustre la figure suivante, on obtient :

$$\widehat{XAX'} = \widehat{XBX''}$$



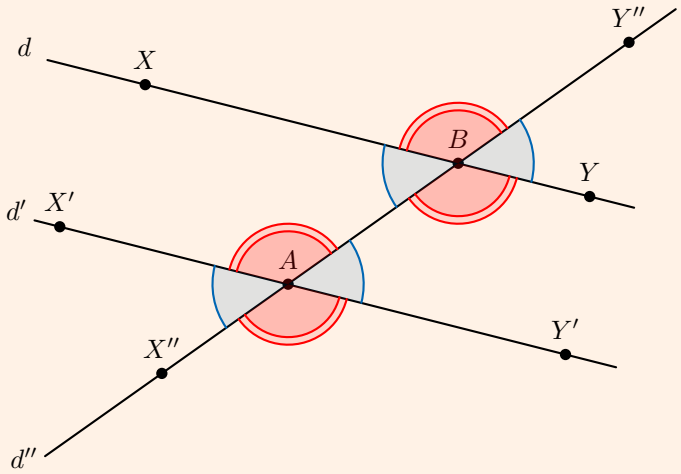
Dans le cadre de la ***géométrie Euclidienne***, dans laquelle l'axiome 1.4 est considéré vrai, la proposition 1.2 est valide et nous avons bien que la somme des angles d'un triangle est un angle plat[3].

Afin de simplifier le discours, on peut formuler le corollaire suivant :

Corollaire 1.5: (Translations des angles)

Soient d et d' deux droites parallèles et d'' une droite sécante à d et d'. En posant les points définis sur la figure suivante, on a :

$$\widehat{X'AX''} = \widehat{XBX''} = \widehat{Y''AY'} = \widehat{Y''BY} \quad \text{et} \quad \widehat{XBY''} = \widehat{YBX''} = \widehat{X'AY''} = \widehat{X''AY'}$$



On dit aussi que :

- ***(i)*** les angles ***alternes internes*** sont égaux ;
- ***(ii)*** les angles ***alternes externes*** sont égaux.

3. Attention, bien que ce résultat soit vrai en géométrie Euclidienne, il existe d'autres géométries dans lesquels l'axiome 1.4 n'est pas admis. Dans de tels cas, la somme des angles d'un triangle n'égale pas toujours π. De telles géométries seront couvertes dans le cours MAT2400.

Démonstration Découle directement de la proposition 1.3 et de l'axiome 1.4.

■

1.2.2 Triangles isométriques

Revenons aux triangles. Les triangles ont été considérés par les mathématiciens grecs comme les objets élémentaires du plan : constitués de trois points distincts et non alignés, reliés par des arêtes ou côtés, les triangles vivent dans un plan $\mathcal{P}$. Avant d'étudier des objets plus complexes (carrés, polygones, etc.) il est naturel de savoir comparer les triangles afin de comprendre leurs différences et leurs similarités. Si un triangle est constitué de trois points fixes, que peut-on dire d'un autre triangle dont les côtés sont en tout point identiques à ceux du triangle de départ ? On observe par exemple que les angles adjacents aux cotés de même longueur sont aussi égaux. Mais une observation n'est pas une preuve, alors, pourquoi cet énoncé est-il vrai ? Commençons par « mathématiser » cet énoncé en le précisant même un peu.

Définition 1.6

Deux triangles sont dits ***isométriques*** si leurs trois côtés sont respectivement isométriques (c-à-d de longueur égale).

Axiome 1.7: (triangles isométriques)

Les trois énoncés suivants sont équivalents (c-à-d : ***(i)*** $\Longleftrightarrow$ ***(ii)*** $\Longleftrightarrow$ ***(iii)***) :

- ***(i)*** Deux triangles sont isométriques ;
- ***(ii)*** Deux triangles ont deux côtés respectivement isométriques adjacents à un même angle ;

- ***(iii)*** Deux triangles ont un côté isométrique compris entre deux angles respectivement égaux.

À nouveau le mathématicien se poserait immanquablement les questions suivantes : est-ce que cet énoncé est vrai ? Si oui, comment le démontrer ? C'est en explorant ce genre de question que les mathématiques se sont développées. Dans ce cas, nous ne sommes à nouveau pas capable de démontrer cet énoncé ; cette propriété est encore un ***axiome***. On peut par contre en déduire la propriété bien connue suivante en utilisant l'équivalence ***(i)*** $\Longleftrightarrow$ ***(ii)*** tout en alternant successivement les rôles de A, B et C.

Corollaire 1.8

Si deux triangles sont isométriques, alors leurs angles sont égaux.

⚠ **Remarque** La réciproque de cet énoncé est fausse : deux triangles dont les angles sont égaux ne sont pas forcément isométriques. On peut penser par exemple à deux triangles équilatéraux dont l'un est plus petit que l'autre. On dit que deux triangles dont les angles sont deux à deux égaux sont ***semblables***.

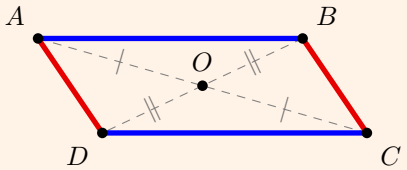
1.2.3 Règle du parallélogramme

Le rôle du parallélogramme est prépondérant comme outil de démonstration, mais aussi comme outil de construction comme nous le verrons dans la suite de ce chapitre. Nous allons tout d'abord commencer par rappeler la ***règle du parallélogramme***.

Proposition 1.9: (Règle du parallélogramme)

Soit $ABCD$ un quadrilatère convexe. Les énoncés suivants sont équivalents :

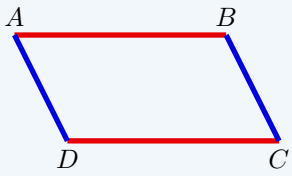
- ***(i)*** $ABCD$ est un parallélogramme ;
- ***(ii)*** $AB = CD$ et $AD = BC$;
- ***(iii)*** les diagonales de $ABCD$ se coupent en leur milieu ;
- ***(iv)*** $AB = CD$ et $(AB) \parallel (CD)$.



Comme avant, posons nous les questions suivantes : quelle est la définition d'un « parallélogramme » ? Pourquoi cet énoncé est-il vrai ? La définition ne pose évidement pas de problème, rappelons-la tout de même afin de s'habituer à la manière de présenter les textes mathématiques.

Définition 1.10: (Parallélogramme)

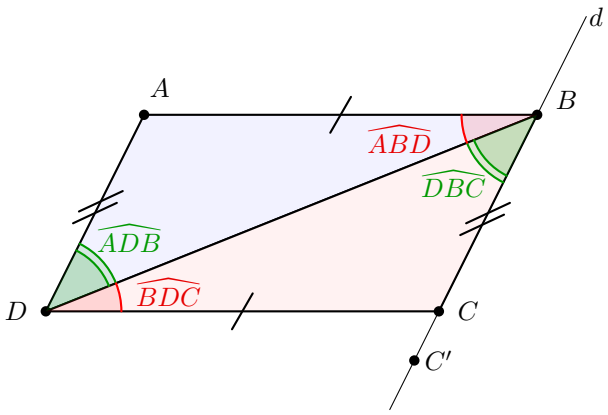
Un ***parallélogramme*** $ABCD$ est la donnée de quatre points A, B, C et D de $\mathcal{P}$ tels que $(AB) \parallel (CD)$ et $(AD) \parallel (BC)$.



Remarque Un parallélogramme est un quadrilatère convexe (c-à-d non croisé).

Démonstration (Règle du parallélogramme)

Montrons *(i)* $\iff$ *(ii)* (Pour le reste des équivalences, voir l'exercice 1.1).



(i) $\Longrightarrow$ *(ii)* Il suffit de montrer que les triangles ABD et BCD sont isométriques.

D'abord, on a $\widehat{ADB} = \widehat{DBC}$ (Il s'agit d'angles alternes internes formés par la droite (BD) coupant les droites parallèles (AD) et (BC)). De même, $\widehat{ABD} = \widehat{BDC}$, car $(AB) \parallel (CD)$.

Ainsi, ABD et BCD sont isométriques, donc $AB = CD$ et $AD = BC$.

(i) $\Longleftarrow$ *(ii)* L'hypothèse de départ est $AB = CD$ et $AD = BC$. Montrons que $(AB) \parallel (CD)$ et $(AD) \parallel (BC)$.

Soit d la droite parallèle à (AD) passant par B. On veut montrer que $d = (BC)$.

Comme $AB = CD$ et $AD = BC$, les triangles ABD et BCD sont isométriques, car $BD = BD$. Ainsi, $\widehat{ADB} = \widehat{DBC}$.

Soit C' un point sur d du même côté de (AB) que C. Comme les angles sont invariants par translation, on a que $\widehat{ADB} = \widehat{DBC'}$. Donc $\widehat{DBC'} = \widehat{ADB} = \widehat{DBC}$. Autrement dit, les points B, C et C' sont alignés, d'où $d = (BC)$.

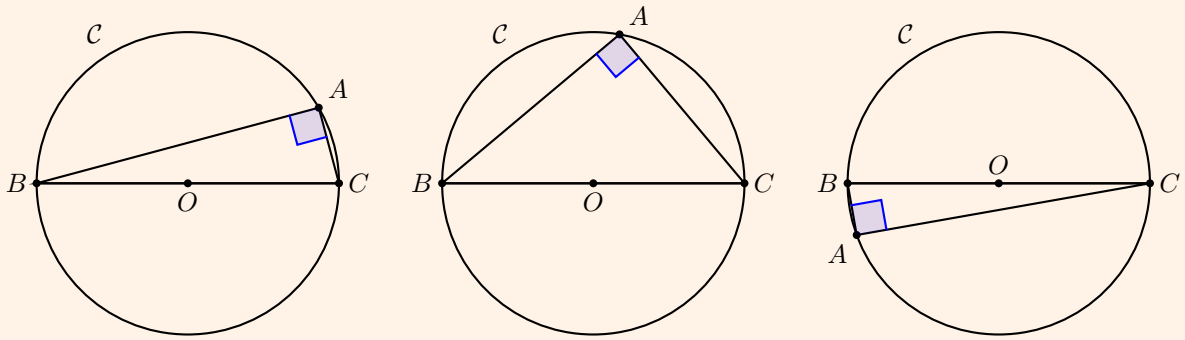
On procède de même pour montrer que $(AB) \parallel (DC)$.

■

1.2.4 Première construction d'un angle droit

Proposition 1.11

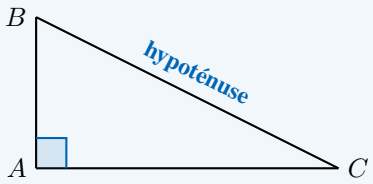
Soientt $\mathcal{C}$ un cercle de centre O, $[BC]$ un diamètre de $\mathcal{C}$ et $A \in \mathcal{C} \setminus \{B, C\}$. Alors ABC est un triangle rectangle en A.



Comme avant, posons nous les questions suivantes : quelle est la définition d'un ***triangle rectangle en*** A ? Pourquoi cette énoncé est-il vrai ? La définition ne pose pas non plus ici de problème, mais rappelons-la tout de même afin de s'habituer à la manière de présenter les textes mathématiques.

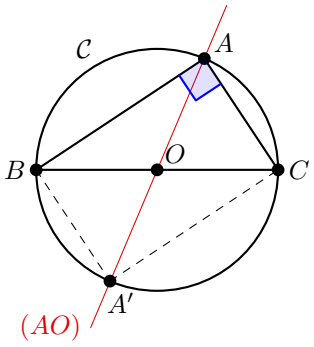
Définition 1.12

On dit qu'un triangle ABC est ***rectangle en*** A si $\widehat{BAC} = \frac{\pi}{2}$ (angle droit). Le segment $[BC]$ est l'***hypoténuse*** de ABC.



Démonstration (proposition 1.11) Soit $A \in \mathcal{C}$ tel que $A \neq B$ et $A \neq C$. Alors, ABC est un triangle (et $\mathcal{C}$ est un cercle circonscrit à ABC). On a bien entendu que O est le point milieu de $[BC]$.

Soit $A' \in (AO)$ tel que O soit le milieu de $[AA']$. Donc $A' \in \mathcal{C}$, car $AO = OA'$.



Le quadrilatère $ACA'B$ a ses diagonales qui se coupent en leur milieu O, c'est donc un parallélogramme. De plus, ses diagonales sont de même longueur ($BC = 2OB = 2OA = AA'$), c'est dont un rectangle (voir l'EXERCICE 1.2). D'où ABC est un triangle rectangle en A.

■

1.3 Les théorèmes de Pythagore et de Thalès

Les deux théorèmes que nous présentons ici sont, sans nul doute, les deux théorèmes les plus célèbres issus des recherches des mathématiciens grecs.

1.3.1 Théorème de Pythagore

Intéressons nous d'abord à l'un des résultats mathématiques les plus connus.

THÉORÈME 1.13: (PYTHAGORE)

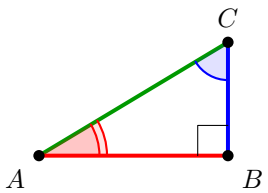
Soit ABC un triangle, alors :

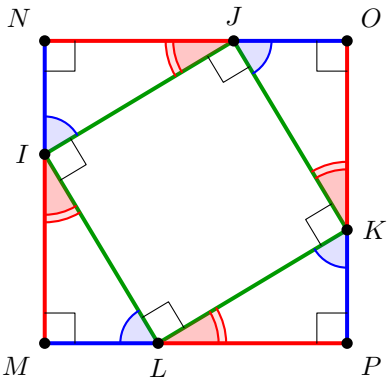
$$ABC \text{ est rectangle en } B \iff AB^2 + BC^2 = AC^2$$

DÉMONSTRATION

($\Longrightarrow$) On considère un carré $MNOP$ de côté $\alpha = AB + BC$. On place les points I, J, K et L comme suit :

$$\begin{aligned} I \in [MN] \quad &\text{et} \quad MI = AB \quad (\text{donc } IN = BC) \\ J \in [ON] \quad &\text{et} \quad NJ = AB \quad (\text{donc } JO = BC) \\ K \in [OP] \quad &\text{et} \quad OK = AB \quad (\text{donc } KP = BC) \\ L \in [MP] \quad &\text{et} \quad PL = AB \quad (\text{donc } ML = BC) \end{aligned}$$





On obtient ainsi que les triangles MLI, NIJ, JOK et KPL sont rectangles et isométriques à ABC. En particulier,

$$\begin{cases} IJ = JK = KL = IL = AC \\ \widehat{NIJ} = \widehat{ILM} = \widehat{BCA} \\ \widehat{MIL} = \widehat{NJI} = \widehat{CAB}. \end{cases}$$

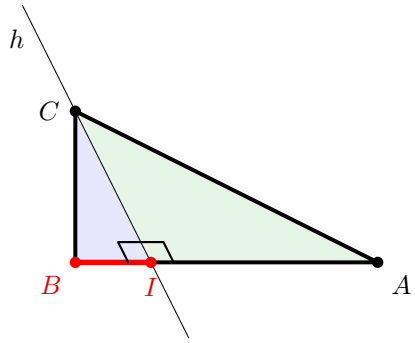
Donc :

$$\widehat{JIL} = \pi - \widehat{NIJ} - \widehat{MIL} = \pi - \widehat{BCA} - \widehat{CAB} = \widehat{ABC} = \frac{\pi}{2}.$$

Donc $IJKL$ est un carré. D'où :

$$\begin{aligned} \text{Aire}(MNOP) &= \text{Aire}(IJKL) + 4 \cdot \text{Aire}(ABC) \\ \Longrightarrow \quad (AB + BC)^2 &= AC^2 + 4 \cdot \frac{AB \cdot BC}{2} \\ \Longrightarrow \quad AB^2 + BC^2 + 2 \cdot AB \cdot BC &= AC^2 + 2 \cdot AB \cdot BC \\ \Longrightarrow \quad AB^2 + BC^2 &= AC^2 \end{aligned}$$

$(\Longleftarrow)$ Soit h la hauteur issue de C dans ABC. On veut montrer que $h = (BC)$. Soit I le point d'intersection de h avec (AB). Montrons alors que $IB = 0$ et donc que $I = B$.



Comme AIC et BIC sont rectangles en I, on a, par le sens direct du théorème, démontré ci-dessus, que :

$$IC^2 + IB^2 = BC^2 \quad \text{et} \quad IA^2 + IC^2 = AC^2.$$

Et comme $AB = AI + IB$ et $AB^2 + BC^2 = AC^2$, on en déduit que :

$$\begin{aligned} IA^2 + IC^2 &= AC^2 \\ \Longrightarrow \quad (AB - IB)^2 + IC^2 &= AB^2 + BC^2 \\ \Longrightarrow \quad AB^2 + IB^2 - 2 \cdot AB \cdot IB + IC^2 &= AB^2 + IC^2 + IB^2 \\ \Longrightarrow \quad 2 \cdot AB \cdot IB &= 0 \\ \Longrightarrow \quad IB &= 0 \qquad (\text{ car } AB \neq 0\ ). \end{aligned}$$

Donc $B = I$, ce qui implique que ABC est rectangle en B.

■

Application. Le théorème de Pythagore permet surtout de vérifier si deux droites sont perpendiculaires ou non. Pour cela, il suffit de nommer A le point d'intersection de ces deux droites, de choisir un point B sur la première et un point C sur la seconde, puis de calculer AB^2, AC^2 et BC^2. Si $AB^2 + AC^2 = BC^2$, alors ces deux droites sont perpendiculaires ; sinon, elles ne le sont pas, en vertu du théorème de Pythagore.

1.3.2 Théorème de Thalès

Voici maintenant l'autre résultat majeur issu des travaux des géomètres de la Grèce Antique. Bien entendu, comme avant, nous allons nous intéresser à pourquoi ce théorème est vrai.

Théorème 1.14: (Thalès)

Soient ABC et AEF deux triangles tels que $B \in (AE)$ et $C \in (AF)$.

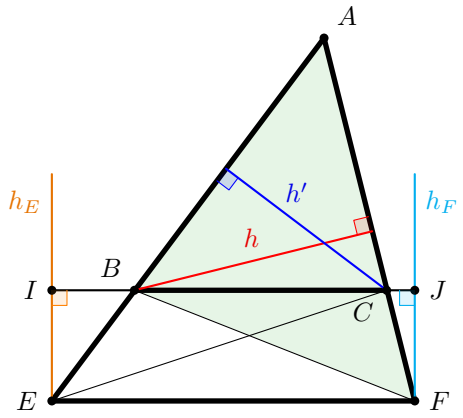
(i) Si $(BC) \parallel (EF)$, alors $\frac{AE}{AB} = \frac{AF}{AC} = \frac{EF}{BC}$.

(ii) Réciproquement, si $\frac{AE}{AB} = \frac{AF}{AC}$, alors $(BC) \parallel (EF)$.

Démonstration On suppose que $B \in [AE]$ et $C \in [AF]$. Ce cas est suffisant pour démontrer le théorème. On laisse le soin au lecteur de s'en convaincre.

(i) Soit h la hauteur issue de B dans le triangle ABC. Alors

$$\left.\begin{array}{l} \text{Aire}(ABC) = \frac{AC \cdot h}{2} \\ \text{Aire}(\ ABF\ ) = \frac{AF \cdot h}{2} \end{array}\right\} \Longrightarrow \frac{AF}{AC} = \frac{\text{Aire}(\ ABF\ )}{\text{Aire}(ABC)}.$$



De même, avec la hauteur h' issue de C dans ABC, on montre que $\frac{AE}{AB} = \frac{\text{Aire}(AEC)}{\text{Aire}(ABC)}$.

Il suffit maintenant montrer que $\text{Aire}(AEC) = \text{Aire}(ABF)$, ou encore que $\text{Aire}(BCE) = \text{Aire}(BCF)$, puisque $\text{Aire}(AEC) = \text{Aire}(ABC) + \text{Aire}(BCE)$ et $\text{Aire}(ABF) = \text{Aire}(ABC) + \text{Aire}(BCF)$.

Soient h_E, la hauteur issue de E dans BCE qui coupe (BC) en I, et h_F, la hauteur issue de F dans BCF qui coupe (BC) en J.

Il est évident que $h_E \parallel h_F$. Et comme $(BC) \parallel (EF)$, $IJFE$ est donc un rectangle. Ainsi, $IE = JF$ et on obtient que

$$\text{Aire}(BCE) = \frac{1}{2}(BC \cdot IE) = \frac{1}{2}(BC \cdot JF) = \text{Aire}(BCF)$$

D'où $\frac{AF}{AC} = \frac{AE}{AB}$.

La preuve de l'égalité $\frac{AE}{AB} = \frac{EF}{BC}$ est laissée en exercice (exercice 1.8).

(ii) Par hypothèse, on a que $\frac{AE}{AB} = \frac{AF}{AC}$.

Soit d, la parallèle à (BC) passant par E et soit F' l'intersection de d avec AF. Par *(i)*, on a que $\frac{AE}{AB} = \frac{AF'}{AC}$. Il en découle alors que :

$$\frac{AF}{AC} = \frac{AF'}{AC} \quad \Longrightarrow \quad AF = AF'.$$

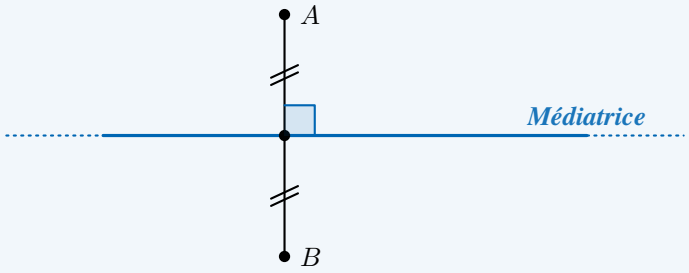
Comme $AF' = AF$ et comme F et F' sont tous les deux sur (AC), on obtient alors que $F = F'$. On en déduit que $d = (EF') = (EF)$ et donc que $(EF) \parallel (BC)$.

■

1.4 Médiatrice

Définition 1.15

Soient $A, B \in \mathcal{P}$ deux points distincts. La ***médiatrice*** du segment $[AB]$ est la droite perpendiculaire à (AB) passant par le milieu de $[AB]$.



Définition 1.16

Soient $A, B \in \mathcal{P}$ distincts. On dit que $M \in \mathcal{P}$ est ***équidistant à A et B*** si $AM = BM$.

Exemple

Si I est le point milieu de $[AB]$, alors $IA = IB$. Donc I est équidistant à A et B et I est aussi sur la médiatrice de $[AB]$.

L'exemple précédent se généralise comme suit :

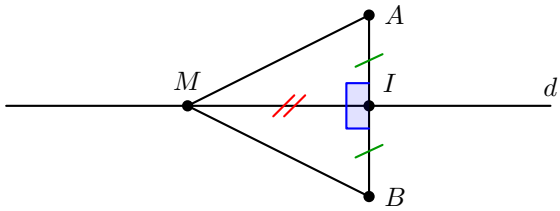
Proposition 1.17

Soit $M \in \mathcal{P}$. M est alors sur la médiatrice de $[AB]$ ***si et seulement si*** M est équidistant à A et à B.

Démonstration Notons d la médiatrice de $[AB]$ et I le milieu de $[AB]$.

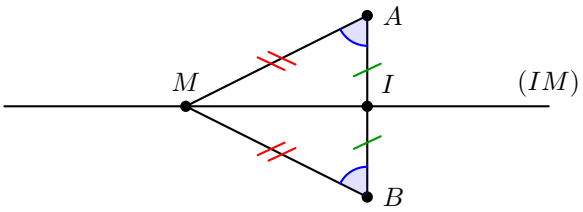
$(\Longrightarrow)$ Supposons que $M \in d$. Alors les triangles MIA et MIB sont isométriques, car

$$\begin{cases} AI = IB \\ MI = MI \\ \widehat{MIA} = \widehat{MIB} = \frac{\pi}{2} \end{cases}$$



D'où $AM = BM$ et donc M est équidistant à A et à B.

$(\Longleftarrow)$ Supposons que M est équidistant à A et à B. Il suffit de montrer que $(IM) \perp (AB)$, car il n'y a qu'une unique droite perpendiculaire à (AB) passant par I.



Le triangle AMB est isocèle en M, car $AM = BM$, donc $\widehat{MAB} = \widehat{MBA}$.
On obtient ainsi :

$$\left.\begin{array}{r} MA = BM \\ AI = BI \\ \widehat{MAI} = \widehat{MBI} \end{array}\right\} \implies \text{les triangles } MAI \text{ et } MBI \text{ sont isométriques.}$$

D'où $\widehat{MIB} = \widehat{MIA}$ et

$$\begin{aligned} 2\widehat{MIB} &= \widehat{MIB} + \widehat{MIA} = \widehat{BIM} + \widehat{MIA} \\ &= \widehat{BIA} \\ &= \pi \qquad (\text{ car } B, I, A \text{ sont alignés. }) \end{aligned}$$

Donc $\widehat{MIB} = \frac{\pi}{2}$ et finalement on obtient que $(IM) \perp (AB)$.

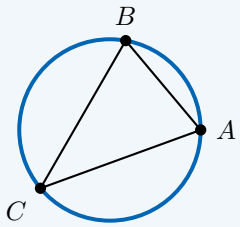
■

1.5 Triangles, droites et points remarquables

1.5.1 Médiatrice et cercle circonscrit

Définition 1.18

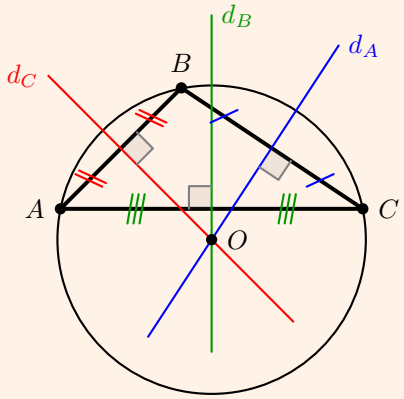
Le ***cercle circonscrit*** à un triangle ABC est le cercle passant par A, B et C.



Il faudrait se poser la question si un tel cercle existe. La réponse est oui, comme le montre la proposition suivante :

Proposition 1.19

Les médiatrices d'un triangle ABC sont ***concourantes*** (se coupent au même point) en le centre du cercle circonscrit à ABC.



Démonstration Soient d_A la médiatrice de $[BC]$, d_B la médiatrice de $[AC]$, d_C la médiatrice de $[AB]$ et O le point d'intersection de d_A et d_B.

On va montrer que $d_A \cap d_C = \{O\}$.

Notons que $d_A \cap d_B \neq \emptyset$, car sinon on aurait que $d_A \parallel d_B$, ce qui impliquerait que A, B, C soient alignés, ce qui est impossible puisque ABC est un triangle.

On a $OA = OC$, car $O \in d_B$, et $OB = OC$, car $O \in d_A$. On a alors que $OA = OB$, ce qui implique que $O \in d_C$. Il s'ensuit que $\{O\} = d_A \cap d_B \cap d_C$.

Et comme $OA = OB = OC$, les points A, B, C sont donc sur un cercle centré en O : le cercle circonscrit à ABC.

■

Corollaire 1.20

Soientt $A, B, C \in \mathcal{P}$ trois points non alignés. Il existe alors un unique cercle passant par A, B et C.

Démonstration

Existence : L'existence suit du fait que ABC est un triangle. On peut alors prendre le cercle circonscrit à ABC.

Unicité : Soit $\mathcal{C}$ un cercle de centre O passant par A, B et C. On a alors $OA = OB = OC$. Ainsi, O est le point d'intersection des médiatrices de ABC et donc $\mathcal{C}$ est le cercle circonscrit à ABC.

■

Remarque Ce corollaire implique en particulier que si deux cercles s'intersectent en trois points distincts, alors ils sont égaux. Ainsi, si deux cercles distincts se coupent, ils se coupent en un point (ils sont tangents) ou en deux points (ils sont sécants).

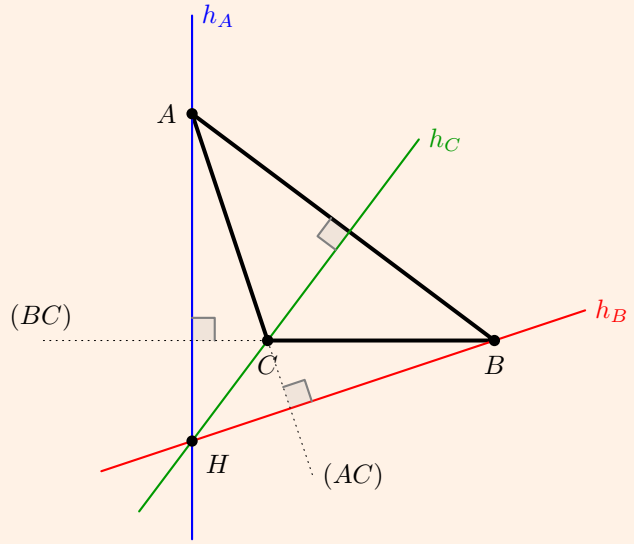
1.5.2 Hauteurs et orthocentre d'un triangle

Définition 1.21: (Hauteur d'un triangle)

La ***hauteur*** d'un triangle ABC issue du sommet A est la droite prependiculaire à (BC) et passant par A.

Proposition 1.22

Les hauteurs d'un triangle ABC sont concourantes au même point H, appelé l'***orthocentre*** de ABC.



Démonstration Soit A' le point d'intersection de (BC) avec la hauteur issue de A, B' le point d'intersection de (AC) avec la hauteur issue de B et C' le point d'intersection de (AB) avec la hauteur issue de C. Les hauteurs sont donc (AA'), (BB') et (CC').

Soient d_A la parallèle à (BC) passant par A, d_B la parallèle à (AC) passant par B et d_C la parallèle à (AB) passant par C. On a que d_A, d_B et d_C ne sont pas parallèles, car $(AB), (BC)$ et (AC) ne le sont pas (ABC est un triangle).

Soient A_1 tel que $\{A_1\} = d_B \cap d_C$, B_1 tel que $\{B_1\} = d_A \cap d_C$ et C_1 tel que $\{C_1\} = d_A \cap d_B$.

De ce fait, on obtient que $ACBC_1$ et AB_1CB sont des parallélogrammes. Donc

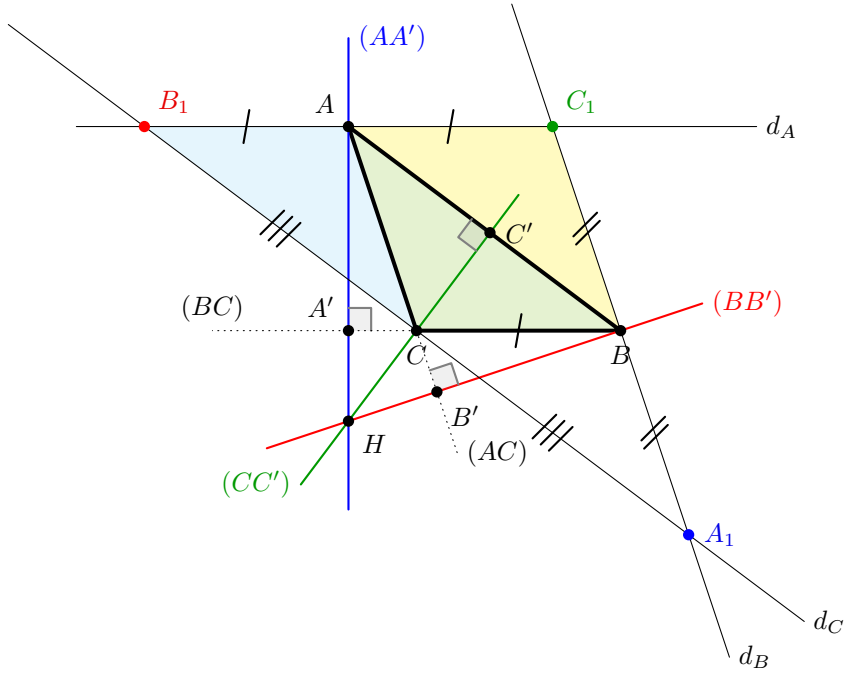
$$C_1A = BC = AB_1 \quad \Longrightarrow \quad A \text{ est le milieu de } [B_1C_1].$$

De même, on montre que B est le milieu de $[A_1C_1]$ et que C est le point milieu de $[A_1B_1]$.

On remarque que :

$$\left.\begin{array}{l}(A_1C_1) \parallel (AC)\\ (BB') \perp (AC)\end{array}\right\} \quad \Longrightarrow \quad (BB') \perp (A_1C_1)$$

Et comme B est le milieu de $[A_1C_1]$, on en déduit que (BB') est la médiatrice de $[A_1C_1]$.



De même, on montre que (CC') est la médiatrice de $[A_1B_1]$ et que (AA') est la médiatrice de $[B_1C_1]$.

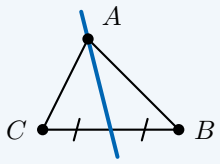
Donc (AA'), (BB') et (CC') sont les médiatrices du triangle $A_1B_1C_1$ et sont donc concourantes.

■

1.5.3 Médianes et centre de gravité

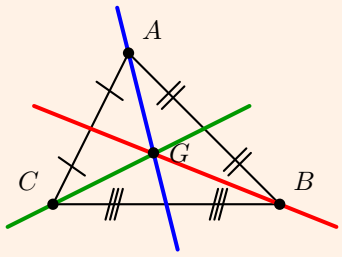
Définition 1.23: (Médiane)

La ***médiane*** issue du sommet A d'un triangle ABC est la droite passant par A et le milieu de $[BC]$.



Proposition 1.24

Soit ABC un triangle. Ses médianes sont concourantes au centre de gravité du triangle : ce point G est situé au $\frac{2}{3}$ de chaque médiane à partir du sommet correspondant.



Démonstration Voir exercice 1.18.

1.6 Axiomes de la géométrie euclidienne du plan et de l'espace

Nous avons rencontré précédemment deux axiomes : la règle de ***l'invariance des angles par translation*** (axiome 1.4) et la règle des ***triangles isométriques*** (axiome 1.7). On a vu l'importance de ces axiomes dans le processus déductif qui nous a permis de démontrer plusieurs résultats fondamentaux en géométrie. Nous allons maintenant nous intéresser de plus près à la notion d'axiome. Lorsqu'un mathématicien se place dans un contexte particulier, ici la géométrie euclidienne du plan et de l'espace, il se dote avant tout de « règles du jeu », d'axiomes, qui sont un ensemble de principes régissant ce monde mathématique particulier. L'objectif étant de se servir de ces seuls axiomes pour expliquer, c'est-à-dire démontrer, toutes les observations qu'il peut faire dans ce contexte particulier. L'avantage d'une telle méthode déductive est, par exemple, que lorsque le mathématicien rencontre un environnement dans lequel tous les axiomes de la géométrie euclidienne du plan et de l'espace sont vérifiés, il sait alors automatiquement que tous les résultats connus en géométrie euclidienne y seront valides.

Notons que la liste présentée dans ce chapitre n'est pas exhaustive. Nous n'exposerons pas, par exemple, les axiomes concernant les angles ; ces derniers seront bien définis au chapitre 3.

On se rappellera que des axiomes sont des énoncés qui ne se démontrent pas, mais ils sont posés comme « règles du jeu » en géométrie euclidienne du plan et de l'espace. Nous allons articuler cette section autour de l'objectif suivant :

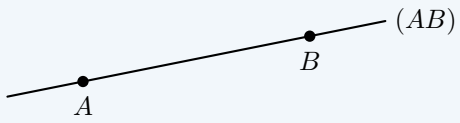
développer l'idée qu'en mathématiques, beaucoup de résultats sont contraints par très peu d'hypothèses de bases (les axiomes).

1.6.1 Axiomes des droites

Tout d'abord, nous allons présenter quelques principes de base qui régissent les droites, les plans et l'espace.

Axiome I

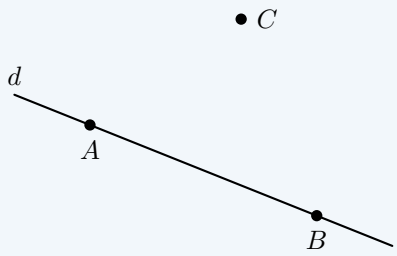
Soient A, B deux points dans l'espace $\mathcal{E}$. Il ***existe*** une ***unique*** droite passant par A et B. On note cette droite (AB).



Nous « savons bien » qu'il existe toujours un point qui n'est pas sur une droite donnée et que sur cette droite on peut toujours prendre deux points distincts ; c'est en fait un axiome :

Axiome II

Soit d une droite de l'espace $\mathcal{E}$. Il existe alors deux points distincts $A, B \in d$, $A \neq B$, tels que $d = (AB)$ et il existe $C \in \mathcal{E}$ tel que $C \notin d$.

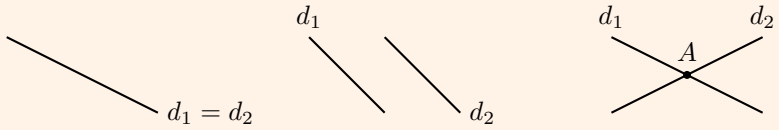


Application (position relative de deux droites) On peut déjà déduire de ces deux seuls axiomes les propriétés bien connues suivantes. Il est intéressant d'observer que ces propriétés, bien que naturelles dans l'imaginaire collectif, ne sont pas des axiomes mais se déduisent immanquablement des deux axiomes ci-dessus.

Proposition 1.25

Soient d_1 et d_2 deux droites de l'espace. On a alors l'un des cas suivants :

- ***(i)*** il existe un point $A \in \mathcal{E}$ tel que $d_1 \cap d_2 = \{A\}$ (on dit que d_1 et d_2 sont ***sécantes***) ;
- ***(ii)*** $d_1 = d_2$;
- ***(iii)*** $d_1 \cap d_2 = \emptyset$.



Démonstration Si $d_1 \cap d_2 = \emptyset$, on se trouve dans la troisième situation.

Supposons maintenant qu'il existe un point $A \in d_1 \cap d_2$. Alors on a deux cas : soit $d_1 \cap d_2 = \{A\}$, ce qui est la première situation, soit il existe au moins un autre point $B \in d_1 \cap d_2$ distinct de A. Dans ce cas $A, B \in d_1$ et $A, B \in d_2$. l'axiome I nous garantit alors que $d_1 = (AB) = d_2$, ce qui est la deuxième situation.

■

Remarque La situation $d_1 \cap d_2 = \emptyset$ ne veut pas forcément dire que ces droites sont parallèles dans l'espace. Nous allons revenir sur ce point un plus loin dans cette section.

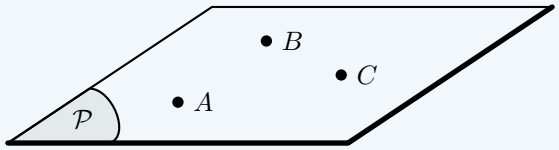
Bien entendu, un lecteur pourrait se demander pourquoi nous ne prenons pas pour axiome toutes les propriétés qui nous semblent naturelles. Et bien, une des raisons est que le mathématicien aime réduire au maximum ses hypothèses de travail afin de maximiser ce qu'il doit retenir. Un deuxième argument est qu'il désire rendre ses prédictions les plus précises possibles. En quelque sorte, on pourrait dire que le mathématicien croit que moins il y a d'inconnus, ici les axiomes, plus les prédictions seront fiables.

On va maintenant se doter de règles concernant les plans dans l'espace.

1.6.2 Axiomes des plans (section facultative)

Axiome III

Par trois points non alignés passe un et un seul plan. On note ce plan $\mathcal{P} = (ABC)$.



Ceci donné, on se pose la question suivante : Peut-on déduire de ce troisième axiome que la droite (AB) est entièrement contenue dans le plan ? En d'autres mots, peut-on déduire de ce troisième axiome que n'importe quel point de (AB) est aussi un point de (ABC) ? La réponse est non, et c'est pourquoi nous posons ce quatrième axiome :

Axiome IV

Si A et B sont deux points d'un plan $\mathcal{P}$, alors (AB) est entièrement incluse dans ce plan. On note $(AB) \subseteq \mathcal{P}$.

Application 1 : On peut déduire avec l'ajout de ces axiomes la propriétés bien connue suivante. Il est à nouveau intéressant d'observer que cette propriété se déduit immanquablement des axiomes ci-dessus.

Proposition 1.26

(i) Soit d une droite et un point C tel que $C \notin d$. Alors il existe un unique plan passant par C et contenant d.

(ii) Si $\mathcal{P}$ est un plan, alors il existe trois points non alignés A, B, C tel que $\mathcal{P} = (ABC)$.

Démonstration En vertu de l'axiome II, on peut prendre deux points distincts A, B sur d.

Comme $C \notin d$, A, B et C ne sont pas alignés.

l'axiome III nous assure alors qu'il existe un unique plan $\mathcal{P} = (ABC)$.

Enfin, l'axiome IV nous assure que $d = (AB)$ est contenu dans cet unique plan $\mathcal{P}$. Ceci montre les deux énoncés cherchés.

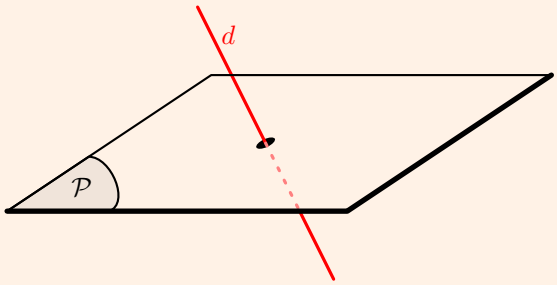
■

Application 2 (position relative d'un plan et d'une droite) :

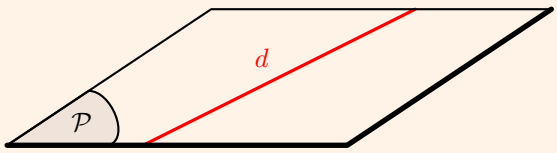
Proposition 1.27

Soient d une droite et $\mathcal{P}$ un plan. On a alors l'un des cas suivants :

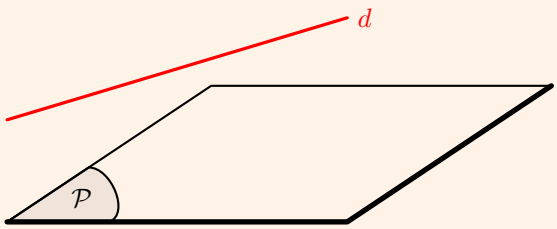
(i) d coupe $\mathcal{P}$ en un point ;



(ii) $d \subset \mathcal{P}$;



(iii) $d \cap \mathcal{P} = \emptyset$.



DÉMONSTRATION Si $d \cap \mathcal{P} = \emptyset$, on a la situation ***(iii)***.

Si $d \cap \mathcal{P} \neq \emptyset$ on a deux cas possibles :

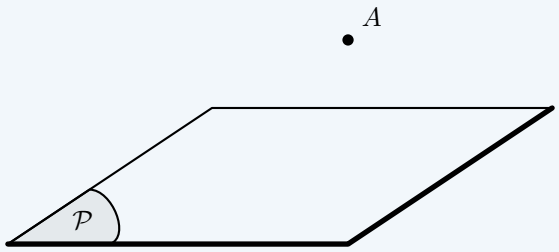
- $d \cap \mathcal{P} = \{A\}$, donc on est dans la situation ***(i)*** ;
- d coupe $\mathcal{P}$ en au moins deux points distincts A et B. En vertu de l'AXIOME IV, on obtient $d = (AB) \subseteq \mathcal{P}$, car $A, B \in \mathcal{P}$. On est donc dans la situation ***(ii)***.

■

Finalement, il nous faut un dernier axiome pour s'assurer des trois dimensions de l'espace, car cette propriété ne découle pas des axiomes précédents.

AXIOME V

Il existe toujours un point de l'espace non contenu dans un plan donné.



REMARQUE Ce cinquième axiome peut être vu comme l'équivalent pour les plans de l'AXIOME II concernant les droites.

Position relative de deux plans de l'espace :

Nous avions conclu la partie sur les axiomes de droites par la position relative de deux droites dans l'espace, déduite des axiomes des droites. De façon surprenante, il n'est pas possible de faire la même chose pour les plans. Pourquoi ? Recommençons le même raisonnement que dans la démonstration de la PROPOSITION 1.25[4].

Deux situations sont possibles :

- Soit les deux plans $\mathcal{P}$ et $\mathcal{P}'$ sont disjoints (c'est-à-dire $\mathcal{P} \cap \mathcal{P}' = \emptyset$),
- soit ils ne le sont pas (c'est-à-dire $\mathcal{P} \cap \mathcal{P}' \neq \emptyset$).

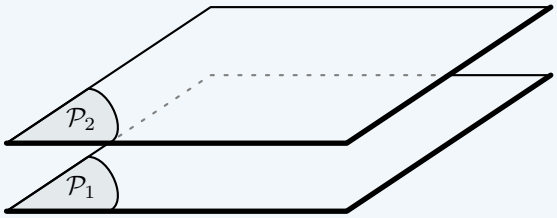
Supposons que $\mathcal{P} \cap \mathcal{P}'$ contiennent au moins trois points A, B, C non alignés. Alors en vertu de l'AXIOME III, on a $\mathcal{P} = (ABC) = \mathcal{P}'$. Dans le cas où $\mathcal{P} \cap \mathcal{P}'$ ne contient que des points alignés, alors l'intersection $\mathcal{P} \cap \mathcal{P}'$ est une droite, en vertu de l'AXIOME IV.

Mais que peut-on déduire si $\mathcal{P} \cap \mathcal{P}' = \{A\}$ un unique point ? Souhaite-t-on que l'intersection de deux plans dans l'espace puisse être un point ? Dans le contexte de la géométrie euclidienne, la position relative de deux plans ne peut pas se déduire des axiomes précédents. Il faut donc se donner en axiome ce qu'on entend par position relative de deux plans.

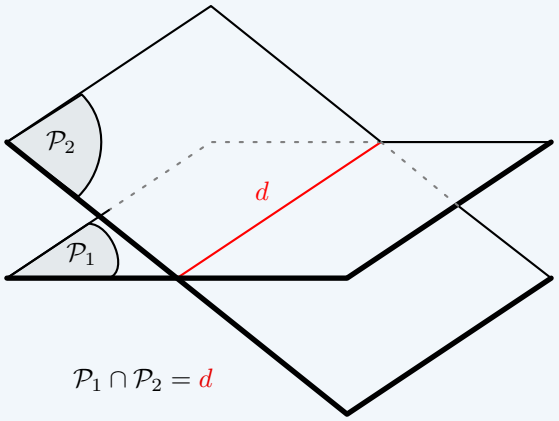
4. On invite le lecteur à aller relire cette démonstration pour réaliser à quel point ces deux raisonnements sont similaires.

Axiome VI

L'intersection de deux plans distincts est soit vide, soit une droite.



$\mathcal{P}_1 \cap \mathcal{P}_2 = \emptyset$



$\mathcal{P}_1 \cap \mathcal{P}_2 = d$

1.7 Droites coplanaires et parallélisme

Nous avions fait la remarque plus haut que deux droites de l'espace d'intersection vide ne sont pas forcément parallèles. Pour justifier cela, nous allons devoir préciser la définition de droites parallèles.

1.7.1 Droites parallèles dans un plan

Définition 1.28

Ont dit que deux droites d'un même plan sont ***parallèles*** si elle ne se croisent pas ou si elles sont confondues.

Notations

Soient d et d' deux droites d'un plan. On note $d \cap d'$ l'ensemble des points d'intersection de d et d'. De plus,

- $d \parallel d'$ est la notation pour les droites d et d' sont parallèles ;
- $(d \parallel d') \iff \big(d \cap d' = \emptyset \ \vee \ d \cap d' = d\big)$ (Attention ! Ceci n'est plus vrai pour deux droites quelconques de l'espace, comme nous allons le voir dans la partie suivante.)

Proposition 1.29

Soient d et d' deux droites d'un plan $\mathcal{P}$. Il y a deux cas possibles :

- $d \parallel d'$: les deux droites sont parallèles ;
- $d \cap d' = \{A\}$ où $A \in \mathcal{P}$ est un point : les droites sont sécantes (elles se coupent en un point).

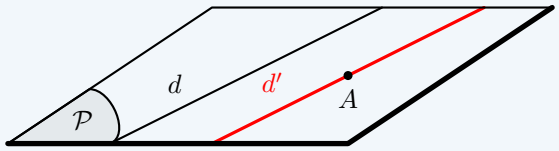
Démonstration Cette proposition est une reformulation de la proposition 1.25.

La question que nous devrions immanquablement nous poser est la suivante : existe-t-il une unique parallèle à une droite donnée passant par un point donné ? On ne peut pas répondre à cette question en géométrie sans poser le célèbre axiome d'Euclide.

1.7.2 Axiome d'Euclide et transitivité du parallélisme

Axiome d'Euclide (postulat des parallèles)

Soient d une droite et A un point qui n'est pas sur d. Soit $\mathcal{P}$ l'unique plan défini par d et A. Il ***existe*** une ***unique*** droite d' dans $\mathcal{P}$ passant par A et parallèle à d.



Remarque Les mathématiciens ont longtemps essayé de démontrer cet axiome à partir des autres. C'est au XIX^{e} siècle que l'on a découvert des modèles d'« autres géométries » où le cinquième axiome d'Euclide n'est pas vérifié (ex : géométrie elliptique et hyperbolique). Cela révolutionna les mathématiques, et par extension la physique (théorie de la relativité), et par extension...

La proposition qui suit, et en particulier le troisième point, est fortement liée au postulat d'Euclide : il existe des géométries dans lesquelles la transitivité du parallélisme n'est pas vérifiée.

La notion de relation d'équivalence, qui intervient dans la proposition suivante, est présentée dans l'annexe B. Le lecteur y trouvera les définitions de réflexivité, de symétrie et de transitivité, accompagnées d'exemples.

Proposition 1.30

La relation ***être parallèle*** dans le plan est une relation d'équivalence, c'est-à-dire :
Si d_1, d_2, d_3 sont trois droites d'un plan $\mathcal{P}$, on a

- $d_1 \parallel d_1$ (***réflexivité***) ;
- $d_1 \parallel d_2 \implies d_2 \parallel d_1$ (***symétrie***) ;
- $d_1 \parallel d_2$ et $d_2 \parallel d_3 \implies d_1 \parallel d_3$ (***transitivité***).

Démonstration Le fait que la relation ***être parallèle*** soit symétrique et réflexive suit immédiatement des définitions. Pour le fait qu'elle soit transitive, voir exercice 1.20***(b)*** (ce résultat nécessite l'axiome d'Euclide).

1.7.3 Droites parallèles dans l'espace (section facultative)

Définition 1.31

(i) On dit que des points sont ***coplanaires*** s'ils sont contenus dans le même plan ;

(ii) On dit que deux droites sont ***coplanaires*** si elles sont contenues dans un même plan ;

(iii) Deux droites sont ***parallèles*** si elles satisfont les deux conditions suivantes :

- elles sont coplanaires ;
- elles sont parallèles dans l'unique plan qui les contient.

Remarque

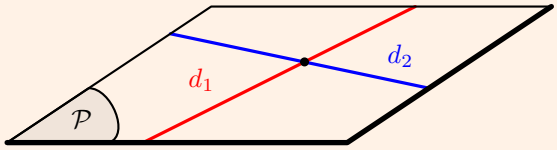
- On déduit du troisième et du cinquième axiome la proposition suivante : dans l'espace, il existe toujours 4 points non coplanaires ;
- Deux droites non sécantes et non coplanaires ne sont pas parallèles ;
- Il existe un unique plan contenant deux droites parallèles distinctes (pourquoi ?).

On peut maintenant reformuler de manière plus précise la proposition 1.25.

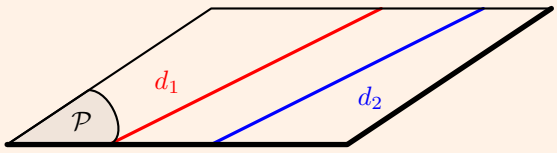
Proposition 1.32

Soient d_1 et d_2 deux droites de l'espace. Alors on a l'un des cas suivants :

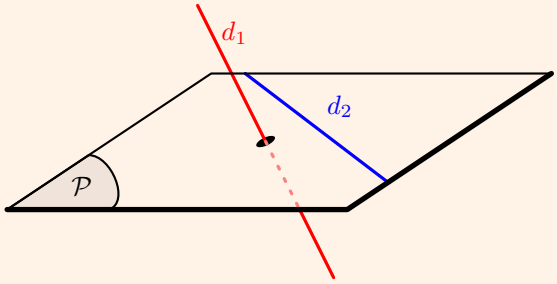
(i) d_1 et d_2 sont sécantes (et donc coplanaires) ;



(ii) $d_1 \parallel d_2$ (et donc coplanaires) ;



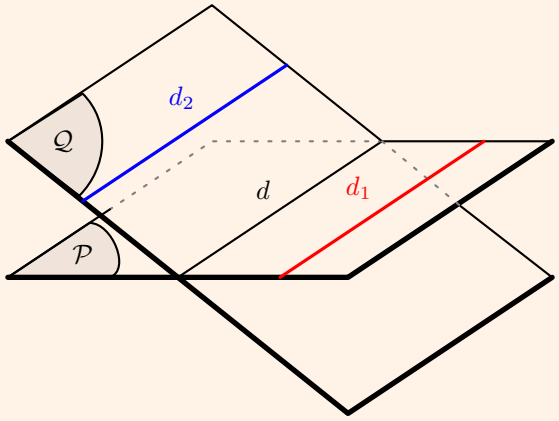
(iii) $d_1 \cap d_2 = \emptyset$ et ne sont pas coplanaires.



Nous voulons maintenant démontrer que la relation ***être parallèle dans l'espace*** pour les droites est une relation d'équivalence. Pour cela nous aurons besoin du résultat préliminaire suivant :

Théorème 1.33: (théorème du toit)

Soient $\mathcal{P}$ et $\mathcal{Q}$ deux plans sécants (donc distincts) et soit $d = \mathcal{P} \cap \mathcal{Q}$. Si $d_1 \subseteq \mathcal{P}$ et $d_2 \subseteq \mathcal{Q}$ sont parallèles, alors $d \parallel d_1$ et $d \parallel d_2$.



Démonstration Supposons que d_1 coupe d en A. Montrons que l'on obtient une contradiction.

Soit $\mathcal{R}$ le plan contenant d_1 et d_2 (ce plan existe, car $d_1 \parallel d_2$). Alors

$$\left.\begin{array}{r} A \in d_1 \cap d \\ d_1 \subset \mathcal{R} \\ d \subset \mathcal{Q} \end{array}\right\} \implies A \in \mathcal{R} \cap \mathcal{Q}$$

On sait aussi que $d_2 \subset \mathcal{R}$, donc $\mathcal{R}$ est l'unique plan qui contient d_2 et A. Or, comme $d_2 \subset \mathcal{Q}$, $\mathcal{Q}$ est aussi l'unique plan contenant d_2 et A. Alors $\mathcal{R} = \mathcal{Q}$. Ainsi, d, d_1 et d_2 sont coplanaires et donc $\mathcal{P} = \mathcal{Q}$, ce qui est absurde, car par hypothèse ces deux plans sont sécants. On obtient donc que $d_1 \parallel d$. On procède de même pour montrer que $d_2 \parallel d$.

■

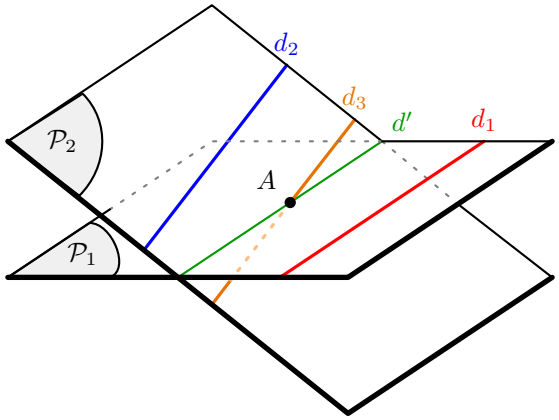
Corollaire 1.34

La relation ***être parallèle dans l'espace*** pour les droites est une relation d'équivalence, c'est-à-dire : si d_1, d_2, d_3 sont trois droites de $\mathcal{E}$, on a

- $d_1 \parallel d_1$ (***symétrique***) ;
- $d_1 \parallel d_2 \implies d_2 \parallel d_1$ (***réflexive***) ;
- $d_1 \parallel d_2$ et $d_2 \parallel d_3 \implies d_1 \parallel d_3$ (***transitive***).

Démonstration (transitivité) On fait l'hypothèse que $d_1 \parallel d_2$ et $d_2 \parallel d_3$.

Soit $\mathcal{P}_1$ le plan contenant d_1 et $A \in d_3$ et soit $\mathcal{P}_2$ le plan contenant d_2 et d_3 ($d_2 \parallel d_3$).



Soit $d' = \mathcal{P}_1 \cap \mathcal{P}_2$. Par le THÉORÈME DU TOIT, on obtient que d' est parallèle à d_1 et à d_2, car $d_1 \parallel d_2$. Or, il existe une unique droite parallèle à d_2 et passant par A (AXIOME AXIOME D'EUCLIDE (POSTULAT DES PARALLÈLES)) :

$$\left.\begin{array}{r} d' \parallel d_2 \\ d_3 \parallel d_2 \\ A \in d_3 \cap d' \end{array}\right\} \implies d_3 = d' \parallel d_1.$$

■

1.7.4 Plans parallèles (section facultative)

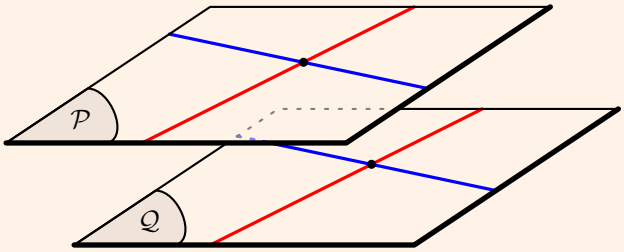
DÉFINITION 1.35

On dit que deux plans sont ***parallèles*** (noté $\mathcal{P}_1 \parallel \mathcal{P}_2$) s'ils sont égaux ou d'intersection vide.

PROPOSITION 1.36

Soient $\mathcal{P}$, $\mathcal{Q}$ et $\mathcal{R}$ trois plans.

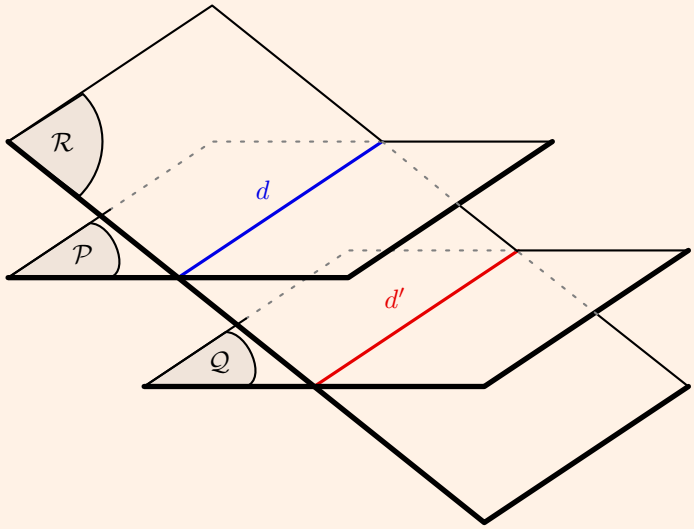
(i) Si deux droites sécantes de $\mathcal{P}$ sont parallèles à deux droites sécantes de $\mathcal{Q}$, alors $\mathcal{P} \parallel \mathcal{Q}$.



(ii) La relation ***être parallèle dans l'espace*** pour les plans est une relation d'équivalence. C'est-à-dire :

- $\mathcal{P} \parallel \mathcal{P}$ (***symétrique***).
- $\mathcal{P} \parallel \mathcal{Q} \implies \mathcal{Q} \parallel \mathcal{P}$ (***réflexive***).
- $\mathcal{P} \parallel \mathcal{Q}$ et $\mathcal{Q} \parallel \mathcal{R} \implies \mathcal{P} \parallel \mathcal{R}$ (***transitive***).

(iii) Si $\mathcal{P} \parallel \mathcal{Q}$ et $\mathcal{R}$ coupe $\mathcal{P}$ en une droite d, alors $\mathcal{R}$ coupe $\mathcal{Q}$ en $d' \parallel d$.



Démonstration

(i) Supposons que $\mathcal{P} \cap \mathcal{Q} \neq \emptyset$, alors il existe une droite $d \subseteq \mathcal{P} \cap \mathcal{Q}$ (On va montrer en fait que $\mathcal{P} = \mathcal{Q}$). On a deux cas : soit $\mathcal{P} \cap \mathcal{Q} = \mathcal{P}$ et alors $\mathcal{P} = \mathcal{Q}$, soit $\mathcal{P} \cap \mathcal{Q} = d$. On va montrer que ce dernier cas est absurde. Posons d_1 et d_1' les deux droites sécantes de $\mathcal{P}$ respectivement parallèles à d_2 et d_2', les deux droites sécantes de $\mathcal{Q}$.

Comme $\mathcal{P}$ et $\mathcal{Q}$ sont sécants en d et que $d_1 \subseteq \mathcal{P}, d_2 \subseteq \mathcal{Q}$ et $d_1 \parallel d_2$, on a par le théorème du toit que $d \parallel d_1$ et $d \parallel d_2$. De même, on montre que $d \parallel d_1'$ et $d \parallel d_2'$. Par transitivité, on obtient que $d_1 \parallel d_1'$, ce qui est absurde. Donc $\mathcal{P} \cap \mathcal{Q} \neq d$ et ainsi $\mathcal{P} = \mathcal{Q}$.

(ii) Le fait que cette relation est réflexive et symétrique se déduit facilement de la définition. On suppose que $\mathcal{P}$, $\mathcal{Q}$ et $\mathcal{R}$ sont deux à deux distincts (sinon il n'y a rien à démontrer). Soit d et d' deux droites sécantes de $\mathcal{Q}$ et soit $A \in \mathcal{P}$, alors le plan contenant A et d coupe $\mathcal{P}$ en une droite $d_P \subseteq \mathcal{P}$. Donc d_P et d sont coplanaires. Comme $\mathcal{P} \cap \mathcal{Q} = \emptyset$ ($\mathcal{P} \parallel \mathcal{Q}$ et $\mathcal{P} \neq \mathcal{Q}$), on a $d_P \cap d = \emptyset$, car $d_P \subseteq \mathcal{P}$ et $d \subseteq \mathcal{Q}$. Donc $d_p \parallel d$. La relation est donc aussi transitive, c'est une relation d'équivalence.

De même, on construit la droite $d_p' \parallel d', d_P' \subseteq \mathcal{P}$. Comme d et d' sont sécantes, d_P et d_P' le sont aussi (à vérifier).

Procédant de même, on construit deux droites sécantes dans $\mathcal{R}$, d_R et d_R' tel que $d_R \parallel d$ et $d_R' \parallel d'$. Par transitivité des droites parallèles dans l'espace et par (1), on obtient donc que $\mathcal{P} \parallel \mathcal{R}$.

(iii) Supposons $\mathcal{P} \neq \mathcal{Q}$, on a donc que $\mathcal{P} \cap \mathcal{Q} = \emptyset$. Si $\mathcal{R} \cap \mathcal{Q} = \emptyset \Longrightarrow \mathcal{R} \parallel \mathcal{Q}$. Donc, $\mathcal{R} \parallel \mathcal{P}$, car $\mathcal{P} \parallel \mathcal{Q}$ par (2). Or $\mathcal{R} \cap \mathcal{P} = d$ ce qui, par contradiction, entraine que $\mathcal{R} \cap \mathcal{Q} \neq \emptyset$ et $\mathcal{R} \neq \mathcal{Q}$. Donc $\mathcal{R}$ coupe $\mathcal{Q}$ en une droite $d' \subseteq \mathcal{Q}$. Comme $\mathcal{P} \cap \mathcal{Q} = \emptyset$, $d' \subseteq \mathcal{Q}$ et $d \subseteq \mathcal{P}$, on a que $d \cap d' = \emptyset$. Or $d, d' \subseteq \mathcal{R}$ sont coplanaires, donc $d \parallel d'$.

■

Contrairement au cas des droites, l'unicité d'un plan parallèle à un plan donné passant par une droite donnée ne nécessite pas de nouvel axiome.

Corollaire 1.37

Soit $\mathcal{P}$ un plan et $A \notin \mathcal{P}$. Il ***existe*** alors un ***unique*** plan $\mathcal{Q}$ passant par A et parallèle à $\mathcal{P}$.

Démonstration Supposons par l'absurde qu'il existe $\mathcal{Q}$ et $\mathcal{R}$ deux plans tels que $\mathcal{Q} \parallel \mathcal{P}$ et $\mathcal{R} \parallel \mathcal{P}$ et $A \in \mathcal{Q} \cap \mathcal{R} = d$. Alors, par ***(iii)*** de la précédente proposition, on a que $\mathcal{R} \cap \mathcal{P} = d'$ une droite. Ceci contredit $\mathcal{R} \parallel \mathcal{P}$. Donc $\mathcal{Q} \cap \mathcal{R} \neq d \Longrightarrow \mathcal{Q} = \mathcal{R}$ (car $\mathcal{Q} \cap \mathcal{R} \neq \emptyset$).

1.8 Orthogonalité dans l'espace (section facultative)

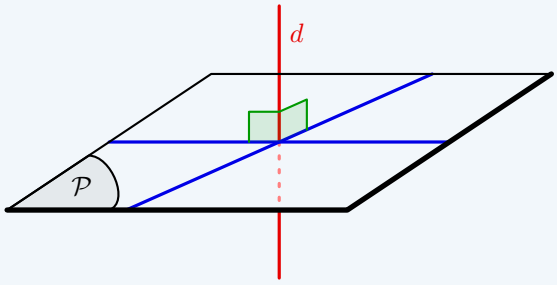
1.8.1 Droites orthogonales et plans perpendiculaires

Avant de conclure ce chapitre, nous allons passer en revue les définitions et certains des résultats les plus utiles concernant la notion d'orthogonalité dans l'espace. Ces notions s'appuient sur la notion d'angle dont nous n'exposerons les principes précis que dans le chapitre 3. On invite le lecteur à penser à démontrer ces résultats dans le but de parfaire la compréhension de la différence entre axiomes et propositions démontrables.

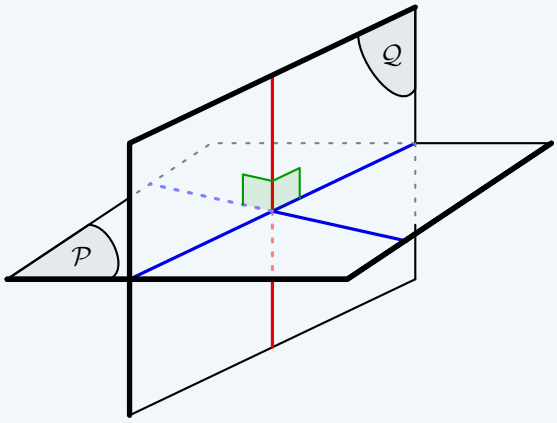
Définition 1.38

(i) Deux droites d et d' sont dites ***orthogonales*** si elles sont parallèles à deux droites perpendiculaires (c-à-d à deux droites qui se coupent en angle droit). On note $d \perp d'$.

(ii) Une droite d et un plan $\mathcal{P}$ sont ***orthogonaux*** si d est orthogonale à toutes les droites de $\mathcal{P}$. On note $d \perp \mathcal{P}$.

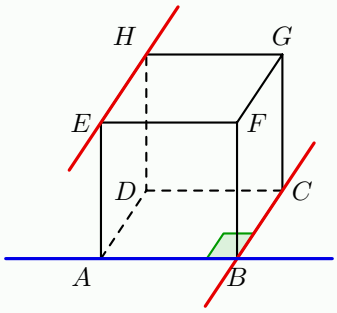


(iii) Deux plans sont ***perpendiculaires*** si l'un d'eux contient une droite orthogonale à l'autre plan. On note $\mathcal{P} \perp \mathcal{Q}$.



Exemple

Soit $ABCDEFGH$ un cube. Malgré qu'elles ne se coupent pas, les groites (EH) et (AB) sont orthogonales, car $(EH) \parallel (BC)$ et les droites (AB) et (BC) sont perpendiculaires.



Proposition 1.39

Si $d \parallel d'$ et $d \perp d''$, alors $d' \perp d''$.

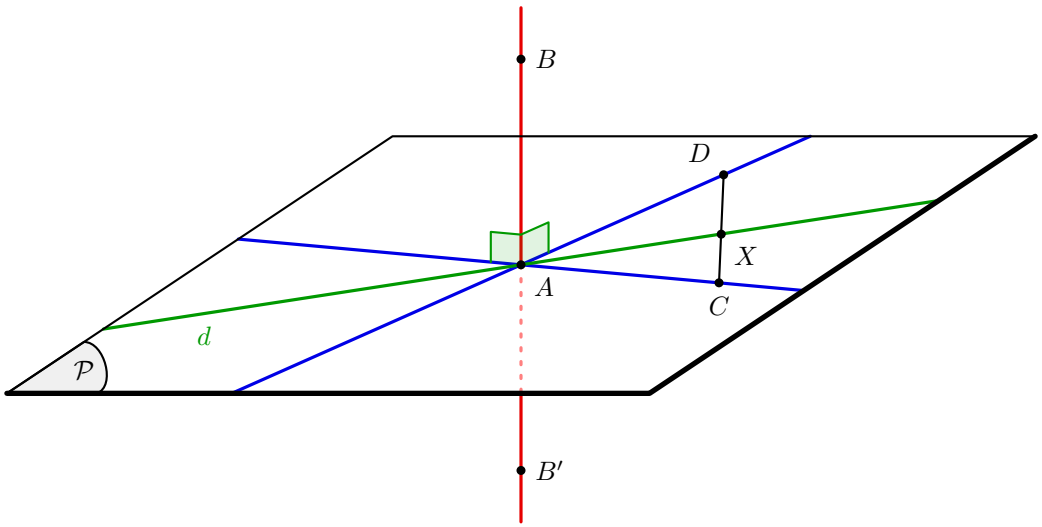
Démonstration Voir exercice 1.21*(a)*.

■

Théorème 1.40

Si une droite est orthogonale à deux droites sécantes d'un plan, alors elle est orthogonale à ce plan. Autrement dit, il suffit qu'une droite soit orthogonale à deux droites sécantes d'un plan pour qu'elle soit orthogonale à toutes les droites de ce plan.

Démonstration (Idée de la preuve)



Hypothèses : $(B'B) \perp (AD)$ et $(BB') \perp (AC)$.

Question : Est-ce que $(BB') \perp d$?

On choisit B, B' tels que A est le milieu de $[BB']$ et on choisit X tel que $\{X\} = (DC) \cap d$.

Par hypothèse (AC) est la médiatrice de $[BB']$ dans le plan (ABC), donc $BC = B'C$. De même, $BD = B'D$.

$\Longrightarrow$ BDC et $B'DC$ sont des triangles isométriques.

$\Longrightarrow$ $\widehat{BCD} = \widehat{B'CD}$ et $BC = B'C$ et $CX = CX$.

$\Longrightarrow$ $B'CX$ et BCX sont des triangles isométriques.

$\Longrightarrow$ $BX = B'X$.

$\Longrightarrow$ X est sur la médiatrice de $[BB']$ dans le plan (BB'X).

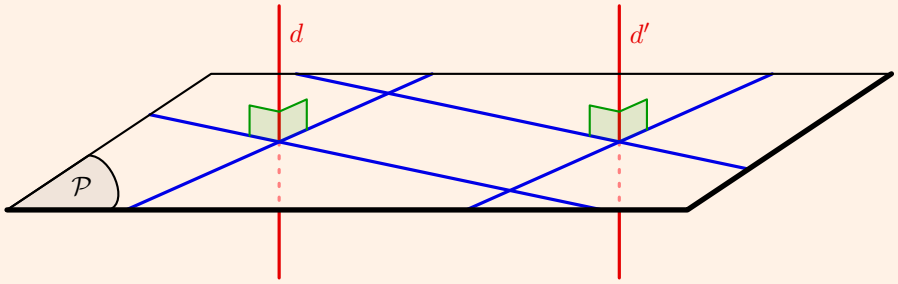
$\Longrightarrow$ $d = (AX) \perp (BB')$.

La suite de la preuve est laissée en exercice.

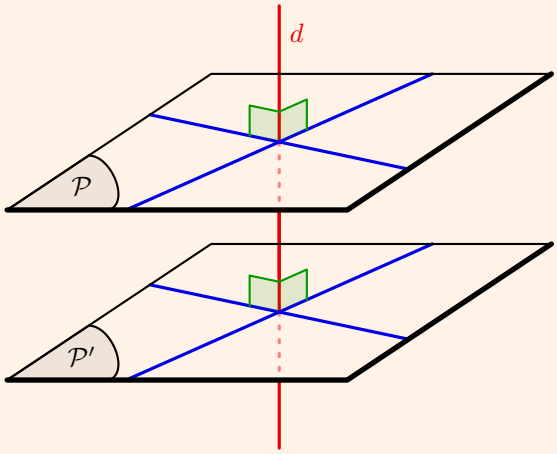
■

Corollaire 1.41

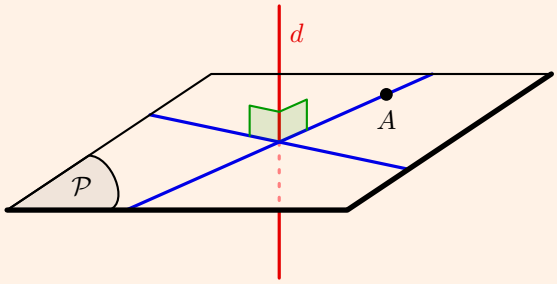
(i) Si deux droites sont parallèles, alors un plan orthogonal à l'une l'est aussi à l'autre.



(ii) Si deux plans sont parallèles, alors toute droite orthogonale à l'un l'est aussi à l'autre.



(iii) Par un point de l'espace, il ne passe qu'un unique plan orthogonal à une droite donnée.

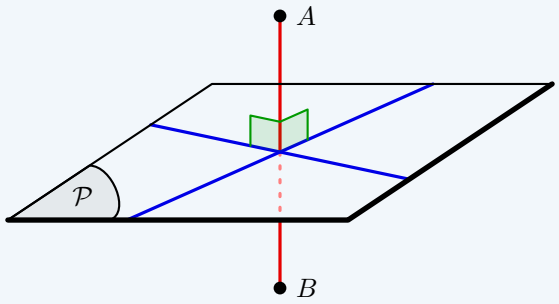


Démonstration Voir exercice 1.22.

On termine cette section en donnant la définition du plan médiateur, dont le rôle dans l'espace est analogue au rôle de la médiatrice dans le plan.

Définition 1.42: (Plan médiateur)

Le ***plan médiateur*** d'un segment $[AB]$ est le plan orthogonal à (AB) passant par le milieu de $[AB]$.



Proposition 1.43

M est dans le plan médiateur de $[AB] \iff AM = BM$.

Démonstration Il suffit de noter que M est sur la médiatrice de $[AB]$ dans le plan (ABM).

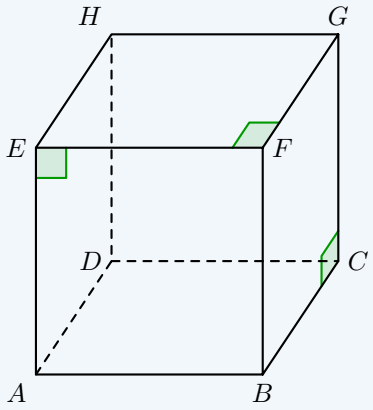
■

1.8.2 Application : le cube

Grâce aux quelques axiomes que nous nous sommes donnés et aux résultats que l'on en a déduit, nous sommes capables de démontrer, de prédire, les propriétés bien connues du cube en partant de sa plus simple définition.

Définition 1.44

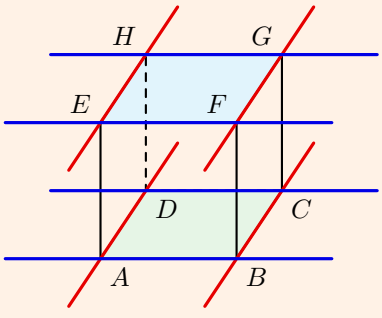
Un cube $ABCDEFGH$ est un solide dont toutes les faces sont des carrés.



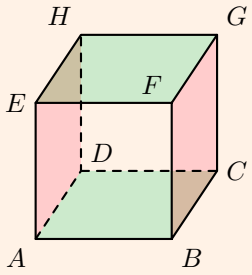
Proposition 1.45

Le cube $ABCDEFGH$ a les propriétés suivantes :

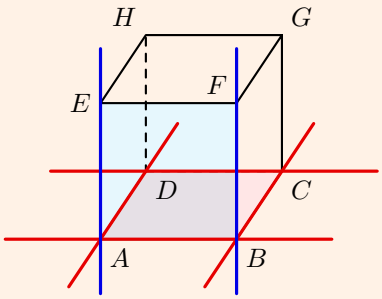
(i) les droites définies par les arêtes des faces opposées $ABCD$ et $EFGH$ sont telles que $(AB) \parallel (DC) \parallel (EF) \parallel (HG)$ et $(AD) \parallel (BC) \parallel (EH) \parallel (FG)$;



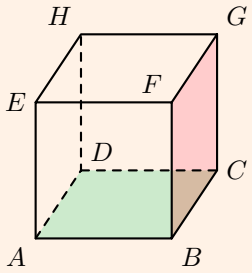
(ii) les plans définis par les faces opposées sont parallèles ;



(iii) les droites définies par les arêtes de la face $ABCD$ sont orthogonales aux droites (AE) et (FB) de la face $AEFB$;



(iv) les plans définis par des faces adjacentes sont perpendiculaires.



Démonstration

(i) Montrons par exemple que $(AB) \parallel (HG)$. Comme $ABCD$ est un carré, $(AB) \parallel (CD)$. Comme $HDCG$ est un carré, $(CD) \parallel (HG)$. Par transitivité de la relation ***être parallèle***, on en déduit que $(AB) \parallel (HG)$. On procède de même pour les autres arêtes.

(ii) Montrons par exemple que $(ABC) \parallel (EFG)$. On sait que les deux droites sécantes (AB) et (BC) sont respectivement parallèles aux deux droites sécantes (EF) et (FG), car $ABFE$ et $BCGF$ sont des carrés. En vertu de la PROPOSITION 1.36*(i)*, on en déduit que $(ABC) \parallel (EFG)$. On procède de même pour les autres plans.

(iii) Montrons par exemple que $(CD) \perp (AE)$. Comme $AEHD$ est un carré, $(AE) \parallel (HD)$. Comme $HDCG$ est un carré, $(HD) \perp (CD)$. Par définition on obtient bien que $(CD) \perp (AE)$. On procède de même pour toutes les autres arêtes.

(iv) Montrons par exemple que $(BFG) \perp (ABC)$. Comme (BFG) contient la droite (BF) qui est perpendiculaire aux droites sécantes (AB) et (BC), on déduit du THÉORÈME 1.40 que $(BF) \perp (ABC)$ et donc que $(BFG) \perp (ABC)$. On procède de même pour les autres plans.

■

1.9 Construction à la règle et au compas (section facultative)

Dans l'Antiquité, les mathématiciens ne concevaient pas les nombres comme nous le faisons aujourd'hui. Les mathématiciens grecs, en particulier, représentaient souvent les grandeurs numériques par des longueurs de segments : le nombre 5, par exemple, pouvait être représenté par un segment dont la longueur était égale à cinq fois une longueur choisie comme unité. Ils se passionnaient donc pour les problèmes de construction géométrique, puisque la construction de nouvelles longueurs leur permettait de représenter de nouvelles grandeurs. Certains de ces problèmes, tels que la quadrature du cercle, sont restés ouverts pendant plus de deux millénaires ; leur impossibilité n'a été démontrée qu'au XIX^{e} siècle.

Les règles utilisées pour ces constructions étaient simples. Les voici.

On se donne :

- une unité de longueur (un bout de bois, par exemple) ;
- une règle non graduée (pour tracer des droites et des segments) ;
- un compas (pour tracer des cercles).

On peut donc :

- avec la règle, tracer le segment $[AB]$, et donc considérer sa longueur AB, lorsque les points A et B sont donnés ;
- avec la règle, tracer la droite (AB) lorsque les points A et B sont donnés ;
- avec le compas, étant donnés deux points O et A, tracer le cercle de centre O et de rayon OA.

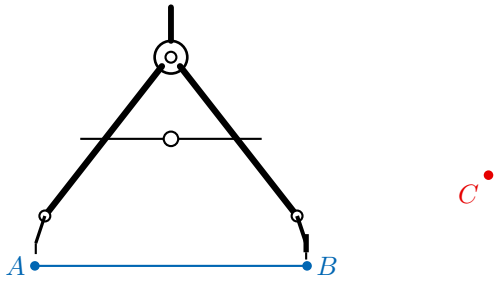
Dans la réalité, une corde pouvait jouer à la fois le rôle de la règle et celui du compas, comme nous l'avons vu lorsque nous avons formulé les hypothèses permettant de résoudre le problème de l'architecte en fonction du nombre de points d'attache utilisés.

1.9.1 Report de longueurs à la règle et au compas

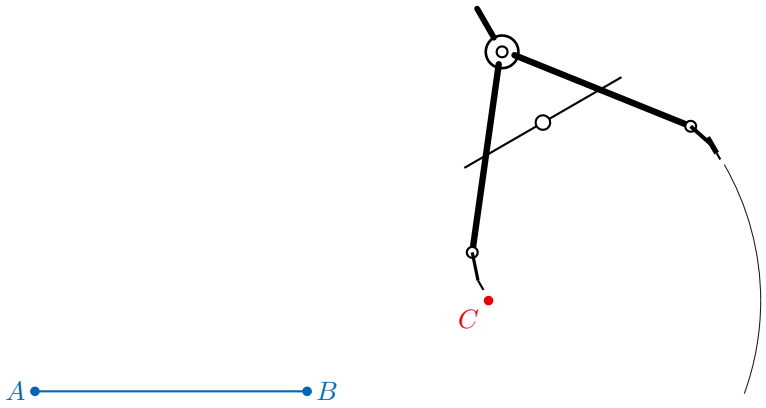
La première question que l'on peut se poser est la suivante :

> Étant donné un segment $[AB]$ de longueur AB et un point C, comment construire un segment $[CD]$ ayant la même longueur que $[AB]$, c'est-à-dire tel que $CD = AB$?

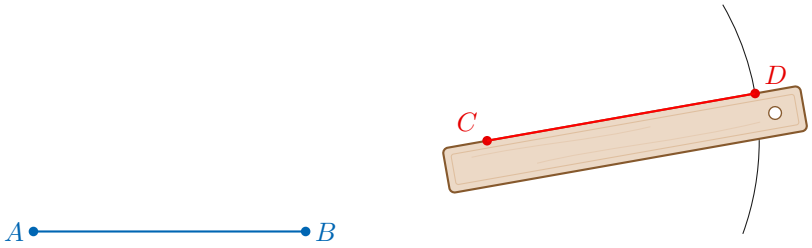
Commençons par placer la pointe du compas en A, puis ouvrons-le jusqu'au point B. L'écartement du compas est alors exactement égal à la longueur AB.



Sans modifier cet écartement, plaçons ensuite la pointe du compas en C et traçons un arc de cercle de centre C et de rayon AB.



Choisissons enfin un point D quelconque sur cet arc de cercle et traçons le segment $[CD]$ à l'aide de la règle.



Puisque D appartient à l'arc de cercle de centre C et de rayon AB, nous avons nécessairement

$$CD = AB.$$

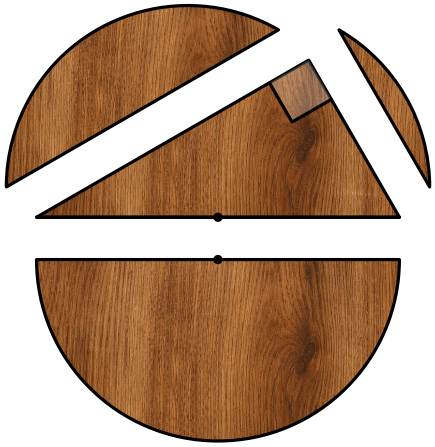
Nous avons donc reporté la longueur AB à partir du point C.

Dans la suite de cette section, nous utiliserons ce principe de base pour construire différents objets à la règle et au compas.

1.9.2 Construction d'un angle droit et d'une équerre.

Pour construire un angle droit, il suffit de tracer un cercle puis de tracer un diamètre $[BC]$ et enfin de choisir un point A sur ce cercle qui n'est pas sur le diamètre. L'angle $\widehat{BAC}$ est donc un angle droit. Autrement dit, les droites (AB) et (AC) sont perpendiculaires.

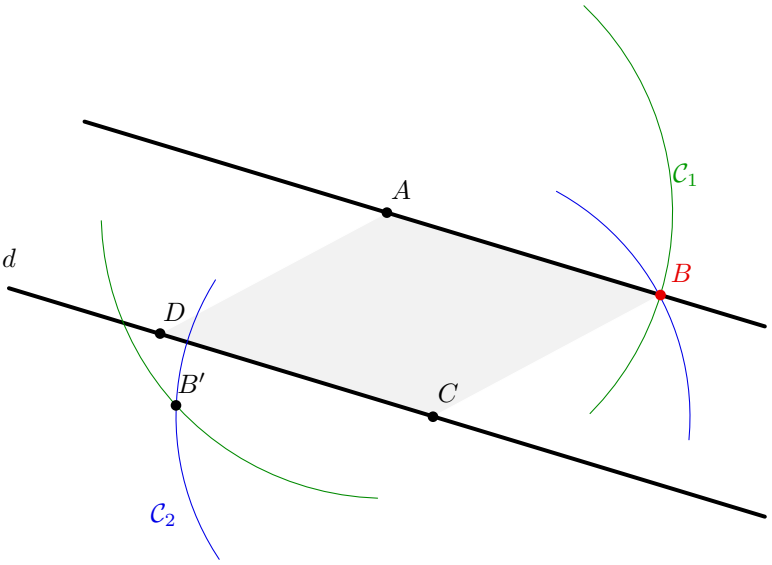
Il suffit donc, pour construire une équerre, de prendre une planche de bois, d'y tracer un cercle, puis un diamètre, et enfin de choisir un point du cercle qui n'est pas sur le diamètre. On scie alors la planche afin d'obtenir un triangle rectangle, en vertu de la proposition ci-dessus.



1.9.3 Construction de la parallèle à une droite donnée passant par un point donné.

La construction qui suit est une conséquence de la règle du parallélogramme (PROPOSITION 1.9).

On se donne un droite d et un point $A \notin d$.



On va utiliser ce que l'on sait du parallélogramme. On trace deux points C et D sur d. Il suffit maintenant de construire le point B pour que $ABCD$ soit un parallélogramme. En effet, on aura ainsi que $d = (CD) \parallel (AB)$ et (AB) sera la droite parallèle à d passant par A.

Pour cela, il suffit de tracer le point B tel que $AB = DC$ et $AD = BC$. Soit $\mathcal{C}_1$ le cercle de centre A et de rayon DC et $\mathcal{C}_2$ le cercle de centre C et de rayon AD. Ces deux cercles se coupent en deux points : seul l'un de ces deux points fera en sorte que $ABCD$ soit un parallélogramme, c'est celui du même côté que A de d (sinon (AB) couperait d). Il suffit alors de tracer la droite (AB).

1.9.4 Les nombres constructibles

La constructibilité des nombres à la règle et au compas est importante. Nous allons voir par exemple que nous pouvons construire $\sqrt{2}$. La question est maintenant : peut-on construire n'importe quel nombre ? Donnons un sens mathématique à cela.

Définition 1.46: (Nombre constructible)

Un nombre a est ***constructible*** s'il existe $A, B \in \mathcal{P}$ que l'on peut construire à la règle et au compas tel que $a = AB$. Autrement dit, s'il existe un segment $[AB]$ de longueur a que l'on peut construire à la règle et au compas.

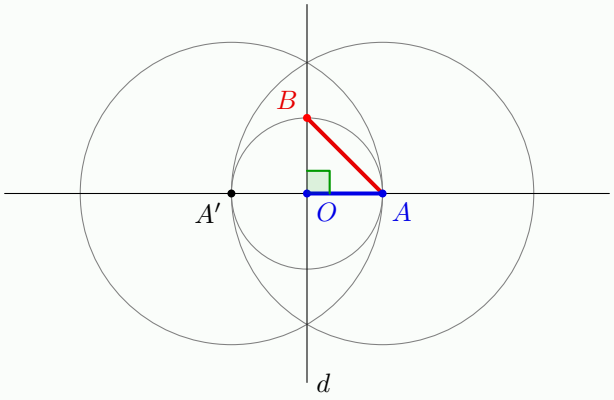
Exemple

Le nombre $\sqrt{2}$ est un nombre constructible. En voici une construction :

Soit le segment unitaire $[OA]$.

On construit ensuite une droite d perpendiculaire à (OA) passant par le point O. Cette construction, illustrée dans la figure qui suit, sera présentée dans les sections suivantes.

On construit finalement $B \in d$ tel que $OB = OA$. Autrement dit, le point B est à une intersection entre la droite d et le cercle de rayon OA centré en O.

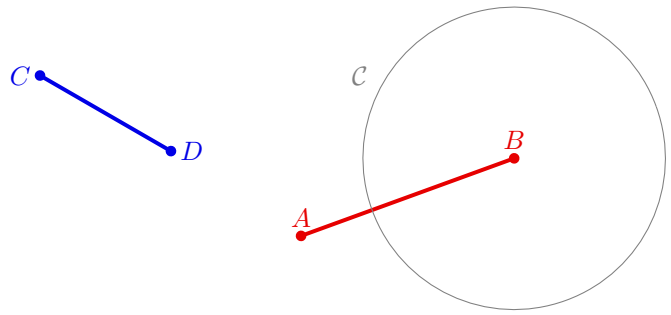


Le segment $[AB]$ est donc de longueur $\sqrt{2}$, selon le théorème de Pythagore.

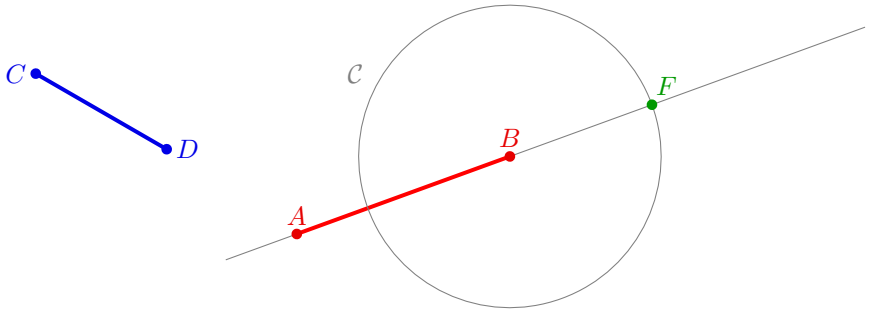
Une question importante est : ***peut-on additionner, soustraire, multiplier ou diviser des nombres constructibles ?***

Addition : On se donne deux segments $[AB]$ et $[CD]$. Peut-on construire un segment $[EF]$ tel que $EF = AB + CD$?

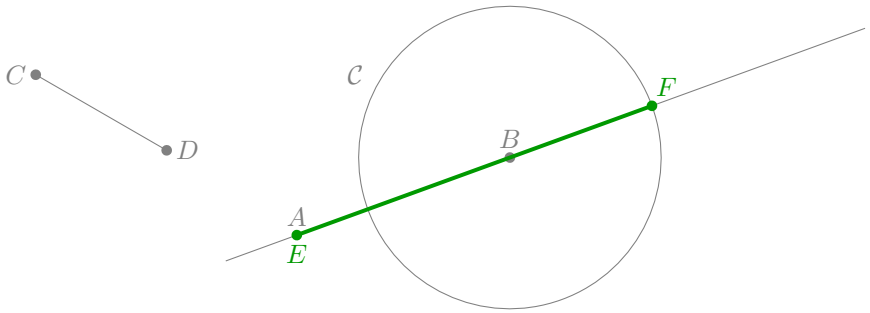
(i) On trace le cercle $\mathcal{C}$ de centre B de rayon CD :



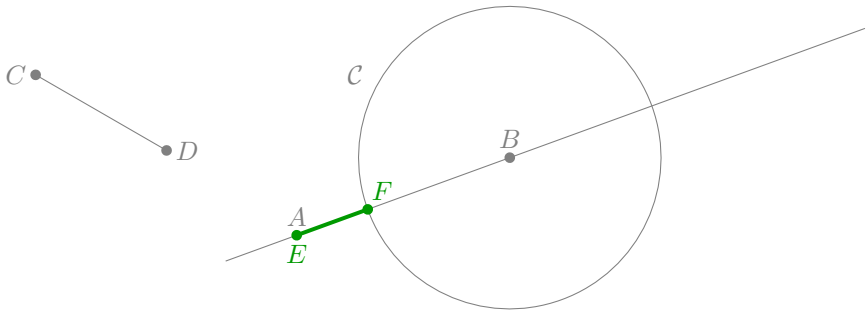
(ii) On trace la droite (AB), puis on note $F \in (AB) \cap \mathcal{C}$ de sorte que A, B et F soient alignés dans cet ordre :



(iii) En posant $E = A$, On obtient le segment $[EF]$ de longueur $EF = AB + BF = AB + CD$:

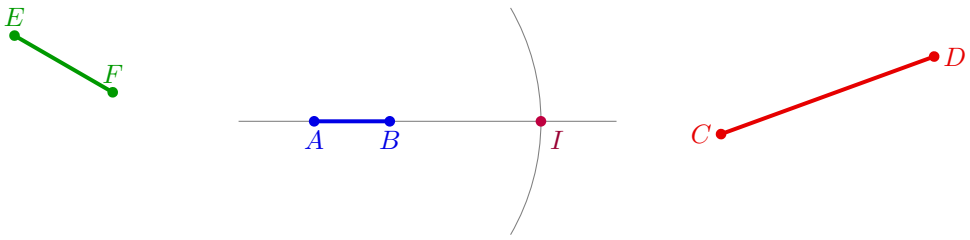


Soustraction : Supposons que $AB > CD$. La construction du segment $[EF]$ tel que $EF = AB - CD$ est similaire à celle de l'addition. Il suffit de poser $E = A$ et $F = [AB] \cap \mathcal{C}$:

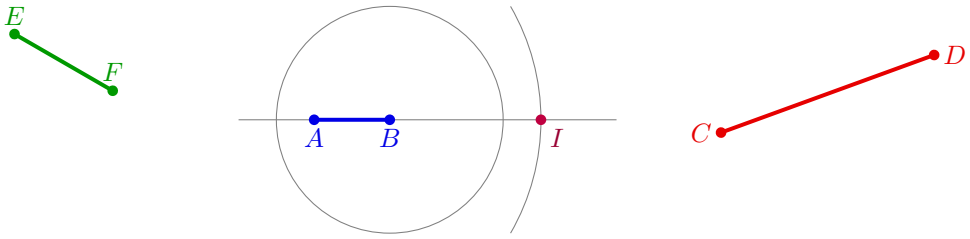


Multiplication : On se donne une unité (un segment $[AB]$ tel que $AB = 1$). Soient deux segments $[CD]$ et $[EF]$, peut-on construire un segment $[IJ]$ tel que $IJ = CD \cdot EF$? Oui ! Grâce au théorème de Thalès :

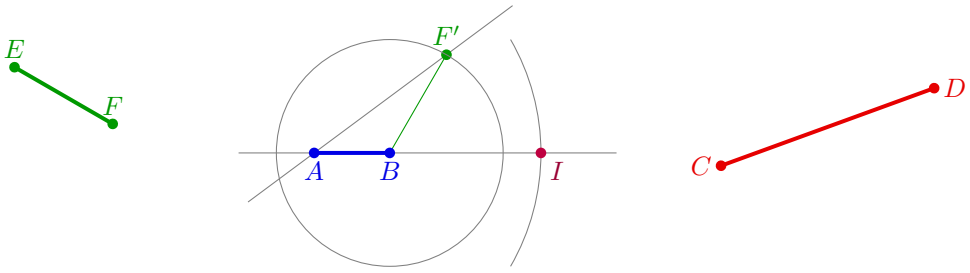
(i) On reporte la longueur CD sur la droite (AB) et on construit I tel que $AI = CD$ et $B \in [AI]$:



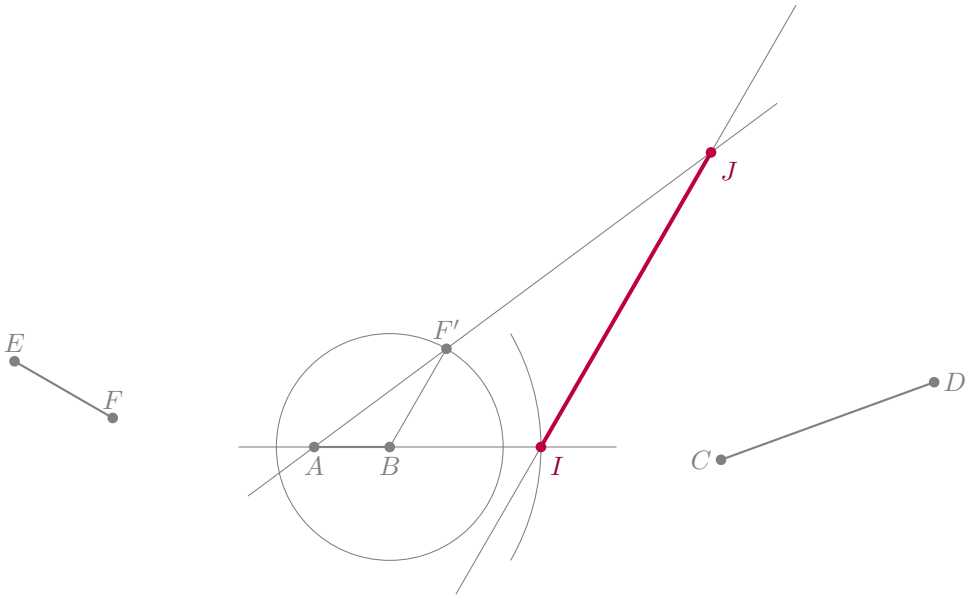
(ii) On trace le cercle de centre B et de rayon EF :



(iii) On trace une droite passant par A et coupant le cercle en F'. On a alors $BF' = EF$:



(iv) En utilisant la méthode vue précédement, on trace la droite parallèle à (BF') passant par I, et on note J son intersection avec (AF') :



Par le THÉORÈME DE THALÈS, on a :

$$\frac{IJ}{BF'} = \frac{AI}{AB} \iff \frac{IJ}{EF} = \frac{CD}{1} \implies IJ = EF \cdot CD$$

Division : À faire à l'EXERCICE 1.10*(d)*.

La recherche des nombres constructibles débouchera sur le développement de l'algèbre et de la théorie de Galois (groupes). Par exemple, l'impossibilité de la quadrature du cercle se traduit par le fait que le nombre π n'est pas constructible.

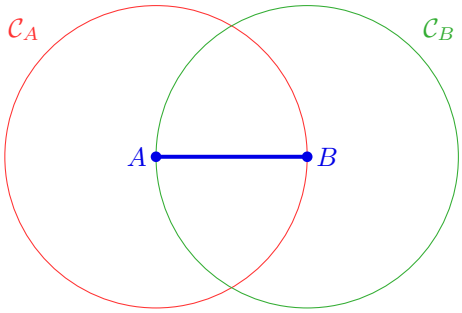
1.9.5 Médiatrice et autres constructions à la règle et au compas

Nul doute qu'il faut être capable de construire une droite perpendiculaire passant par un point donné. La méthode de construction d'un angle droit que nous avons vue auparavant n'est pas adaptée à cet usage. Voici une méthode qui va répondre à nos besoins et qui s'appuie sur la notion de médiatrice.

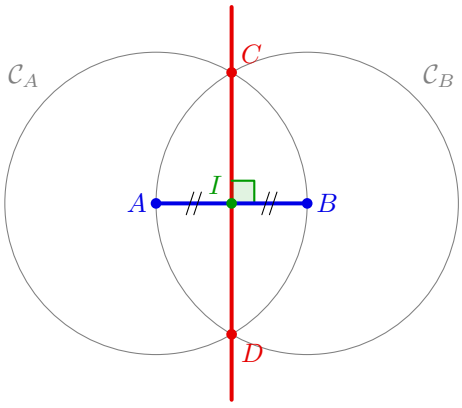
1.9.6 Comment construire le milieu d'un segment (et sa médiatrice) ?

On veut trouver I, le point milieu du segment $[AB]$.

(i) On trace le cercle $\mathcal{C}_A$ de centre A et de rayon AB et le cercle $\mathcal{C}_B$ de centre B et de rayon AB. :



(ii) Les cercles $\mathcal{C}_A$ et $\mathcal{C}_B$ se coupent aux points C et D, puis on trace la droite (CD), qui coupe $[AB]$ au point I :

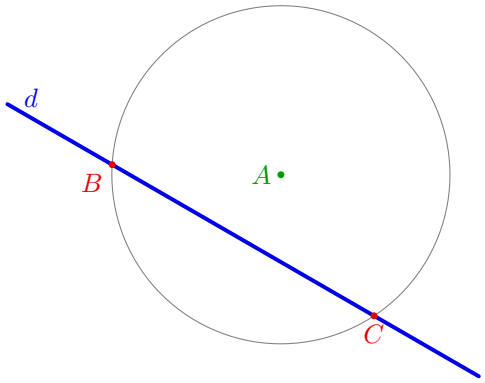


La droite (CD) est la médiatrice du segment $[AB]$. En effet, comme C et D sont équidistants de A et de B, ces deux points appartiennent à la médiatrice de $[AB]$. Par conséquent, (CD) est la médiatrice de $[AB]$. Le milieu de $[AB]$ est donc le point d'intersection I des droites (AB) et (CD).

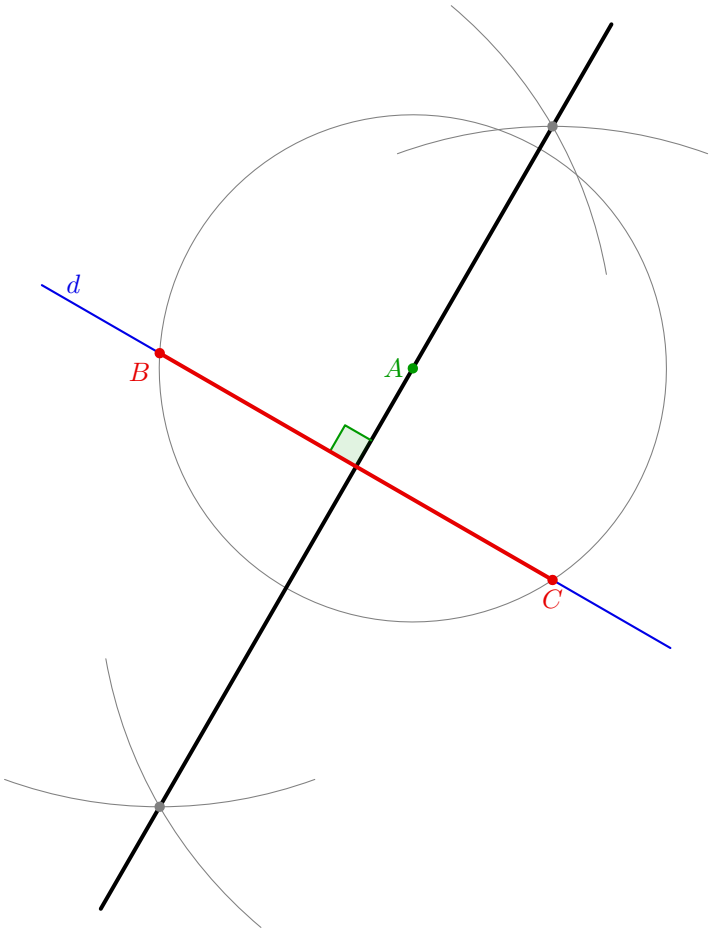
1.9.7 Comment tracer la perpendiculaire à une droite passant par un point donné ?

Soit d une droite et A un point quelconque du plan (pas nécessairement sur la droite). On veut construire la droite perpendiculaire à d qui passe par A.

(i) On trace un cercle de centre A suffisamment grand pou que le cercle coupe d en deux points B et C :



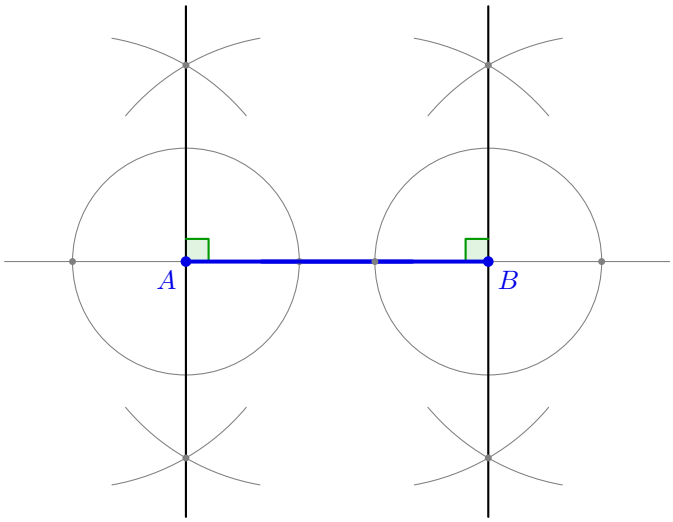
(ii) Comme B et C sont équidistant de A, le point A est sur la médiatrice de $[BC]$, qui est perpendiculaire à d passant par A. Il suffit donc de tracer cette médiatrice (voir SECTION 1.9.6) :



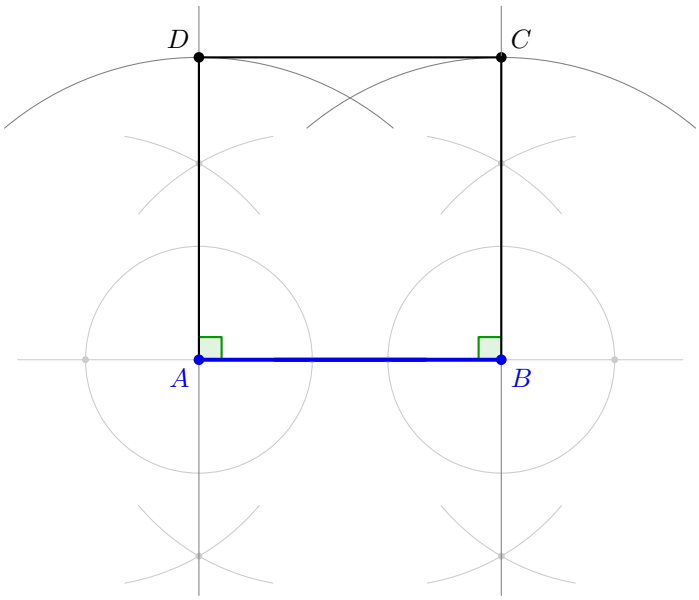
1.9.8 Comment construire un carré dont un côté est un segment $[AB]$ donné ?

Soit le segment $[AB]$. On veut construire un carré dont $[AB]$ est l'un des côtés.

(i) On trace la droite perpendiculaire à (AB) passant par A et la droite perpendiculaire à (AB) passant par B (voir SECTION 1.9.7) :



(ii) On reporte la longueur AB sur ces perpendiculaires en traçant des arcs de cercles de rayon AB et de centres A et B :



On obtient les points C et D. On a finalement que $AB = AD = BC$ et $\widehat{DAB} = \widehat{ABC} = \frac{\pi}{2}$: $ABCD$ est un carré !

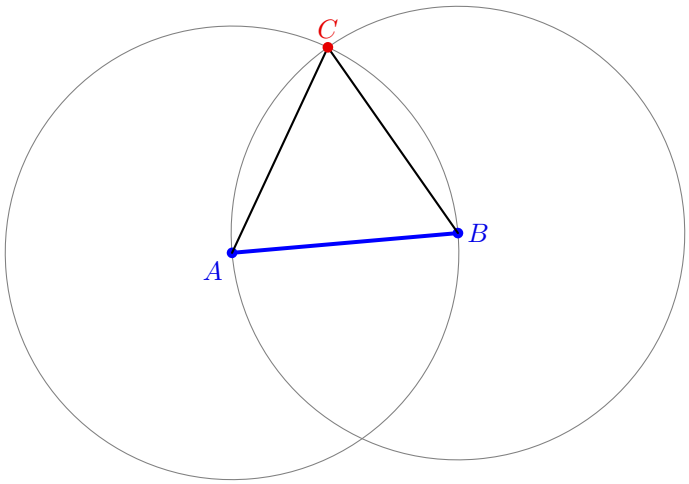
1.9.9 Comment construire un polygone régulier ?

Comment construire un triangle équilatéral de côté $[AB]$ donné ? Tout d'abord, rappelons la définition d'un triangle équilatéral.

Définition 1.47: (Triangle équilatéral)

On dit que ABC est ***équilatéral*** si chacun de ses sommets est équidistant aux deux autres.

À partir d'un segment $[AB]$, on trace le cercle de centre A et de rayon AB et le cercle de centre B et de rayon AB. Ces deux cercles se coupent en deux points. Appelons C l'un de ces points : C est équidistant de A et de B, donc $AB = AC = BC$ et donc ABC est un triangle équilatéral.



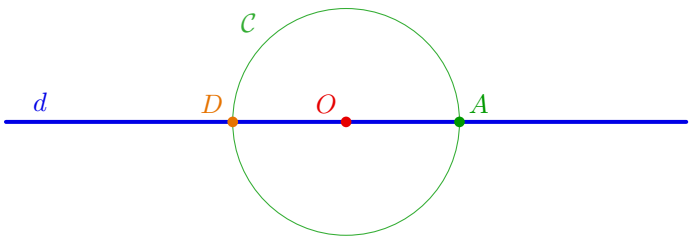
Comment construire un hexagone régulier ?

Définition 1.48: (Hexagone régulier)

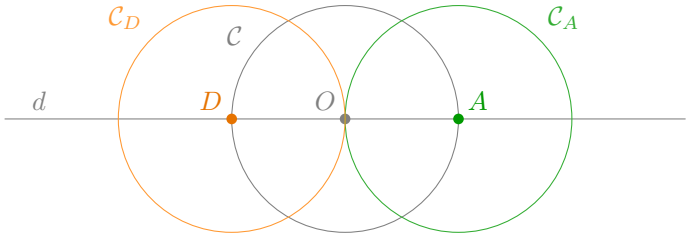
Un ***hexagone régulier*** $ABCDEF$ est la donnée de 6 points tels que $AB = BC = CD = DE = EF = AF$ et les angles sont tous $2\pi/3$.

On considère une droite d et un point $O \in d$.

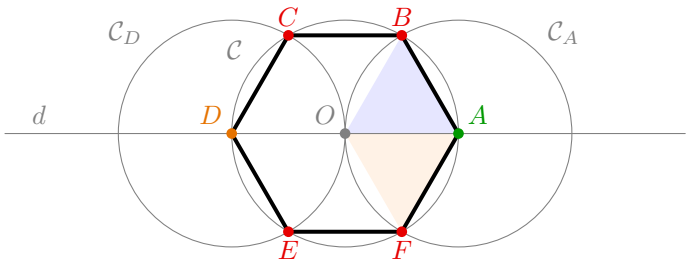
(i) On trace un cercle $\mathcal{C}$ de centre O. On appelle A et D les points d'intersection de $\mathcal{C}$ et d :



(ii) On trace les cercles $\mathcal{C}_A$ et $\mathcal{C}_D$ de centres A et D respectivement et de même rayon $OA = OD =$ rayon de $\mathcal{C}$:



(iii) On note B, C, E et F les nouveaux points obtenus par l'intersection de $\mathcal{C}_A$ et $\mathcal{C}_D$ avec $\mathcal{C}$:



Les triangles OAB et OAF sont équilatéraux, car $OB = OA = OF = AF = AB$. Donc

$$\widehat{BAF} = \widehat{BAO} + \widehat{OAF} = \frac{\pi}{3} + \frac{\pi}{3} = \frac{2\pi}{3}.$$

On peut montrer que l'angle des autres sommets est aussi $\frac{2\pi}{3}$. Ainsi, $ABCDEF$ est un hexagone régulier

Remarque Le problème de la constructibilité des polygones réguliers fut résolu par Gauss et Wantzel (1796-1837) :

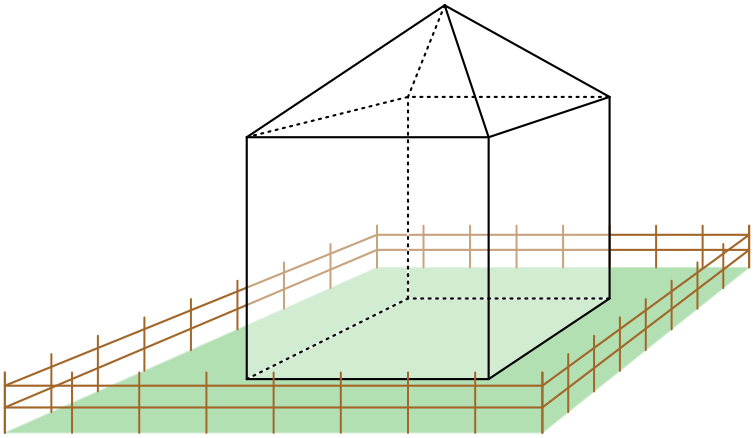
Théorème 1.49: (Gauss-Wantzel)

Un polygone régulier est constructible si et seulement si son nombre de sommet (n) est le produit de puissance de 2 et de nombres premiers distincts de la forme $2^{2^k} + 1$ où $k \in \mathbb{N}$.

Par exemple : $n = 2, 3 = (2^{2^0}+1), 4 = 2^2, 5 = \left(2^{2^1}+1\right), 6 = 2\cdot\left(2^{2^0}+1\right), 8 = 2^3, 10, 12, 15, 16, 17, 20, 24, \ldots$

1.10 Réponse au problème de l'architecte

Après quelques jours de réflexion, notre architecte revint voir le riche citoyen d'Athènes et lui remis le plan ci-dessous :



Il commença alors à lui expliquer comment, avec pour seules ressources une corde et un bout de bois d'un mètre, il pouvait donner des indications aux ouvriers afin de construire un cube parfait de 7 mètres de côté, à partir de la construction de six carrés parfaits de 7 mètres de côté. Le riche citoyen d'Athènes, étant lui-même quelque peu versé dans l'art de la géométrie développé par la jeune école pythagoricienne, acquiesça. Puis l'architecte expliqua une construction de triangles équilatéraux de 7 mètres de côté, destinés à devenir le toit. Le riche citoyen acquiesça encore. Alors l'architecte lui expliqua comment, à l'aide des théorèmes de Thalès et de Pythagore, il lui était possible de placer parfaitement la clôture, dont la longueur mesurerait la hauteur de la pyramide multipliée par la longueur de la diagonale d'un mur.

« Ha ! ha ! » s'écria le riche citoyen d'Athènes, « voici ce qu'il me manquait ! ». Il poursuivit : « Bravo, grand architecte, tu m'as convaincu, mais avant de te donner le contrat, réponds à la question suivante : quelle sera exactement la longueur de ma clôture ? ». L'architecte lui répondit rapidement : « la longueur de la diagonale au carré, soit 49 mètres, ô illustre citoyen ». Le citoyen lui confia alors la réalisation de sa demeure, qui fut longtemps connue comme l'une des plus parfaites d'Athènes.

Nous invitons le lecteur qui se demanderait pourquoi la clôture mesure 49 mètres de long de faire l'EXERCICE 1.29.

1.11 Exercices

Quelques résultats classiques

Exercice 1.1 (Démonstration de la Règle du parallélogramme) Soit $ABCD$ un quadrilatère convexe. Montrer l'équivalence des énoncés suivants :

- ***(i)*** $ABCD$ est un parallélogramme ;
- ***(ii)*** Les diagonales de $ABCD$ se coupent en leur milieu ;
- ***(iii)*** $AB = CD$ et $(AB) \parallel (CD)$.

Exercice 1.2 Soit $ABCD$ un parallélogramme. Montrer l'équivalence des énoncés suivants :

- ***(i)*** $ABCD$ est un rectangle (c-à-d un de ses angles est droit) ;
- ***(ii)*** Tous ses angles sont droits ;
- ***(iii)*** Ses diagonales sont de la même longueur.

Exercice 1.3 Montrer que la somme des angles d'un quadrilatère convexe est $0 = 2\pi$.

Exercice 1.4 Soient $\mathcal{C}$ un cercle de centre O et $\mathcal{C}'$ un cercle de centre O'. On suppose que $\mathcal{C}$ et $\mathcal{C}'$ sont sécants en A et B. On note E le point diamétralement opposé à B sur $\mathcal{C}$ et F le point diamétralement opposé à B sur $\mathcal{C}'$. Montrer que A, E et F sont alignés.

Les théorèmes de Pythagore et de Thalès

Exercice 1.5 Soit $AZST$ un rectangle avec $AT = 6\,\text{cm}$ et $TS = 5\,\text{cm}$. Soient C un point sur le segment $[TS]$ et R un point sur $[SZ]$. On suppose que $TC = 2\,\text{cm}$ et $SR = 1\,\text{cm}$. Le triangle ACR est-il rectangle ?

Exercice 1.6 Un avion vole au dessus de Montréal. Il doit atterrir dans l'aéroport situé à $19\,\text{km}$ du centre-ville. Pour descendre, il parcourt $20\,\text{km}$. À quelle altitude volait-il au-dessus du centre-ville ?

Exercice 1.7 Soit $ABCD$ un quadrilatère convexe quelconque. Soient I milieu de $[AB]$, J milieu de $[BC]$, K milieu de $[CD]$ et L milieu de $[AD]$. Montrer que $IJKL$ est un parallélogramme.

Exercice 1.8 (Démonstration du théorème Thalès) Soient ABC et AEF deux triangles tels que $B \in (AE)$ et $C \in (AF)$. On a déjà montré que si $(BC) \parallel (EF)$, alors $\frac{AE}{AB} = \frac{AF}{AC}$. Montrer qu'on a aussi $\frac{AE}{AB} = \frac{EF}{BC}$.

Exercice 1.9

- ***(a)*** Le mathématicien Thalès sait qu'il mesure $1,80\,\text{m}$. Il se place en plein soleil au pied de la grande pyramide de Khéops. Au même moment, une personne mesure la longueur de l'ombre de Thalès et une autre personne mesure celle de l'ombre de la pyramide. Ils trouvent respectivement $1,50\,\text{m}$ pour l'ombre de Thalès et $122\,\text{m}$ pour l'ombre de la Pyramide. En déduire la hauteur de la pyramide de Kheops. (On supposera que les rayons de Soleil sont parallèles)
- ***(b)*** La mesure de la base de la pyramide de Khéops est environ $130\,\text{m}$. Quelle est la mesure d'une de ses arêtes ?

Médiatrices et autres constructions à la règle et au compas

EXERCICE 1.10 Donner, tout en justifiant, la construction à la règle et au compas des objets suivants :

- ***(a)*** Le centre d'un cercle donné.
- ***(b)*** La tangente au point P d'un cercle donné. On rappelle que la tangente à un cercle en P est la droite perpendiculaire à (OP) passant par P (O étant le centre du cercle).
- ***(c)*** Les deux tangentes à un cercle donné passant par un point P à l'extérieur de ce cercle.
- ***(d)*** Un segment dont la longueur est le quotient de deux nombres constructibles (division).
- ***(e)*** Diviser en cinq parties d'égales longueurs un segment donné.
- ***(f)*** Un segment de longueur $\sqrt{3}$, puis $\sqrt{4}$, puis $\sqrt{5}$ et puis $\sqrt{7}$. En déduire un procédé pour $\sqrt{n}$.
- ***(g)*** Un triangle rectangle isocèle en C dont on connaît l'hypoténuse AB.

EXERCICE 1.11 (Examen 2009) Soient $\mathcal{C}$ et $\mathcal{C}'$ deux cercles de centres respectifs O et O' et de rayon r et r'. On suppose que $\mathcal{C}$ et $\mathcal{C}'$ soient sécants en deux points distincts A et B. Montrer que $(OO') \perp (AB)$.

EXERCICE 1.12 Soient O_1, O_2 et O_3 trois points distincts non alignés, et soit $r > 0$. Soit $\mathcal{C}_i$ ($i = 1, 2, 3$) le cercle de centre O_i et de rayon r. On suppose que ces cercles soient sécants 2 à 2 (voir EXERCICE 1.11). On note A et B les points d'intersection de $\mathcal{C}_1$ et $\mathcal{C}_2$; C et D les points d'intersection de $\mathcal{C}_1$ et $\mathcal{C}_3$; E et F les points d'intersection de $\mathcal{C}_2$ et $\mathcal{C}_3$.

- ***(a)*** Montrer que (AB) est la médiatrice de $[O_1\,O_2]$.
- ***(b)*** En déduire que les droites (AB), (CD) et (EF) sont concourantes.

EXERCICE 1.13 (Examen 2010) Soient $\mathcal{C}$ et $\mathcal{C}'$ deux cercles de centres respectifs O et O' et de rayons r et r'. On suppose que $\mathcal{C}$ et $\mathcal{C}'$ soient sécants en deux points distincts A et B. Soient C et D deux points tels que $[AC]$ soit un diamètre de $\mathcal{C}$ et $[AD]$ soit un diamètre de $\mathcal{C}'$.

- ***(a)*** Faire un dessin de la situation.
- ***(b)*** Montrer que $(OO') \perp (AB)$.
- ***(c)*** Montrer que B, C et D sont alignés.
- ***(d)*** Montrer que $(CD) \parallel (OO')$.
- ***(e)*** Montrer que $CD = 2\,OO'$.

Triangles, droites et points remarquables

EXERCICE 1.14 Soient d une droite et E qui n'est pas sur d. Le ***projeté orthogonal*** de E sur d est le point d'intersection de d avec la perpendiculaire à d passant par E.

Soit $ABCD$ un parallélogramme. Soient H le projeté orthogonal de C sur (AD) et K le projeté orthogonal de D sur (AC).

- ***(a)*** Montrer que (CH) et (DK) se coupent en un point I.
- ***(b)*** Montrer que (AI) est perpendiculaire à (AB).

Exercice 1.15 Soit $ABCD$ un rectangle. La médiatrice de $[AC]$ coupe (AB) en I et (BC) en J. Montrer que (CI) est perpendiculaire à (AJ).

Exercice 1.16 Soit $\mathcal{C}$ un cercle de centre O et de diamètre $[IJ]$. On note $\mathcal{C}'$ le cercle de diamètre $[OI]$. Soit M un point du cercle $\mathcal{C}$ différent de I et J. La droite (MI) coupe le cercle $\mathcal{C}'$ en S et la droite (MO) coupe le cercle $\mathcal{C}'$ en T. La droite perpendiculaire à (IJ) passant par M coupe la droite (IT) en P.

(a) Faire un dessin de la situation.

(b) Montrer que (OP) est une hauteur du triangle IPM.

(c) Déduire de la question précédente que les points P, O et S sont alignés.

(d) En utilisant le théorème de Thalès, démontrer que S est le milieu du segment $[IM]$.

(e) Quelle est la nature du triangle IPM ? Justifier.

Exercice 1.17 On considère un triangle ABC. Le but de cet exercice est de montrer que les bissectrices de ABC sont concourantes. On rappelle que

- la ***bissectrice*** d'un angle est la droite qui partage cet angle en deux angles égaux ;
- la distance d'un point M à une droite d est la longueur du segment $[M\,I]$ où I est l'intersection entre d et la perpendiculaire à d passant par M.

(a) Montrer que d_A est la bissectrice de l'angle $\widehat{BAC}$ si et seulement si pour tout point $M \in d_A$, la distance de M à (AB) est égale à la distance de M à (AC).

(b) Montrer que les bissectrices de ABC sont concourantes.

(c) Construire les bissectrices de ABC à la règle et au compas (justifier la construction).

Exercice 1.18 (Démonstration de la proposition 1.24) Soit ABC un triangle. Le but de cet exercice est de montrer que les médianes de ABC sont concourantes en le centre de gravité G. De plus, G se situe au $\frac{2}{3}$ de chaque médiane à partir du sommet correspondant.

Soit A' le milieu de $[BC]$, B' le milieu de $[AC]$ et C' le milieu de $[AB]$. Les médianes sont donc les droites (AA'), (BB') et (CC'). Posons maintenant A_1 (respectivement B_1 et C_1) le ***symétrique*** de G par rapport à A' (respectivement B' et C'), c'est-à-dire le point de la droite $(A'G)$ tel que A' est milieu de $[A_1\,A']$. Soit G le point d'intersection de (AA') et (BB').

(a) Faire un dessin de la situation.

(b) Montrer que A_1BGC, AB_1CG et $BGAC_1$ sont des parallélogrammes.

(c) Montrer que ABA_1B_1 est un parallélogramme.

(d) Montrer que G est le milieu de $[A_1\,A]$.

(e) Montrer que ACA_1C_1 est un parallélogramme et que G est le milieu de $[C\,C_1]$. En déduire que (AA'), (BB') et (CC') se coupent en G.

(f) Montrer que $AG = \frac{2}{3}AA'$, $BG = \frac{2}{3}BB'$ et $CG = \frac{2}{3}CC'$.

Exercice 1.19 Soit $ABCD$ un parallélogramme. Soit E le ***symétrique*** de A par rapport à C (c'est à dire le point de la droite (AC) tel que C est milieu de $[A\,E]$). Quel est le centre de gravité du triangle DEB ?

Droites coplanaires et parallélisme

Exercice 1.20 Soient d, d' et d'' trois droites distinctes d'un même plan.

(a) Montrer que si $d \parallel d'$ et si d'' coupe d, alors d'' coupe aussi d'.

(b) Montrer que si $d \parallel d'$ et $d' \parallel d''$, alors $d \parallel d''$ (Démonstration de la proposition 1.30).

Orthogonalité dans l'espace

Exercice 1.21 Soient d, d', d'' trois droites distinctes de l'espace. Montrer que

(a) Si $d \perp d'$ et $d' \parallel d''$ alors $d \perp d''$ (Démonstration de la proposition 1.39).

(b) Si $d \perp d'$, $d' \perp d''$ et si d et d'' sont coplanaires, alors $d \parallel d''$.

Exercice 1.22 [Démonstration du corollaire 1.41] Démontrer les propositions suivantes :

(a) Si deux droites sont parallèles, alors un plan orthogonal à l'une l'est aussi à l'autre.

(b) Si deux plans sont parallèles, alors une droite orthogonale à l'un l'est aussi à l'autre.

(c) Par un point de l'espace, il ne passe qu'un unique plan orthogonal à une droite donnée.

Exercice 1.23 Démontrer les propositions suivantes :

(a) Par un point de l'espace, il passe une et une seule droite orthogonale à un plan donné.

(b) Si P_1 et P_2 sont des plans perpendiculaires, alors P_1 et P_2 sont sécants.

(c) Soient P_1, P_2 et P_3 trois plans tels que $P_1 \cap P_2 = d$ une droite, et $P_1 \perp P_3$ et $P_2 \perp P_3$. Alors d est orthogonale à P_3.

(d) Deux droites orthogonales à un même plan sont parallèles.

Exercice 1.24 (Examen 2009) On considère un parallélogramme $ABCD$ de centre O (l'intersection des diagonales) et I l'orthocentre du triangle OBC.

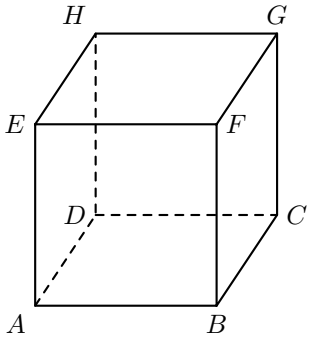
(a) Montrer que les droites (OI) et (BC) sont perpendiculaires.

(b) Soit K l'orthocentre du triangle OAD.

- ***(i)*** Montrer que les points K, O et I sont alignés.
- ***(ii)*** Montrer que (AK) et (IC) sont parallèles.
- ***(iii)*** Montrer que $OK = OI$.
- ***(iv)*** En déduire que O est le milieu de $[IK]$.

(c) Soient les points J et L, orthocentres respectifs des triangles OCD et AOB. Quelle est la nature du quadrilatère $IJKL$?

Exercice 1.25 Soit $ABCDEFGH$ un cube.



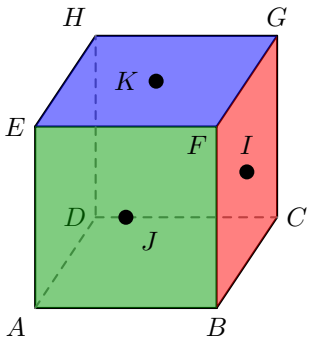
(a) Montrer que les faces adjacentes sont perpendiculaires.

(b) Montrer que $ABGH$ est un rectangle. Calculer AG en fonction de AB.

(c) Montrer que $[AG]$ et $[BH]$ se coupent en leur milieu. Notons ce milieu O.

(d) Les diagonales d'un cube sont-elles perpendiculaires ?

EXERCICE 1.26 On considère un cube $ABCDEFGH$, où les points I, J et K sont les centres respectifs des faces $(BCGF)$, $(ABEF)$ et $(EFGH)$.



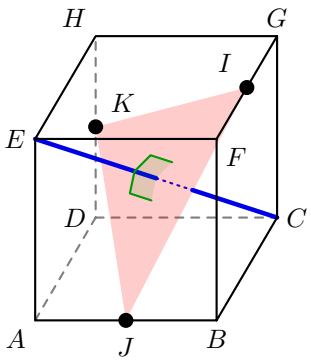
(a) Quelle est la nature du triangle IJK ? (Justifier.)

(b) Démontrer que F est équidistants des points I, J et K.

(c) Démontrer que D est équidistants des points I, J et K.

(d) En déduire que la droite (FD) est orthogonale au plan (IJK).

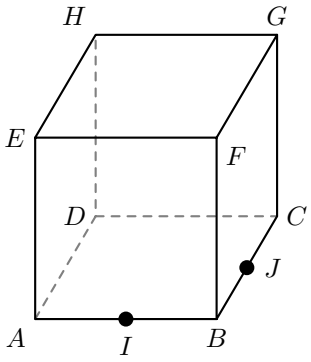
EXERCICE 1.27 On considère un cube $ABCDEFGH$, où les points I, J et K sont les milieux respectifs de $[FG]$, $[AB]$ et $[DH]$.



(a) Démontrer que la droite (EC) est orthogonale au plan (IJK).

(b) Démontrer que IJK est un triangle équilatéral.

EXERCICE 1.28 Soit $ABCDEFGH$ un cube. Soit I le milieu de $[AB]$ et J le milieu de $[BC]$.

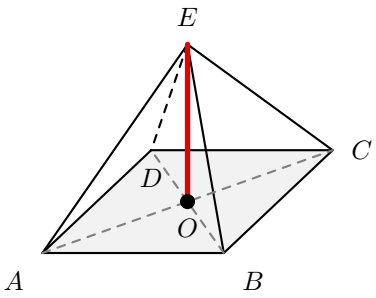


(a) Quelle est la droite parallèle à (HF) passant par B ?

(b) Donner le tracé de la droite parallèle à (EG) passant par I. (Justifier.)

(c) (IJ) et (EG) sont-elles parallèles ?

EXERCICE 1.29 Soit $ABCDE$ une pyramide de base $ABCD$ et dont tous les côtés sont de longueur 7 m. Soit O l'intersection des diagonales du carré $ABCD$. La hauteur de la pyramide est la longueur du segment $[OE]$.

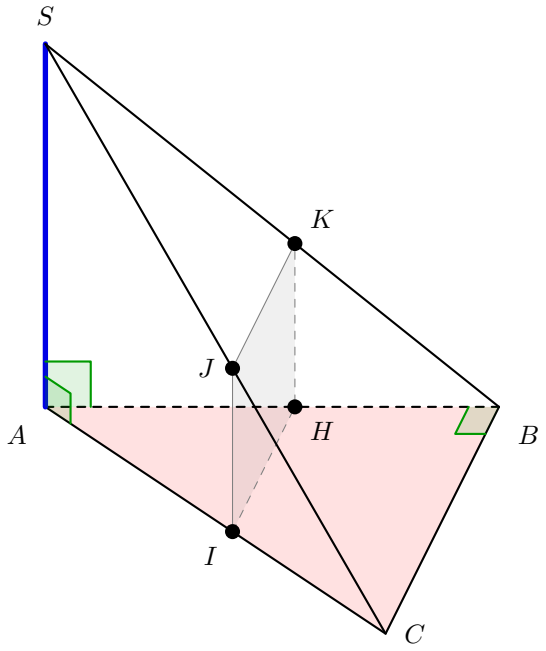


(a) Calculer la hauteur de la pyramide.

(b) En déduire que la hauteur de la pyramide multipliée par la longueur de la diagonale de la base est égale à 49 m :

$$OE \cdot AC \ = \ 49\,m$$

Exercice 1.30 Soit $SABC$ un tétraèdre. La droite (SA) est orthogonale au plan (ABC) et le triangle ABC est rectangle en B.



(a) Le but de cette question est de montrer que le triangle SBC est rectangle en B.

- ***(i)*** Montrer que $(BC) \perp (SA)$.
- ***(ii)*** Montrer que le triangle SBC est rectangle en B.

(b) H est un point de l'arête $[AB]$; on trace par H le plan orthogonal à (AB). On suppose que ce plan coupe (AC) en I, (SC) en J et (SB) en K.

- ***(i)*** Montrer que $(HI) \parallel (BC)$.
- ***(ii)*** En déduire que $(HI) \parallel (KJ)$.
- ***(iii)*** Montrer que $(KH) \parallel (SA)$.
- ***(iv)*** En déduire que $(HK) \parallel (IJ)$.
- ***(v)*** Montrer que $HIJK$ est un rectangle.

(c) On suppose à présent que $AB = 1$ et que $SA = BC = 2$. On pose $AH = x$.

- ***(i)*** Montrer, en utilisant le théorème de Thalès dans le triangle ABC, que $HI = 2x$.
- ***(ii)*** Montrer, en utilisant le théorème de Thalès dans le triangle SAB, que $HK = 2(1 - x)$.
- ***(iii)*** Calculer l'aire du rectangle $HIJK$ en fonction de x. On note $A(x)$ cette aire.

(d) Le but de cette question est de déterminer la nature du quadrilatère $HIJK$.

- ***(i)*** Montrer que $4x(1 - x) = 1 - (1 - 2x)^2$.
- ***(ii)*** Pour quelle valeur de x l'aire $A(x)$ est-elle maximale ?
- ***(iii)*** Quelle est alors la position du point H sur $[AB]$?
- ***(iv)*** Quelle est alors la nature du quadrilatère $HIJK$?

Chapitre 2

Introduction à la géométrie vectorielle

En étudiant la géométrie à la manière des savants grecs de l'Antiquité, nous nous sommes rendu compte que raisonner à l'aide de concepts géométriques tels que le parallélisme, la coplanarité ou l'orthogonalité pouvait s'avérer très difficile lorsque l'on ne dispose que des outils de la géométrie antique. Nous allons, dans ce chapitre, présenter un nouvel outil, ***les vecteurs***, qui permettra d'introduire l'algèbre — et donc des notions de calcul — dans les raisonnements géométriques. Nous verrons que la notion de vecteur, plus abstraite, simplifie et clarifie grandement les énoncés géométriques ainsi que le « pourquoi » de leur véracité, en particulier ceux portant sur le parallélisme, la coplanarité et l'orthogonalité. Les vecteurs sont le fruit du travail de plusieurs mathématiciens du début du XIX^{e} siècle (Bolzano, Chasles, etc.). Ce chapitre constitue en quelque sorte un pont entre la géométrie de l'Antiquité et celle du XX^{e} siècle.

2.1 Les vecteurs

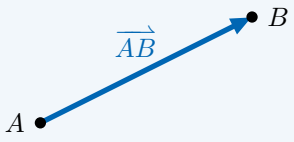
On se place dans l'espace $\mathcal{E}$ (ou dans un plan $\mathcal{P}$ vu dans l'espace).

2.1.1 Généralités

Définition 2.1: (Vecteur)

Un ***vecteur*** est la donnée

- d'une longueur (sa ***norme***) ;
- d'une ***direction*** ;
- d'un ***sens***.



Il se représente par une flèche entre deux points A et B : c'est le vecteur $\overrightarrow{AB}$. Il représente en quelque sorte le « mouvement » d'aller de A vers B. La norme d'un vecteur se note $\left\|\overrightarrow{AB}\right\| = AB$, c'est la longueur AB du segment $[AB]$.

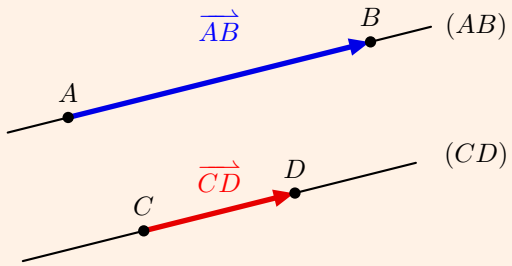
⚠ **Remarque** La ***direction*** correspond à l'orientation géométrique d'une droite (par exemple « horizontale », « verticale », ou plus généralement une droite donnée), tandis que le ***sens*** indique vers quel côté on se déplace le long de

cette direction. Deux vecteurs peuvent donc avoir la même direction mais des sens opposés (par exemple $\overrightarrow{AB}$ et $\overrightarrow{BA}$).

Cette définition nous donne une première réinterprétation d'une notion géométrique grâce aux vecteurs :

Proposition 2.2

Deux droites (AB) et (CD) sont ***parallèles*** si et seulement si $\overrightarrow{AB}$ et $\overrightarrow{CD}$ sont ***colinéaires*** (c'est-à-dire de même direction).



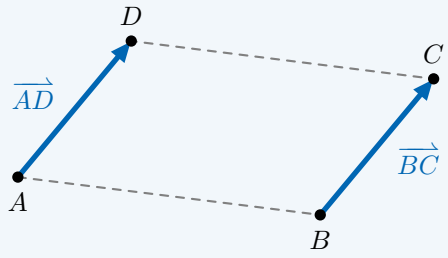
Démonstration Cette proposition sera prise comme une définition et on l'acceptera sans preuve.

■

Définition 2.3: (Égalité de vecteurs)

On dit que deux vecteurs $\overrightarrow{AD}$ et $\overrightarrow{BC}$ sont ***égaux*** si le quadrilatère $ABCD$ est un parallélogramme (ces points sont alors coplanaires). Autrement dit,

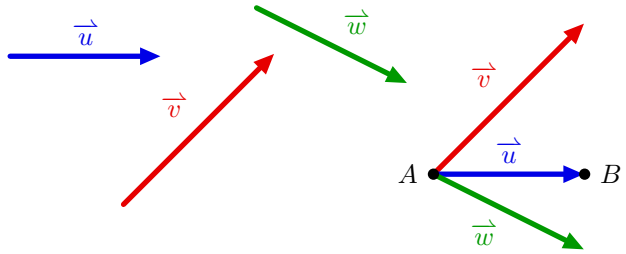
$$\overrightarrow{AD} = \overrightarrow{BC} \iff ABCD \text{ est un parallélogramme.}$$



Remarque Si $ABCD$ est un parallélogramme, il en est de même pour $BCDA$, $CDAB$ et $DABC$. On remarque alors que :

$$\overrightarrow{AD} = \overrightarrow{BC} \iff \overrightarrow{BA} = \overrightarrow{CD} \iff \overrightarrow{CB} = \overrightarrow{DA} \iff \overrightarrow{AB} = \overrightarrow{DC}.$$

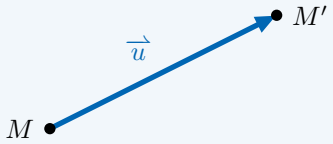
Représentation d'un vecteur : Si on fixe un point A, tout vecteur $\vec{u}$ peut se représenter avec A comme point de départ et un point d'arrivée B : $\vec{u} = \overrightarrow{AB}$.



Cette propriété des vecteurs nous amène naturellement à la définition suivante :

Définition 2.4: (Translation)

La ***translation*** est la transformation affine qui déplace un point M dans la direction, le sens et la longueur d'un vecteur $\vec{u}$. Plus précisément, la ***translation $t_{\vec{u}}$ de vecteur $\vec{u}$*** est la fonction qui envoie un point M sur un point $M' = t_{\vec{u}}(M)$ tel que $\overrightarrow{MM'} = \vec{u}$.



Définition 2.5: (Transformation affine)

Une ***transformation affine*** est une transformation du plan (ou de l'espace) qui préserve la structure relative des figures : elle conserve notamment l'alignement, le parallélisme et les rapports de longueurs sur une même droite. Plus précisément, si les points A, B et M vérifient

$$\overrightarrow{AM} = \lambda \overrightarrow{AB},$$

alors leurs images vérifient

$$\overrightarrow{f(A)f(M)} = \lambda \overrightarrow{f(A)f(B)}.$$

Une transformation affine f, qui agit d'abord sur les points, agit également sur les vecteurs. On définit cette action par

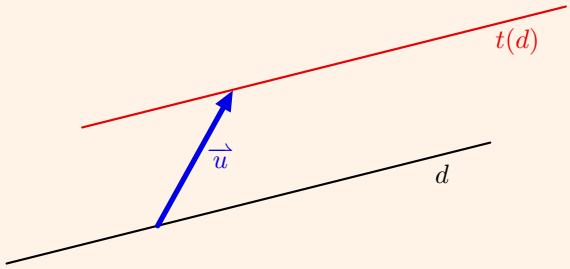
$$f\left(\overrightarrow{AB}\right) = \overrightarrow{f(A)f(B)}.$$

⚠ **Remarque** Une translation peut aussi se définir par un point et son image : si A et B sont deux points donnés alors il existe une unique translation t tel que $t(A) = B$. Bien entendu, c'est la translation de vecteur $\overrightarrow{AB}$.

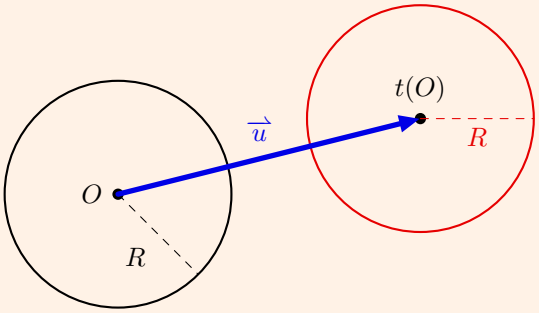
Proposition 2.6

Soit t une translation.

(i) Si d est une droite, alors $t(d)$ est une droite et $t(d) \parallel d$;



(ii) L'image par t d'un cercle de centre O et de rayon R est un cercle de centre $t(O)$ et de rayon R.



Démonstration Voir exercice 2.1.

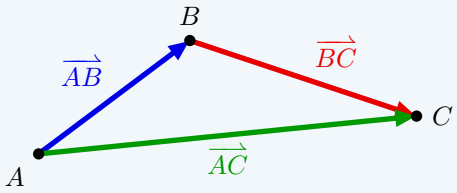
■

2.1.2 Addition de vecteurs et triangle

L'addition des vecteurs se définit par la relation de Chasles, qui peut être vue comme une représentation algébrique de la notion de triangle.

Définition 2.7: (Relation de Chasles)

Pour tous points A, B et C de $\mathcal{E}$, on a $\overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$.



Intuitivement, la relation de Chasles nous dit que partir de A pour se rendre directement à C est équivalent à partir de A pour aller à C en passant par B.

Afin que l'addition des vecteurs soit bien définie et admette un élément neutre — c'est-à-dire un vecteur qui ne modifie aucun autre par addition — il est nécessaire d'introduire le vecteur nul.

Définition 2.8: (Vecteur nul)

Le vecteur $\overrightarrow{AA}$ est appelé le ***vecteur nul*** et est noté $\overrightarrow{0}$. Pour tout point A, on a donc

$$\overrightarrow{AA} = \overrightarrow{0}.$$

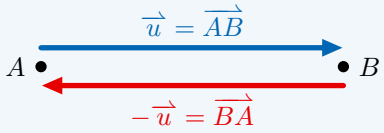
De plus, si $\overrightarrow{AM} = \overrightarrow{0}$, alors $A = M$.

L'existence d'un élément neutre pour l'addition des vecteurs permet maintenant d'introduire la notion de vecteur opposé, qui joue le rôle d'inverse additif.

Définition 2.9: (Vecteur opposé)

Soit $\overrightarrow{u} = \overrightarrow{AB}$. Le ***vecteur opposé*** de $\overrightarrow{u}$ est le vecteur de même direction et de même norme, mais de sens contraire ; il est noté $-\overrightarrow{u}$. En particulier,

$$-\overrightarrow{AB} = \overrightarrow{BA}.$$



Proposition 2.10: (Propriétés des vecteurs)

(i) $\overrightarrow{u} + \overrightarrow{0} = \overrightarrow{u}$ (***Élément neutre***) ;

(ii) $\overrightarrow{u} + (-\overrightarrow{u}) = \overrightarrow{0}$. ***Soustraction*** : $\overrightarrow{u} - \overrightarrow{v} = \overrightarrow{u} + (-\overrightarrow{v})$;

(iii) $\overrightarrow{u} + \overrightarrow{v} = \overrightarrow{v} + \overrightarrow{u}$ (***Commutativité***) ;

(iv) $\overrightarrow{u} + (\overrightarrow{v} + \overrightarrow{w}) = (\overrightarrow{u} + \overrightarrow{v}) + \overrightarrow{w}$ (***Associativité***).

Démonstration Tout vecteur s'écrit avec deux points : $\overrightarrow{u} = \overrightarrow{AB}$.

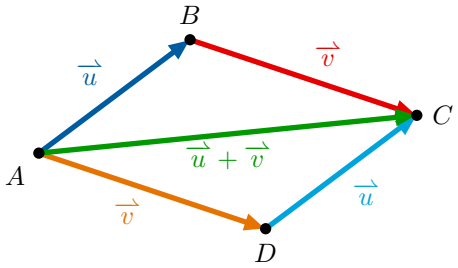
(i) On a $\overrightarrow{u} + \overrightarrow{0} = \overrightarrow{AB} + \overrightarrow{BB} = \overrightarrow{AB} = \overrightarrow{u}$.

(ii) On a $\overrightarrow{u} + (-\overrightarrow{u}) = \overrightarrow{AB} + (-\overrightarrow{AB}) = \overrightarrow{AB} + \overrightarrow{BA} = \overrightarrow{AA} = \overrightarrow{0}$.

(iii) D'abord, si $\overrightarrow{u} = \overrightarrow{AB}$ et $\overrightarrow{v} = \overrightarrow{BC}$, alors $\overrightarrow{u} + \overrightarrow{v} = \overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$.

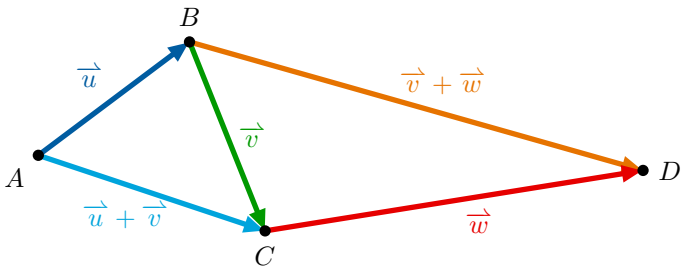
Soit D le point tel que $\overrightarrow{AD} = \overrightarrow{v} = \overrightarrow{BC}$. On obtient donc que $ABCD$ est un parallélogramme. Ainsi, $\overrightarrow{AB} = \overrightarrow{DC} = \overrightarrow{u}$.

On en déduit que $\overrightarrow{v} + \overrightarrow{u} = \overrightarrow{AD} + \overrightarrow{DC} = \overrightarrow{AC} = \overrightarrow{u} + \overrightarrow{v}$.



(iv) On pose $\overrightarrow{u} = \overrightarrow{AB}, \overrightarrow{v} = \overrightarrow{BC}, \overrightarrow{w} = \overrightarrow{CD}$

$$\Longrightarrow \begin{cases} \overrightarrow{u} + (\overrightarrow{v} + \overrightarrow{w}) = \overrightarrow{AB} + (\overrightarrow{BC} + \overrightarrow{CD}) = \overrightarrow{AB} + \overrightarrow{BD} = \overrightarrow{AD} \\ (\overrightarrow{u} + \overrightarrow{v}) + \overrightarrow{w} = (\overrightarrow{AB} + \overrightarrow{BC}) + \overrightarrow{CD} = \overrightarrow{AC} + \overrightarrow{CD} = \overrightarrow{AD} \end{cases}$$



■

Le fait de pouvoir additionner deux vecteurs nous donne la propriété suivante :

COROLLAIRE 2.11

Si $\overrightarrow{u}$ est un vecteur et A un point, alors il existe un unique point B tel que $\overrightarrow{u} = \overrightarrow{AB}$.

DÉMONSTRATION Si $\overrightarrow{u} = \overrightarrow{AB} = \overrightarrow{AB'}$, alors

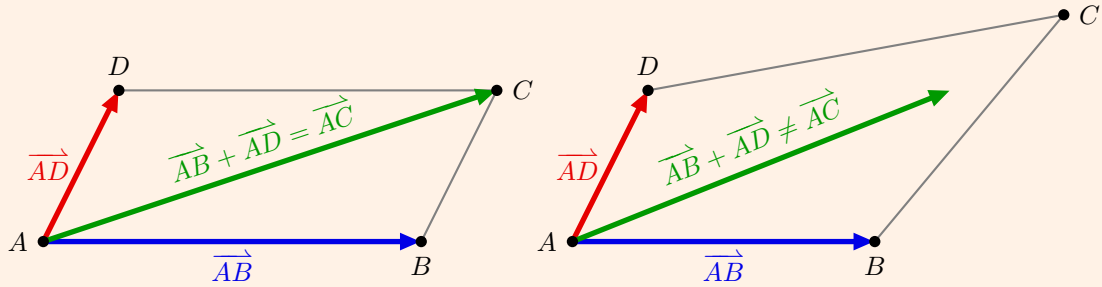
$$\overrightarrow{0} = \overrightarrow{u} - \overrightarrow{u} = \overrightarrow{AB'} - \overrightarrow{AB} = \overrightarrow{AB'} + \overrightarrow{BA} = \overrightarrow{BB'}.$$

Et donc $B = B'$.

■

Proposition 2.12: (Règle du parallélogramme)

$ABCD$ est un parallélogramme $\iff$ $\overrightarrow{AB} + \overrightarrow{AD} = \overrightarrow{AC}$.



Démonstration

$(\Longleftarrow)$

$$\begin{aligned} \overrightarrow{AC} = \overrightarrow{AB} + \overrightarrow{AD} &\implies \overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AB} + \overrightarrow{AD} \\ &\implies \overrightarrow{BC} = \overrightarrow{AD} \quad \text{(en soustrayant } \overrightarrow{AB}\text{)} \\ &\implies ABCD \text{ est un parallélogramme.} \end{aligned}$$

$(\Longrightarrow)$

$$\begin{aligned} ABCD \text{ est un parallélogramme} &\implies \overrightarrow{AD} = \overrightarrow{BC} \\ &\implies \overrightarrow{AB} + \overrightarrow{AD} = \overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}. \end{aligned}$$

■

2.1.3 Multiplication d'un vecteur par un réel

Définition 2.13

Soit $\overrightarrow{u}$ un vecteur et k un réel. Le vecteur $k\overrightarrow{u}$ est défini par

- $||k\overrightarrow{u}|| = |k| \cdot ||\overrightarrow{u}||$ i.e. si $\overrightarrow{u} = \overrightarrow{AB}$, alors $||k\overrightarrow{u}|| = |k| \cdot \left|\left|\overrightarrow{AB}\right|\right|$;
- la même direction que $\overrightarrow{u}$ ($k\overrightarrow{u}$ et $\overrightarrow{u}$ sont colinéaires) ;
- le même sens que $\overrightarrow{u}$ si $k > 0$ et de sens opposé si $k < 0$.

Proposition 2.14: (Propriétés de la multiplication d'un vecteur par un réel)

Soient $x, y \in \mathbb{R}$ et $\overrightarrow{u}$ un vecteur.

- ***(i)*** $1 \cdot \overrightarrow{u} = \overrightarrow{u}$, $x \cdot \overrightarrow{0} = \overrightarrow{0}$ et $0 \cdot \overrightarrow{u} = \overrightarrow{0}$;
- ***(ii)*** $x \cdot (y\overrightarrow{u}) = (xy) \cdot \overrightarrow{u}$;
- ***(iii)*** $(x+y) \cdot \overrightarrow{u} = x\overrightarrow{u} + y\overrightarrow{u}$ (***Distributivité***);
- ***(iv)*** $x \cdot (\overrightarrow{u} + \overrightarrow{v}) = x\overrightarrow{u} + x\overrightarrow{v}$ (***Théorème de Thalès***).

Démonstration (Idée de la preuve) Pour établir l'égalité de deux vecteurs, nous pouvons comparer leur direction, leur sens et leur norme, ou encore utiliser la règle du parallélogramme.

- ***Propriétés (i) et (ii).***

  Elles découlent directement de la définition et de l'égalité

$$\left\|k\overrightarrow{u}\right\| = |k| \left\|\overrightarrow{u}\right\|.$$

  La multiplication des normes réelles fournit notamment $\|x(y\overrightarrow{u})\| = \|(xy)\overrightarrow{u}\|$, tandis que les signes de x, de y et de xy donnent les mêmes direction et sens aux deux vecteurs.

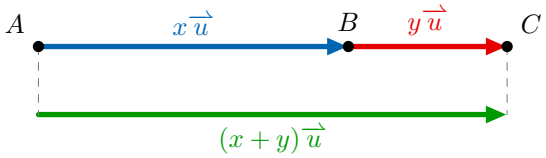
- ***Distributivité par rapport aux réels — propriété (iii).***

  Plaçons bout à bout les vecteurs $x\overrightarrow{u} = \overrightarrow{AB}$ et $y\overrightarrow{u} = \overrightarrow{BC}$. Par la relation de Chasles,

$$\overrightarrow{AC} = x\overrightarrow{u} + y\overrightarrow{u}.$$

  Tous ces vecteurs sont colinéaires à $\overrightarrow{u}$. Lorsque x et y ont le même signe, leurs longueurs s'additionnent :

$$\begin{aligned} \left\|(x+y)\overrightarrow{u}\right\| &= (|x| + |y|) \left\|\overrightarrow{u}\right\| \\ &= \left\|x\overrightarrow{u}\right\| + \left\|y\overrightarrow{u}\right\| \\ &= AB + BC \quad = \quad AC. \end{aligned}$$



  Les deux vecteurs comparés ont donc la même direction, le même sens et la même norme. Si x et y sont de signes contraires, le même raisonnement s'applique en soustrayant les longueurs ; le point B se trouve alors à l'extérieur du segment $[AC]$ ou le point C entre A et B. On obtient dans tous les cas

$$(x+y)\overrightarrow{u} \quad = \quad x\overrightarrow{u} + y\overrightarrow{u}.$$

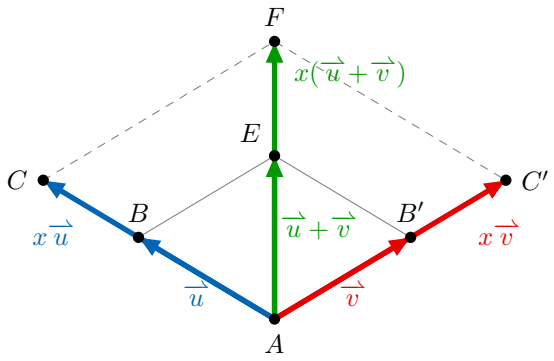
- ***Distributivité par rapport aux vecteurs — propriété (iv).***

Supposons d'abord $x > 0$. Choisissons les points B, B' et E de manière que

$$\overrightarrow{AB} = \vec{u}, \qquad \overrightarrow{AB'} = \vec{v}, \qquad \overrightarrow{AE} = \vec{u} + \vec{v}.$$

Ainsi, $ABEB'$ est un parallélogramme. Plaçons ensuite C, C' et F sur les demi-droites issues de A de sorte que

$$\overrightarrow{AC} = x\vec{u}, \qquad \overrightarrow{AC'} = x\vec{v}, \qquad \overrightarrow{AF} = x(\vec{u} + \vec{v}).$$



Puisque $\frac{AC}{AB} = x = \frac{AF}{AE}$, la réciproque du théorème de Thalès donne $(CF) \parallel (BE)$. De même, $(C'F) \parallel (B'E)$. Le quadrilatère $ACFC'$ est donc un parallélogramme, d'où

$$\begin{aligned} x\vec{u} + x\vec{v} &= \overrightarrow{AC} + \overrightarrow{AC'} \\ &= \overrightarrow{AF} \\ &= x(\vec{u} + \vec{v}). \end{aligned}$$

Le cas $x = 0$ est immédiat ; lorsque $x < 0$, la même construction est obtenue en renversant le sens des trois vecteurs.

■

⚠ **Remarque** On vient de voir que les principaux objets de la géométrie ont été « traduits » en propriété algébrique : ***l'algèbre linéaire est née !*** Nous invitons le lecteur à aller consulter un livre de géométrie moderne, par exemple [Audin 2006], pour apprécier l'importance de l'algèbre linéaire en géométrie.

Exemple: (Deux caractérisations du milieu)

Soient A et B deux points. La multiplication d'un vecteur par un réel permet de caractériser le ***milieu*** I du segment $[AB]$ par

$$\overrightarrow{AI} = \frac{1}{2}\overrightarrow{AB}.$$

En utilisant également l'addition des vecteurs, cette condition peut s'écrire de manière symétrique :

$$\overrightarrow{IA} + \overrightarrow{IB} = \vec{0}.$$

Chacune de ces deux égalités détermine le point I de manière unique.

2.1.4 Homothétie

Nous avons vu au début de ce chapitre que la définition même de vecteur pouvait être vue comme une transformation de l'espace : la ***translation***. Il en est de même avec la multiplication d'un vecteur par un réel.

Définition 2.15: (homothétie)

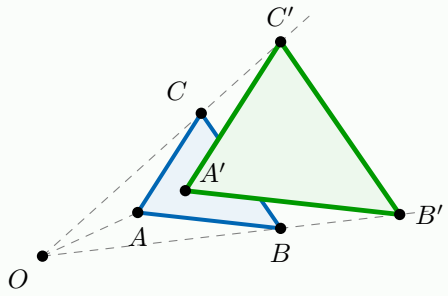
L'homothétie est la transformation qui contracte un point M vers un point A, son centre, selon une proportion k. Plus précisément, l'***homothétie $h_{A,k}$ de centre A et de rapport $k \in \mathbb{R}^*$*** est la fonction qui envoie un point M sur un point $M' = h_{A,k}(M)$ tel que $\overrightarrow{AM'} = k\overrightarrow{AM}$.

⚠ **Remarque** Une homothétie peut aussi se définir par son centre, un point et son image : si A, B et B' sont trois points distincts alignés, alors il existe une unique homothétie h de centre A telle que $h(B) = B'$. Le rapport de h est $\pm\frac{AB'}{AB}$; le signe est positif si et seulement si $\overrightarrow{AB}$ et $\overrightarrow{AB'}$ ont même sens.

Exemple: (Agrandissement d'un triangle)

Considérons l'homothétie $h_{O,\frac{3}{2}}$ de centre O et de rapport $\frac{3}{2}$. Elle transforme le triangle ABC en un triangle $A'B'C'$, où

$$\overrightarrow{OA'} = \frac{3}{2}\overrightarrow{OA}, \qquad \overrightarrow{OB'} = \frac{3}{2}\overrightarrow{OB}, \qquad \overrightarrow{OC'} = \frac{3}{2}\overrightarrow{OC}.$$



Les points O, A et A' sont alignés, tout comme O, B et B', ainsi que O, C et C'. Puisque le rapport est supérieur à 1, le triangle image est un agrandissement du triangle initial.

Proposition 2.16: (Propriétés d'une homothétie)

Soit h une homothétie de centre A et de rapport $k \in \mathbb{R}^*$. Alors :

- ***(i)*** si $k \neq 1$, le centre A est l'unique point fixe de h ;
- ***(ii)*** pour tout point M, les points A, M et $h(M)$ sont alignés ;
- ***(iii)*** l'image de toute droite d est une droite parallèle à d ;
- ***(iv)*** l'image d'un cercle de centre O et de rayon R est le cercle de centre $h(O)$ et de rayon $|k|R$.

Démonstration Voir exercice 2.2.

■

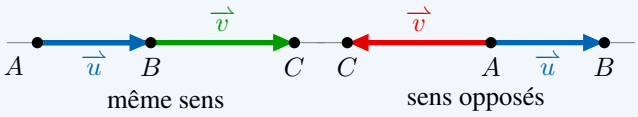
2.2 Vecteurs colinéaires, droites et parallélisme

Définition 2.17: (Vecteurs colinéaires)

Deux vecteurs non nuls $\vec{u}$ et $\vec{v}$ sont ***colinéaires*** s'ils ont la même direction. Autrement dit, si

$$\vec{u} = \overrightarrow{AB} \qquad \text{et} \qquad \vec{v} = \overrightarrow{AC},$$

alors $\vec{u}$ et $\vec{v}$ sont colinéaires si et seulement si les points A, B et C sont alignés.



Remarque $\vec{u}$ et $\vec{u}$ sont bien entendu colinéaires.

Proposition 2.18: (Caractérisation de la colinéarité)

Soient $\vec{u}$ et $\vec{v}$ deux vecteurs non nuls. Alors

$$\vec{u} \text{ et } \vec{v} \text{ sont colinéaires} \iff \exists\, k \in \mathbb{R}^* \text{ tel que } \vec{u} = k\vec{v}.$$

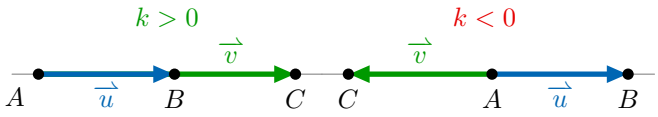
Démonstration

($\Longrightarrow$) Supposons $\vec{u}$ et $\vec{v}$ colinéaires. Puisqu'ils sont non nuls, le quotient

$$\frac{\|\vec{u}\|}{\|\vec{v}\|}$$

est bien défini. Le signe de k doit cependant tenir compte du sens des deux vecteurs. Posons donc

$$k = \begin{cases} \dfrac{\|\vec{u}\|}{\|\vec{v}\|}, & \text{si les vecteurs ont le même sens,} \\ -\dfrac{\|\vec{u}\|}{\|\vec{v}\|}, & \text{s'ils ont des sens opposés.} \end{cases}$$



Dans les deux cas,

$$\|k\vec{v}\| = |k|\,\|\vec{v}\| = \|\vec{u}\|.$$

De plus, le choix du signe de k garantit que $k\vec{v}$ et $\vec{u}$ ont le même sens. Ces deux vecteurs ont donc la même direction, le même sens et la même norme ; par conséquent,

$$\vec{u} = k\vec{v}.$$

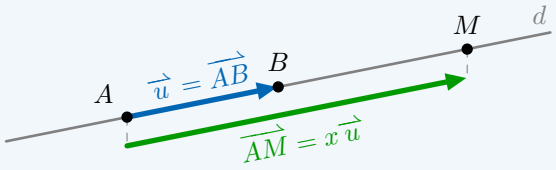
($\Longleftarrow$) Supposons qu'il existe $k \neq 0$ tel que $\vec{u} = k\vec{v}$. La multiplication par un réel non nul ne change pas la direction d'un vecteur. Ainsi, $\vec{u}$ et $\vec{v}$ ont la même direction ; ils sont donc colinéaires.

■

Définition 2.19: (Vecteur directeur)

Soient d une droite et A un point de d. Un vecteur non nul $\vec{u}$ est appelé ***vecteur directeur*** de d s'il existe un point $B \in d$ tel que

$$\vec{u} = \overrightarrow{AB}.$$



- Le couple $(A, \vec{u})$ constitue un ***repère (affine)*** de la droite d.
- À chaque point $M \in d$ correspond un unique réel x, appelé la ***coordonnée*** de M dans ce repère, tel que

$$\overrightarrow{AM} = x\vec{u}.$$

Corollaire 2.20: (Alignement et parallélisme)

(i) Soient A, B et C trois points distincts. Alors

$$A,\ B,\ C \text{ sont alignés} \iff \overrightarrow{AB} \text{ et } \overrightarrow{AC} \text{ sont colinéaires.}$$

(ii) Soient A, B, C et D quatre points tels que $A \neq B$ et $C \neq D$. Alors

$$(AB) \parallel (CD) \iff \overrightarrow{AB} \text{ et } \overrightarrow{CD} \text{ sont colinéaires.}$$

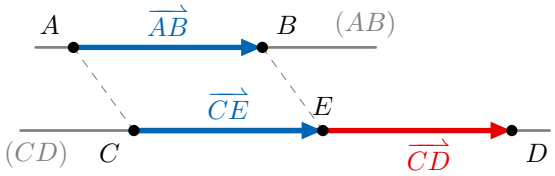
Démonstration

- ***Alignement — (i).***

Cette équivalence est précisément la définition de la colinéarité lorsque les deux vecteurs ont la même origine A.

- ***Parallélisme — (ii).***

La construction utilisée dans les deux sens est représentée ci-dessous. Le point E est choisi de manière que $\overrightarrow{CE} = \overrightarrow{AB}$; le quadrilatère $ABEC$ est alors un parallélogramme.



($\Longrightarrow$) Supposons $(AB) \parallel (CD)$. La droite (CD) est l'unique parallèle à (AB) passant par C. Le point E défini par $\overrightarrow{CE} = \overrightarrow{AB}$ appartient donc à (CD). Ainsi, $\overrightarrow{AB} = \overrightarrow{CE}$ est colinéaire à $\overrightarrow{CD}$.

($\Longleftarrow$) Supposons $\overrightarrow{AB}$ et $\overrightarrow{CD}$ colinéaires. Il existe alors $k \neq 0$ tel que $\overrightarrow{AB} = k\overrightarrow{CD}$. Définissons E par

$$\overrightarrow{CE} = k\overrightarrow{CD} = \overrightarrow{AB}.$$

D'après ***(i)***, les points C, D et E sont alignés. De plus, $\overrightarrow{AB} = \overrightarrow{CE}$, donc $ABEC$ est un parallélogramme et $(AB) \parallel (CE)$. Comme $(CE) = (CD)$, nous obtenons $(AB) \parallel (CD)$.

■

2.3 Repère affine du plan

Définition 2.21: (Repère affine du plan)

Soient O un point d'un plan $\mathcal{P}$ et $\vec{i}$, $\vec{j}$ deux vecteurs non colinéaires de ce plan. Le triplet

$$(O, \vec{i}, \vec{j})$$

est appelé un ***repère affine*** de $\mathcal{P}$. Le point O en est l'***origine***, tandis que $\vec{i}$ et $\vec{j}$ en sont les ***vecteurs de base***.

Proposition 2.22: (Coordonnées dans le plan)

Dans un repère affine $(O, \vec{i}, \vec{j})$:

(i) pour tout point $M \in \mathcal{P}$, il existe un unique couple $(x, y) \in \mathbb{R}^2$ tel que

$$\overrightarrow{OM} = x\vec{i} + y\vec{j};$$

(ii) pour tout vecteur $\vec{u}$ de $\mathcal{P}$, il existe un unique couple $(x, y) \in \mathbb{R}^2$ tel que

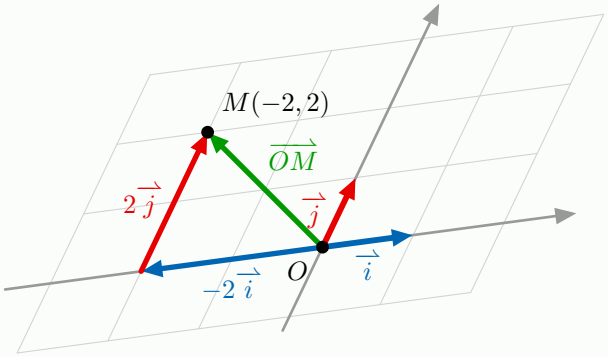
$$\vec{u} = x\vec{i} + y\vec{j}.$$

Dans chaque cas, le couple (x, y) est appelé le couple de ***coordonnées*** du point ou du vecteur considéré.

Exemple

Dans le repère affine illustré ci-dessous, le point $M(-2,2)$ vérifie

$$\overrightarrow{OM} \quad = \quad -2\,\vec{i} + 2\,\vec{j}\,.$$



Démonstration (proposition 2.22)

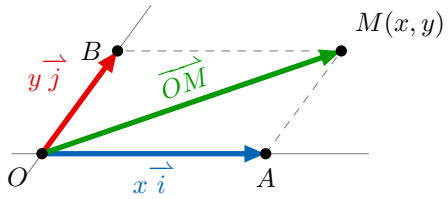
- ***(i) Coordonnées d'un point.***

  Par M, traçons les parallèles aux directions de $\vec{j}$ et de $\vec{i}$; elles rencontrent respectivement les droites dirigées par $\vec{i}$ et par $\vec{j}$ en A et en B. Ainsi, pour certains réels x et y,

  $$\overrightarrow{OA} = x\,\vec{i}\,, \qquad \overrightarrow{OB} = y\,\vec{j}\,,$$

  et, puisque $OAMB$ est un parallélogramme, la règle du parallélogramme donne

  $$\overrightarrow{OM} \quad = \quad x\,\vec{i} + y\,\vec{j}\,.$$

  Pour vérifier l'unicité, supposons que deux couples conviennent. Alors

  $$x\,\vec{i} + y\,\vec{j} \;=\; x'\,\vec{i} + y'\,\vec{j} \quad \Longrightarrow \quad (x-x')\,\vec{i} \;=\; -(y-y')\,\vec{j}\,.$$

  La non-colinéarité de $\vec{i}$ et de $\vec{j}$ impose alors $x = x'$ et $y = y'$.

- ***(ii) Coordonnées d'un vecteur.***

  Soit $\vec{u}$ un vecteur du plan. Il existe un unique point M tel que $\vec{u} = \overrightarrow{OM}$. En appliquant ***(i)*** à ce point, nous obtenons un unique couple (x,y) tel que

  $$\vec{u} \quad = \quad \overrightarrow{OM} \quad = \quad x\,\vec{i} + y\,\vec{j}\,.$$

■

⚠ Remarque

(i) $\overrightarrow{OO} = \overrightarrow{0}$, donc O a pour coordonnées $(0,0)$.

(ii) $\overrightarrow{i}$ a pour coordonnées $(1,0)$ et $\overrightarrow{j}$ a pour coordonnées $(0,1)$.

(iii) Le vecteur $\overrightarrow{AB}$ a pour coordonnées $(x_B - x_A,\ y_B - y_A)$, car

$$\begin{aligned}\overrightarrow{AB} &= \overrightarrow{AO} + \overrightarrow{OB} = -\overrightarrow{OA} + \overrightarrow{OB}\\ &= -(x_A, y_A) + (x_B, y_B)\\ &= (x_B - x_A,\ y_B - y_A).\end{aligned}$$

(iv) Le milieu I de $[AB]$ a pour coordonnées $\left(\frac{x_B + x_A}{2}, \frac{y_B + y_A}{2}\right)$, car

$$\overrightarrow{OI} = \overrightarrow{OA} + \overrightarrow{AI} = \overrightarrow{OA} + \frac{1}{2}\overrightarrow{AB} = \frac{1}{2}\overrightarrow{OA} + \frac{1}{2}\overrightarrow{OB}.$$

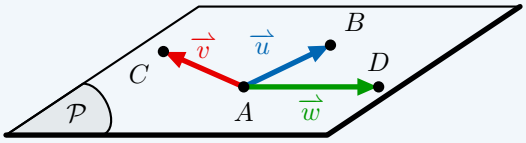
2.4 Vecteurs coplanaires

Nous venons de voir que, dans le plan, tout point est entièrement déterminé par ses coordonnées par rapport à un point et deux vecteurs non colinéaires. Autrement dit, le plan est entièrement déterminé par la donnée d'un repère affine du plan. En se plaçant dans l'espace, cette propriété reste vraie : tout plan est entièrement déterminé par la donnée d'un repère affine de ce plan, c'est-à-dire par la donnée d'un point et de deux vecteurs non colinéaires de ce plan.

Définition 2.23: (Vecteurs coplanaires)

Trois vecteurs $\overrightarrow{u}$, $\overrightarrow{v}$ et $\overrightarrow{w}$ sont ***coplanaires*** s'il existe quatre points coplanaires A, B, C et D tels que

$$\overrightarrow{u} = \overrightarrow{AB}, \qquad \overrightarrow{v} = \overrightarrow{AC}, \qquad \overrightarrow{w} = \overrightarrow{AD}.$$



⚠ Remarque Des vecteurs colinéaires sont nécessairement coplanaires.

Corollaire 2.24: (Critère de coplanarité)

Soient $\overrightarrow{u}$, $\overrightarrow{v}$ et $\overrightarrow{w}$ trois vecteurs, tels que $\overrightarrow{u}$ et $\overrightarrow{v}$ sont non colinéaires. Alors

$$\overrightarrow{u}, \overrightarrow{v}, \overrightarrow{w} \text{ sont coplanaires} \iff \exists\, x, y \in \mathbb{R} : \overrightarrow{w} = x\overrightarrow{u} + y\overrightarrow{v}.$$

On dit alors que $\overrightarrow{w}$ est une ***combinaison linéaire*** de $\overrightarrow{u}$ et $\overrightarrow{v}$.

Démonstration Représentons les deux vecteurs à partir d'un même point A : $\vec{u} = \overrightarrow{AB}$ et $\vec{v} = \overrightarrow{AC}$. Puisqu'ils ne sont pas colinéaires, les points A, B et C déterminent un plan, et $(A, \vec{u}, \vec{v})$ en est un repère affine. Le résultat est alors exactement la proposition sur les coordonnées d'un vecteur dans un plan.

■

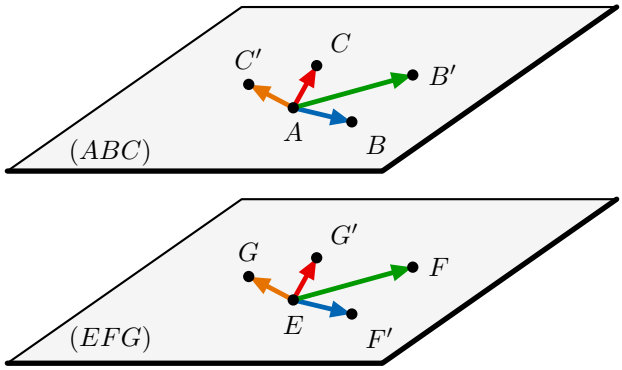
Nous pouvons maintenant simplifier l'énoncé et la preuve de la proposition 1.36 sur le parallélisme des plans.

Proposition 2.25: (Critère de parallélisme des plans de l'espace)

Soient (ABC) et (EFG) deux plans. Alors

$$(ABC) \parallel (EFG) \iff \overrightarrow{AB}, \overrightarrow{AC}, \overrightarrow{EF}, \overrightarrow{EG} \text{ sont coplanaires.}$$

Démonstration Les triplets $(A, \overrightarrow{AB}, \overrightarrow{AC})$ et $(E, \overrightarrow{EF}, \overrightarrow{EG})$ sont des repères respectifs des plans (ABC) et (EFG).



($\Longrightarrow$) Supposons $(ABC) \parallel (EFG)$. Il existe dans (EFG) deux droites sécantes (EF') et (EG'), respectivement parallèles à (AB) et à (AC). Nous pouvons choisir F' et G' de sorte que $\overrightarrow{EF'} = \overrightarrow{AB}$ et $\overrightarrow{EG'} = \overrightarrow{AC}$. Le triplet $(E, \overrightarrow{EF'}, \overrightarrow{EG'})$ est alors un repère de (EFG). Il existe donc des réels x, y, x', y' tels que

$$\begin{cases} \overrightarrow{EF} = x\overrightarrow{EF'} + y\overrightarrow{EG'} = x\overrightarrow{AB} + y\overrightarrow{AC}, \\ \overrightarrow{EG} = x'\overrightarrow{EF'} + y'\overrightarrow{EG'} = x'\overrightarrow{AB} + y'\overrightarrow{AC}. \end{cases}$$

Ainsi, $\overrightarrow{AB}$, $\overrightarrow{AC}$, $\overrightarrow{EF}$ et $\overrightarrow{EG}$ sont coplanaires.

($\Longleftarrow$) Supposons ces quatre vecteurs coplanaires. Il existe alors des réels x, y, x', y' tels que

$$\overrightarrow{EF} = x\overrightarrow{AB} + y\overrightarrow{AC}, \qquad \overrightarrow{EG} = x'\overrightarrow{AB} + y'\overrightarrow{AC}.$$

Soient B' et C' les points de (ABC) définis par

$$\overrightarrow{AB'} = x\overrightarrow{AB} + y\overrightarrow{AC}, \qquad \overrightarrow{AC'} = x'\overrightarrow{AB} + y'\overrightarrow{AC}.$$

Nous avons alors $(AB') \parallel (EF)$ et $(AC') \parallel (EG)$. De plus, (AB') et (AC') sont sécantes, tout comme (EF) et (EG). Par le critère de parallélisme de deux plans, nous concluons que $(ABC) \parallel (EFG)$.

■

2.5 Repère de l'espace

Définition 2.26: (Repère affine de l'espace)

Soient O un point de $\mathcal{E}$ et $\vec{i}$, $\vec{j}$, $\vec{k}$ trois vecteurs non coplanaires. Le quadruplet

$$(O, \vec{i}, \vec{j}, \vec{k})$$

est appelé un ***repère affine*** de l'espace.

Proposition 2.27: (Coordonnées dans l'espace)

Pour tout point $M \in \mathcal{E}$, il existe un unique triplet $(x, y, z) \in \mathbb{R}^3$ tel que

$$\overrightarrow{OM} = x\vec{i} + y\vec{j} + z\vec{k}.$$

Le triplet (x, y, z) est le triplet de ***coordonnées*** de M dans ce repère.

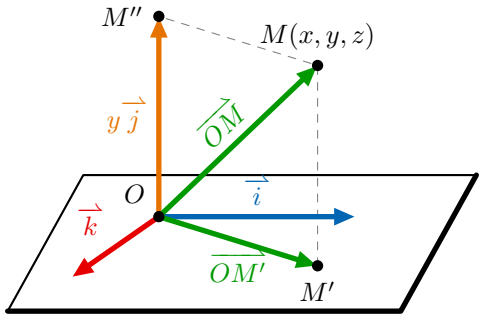
Démonstration Soit M' le point d'intersection de la droite passant par M et dirigée par $\vec{j}$ avec le plan $(O, \vec{i}, \vec{k})$. Soit également M'' le point d'intersection de la droite $(O, \vec{j})$ avec le plan passant par M et dirigé par $\vec{i}$ et $\vec{k}$, lequel est parallèle à $(O, \vec{i}, \vec{k})$.

Il existe alors des réels x, y et z tels que

$$\overrightarrow{OM''} = y\vec{j}, \qquad \overrightarrow{OM'} = x\vec{i} + z\vec{k}.$$

Le quadrilatère $OM''MM'$ est un parallélogramme dans le plan (OMM'). Par conséquent,

$$\overrightarrow{OM} = \overrightarrow{OM'} + \overrightarrow{OM''} = x\vec{i} + y\vec{j} + z\vec{k}.$$



Pour l'unicité, la différence de deux décompositions donnerait une combinaison linéaire nulle de $\vec{i}$, $\vec{j}$, $\vec{k}$. Leur non-coplanarité force alors chacun des trois coefficients à être nul.

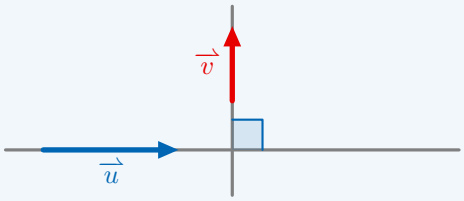
■

2.6 Orthogonalité et produit scalaire

2.6.1 Repères orthonormés

Définition 2.28: (Orthogonalité et repères orthonormés)

- Deux vecteurs $\vec{u}$ et $\vec{v}$ sont ***orthogonaux***, ce que l'on note $\vec{u} \perp \vec{v}$, si une droite dirigée par $\vec{u}$ est perpendiculaire à une droite dirigée par $\vec{v}$ (leurs directions sont perpendiculaires).



- Un repère $(O, \vec{i}, \vec{j})$ du plan est ***orthogonal*** si $\vec{i} \perp \vec{j}$. Un repère $(O, \vec{i}, \vec{j}, \vec{k})$ de l'espace est orthogonal si $\vec{i}$, $\vec{j}$ et $\vec{k}$ sont deux à deux orthogonaux.

- Un repère orthogonal $(O, \vec{i}, \vec{j})$ est ***orthonormé*** si $\|\vec{i}\| = \|\vec{j}\| = 1$. De même, un repère orthogonal $(O, \vec{i}, \vec{j}, \vec{k})$ est orthonormé si $\|\vec{i}\| = \|\vec{j}\| = \|\vec{k}\| = 1$.

2.6.2 Produit scalaire et théorème de Pythagore

Définition 2.29: (Produit scalaire)

Dans un repère orthonormé, soient

$$\vec{u} = (x, y, z) \qquad \text{et} \qquad \vec{v} = (x', y', z').$$

Le ***produit scalaire*** de $\vec{u}$ et $\vec{v}$ est le nombre réel

$$\vec{u} \cdot \vec{v} \quad = \quad xx' + yy' + zz'.$$

Proposition 2.30: (Norme et produit scalaire)

Pour tout vecteur $\vec{u} = (x, y, z)$ exprimé dans un repère orthonormé,

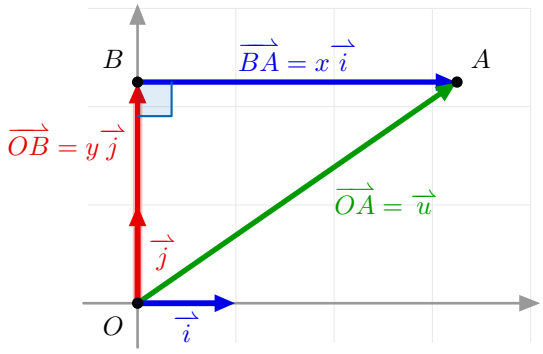
$$\|\vec{u}\|^2 \quad = \quad \vec{u} \cdot \vec{u} \quad = \quad x^2 + y^2 + z^2.$$

Démonstration

- ***Cas où*** $z = 0$.

  Soient A et B les points définis par

$$\overrightarrow{OB} = y\,\vec{j}, \qquad \overrightarrow{OA} = \vec{u} = x\,\vec{i} + y\,\vec{j}.$$



Alors

$$\overrightarrow{BA} \quad = \quad -\overrightarrow{OB} + \overrightarrow{OA} \quad = \quad -y\,\vec{j} + x\,\vec{i} + y\,\vec{j} \quad = \quad x\,\vec{i}\,.$$

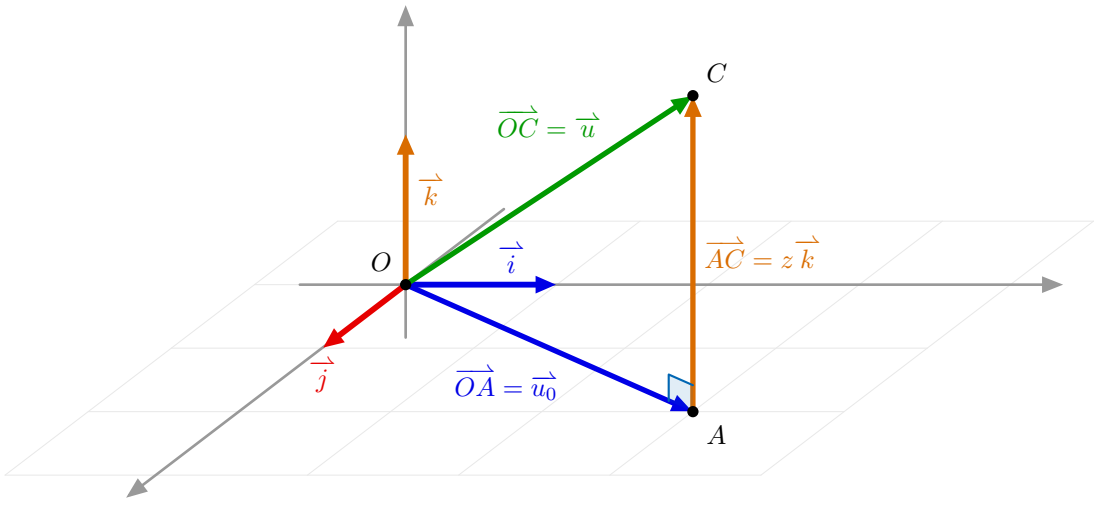
Le vecteur $\overrightarrow{BA} = x\,\vec{i}$ est orthogonal à $\overrightarrow{OB} = y\,\vec{j}$; le triangle OBA est donc rectangle en B. En vertu du THÉORÈME DE PYTHAGORE,

$$\begin{aligned} \|\vec{u}\|^2 \quad &= \quad OA^2 \quad = \quad OB^2 + BA^2 \\ &= \quad \|y\,\vec{j}\,\|^2 + \|x\,\vec{i}\,\|^2 \\ &= \quad x^2 + y^2 \quad = \quad \vec{u} \cdot \vec{u}\,. \end{aligned}$$

- ***Cas général.***

Posons $\vec{u_0} = x\,\vec{i} + y\,\vec{j}$, de sorte que $\vec{u} = \vec{u_0} + z\,\vec{k}$. Soient A et C les points tels que

$$\overrightarrow{OA} = \vec{u_0}, \qquad \overrightarrow{OC} = \vec{u}\,.$$



Nous avons alors

$$\overrightarrow{AC} \quad = \quad -\overrightarrow{OA} + \overrightarrow{OC} \quad = \quad -\vec{u_0} + \vec{u_0} + z\,\vec{k} \quad = \quad z\,\vec{k}\,.$$

Ainsi, $\overrightarrow{AC}$ est orthogonal à $\overrightarrow{OA} = \vec{u_0}$, et le triangle OAC est rectangle en A. Le THÉORÈME DE PYTHAGORE et le cas

précédent donnent

$$\begin{aligned} \|\overrightarrow{u}\|^2 &= OC^2 = OA^2 + AC^2 \\ &= \|\overrightarrow{u_0}\|^2 + \|z\overrightarrow{k}\|^2 \\ &= x^2 + y^2 + z^2 = \overrightarrow{u} \cdot \overrightarrow{u}. \end{aligned}$$

■

Par un simple calcul du produit scalaire utilisant la proposition précédente, nous obtenons le corollaire suivant.

Corollaire 2.31: (Propriétés du produit scalaire)

Pour tous vecteurs $\overrightarrow{u}$, $\overrightarrow{v}$, $\overrightarrow{w}$ et tout $\lambda \in \mathbb{R}$:

(i) $\overrightarrow{u} \cdot \overrightarrow{v} = \frac{1}{2}(\|\overrightarrow{u} + \overrightarrow{v}\|^2 - \|\overrightarrow{u}\|^2 - \|\overrightarrow{v}\|^2)$;

(ii) $\overrightarrow{u} \cdot (\overrightarrow{v} + \overrightarrow{w}) = \overrightarrow{u} \cdot \overrightarrow{v} + \overrightarrow{u} \cdot \overrightarrow{w}$ (***distributivité***) ;

(iii) $(\lambda\overrightarrow{u}) \cdot \overrightarrow{v} = \lambda(\overrightarrow{u} \cdot \overrightarrow{v}) = \overrightarrow{u} \cdot (\lambda\overrightarrow{v})$ (pour tout scalaire $\lambda \in \mathbb{R}$) ;

(iv) $\overrightarrow{u} \cdot \overrightarrow{v} = \overrightarrow{v} \cdot \overrightarrow{u}$ (***commutativité***).

Nous sommes maintenant en mesure de « traduire » le théorème de Pythagore sous forme algébrique. Soient $\overrightarrow{u}$ et $\overrightarrow{v}$ deux vecteurs, et soient A, B et C trois points tels que

$$\overrightarrow{AB} = \overrightarrow{u}, \qquad \overrightarrow{BC} = \overrightarrow{v}.$$

Par la relation de Chasles, $\overrightarrow{u} + \overrightarrow{v} = \overrightarrow{AC}$. Ainsi,

$$AC^2 = \|\overrightarrow{u} + \overrightarrow{v}\|^2 = \|\overrightarrow{u}\|^2 + \|\overrightarrow{v}\|^2 = AB^2 + BC^2$$

si et seulement si le triangle ABC est rectangle en B, en vertu du théorème de Pythagore. Autrement dit, ces égalités sont vraies si et seulement si $\overrightarrow{u} \perp \overrightarrow{v}$. Nous obtenons donc le résultat suivant.

Théorème 2.32: (Forme vectorielle du théorème de Pythagore)

Soient $\overrightarrow{u}$ et $\overrightarrow{v}$ deux vecteurs. Les conditions suivantes sont équivalentes :

(i) $\|\overrightarrow{u} + \overrightarrow{v}\|^2 = \|\overrightarrow{u}\|^2 + \|\overrightarrow{v}\|^2$;

(ii) $\overrightarrow{u} \perp \overrightarrow{v}$;

(iii) $\overrightarrow{u} \cdot \overrightarrow{v} = 0$.

Démonstration D'après la première identité du corollaire précédent,

$$\|\overrightarrow{u} + \overrightarrow{v}\|^2 = \|\overrightarrow{u}\|^2 + \|\overrightarrow{v}\|^2 \iff \overrightarrow{u} \cdot \overrightarrow{v} = 0.$$

Par ailleurs, la forme géométrique du théorème de Pythagore affirme précisément que cette égalité de normes équivaut à $\overrightarrow{u} \perp \overrightarrow{v}$.

■

2.7 Barycentres

En physique, et surtout en mécanique, la notion de ***point d'équilibre*** ou de ***centre de masse*** d'un solide est fondamentale. Le modèle mathématique le plus simple illustrant ce phénomène physique est la notion de barycentre. Pour bien comprendre cette notion, prenons l'exemple d'un polygone à n sommets, auxquels on aurait attaché des poids $a_1, \dots, a_n$. Comment calculer son centre de masse, son point d'équilibre ? La notion de barycentre répond à cette question.

Définition 2.33: (Système de points pondérés)

Soient $A_1, \dots, A_n$ des points de $\mathcal{E}$ et $a_1, \dots, a_n$ des réels. Le n-uplet

$$\big((A_1, a_1), \dots, (A_n, a_n)\big)$$

est appelé un ***système de points pondérés*** ; le réel a_i est le poids associé au point A_i.

Proposition 2.34: (Existence et unicité du barycentre)

Soit $\big((A_1, a_1), \dots, (A_n, a_n)\big)$ un système de points pondérés tel que

$$s = \sum_{i=1}^{n} a_i \neq 0.$$

Il existe un unique point G, appelé le ***barycentre*** du système, tel que

$$\sum_{i=1}^{n} a_i \overrightarrow{GA_i} = \overrightarrow{0}\,.$$

De plus, pour tout point $M \in \mathcal{E}$,

$$\sum_{i=1}^{n} a_i \overrightarrow{MA_i} = s\overrightarrow{MG}.$$

⚠ **Remarque** Lorsque tous les poids sont égaux et non nuls, le barycentre est appelé le ***centre de gravité*** des points $A_1, \dots, A_n$.

Exemple: (Deux barycentres)

- Le milieu I de $[AB]$ est le centre de gravité de A et B. En effet,

$$\begin{aligned} \overrightarrow{IA} = \overrightarrow{BI} \quad &\iff \quad \overrightarrow{IA} - \overrightarrow{BI} = \overrightarrow{IA} + \overrightarrow{IB} = \overrightarrow{0} \\ &\iff \quad I \text{ est le centre de gravité de } A \text{ et } B. \end{aligned}$$

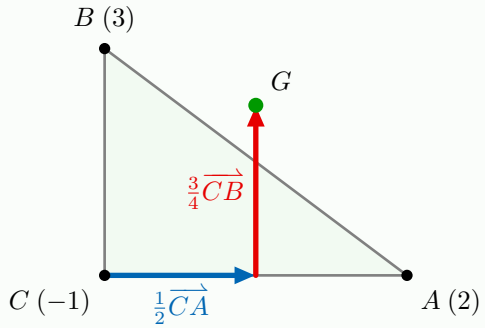
- Attachons les poids 2, 3 et -1 aux sommets respectifs A, B et C d'un triangle. On peut imaginer qu'au lieu d'un poids, quelqu'un tire vers le haut sur le sommet C. Voici comment trouver et placer le barycentre G de $(A, 2)$, $(B, 3)$ et $(C, -1)$. Pour tout point M, puisque $2 + 3 + (-1) = 4 \neq 0$, nous avons

$$4\overrightarrow{MG} \quad = \quad 2\overrightarrow{MA} + 3\overrightarrow{MB} - \overrightarrow{MC}.$$

En considérant le cas particulier $M = C$, nous obtenons

$$\overrightarrow{CG} \quad = \quad \frac{1}{2}\overrightarrow{CA} + \frac{3}{4}\overrightarrow{CB}.$$

Comme les points A, B et C sont donnés, cette équation vectorielle permet de construire G.



Démonstration (Proposition 2.34)

Fixons un point $M \in \mathcal{E}$ et posons $s = \sum_{i=1}^{n} a_i$.

- ***Existence.***

  Puisque $s \neq 0$, il existe un point G déterminé par

$$\overrightarrow{MG} \quad = \quad \frac{1}{s}\sum_{i=1}^{n} a_i \overrightarrow{MA_i}.$$

  En utilisant $\overrightarrow{GA_i} = \overrightarrow{MA_i} - \overrightarrow{MG}$, nous obtenons

$$\sum_{i=1}^{n} a_i \overrightarrow{GA_i} \quad = \quad \sum_{i=1}^{n} a_i \overrightarrow{MA_i} - s\overrightarrow{MG} \quad = \quad \vec{0}\,.$$

- ***Unicité.***

  Si un autre point G' satisfait la même condition, alors

$$\begin{aligned} \vec{0} \quad &= \quad \sum_{i=1}^{n} a_i \overrightarrow{G'A_i} \\ &= \quad \sum_{i=1}^{n} a_i \left(\overrightarrow{G'G} + \overrightarrow{GA_i}\right) \\ &= \quad s\overrightarrow{G'G}. \end{aligned}$$

  Comme $s \neq 0$, nous avons $\overrightarrow{G'G} = \vec{0}$, donc $G' = G$.

Enfin, pour tout point N,

$$\sum_{i=1}^{n} a_i \overrightarrow{NA_i} \quad = \quad \sum_{i=1}^{n} a_i \left(\overrightarrow{NG} + \overrightarrow{GA_i}\right) \quad = \quad s\overrightarrow{NG}.$$

Proposition 2.35: (Associativité du barycentre)

Soit G le barycentre de $\big((A,a),(B,b),(C,c)\big)$, où $a+b+c\neq 0$. Si $b+c\neq 0$ et si K est le barycentre de $\big((B,b),(C,c)\big)$, alors G est le barycentre de

$$\big((A,a),(K,b+c)\big).$$

Démonstration Il suffit de montrer que $a\overrightarrow{GA}+(b+c)\overrightarrow{GK}=\overrightarrow{0}$. Puisque K est le barycentre de $\big((B,b),(C,c)\big)$, la formule du barycentre donne, en prenant $M=G$,

$$(b+c)\overrightarrow{GK} \quad = \quad b\overrightarrow{GB}+c\overrightarrow{GC}.$$

Par conséquent,

$$a\overrightarrow{GA}+(b+c)\overrightarrow{GK} \quad = \quad a\overrightarrow{GA}+b\overrightarrow{GB}+c\overrightarrow{GC} \quad = \quad \overrightarrow{0},$$

car G est le barycentre de $\big((A,a),(B,b),(C,c)\big)$.

2.8 Exercices

Homothétie et translation

Exercice 2.1 (Démonstration de la proposition 2.6) Soit t une translation, montrer que :

- ***(a)*** Si d est une droite alors $t(d)$ est une droite et $t(d)\parallel d$.
- ***(b)*** L'image par t d'un cercle de centre O et de rayon R est un cercle de centre $t(O)$ et de rayon R.

Exercice 2.2 (Démonstration de la proposition 2.16) Soit h une homothétie de centre A et de rapport k non nul, montrer que :

- ***(a)*** Si $k\neq 1$, A est l'unique point fixe de h.
- ***(b)*** Pour tout point M, on a que A, M et $h(M)$ sont alignés.
- ***(c)*** Si d est une droite alors $h(d)$ est une droite et $h(d)\parallel d$.
- ***(d)*** L'image par h d'un cercle de centre O et de rayon R est un cercle de centre $h(O)$ et de rayon $R|k|$.

Exercice 2.3 Montrer que l'image de deux droites perpendiculaires par une homothétie ou une translation sont deux droites perpendiculaires.

Exercice 2.4 Montrer que l'image du milieu d'un segment $[AB]$ par une homothétie ou une translation est le milieu de l'image du segment $[AB]$. Plus généralement, montrer que les homothéties et translations conservent les barycentres.

Exercice 2.5 (Examen 2012) Soit ODF un triangle. Soit $C \in [OD]$ et $A, B, E \in [OF]$ les points tels que $(AC) \parallel (BD)$ et $(EC) \parallel (DF)$. On considère l'homothétie h de centre O qui transforme A en B.

- ***(a)*** Montrer que $h(C) = D$.
- ***(b)*** Montrer que $h(E) = F$.

Exercice 2.6 Soit ABC un triangle, $\mathcal{C}$ son cercle circonscrit et O le centre de $\mathcal{C}$. Soit H le milieu de $[BC]$ et D le point de $\mathcal{C}$ diamétralement opposé à A. Soit $B' = h_{B,-1}(A)$ le symétrique de A par rapport à B et $C' = h_{C,-1}(A)$ le symétrique de A par rapport à C. Soit K le point d'intersection de $(B'C')$ avec la perpendiculaire à $(B'C')$ passant par D (i.e. K est le projeté orthogonal de D sur $(B'C')$).

Le but de l'exercice est de démontrer que K est le milieu de $[B'C']$ et que les points A, H et K sont alignés. Pour cela on considère l'homothétie h de centre A qui transforme B en B'.

- ***(a)*** Faire un dessin.
- ***(b)*** Quel est le rapport de h ?
- ***(c)*** Déterminer les images par h des points O et C, puis l'image du segment $[BC]$.
- ***(d)*** Soit $\mathcal{C}'$ l'image du cercle $\mathcal{C}$ par h. Quel est le centre de $\mathcal{C}'$? Montrer que $\mathcal{C}'$ passe par B' et C'.
- ***(e)*** Montrer que (DK) est médiatrice de $[B'C']$. En déduire que $K = h(H)$ puis que les points A, H et K sont alignés.

Repère du plan et de l'espace

Exercice 2.7 Soit $ABCD$ un parallélogramme. Soit E le milieu de $[AD]$ et le point F tel que $\overrightarrow{AF} = \frac{1}{3}\overrightarrow{AC}$.

- ***(a)*** Exprimer $\overrightarrow{BE}$ et $\overrightarrow{BF}$ en fonction de $\overrightarrow{AB}$ et $\overrightarrow{AD}$.
- ***(b)*** Montrer que B, E et F sont alignés.

Exercice 2.8 Montrer qu'une droite d et un plan $\mathcal{P}$ ne se coupe pas ou $d \subseteq \mathcal{P}$ si et seulement si un vecteur directeur de d est coplanaire à deux vecteurs non-colinéaires de $\mathcal{P}$.

Exercice 2.9 Soit $ABCDEFGH$ un cube. Soit I et J les points définis par $\overrightarrow{DI} = \frac{1}{4}\overrightarrow{DC}$ et $\overrightarrow{BJ} = \frac{3}{4}\overrightarrow{BC}$.

- ***(a)*** Exprimer $\overrightarrow{HF}, \overrightarrow{HJ}$ et $\overrightarrow{EI}$ dans le repère $(D, \overrightarrow{DA}, \overrightarrow{DB}, \overrightarrow{DH})$.
- ***(b)*** Peut-on écrire $\overrightarrow{EI}$ comme combinaison linéaire de $\overrightarrow{HF}$ et $\overrightarrow{HJ}$?
- ***(c)*** Montrer que l'intersection du plan (HEI) et du plan (FHJ) n'est pas vide.

Exercice 2.10 (Examen 2009) Soit $ABCDEFGH$ un cube. Soit P et Q les points définis par $\overrightarrow{DP} = \frac{1}{4}\overrightarrow{DC}$ et $\overrightarrow{BQ} = \frac{3}{4}\overrightarrow{BC}$.

- ***(a)*** Peut-on écrire $\overrightarrow{PH}$ dans le repère $(E, \overrightarrow{GE}, \overrightarrow{GQ})$ du plan (EGQ).
- ***(b)*** Montrer que l'intersection de la droite (HP) et du plan (EGQ) est vide.

Exercice 2.11 On considère un tétraèdre $ABCD$. On appelle I, J, K et L les points définis respectivement par :

$$\overrightarrow{AI} = \frac{2}{3}\overrightarrow{AB}\ ;\ \overrightarrow{BJ} = \frac{1}{3}\overrightarrow{BC}\ ;\ \overrightarrow{CK} = \frac{2}{3}\overrightarrow{CD}\ ;\ \overrightarrow{DL} = \frac{1}{3}\overrightarrow{DA}.$$

(a) Exprimer $\overrightarrow{IJ}$ en fonction de $\overrightarrow{AB}$ et $\overrightarrow{BC}$, puis en fonction de $\overrightarrow{AC}$.

(b) Justifier que les points I, J, K et L sont coplanaires et que l'intersection de la droite (AC) avec le plan $(IJKL)$ est vide.

(c) Montrer que la droite (BD) ne coupe pas le plan $(IJKL)$.

EXERCICE 2.12 Soit $ABCDEFGH$ un parallépipède rectangle. Soit I le milieu du rectangle $ADHE$ et J celui du rectangle $BCGF$.

(a) Montrer que $\overrightarrow{IF} = \overrightarrow{DJ}$.

(b) Justifier que D, J, F et I sont coplanaires. Quel est la nature de $DJFI$?

(c) Montrer que $\overrightarrow{IJ}$, $\overrightarrow{BD}$ et $\overrightarrow{GF}$ sont coplanaires.

EXERCICE 2.13 (Examen 2010) Soit ABCDE une pyramide dont la base ABCD est un quadrilatère convexe tel que $(AB) \parallel (CD)$. Soit I, J et K les points définis par

$$\overrightarrow{AJ} = \frac{3}{4}\overrightarrow{AE}, \quad \overrightarrow{DI} = \frac{3}{4}\overrightarrow{DE}, \quad \overrightarrow{BK} = \frac{3}{4}\overrightarrow{BE}.$$

(a) Donner les coordonnées des points I, J et K dans le repère $(A, \overrightarrow{AB}, \overrightarrow{AD}, \overrightarrow{AE})$.

(b) Montrer les plans (IJK) et (ABC) sont parallèles.

(c) Montrer que la droite $d = (ABE) \cap (CDE)$ est parallèle à la droite (AB).

(d) Montrer que $\overrightarrow{JK}$ est un vecteur directeur de d.

(e) Montrer que la droite d ne coupe pas le plan (IJK).

EXERCICE 2.14 (Examen 2011) Soit $SABCD$ une pyramide dont la base $ABCD$ est un carré. Soit O le centre de gravité du carré $ABCD$ et J le milieu de $[SO]$. Soit K et L les points définis par

$$\overrightarrow{SK} = \frac{1}{3}\overrightarrow{SD}, \quad \overrightarrow{SL} = \frac{2}{3}\overrightarrow{SD}.$$

(a) Donner les coordonnées des points O et J dans le repère $(S, \overrightarrow{SB}, \overrightarrow{SC}, \overrightarrow{SD})$.

(b) Montrer que les vecteurs $\overrightarrow{BK}$, $\overrightarrow{SB}$ et $\overrightarrow{SD}$ sont coplanaires.

(c) Exprimer le vecteur $\overrightarrow{BJ}$ comme combinaison linéaire des seuls vecteurs $\overrightarrow{SB}$ et $\overrightarrow{SD}$.

(d) Montrer que les points B, K et J sont alignés.

(e) Montrer que la droite (OL) est parallèle à la droite (BK).

Produit scalaire

EXERCICE 2.15 Soit $ABCDEFGH$ un cube de côté de longueur 1. On se place dans le repère orthonormé $(A, \overrightarrow{AB}, \overrightarrow{AD}, \overrightarrow{AE})$.

(a) Donner les coordonnées des points A, F, C et G.

(b) Calculer le produit scalaire $\overrightarrow{AF} \cdot \overrightarrow{CH}$. Les droites (AF) et (CH) sont-elles orthogonales ?

(c) Calculer $\overrightarrow{EC} \cdot \overrightarrow{FD}$. Les droites (EC) et (FD) sont-elles orthogonales ?

Exercice 2.16 Soit A, B, C et D quatre points, montrer que $\overrightarrow{AB} \cdot \overrightarrow{CD} = \overrightarrow{AB} \cdot \overrightarrow{C'D'}$, où C', resp. D', est le projeté orthogonal de C, resp. D, sur (AB). En déduire que $\overrightarrow{AB} \cdot \overrightarrow{CD} = AB \cdot C'D'$ si $\overrightarrow{AB}$ et $\overrightarrow{C'D'}$ ont même sens, et $\overrightarrow{AB} \cdot \overrightarrow{CD} = -AB \cdot C'D'$ sinon. (Indice : on se placera dans un repère orthonormé judicieusement choisi)

Exercice 2.17 (Examen 2011) Soit un carré $ABCD$. On construit un rectangle $APQR$ tel que : $P \in [AB]$ et $R \in [AD]$ et $AP = DR$. Le problème a pour but de montrer que les droites (CQ) et (PR) sont perpendiculaires.

(a) Montrer que $\overrightarrow{CQ} \cdot \overrightarrow{PR} = \overrightarrow{CQ} \cdot (\overrightarrow{AR} - \overrightarrow{AP})$.

(b) Montrer que les droites (CQ) et (PR) sont perpendiculaires.

Barycentres

Exercice 2.18

(a) Soit G le barycentre de $((A,a),(B,b),(C,c)))$, $a+b+c \neq 0$. Supposons que $b+c \neq 0$. Montrer que le point d'intersection A' de (AG) avec (BC) est le barycentre de $((B,b),(C,c))$.

(b) Soit G le barycentre de $((A,1),(B,1),(C,1))$. Soit A' le milieu de $[BC]$. Montrer que les médianes du triangles ABC sont concourantes en G et que $\overrightarrow{AG} = \frac{2}{3}\overrightarrow{AA'}$. On retrouve bien que G est le centre de gravité de ABC.

Exercice 2.19 Soit BCD un triangle.

(a) Soient A le barycentre du système pondéré $((B,1),(C,-1),(D,1))$. Montrer que $ABCD$ est un parallélogramme.

(b) Soient I le milieu de $[AB]$, J le milieu de $[BC]$, K le milieu de $[CD]$ et L le milieu de $[AD]$. Montrer que $IJKL$ est un parallélogramme.

Exercice 2.20 (Examen 2010) Soit ABC un triangle et k un réel non nul, on définit les points D et E par les relations :

$$\overrightarrow{AD} = k\overrightarrow{AB} \quad \text{et} \quad \overrightarrow{CE} = k\overrightarrow{CA}.$$

(a) Montrer que D est le barycentre de $((A,1-k),(B,k))$.

(b) Montrer que E est le barycentre de $((C,1-k),(A,k))$.

(c) En déduire que pour tout point M du plan, on a :

$$\overrightarrow{MD} + \overrightarrow{ME} = \overrightarrow{MA} + \overrightarrow{MC} + k\overrightarrow{CB} = 2(\overrightarrow{MB'} + k\overrightarrow{B'C'})$$

où B' et C' sont les milieux respectifs de $[AC]$ et $[AB]$.

(d) Soit I le milieu de $[DE]$, montrer que I, B' et C' sont alignés.

Exercice 2.21 Soit ABC un triangle. Soit H le point défini par $\overrightarrow{AH} = \frac{1}{3}\overrightarrow{AC}$ et K le point défini par $\overrightarrow{AK} = \frac{1}{4}\overrightarrow{AB} + \frac{1}{4}\overrightarrow{AC}$.

(a) Exprimer H comme le barycentre des points A et C.

(b) Exprimer K comme le barycentre des points A, B et C.

(c) En déduire que B, H et K sont alignés.

Exercice 2.22 On considère un tétraèdre $ABCD$. Soit I le milieu de $[AB]$, J le milieu de $[AC]$, K le milieu de $[AD]$, L milieu de $[BC]$, M milieu de $[BD]$, N milieu de $[CD]$. Soit G_1 le centre de gravité de ABC, G_2 celui de ABD, G_3 celui de ACD et G_4 celui de BCD. Montrer que les droites (IN), (JM), (KL), (DG_1), (CG_2), (BG_3) et (AG_4) sont concourantes.

Exercice 2.23 (Examen 2010) Soit A, B, C et D quatre points distincts du plan. On note K le barycentre de $((A,3),(B,1))$, J le milieu de $[DC]$, G le centre de gravité de BCD et I le milieu de $[AG]$.

(a) Montrer que pour tout point M du plan on a $3\overrightarrow{MA} + \overrightarrow{MB} + 2\overrightarrow{MJ} = 6\overrightarrow{MI}$.

(b) En déduire que I est le barycentre de $((K,4),(J,2))$.

(c) Montrer que I, J et K sont alignés.

Exercice 2.24 (Examen 2011) Soit $ABCD$ un parallélogramme de centre de gravité O (l'intersection de ses diagonales) et $k \neq -1$ un réel non nul. Soit I le barycentre de (A,k), $(B,1)$ et J le barycentre de (C,k), $(D,1)$.

(a) Montrer que les droites (AC), (BD) et (IJ) sont concourantes.

(b) Soit E le barycentre de $(A,2-k)$, $(I,k+1)$, $(D,1)$.

(i) Montrer que pour tout point M du plan, on a :

$$2\overrightarrow{MA} + \overrightarrow{MB} + \overrightarrow{MD} = 4\overrightarrow{ME}.$$

(ii) En déduire que E est le milieu de $[AO]$.

(iii) Pour quelle valeur de k les points D, I et E sont-ils alignés ? Justifier.

Exercice 2.25 (La droite et le cercle d'Euler) On considère $\mathcal{P}$ le plan. Soit ABC un triangle, et soit G, O et H ses centres de gravité, centre du cercle circonscrit et orthocentre (respectivement).

(a) Soit $A'B'C'$ le triangle formé des parallèles au côtés de ABC passant par ses sommets.

(i) Montrer que H est le centre du cercle circonscrit à $A'B'C'$.

(ii) Montrer que G est le centre de gravité de $A'B'C'$.

(iii) Montrer que l'homothétie h de centre G et de rapport $-\frac{1}{2}$ envoie $A'B'C'$ sur ABC.

(b) Montrer que $\overrightarrow{GO} = -\frac{1}{2}\overrightarrow{GH}$. En déduire que G, O et H sont alignés (c'est la droite d'Euler).

(c) (Problème difficile) Soit I, J et K les milieux de $[BC]$, $[AC]$ et $[AB]$ et soit $\mathcal{C}$ le cercle circonscrit à IJK. Montrer que $\mathcal{C}$ passe aussi par les pieds des hauteurs de ABC et par les milieux de $[AH]$, $[BH]$ et $[CH]$; c'est le cercle des neufs points d'Euler (indication : on pourra considérer l'homothétie h ainsi que l'homothétie h' de centre H et de rapport $\frac{1}{2}$).

Chapitre 3

Nombres complexes I : algèbre et calcul

Les chapitres précédents nous ont amenés de la géométrie telle que pratiquée par les mathématiciens de l'Antiquité jusqu'à la création de l'algèbre linéaire. Ceci fait, les questions de géométrie classique se traduisent alors souvent sous forme d'équations. C'est le problème de la résolution des équations qui a donné lieu à l'apparition des nombres complexes que nous allons étudier dans ce chapitre.

3.1 Motivation

le problème de trouver des méthodes de résolutions d'équations a passionné, et passionne encore, les mathématiciens. En particulier, les ***équations polynomiales*** sont parmi les premières à avoir été étudiées :

Définition 3.1

Une ***équation polynômiale*** est une équation de la forme

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x^1 + a_0 = 0\ , \quad \text{où} \quad a_i \in \mathbb{R} \quad \text{et} \quad n \in \mathbb{N} \tag{3.1.1}$$

Les plus simples sont les équations du premier degré :

$$ax + b = 0\ , \quad \text{avec} \quad a, b \in \mathbb{R},\ a \neq 0$$

On sait alors que la solution est $x = -\frac{b}{a}$.

Un autre cas très connu est celui des équations de second degré, c'est-à-dire les équations de type

$$ax^2 + bx + c = 0\ , \quad \text{avec} \quad a, b, c \in \mathbb{R},\ a \neq 0.$$

Pour résoudre une telle équation, on calcule d'abord le ***discriminant*** $\Delta = b^2 - 4ac$. Si $\Delta \geqslant 0$, les solutions sont alors

$$x_1 = \frac{-b + \sqrt{\Delta}}{2a} \quad \text{et} \quad x_2 = \frac{-b - \sqrt{\Delta}}{2a}.$$

Dans le cas où $\Delta = 0$, l'unique solution est dite ***double***. On observe alors que l'équation se réécrit de la façon suivante :

$$a(x - x_1)(x - x_2) = 0\ , \quad a \neq 0.$$

Ceci implique que soit $(x - x_1) = 0$, soit $(x - x_2) = 0$. On vient de se ramener à deux équations du premier degré.

De manière générale, la méthode consiste à ***factoriser le polynôme*** $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ ($a_n \neq 0$) sous la forme

$$P(x) = a_n(x - x_n)(x - x_{n-1}) \cdots (x - x_1)$$

où les x_i sont alors les solutions de l'ÉQUATION 3.1.1, que l'on nomme les ***racines*** de $P(x)$.

Revenons aux cas des équations du second degré. Que se passe-t-il si le discriminant $\Delta < 0$? L'équation $ax^2+bx+c = 0$ n'a alors pas de solution.

EXEMPLE

Le polynôme $x^2 + 1$ ne peut pas se factoriser sous la forme

$$x^2 + 1 = (x - x_1)(x - x_2).$$

En effet :

$$x^2 + 1 = 0 \quad \Leftrightarrow \quad x^2 = -1 \quad \Leftrightarrow \quad x = \pm\sqrt{-1}\,,$$

alors que la racine carrée de -1 n'existe pas dans $\mathbb{R}$.

En général, on peut montrer que :

PROPOSITION 3.2

Si $\Delta < 0$, l'équation $ax^2 + bx + c = 0$ n'a pas de solution réelle.

Ceci causera problème si l'on pousse l'étude à des degrés supérieurs :

EXEMPLE

Comment factoriser le polynôme $x^4 + 1$? On peut avoir de la chance et observer que

$$x^4 + 1 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)\,,$$

puis on peut alors factoriser indépendamment chacun de ces polynômes du second degré. Mais comment trouver cette factorisation sans compter sur la chance ? On peut poser $X = x^2$ et résoudre alors l'équation $X^2 + 1 = 0$. Mais on vient de voir que cette équation n'a pas de solution réelle !

La solution à ce problème fut donnée au XVI$^{\text{e}}$ siècle : il suffit d'introduire une solution ***imaginaire***, autrement dit, un nombre imaginaire i tel que $i^2 = -1$. Alors dans ce cas :

$$x^4 + 1 = X^2 + 1 = (X - i)(X + i) = (x^2 - i)(x^2 + i).$$

Imaginons maintenant qu'il y ait une racine carrée à i et $-i$ et continuons ainsi :

$$x^4 + 1 = \left(x + \sqrt{i}\right)\left(x - \sqrt{i}\right)\left(x + \sqrt{-i}\right)\left(x - \sqrt{-i}\right)$$

Pour conclure, on veut imaginer un ensemble dans lequel les lois de calculs seront identiques à celles de $\mathbb{R}$ et qui contiendra toutes les solutions des équations polynômiales : ce sont les ***nombres complexes***. (Nous verrons la fin de la méthode de factorisation de $x^4 + 1$ au cours de ce chapitre.)

3.2 L'ensemble des nombres complexes

Définition 3.3

L'***ensemble des nombres complexes*** est l'ensemble suivant :

$$\mathbb{C} \;=\; \left\{a + ib \;\middle|\; a, b \in \mathbb{R}\right\}.$$

L'écriture $a + ib$ est formelle : la lettre i désigne ici une ***indéterminée***.

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

Soit $z = a + ib \in \mathbb{C}$ un nombre complexe. Le réel a est appelé ***partie réelle*** de z et se note $\mathcal{R}e(z)$. Le réel b est sa ***partie imaginaire*** et se note $\mathcal{I}m(z)$. On admet alors ce qui suit :

$$z = z' \quad \Leftrightarrow \quad \mathcal{R}e(z) = \mathcal{R}e(z') \;\wedge\; \mathcal{I}m(z) = \mathcal{I}m(z') \quad \forall z, z' \in \mathbb{C}$$

Un nombre complexe dont la partie réelle est nulle est dit ***imaginaire pur*** et s'écrit alors $z = ib$. Un nombre complexe dont la partie imaginaire est nulle s'écrit $z = a$: c'est un ***réel***. On a donc une inclusion naturelle de $\mathbb{R}$ dans $\mathbb{C}$: $\mathbb{R} \subseteq \mathbb{C}$.

Avant de pouvoir résoudre des équations, il nous faut définir comment calculer avec des nombres complexes. On va tout d'abord définir une addition sur $\mathbb{C}$ dont la restriction aux nombres réels est l'addition usuelle.

Définition 3.4: (Addition sur $\mathbb{C}$)

Soient $z = a + ib$ et $z' = a' + ib'$ deux nombres complexes. On définit

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

On pose $0 = 0 + i \cdot 0$ et $-z = (-a) + i(-b)$

Exemple

Soient $z = 3 + 2i$ et $z' = -\frac{2}{3} - 5i$. Alors $z + z' = \frac{7}{3} - 3i$.

L'addition complexe vérifie les mêmes propriétés que l'addition réelle :

Proposition 3.5

Soient $x, y, z \in \mathbb{C}$. Alors :

- ***(i)*** $x + y = y + x$ (***commutativité***) ;
- ***(ii)*** $x + (y + z) = (x + y) + z$ (***associativité***) ;
- ***(iii)*** $0 + z = z + 0 = z$ (***élément neutre***) ;
- ***(iv)*** $z + (-z) = 0$ (***opposé***).

Démonstration Voir l'exercice 3.2.

■

On veut maintenant définir sur $\mathbb{C}$ un produit dont la restriction à $\mathbb{R}$ soit la multiplication usuelle de $\mathbb{R}$ et telle que $i^2 = -1$. Effectuons un calcul informel de multiplication en s'autorisant les mêmes principes de calculs dans $\mathbb{R}$ et en supposant que $i^2 = -1$. soient $z = a + ib$ et $z' = a' + b'$ deux nombres complexes. Le produit se calcule ainsi :

$$\begin{aligned} z \cdot z' &= (a + ib) \cdot (a' + ib') = aa' + i^2 bb' + iab' + ia'b \\ &= (aa' - bb') + i(ab' + a'b) \end{aligned}$$

Définition 3.6: (Produit sur $\mathbb{C}$)

Soient $z = a + ib$ et $z' = a' + ib'$ deux nombres complexes. On définit

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

On rappelle que $1 = 1 + i \cdot 0$. Ainsi : $1 \cdot (a + ib) = (1a - 0b) + i(1b + 0a) = a + ib$.

Exemple

Soient $z = 3 + 2i$ et $z' = -\frac{2}{3} - 5i$. Alors :

$$zz' = (3 + 2i)\left(-\frac{2}{3} - 5i\right) = -2 - 15i - \frac{4}{3}i + 10 = 8 - \frac{49}{3}i.$$

Proposition 3.7

Soient $x, y, z \in \mathbb{C}$. Alors :

- ***(i)*** $xy = yx$ (***commutativité***) ;
- ***(ii)*** $x(yz) = (xy)z$ (***associativité***) ;
- ***(iii)*** $1 \cdot z = z \cdot 0 = z$ (***élément neutre***) ;
- ***(iv)*** $x(y + z) = xy + xz$ (***distributivité***) ;
- ***(v)*** si $z \neq 0$, il existe un unique nombre complexe noté z^{-1} tel que $zz^{-1} = 1$ (***inverse***).

Démonstration Voir l'exercice 3.3.

■

Remarque

(i) On dit alors que $(\mathbb{C}, +, \cdot)$ est un ***corps***. On l'appelle le ***corps des nombre complexes***.

(ii) L'inverse d'un nombre complexe non nul est

$$(a+ib)^{-1} = \frac{1}{a+ib} = \left(\frac{a}{a^2+b^2} + i\frac{-b}{a^2+b^2}\right)$$

En effet, si $z \in \mathbb{C}^* = \mathbb{C}\backslash\{0\}$, alors $z = a + ib$ avec a, b qui ne sont pas nuls en même temps. On obtient

$$z \cdot \left(\frac{a}{a^2+b^2} + i\frac{-b}{a^2+b^2}\right) = \left(a\frac{a}{a^2+b^2} - b\frac{-b}{a^2+b^2}\right) + i\left(b\frac{a}{a^2+b^2} + a\frac{-b}{a^2+b^2}\right) = 1,$$

d'où le résultat de l'énoncé.

3.2.1 Module et conjugué d'un nombre complexe

Dans le souci de vouloir simplifier la formule de l'inverse, nous posons les définitions suivantes :

Définition 3.8

Soit $z = a + ib$ un nombre complexe.

(i) Le ***module*** de z est le nombre $|z| = \sqrt{a^2+b^2}$.

(ii) Le nombre complexe $\overline{z} = a - ib$ est le ***conjugué*** de z.

L'inverse d'un nombre complexe $z \in \mathbb{C}$ est alors

$$z^{-1} = \frac{1}{z} = = \frac{\overline{z}}{|z|^2}.$$

Exemple

Si $z = 3 - 4i$, alors $|z| = 5$ et $\overline{z} = 3 + 4i$. On observe alors que

$$z\overline{z} = (3-4i)(3+4i) = (9+16) + i(12-12) = 25 = |z|^2.$$

Proposition 3.9

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

(i) $z\overline{z} = |z|^2 \in \mathbb{R}$;

(ii) $z + \overline{z} = 2\mathcal{R}e(z)$;

(iii) $z - \overline{z} = 2\mathcal{I}m(z)$;

(iv) $|zz'| = |z||z'|$ et $|z| = |\overline{z}|$;

(v) $z \in \mathbb{R} \Leftrightarrow \mathcal{I}m(z) = 0 \Leftrightarrow \overline{z} = z$.

DÉMONSTRATION Voir l'EXERCICE 3.4.

■

REMARQUE Il est souvent utile d'exprimer tout nombre complexe sous sa forme canonique $A + iB$, avec $A, B \in \mathbb{R}$. En particulier, si $z, z' \in \mathbb{C}$, alors pour écrire $\frac{z}{z'} = A + iB$ il suffira de multiplier le numérateur et le dénominateur de la fraction par $\overline{z'}$:

$$\frac{z}{z'} = \frac{z}{z'} \cdot \frac{\overline{z'}}{\overline{z'}} = \frac{\mathcal{R}e(z\overline{z'})}{|z'|^2} + i\frac{\mathcal{I}m(z\overline{z'})}{|z'|^2}$$

3.2.2 Forme trigonométrique, forme exponentielle et formule de *De Moivre*

Toujours dans un souci d'apprendre à calculer avec les nombres complexes afin de résoudre des équations polynomiales, nous voudrions trouver une façon de simplifier l'écriture des puissances $z^n = (a + ib)^n$ d'un nombre complexe $z = a + ib \in \mathbb{C}$. Pour cela, nous allons nous servir de notions géométriques.

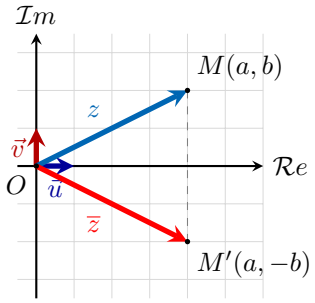
Identification du plan avec $\mathbb{C}$. Le plan usuel peut être vu à la fois comme l'ensemble $\mathbb{R}^2$ des couples (x, y) de réels et comme l'ensemble $\mathbb{C}$ des nombres complexes. On établit entre ces deux ensembles une bijection naturelle en associant à tout point $M(x, y)$ du plan le nombre complexe $z_M = x + iy$. Ainsi, chaque point du plan correspond à un unique nombre complexe, et réciproquement, chaque nombre complexe représente un point du plan.

On munit le plan $\mathcal{P}$ d'un repère orthonormé $(O, \vec{u}, \vec{v})$, où $\vec{u}$ et $\vec{v}$ sont les vecteurs unitaires associés aux axes des abscisses et des ordonnées. Les nombres complexes admettent alors une ***interprétation géométrique*** : si $z = a + ib$, le point M d'affixe z a pour coordonnées (a, b) dans ce repère. On dit que z est l'***affixe*** du point M. Dans cette identification, l'axe des abscisses correspond à l'ensemble des réels et l'axe des ordonnées à celui des imaginaires purs.

REMARQUE

(i) Le segment $[OM]$ est de longueur $|z|$. Autrement dit : $OM = ||\overrightarrow{OM}|| = |z|$.

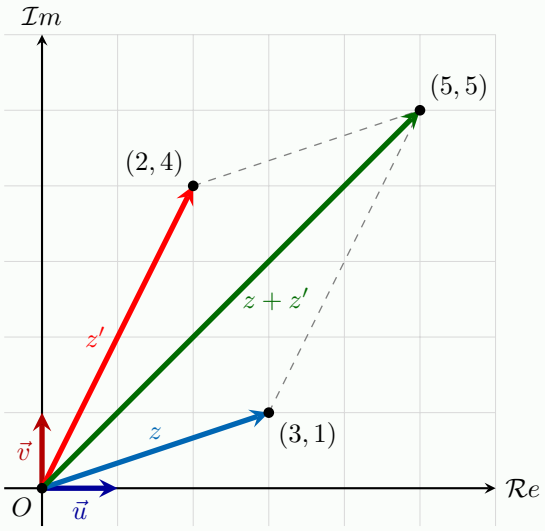
(ii) Soit M' le symétrique de M par rapport à l'axe des abscisses. M' a donc pour coordonnée $(a, -b)$ et son affixe est $\overline{z}$.



On remarque aussi que l'addition des éléments de $\mathbb{C}$ coïncide avec l'addition des vecteurs du plan :

Exemple

Soient $z = 3 + i$ et $z' = 2 + 4i$. On calcule facilement que $z + z' = 5 + 5i$. Remarquons que cette addition coïncide avec l'addition des vecteurs $(3, 1)$ et $(2, 4)$:



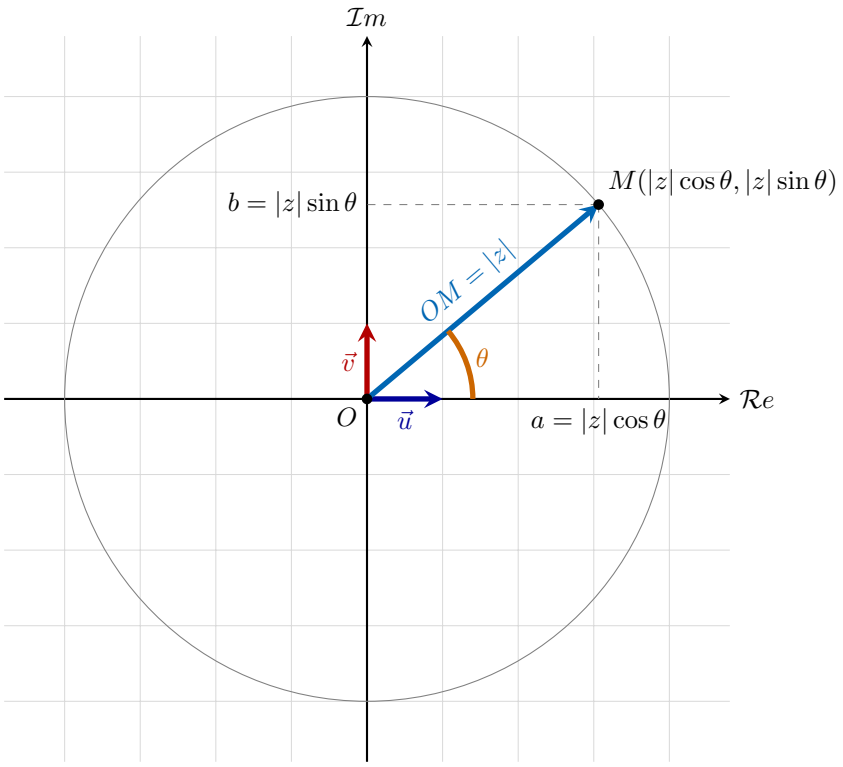
Si $|z| = 1$, alors le point M correspondant se trouve sur le cercle de centre O (de coordonnée $(0, 0)$) et de rayon 1. En vertu de la définition des fonction ***cosinus*** et ***sinus***, il existe un unique $\theta \in [0, 2\pi[$ tel que $z = a + ib = \cos\theta + i\sin\theta$, et tout nombre complexe de cette forme est de module 1, car $\cos^2\theta + \sin^2\theta = 1$. On peut généraliser pour tout $|z| > 0$:

Proposition 3.10

Soit $z = a + ib \in \mathbb{C}$. Alors il existe un unique $\theta \in [0, 2\pi[$ tel que $z = |z|\big(\cos\theta + i\sin\theta\big)$. Le nombre θ est appelé l'***argument*** de z et est noté $\arg(z)$.

Démonstration Voir l'exercice 3.8.

Visuellement, voici un nombre $z = a + ib \in \mathbb{C}$, représenté par le point M dans le plan complexe et dont les coordonnées peuvent être calculées à partir de $|z|$ et $\arg(z) = \theta$:



Définition 3.11

L'écriture $z = a + ib$ de $z \in \mathbb{C}$ est appelée la ***forme algébrique*** de z, tandis que $z = |z|\big(\cos\theta + i\sin\theta\big)$ est appelée la ***forme trigonométrique*** de z.

Exemple

Considérons $z = 2 + 2i$. Trouvons l'argument de z. On a $|z| = \sqrt{2^2 + 2^2} = 2\sqrt{2}$ et donc

$$z = 2\sqrt{2}\left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right).$$

En identifiant cette équation avec $z = |z|\big(\cos\theta + i\sin\theta\big)$, on obtient que $\cos\theta = \sin\theta = \frac{\sqrt{2}}{2}$. On en déduit donc que $\theta = \arg(z) = \frac{\pi}{2}$.

⚠ **Remarque** L'argument de z est l'angle orienté entre le vecteur $\vec{u}$ de coordonnées $(1, 0)$ et le vecteur $\overrightarrow{OM}$.

Proposition 3.12: (Formule de *De Moivre*)

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

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

On écrit $e^{i\theta}$ pour $\cos\theta + i\sin\theta$ (ceci reçoit sa justification dans un cours d'analyse), et la formule de ***De Moivre*** s'écrit alors plus simplement : $\big(e^{i\theta}\big)^n = e^{in\theta}$.

Démonstration Afin de démontrer cette proposition, nous aurons besoin d'un nouvel outil de preuve : la preuve par récurrence, présentée au chapitre 4.

■

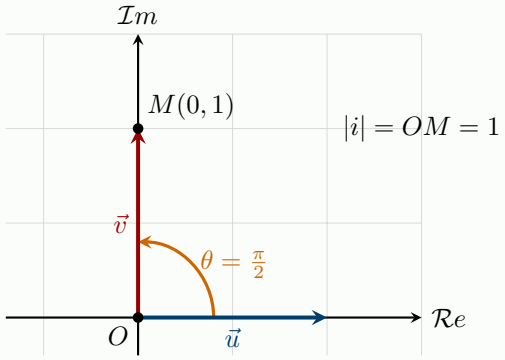
On peut maintenant simplifier la forme trigonométrique d'un nombre complexe trouvée dans la proposition 3.12 :

Définition 3.13: (Notation exponentielle)

Un nombre complexe s'écrit sous la forme $z = re^{i\theta}$, où $r = |z|$ est le ***module*** de z et θ est son ***argument***. Le couple (r, θ) sont les ***coordonnées polaires*** du point d'affixe z.

Exemple

Trouvons la forme exponentielle de $z = i$. Le point M correspondant possède les coordonnées $(0, 1)$. On a que $|z| = 1$ et $\arg(z) = \frac{\pi}{2}$. Ainsi, on trouve que $i = e^{i\frac{\pi}{2}}$.



Similairement, on obtient aussi que $-i = e^{-i\frac{\pi}{2}}$.

Cette notation exponentielle facilite grandement le calcul du produit de deux nombres complexes. Deux nombres complexes se multiplient alors selon la formule suivante :

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

En particulier,

$$\arg(zz') = \arg(z) + \arg(z') \quad \text{et} \quad \arg\left(\frac{z}{z'}\right) = \arg(z) - \arg(z').$$

De plus, $\left(e^{i\theta}\right)^n = r^n e^{in\theta}$ et $\sqrt{re^{i\theta}} = \left(re^{i\theta}\right)^{\frac{1}{2}} = \sqrt{r}e^{i\frac{\theta}{2}}$ (ici $r \geqslant 0$, donc $\sqrt{r}$ existe).

Exemple

On a vu au début du chapitre que $x^4 + 1 = (x^2 - i)(x^2 + i)$. Sachant que

$$i = e^{i\frac{\pi}{2}} \quad \text{et} \quad -i = e^{-i\frac{\pi}{2}},$$

on trouve

$$x^4+1 \;=\; \left(x^2-e^{i\frac{\pi}{2}}\right)\left(x^2-e^{-i\frac{\pi}{2}}\right) \;=\; \left(x-e^{i\frac{\pi}{4}}\right)\left(x+e^{i\frac{\pi}{4}}\right)\left(x-e^{-i\frac{\pi}{4}}\right)\left(x+e^{-i\frac{\pi}{4}}\right).$$

Posons $z=e^{i\frac{\pi}{4}}$. Alors $\overline{z}=e^{-i\frac{\pi}{4}}$. L'équation ci-dessus se réécrit alors

$$x^4+1 \;=\; (x-z)(x-\overline{z})(x+\overline{z})(x+z) \;=\; \left(x^2-(z+\overline{z})x+z\overline{z}\right)\left(x^2+(z+\overline{z})x+z\overline{z}\right).$$

Comme $z\overline{z}=|z|^2=1$ et $z+\overline{z}=2\mathcal{R}e(z)=\sqrt{2}$, on obtient finalement le résultat escompté :

$$x^4+1=\left(x^2-\sqrt{2}x+1\right)\left(x^2+\sqrt{2}x+1)\right).$$

Ce phénomène est plus profond, comme nous le verrons dans la suite de ce chapitre.

Définition 3.14: (Racines de l'unité)

Soit $n\in\mathbb{N}^*$. On dit que $z\in\mathbb{C}$ est une ***racine $n^{ième}$ de l'unité*** si $z^n=1$.

Proposition 3.15

Toute racine de l'unité a pour module 1.

Démonstration Soit $z=re^{i\theta}$ une racine $n^{\text{ième}}$ de l'unité, où $r>0$. Alors $z^n=1$, donc

$$r^n e^{in\theta} \;=\; 1\cdot e^{0i}.$$

Ces deux écritures exponentielles représentent le même nombre complexe ; leurs modules sont donc égaux. Ainsi, $r^n=1$. Comme $n\geqslant 1$, la fonction $x\mapsto x^n$ est strictement croissante sur $\mathbb{R}^+$, d'où $r=1$. Par conséquent, $|z|=r=1$.

3.3 exercices

Exercice 3.1 Écrire les nombres complexes suivants sous la forme $a+ib$:

(a) $1+3i+9i^2+27i^3+81i^4+243i^5$;

(b) $\dfrac{7-3i}{1+5i}$;

(c) $i^{1000}+i^{123}$.

Réponse : (a) $73+219i$; (b) $-\dfrac{11}{13}+\dfrac{16}{13}i$; (c) $1-i$.

Exercice 3.2 (Démonstration de la proposition 3.5) Soient $z, z', z'' \in \mathbb{C}$. Montrer que :

(i) $z + z' = z' + z$ (commutativité) ;

(ii) $z + (z' + z'') = (z + z') + z''$ (associativité) ;

(iii) $0 + z = z + 0 = z$ (élément neutre) ;

(iv) $z + (-z) = 0$ (opposé).

Exercice 3.3 (Démonstration de la proposition 3.7) Soient $z, z', z'' \in \mathbb{C}$. Montrer que :

(i) $zz' = z'z$ (commutativité) ;

(ii) $z(z'z'') = (zz')z''$ (associativité) ;

(iii) $1 \cdot z = z \cdot 1 = z$ (élément neutre) ;

(iv) $z(z' + z'') = zz' + zz''$ (distributivité) ;

(v) si $z \neq 0$, il existe un unique nombre complexe noté z^{-1} tel que $zz^{-1} = 1$ (inverse).

Exercice 3.4 (Démonstration de la proposition 3.9) Soient $z, z' \in \mathbb{C}$. Montrer que :

(i) $z\overline{z} = |z|^2 \in \mathbb{R}$;

(ii) $z + \overline{z} = 2\mathcal{R}e(z)$;

(iii) $z - \overline{z} = 2i\,\mathcal{I}m(z)$;

(iv) $|zz'| = |z||z'|$ et $|\overline{z}| = |z|$;

(v) $z \in \mathbb{R} \iff \mathcal{I}m(z) = 0 \iff z = \overline{z}$.

Exercice 3.5 Montrer que si z est un nombre complexe de module 1, son inverse est $\overline{z}$.

Exercice 3.6

(a) Calculer le module des nombres complexes suivants :

$$z_1 = (7 + 35i)(3 + 2i), \quad z_2 = \frac{7 - 35i}{3 - 2i}, \quad z_3 = \frac{(5 + 3i)(1 + i)}{4 + i}.$$

(b) Mettre sous forme algébrique les nombres complexes suivants : z_1, z_2, z_3, $z_1 + z_2$, $z_2 - z_3$, $z_1 z_2$, $z_1 z_3$.

Réponse : (a) $|z_1| = 91\sqrt{2}$; $|z_2| = 7\sqrt{2}$; $|z_3| = 2$.
(b) $z_1 + z_2 = -42 + 112i$; $z_2 - z_3 = \dfrac{103}{17} - i\dfrac{149}{17}$; $z_1 z_2 = 490 + 1176i$; $z_1 z_3 = -\dfrac{4354}{17} + i\dfrac{434}{17}$.

Exercice 3.7 (Démonstration du cours) Montrer que si $z, z' \in \mathbb{C}^*$, alors

$$\frac{z}{z'} = \frac{\mathrm{Re}(zz')}{|z'|^2} + i\,\frac{\mathrm{Im}(zz')}{|z'|^2}.$$

Exercice 3.8 (Démonstration de la proposition 3.10) Soit $z \in \mathbb{C}$, montrer qu'il existe un unique $\theta \in [0, 2\pi[$ tel que

$$z = |z|(\cos\theta + i\sin\theta).$$

Exercice 3.9 Écrire les nombres complexes suivants sous forme exponentielle :

(a) $z_1 = 1 + i$;

(b) $z_2 = \sqrt{3} + i$;

(c) $z_3 = 1 - i\sqrt{3}$.

Réponse : (a) $z_1 = \sqrt{2}e^{i\frac{\pi}{4}}$; (b) $z_2 = 2e^{i\frac{\pi}{6}}$; (c) $z_3 = 2e^{i\frac{5\pi}{3}}$.

EXERCICE 3.10 Soit $j = -\dfrac{1}{2} + \dfrac{\sqrt{3}}{2}i$.

(a) Calculer $|j|$;

(b) Démontrer que $j^2 = \overline{j}$;

(c) En déduire que j est une racine cubique de l'unité.

Réponse : (a) $|j| = 1$; (b) $j^2 = -\dfrac{1}{2} - \dfrac{\sqrt{3}}{2}i = \overline{j}$; (c) $j^3 = j^2 \cdot j = \overline{j} \cdot j = |j|^2 = 1$.

EXERCICE 3.11 (Examen 2011)

On considère les deux nombres complexes suivants : $z_1 = 1 + i\sqrt{3}$ et $z_2 = 1 - i$.

(a) Écrire z_1 et z_2 sous forme exponentielle ;

(b) Donner la forme algébrique et exponentielle de $z_1 z_2$;

(c) En déduire la valeur exacte de $\cos\frac{\pi}{12}$ et de $\sin\frac{\pi}{12}$.

Chapitre 4

La propriété de récurrence — interlude méthodologique

La formule de ***De Moivre*** (PROPOSITION 3.12), annoncée au chapitre précédent, est un bon exemple d'énoncé vrai pour tout entier naturel n ; pour en établir la preuve, nous introduisons ici le ***raisonnement par récurrence***.

Le ***bon ordre*** est une propriété de l'ensemble $\mathbb{N}$ des entiers naturels, que nous prenons comme un axiome :

AXIOME 4.1: (BON ORDRE)

Tout sous-ensemble non vide de $\mathbb{N}$ admet un plus petit élément. Autrement dit, si $A \subseteq \mathbb{N}$ et $A \neq \emptyset$, il existe $n \in A$ tel que $n \leq x$ pour tout $x \in A$.

EXEMPLE

Soit $A = \{1, 3, 5, \dots\}$ l'ensemble des nombres impairs. Alors $1 \in A$ est son plus petit élément.

Commençons par énoncer une proposition qui servira d'illustration à notre propos :

PROPOSITION 4.2

Pour tout $n \in \mathbb{N}$, la somme de tous les entiers de 0 à n est égale à $n(n+1)/2$.

Comment démontrer que cette proposition est vraie ?

Pour poser le problème autrement, comment démontrer une propriété qu'ont tous les entiers naturels n ? On note $P(n)$ une propriété donnée pour un entier n quelconque (à lire : n a la propriété P). On veut donc montrer que $P(0)$ est vraie, ainsi que $P(1),\ P(2),\ P(3), \dots$ Pour cela, on va utiliser une propriété des nombres entiers : la ***propriété de récurrence***.

Exemple

Revenons à la preuve de la proposition 4.2. Traduite dans le langage des mathématiques, la proposition s'énonce : pour tout $n \in \mathbb{N}$,

$$P(n) \ : \quad \sum_{i=0}^{n} i \ = \ 0+1+2+\cdots+(n-1)+n \ = \ \frac{n(n+1)}{2}.$$

On appelle $P(n)$ l'***hypothèse de récurrence***.

Étape 1. Montrons que $P(0)$ est vraie : pour $n=0$, on a $\sum_{i=0}^{0} i = 0 = \frac{0\times 1}{2}$, donc $P(0)$ est vraie.

Étape 2. Supposons que $P(n)$ soit vraie pour un certain entier naturel n et essayons d'en déduire $P(n+1)$. L'hypothèse de récurrence implique que la somme des entiers de 0 à n vaut $n(n+1)/2$; nous en déduisons

$$\sum_{i=0}^{n+1} i \ = \ \sum_{i=0}^{n} i \ + \ (n+1) \ = \ \frac{n(n+1)}{2} + (n+1) \ = \ (n+1)\Big(\frac{n}{2}+1\Big) = \frac{(n+1)(n+2)}{2},$$

ce qui démontre que $P(n+1)$ est vraie.

Ainsi, nous avons montré que : ***(i)*** $P(0)$ est vraie, et ***(ii)*** si $P(n)$ est vraie, alors $P(n+1)$ est vraie. Mais comment conclure que $\forall n \in \mathbb{N}$, $P(n)$ est vraie ?

Proposition 4.3: (Principe de récurrence — première forme)

Supposons que pour tout entier $n \geqslant 0$ on se voit donné une propriété $P(n)$, et supposons que nous puissions démontrer que :

- ***(i)*** la propriété est vraie au premier rang, c-à-d $P(0)$ est vraie.
- ***(ii)*** ***(Hypothèse de récurrence, première forme)*** la propriété se transmet de rang en rang, c'est-à-dire que si on suppose l'énoncé $P(n)$ vrai pour un entier n fixé, alors on peut montrer que l'énoncé $P(n+1)$ est aussi vrai.

Alors nous pouvons conclure que $P(n)$ est vraie pour tout $n \in \mathbb{N}$.

⚠ **Remarque** La première étape pourrait traiter d'un autre nombre naturel que 0. Par exemple, si on a une propriété $P(n)$ pour tous les entiers naturels $n \geqslant 6$, il faudrait remplacer "***(i)*** $P(0)$ est vraie" par "***(i)*** $P(6)$ est vraie".

Exemple

Revenons à la preuve de la proposition 4.2. Comme nous avons montré précédemment que ***(i)*** $P(0)$ est vraie et ***(ii)*** $P(n) \Rightarrow P(n+1)$, on peut donc conclure que la proposition est vraie.

Ce nouvel outil de preuve semble bien puissant, mais pourquoi est-il correct ? en voici la preuve :

Démonstration (Principe de récurrence — première forme)

Pour une propriété $P(n)$, supposons que $P(0)$ soit vraie et que pour un $n \in \mathbb{N}$ quelconque, on ait $P(n) \Rightarrow P(n+1)$ (hypothèse de récurrence).

Posons $A = \{n \in \mathbb{N} \mid P(n) \text{ est vraie}\}$, l'ensemble des entiers n pour lesquels la propriété est vraie.

On procède à un raisonnement par l'absurde : supposons que $A \neq \mathbb{N}$. Son complément A^C est donc un sous-ensemble non vide de $\mathbb{N}$. Par l'AXIOME DU BON ORDRE, il existe $m \in A^C$ tel que $m \leqslant n$ pour tout $n \in A^C$. Comme $P(0)$ est vraie, $0 \notin A^C$. Donc $m \neq 0$, ce qui implique que $m-1 \geqslant 0$. Par minimalité de m dans A^C, on a que $(m-1) \notin A^C$, signifiant que $(m-1) \in A$ et de ce fait $P(m-1)$ est vraie. Par hypothèse de récurrence, $P(m)$ est donc vraie, contredisant $m \in A^C$. Donc $A = \mathbb{N}$.

■

⚠ REMARQUE Afin d'utiliser une preuve par récurrence, il est fondamental de vérifier l'hypothèse de récurrence, mais aussi l'hypothèse de premier rang. Sans vérification de l'hypothèse au premier rang, mais tout en vérifiant l'hypothèse de récurrence, vous risquez de démontrer que tout nombre dans $\mathbb{Z}$ est positif, ce qui est absurde !

Dans le cas d'un raisonnement par récurrence, on peut supposer non seulement $P(n)$ vraie, mais aussi toutes les propriétés $P(k)$ pour les entiers $k \leqslant n$:

⚠ REMARQUE ***Récurrence (deuxième forme)***

On peut en fait remplacer l'hypothèse ***(ii)*** dans le principe de récurrence par cette hypothèse alternative :

(ii') ***(hypothèse de récurrence, deuxième forme)*** pour un entier $n \in \mathbb{N}$ quelconque, si $P(k)$ est vraie pour tout $0 \leqslant k \leqslant n$, alors $P(n+1)$ est vraie.

La preuve est mot pour mot identique à la preuve du principe de récurrence énoncé ci-dessus. On invite le lecteur à s'en convaincre.

4.1 Exercices

EXERCICE 4.1 (Formule du binôme de Newton)

Montrer par récurrence que pour tout $n \in \mathbb{N}$ et pour tout $x, y \in \mathbb{R}$:

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}.$$

On rappelle que $\binom{n}{i} = \dfrac{n!}{i!(n-i)!}$.

EXERCICE 4.2 Montrer par récurrence les formules suivantes :

(a) $\displaystyle\sum_{k=0}^{n} k(k+1) = \frac{1}{3} n(n+1)(n+2)$;

(b) $\displaystyle\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$;

(c) $\displaystyle\sum_{k=1}^{n} k^3 = \left(\sum_{i=1}^{n} i \right)^2$;

(d) $\displaystyle\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$;

(e) $2^n > n$.

Exercice 4.3 (Examen 2010)

(a) Vérifier que $3^{2n+4} = 7 \cdot 3^{2n+2} + 2 \cdot 3^{2n+2}$;

(b) Démontrer par récurrence que pour tout entier $n \geqslant 1$, 7 divise $3^{2n+2} - 2^{n+1}$

Exercice 4.4 (Examen 2011) Montrer la formule suivante par récurrence :

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} \;=\; 1 - \frac{1}{n+1}\,, \quad \forall n \in \mathbb{N}^*.$$

Chapitre 5

Nombres complexes II : polynômes et interprétation géométrique

5.1 Démonstration de la formule de De Moivre

Maintenant que l'on s'est équipé du principe de récurrence comme outil de démonstration, il nous est maintenant possible de prouver la FORMULE DE DE MOIVRE :

DÉMONSTRATION (FORMULE DE DE MOIVRE)

Nous allons montrer par récurrence sur $n \in \mathbb{N}$ la ***formule de De Moivre :***

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

Soit $\theta \in \mathbb{R}$ un réel quelconque.

Initialisation : pour $n = 0$, $(\cos\theta + i\sin\theta)^0 = 1 = 1 + 0i = \cos(0\theta) + i\sin(0\theta)$.

Hérédité : supposons maintenant la formule vraie pour un $n \in \mathbb{N}$ fixé :

$$\big(\cos\theta + i\sin\theta\big)^n \;=\; \cos(n\theta) + i\sin(n\theta) \qquad (\textbf{\textit{hypothèse de récurrence}})$$

Montrons qu'elle l'est aussi au rang $n+1$, c'est-à-dire que :

$$\big(\cos\theta + i\sin\theta\big)^{n+1} \;=\; \cos\big((n+1)\theta\big) + i\sin\big((n+1)\theta\big)$$

Développons l'expression $\big(\cos\theta + i\sin\theta\big)^{n+1}$ en utilisant l'***hypothèse de récurrence*** :

$$\begin{aligned}
\big(\cos\theta + i\sin\theta\big)^{n+1} &= (\cos\theta + i\sin\theta)^n(\cos\theta + i\sin\theta) \\
&= (\cos(n\theta) + i\sin(n\theta))(\cos\theta + i\sin\theta) \\
&= \big(\cos(n\theta)\cos\theta - \sin(n\theta)\sin\theta\big) + i\big(\sin(n\theta)\cos\theta + \cos(n\theta)\sin\theta\big) \\
&= \cos\big((n+1)\theta\big) + i\sin\big((n+1)\theta\big).
\end{aligned}$$

Ainsi, comme la propriété de la formule de De Moivre est vraie au premier rang, et qu'elle se transmet de rang en rang, elle est vraie pour tout $n \in \mathbb{N}$ par le PRINCIPE DE RÉCURRENCE.

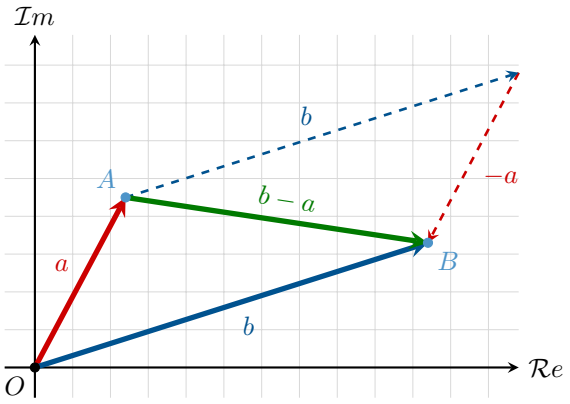
■

5.2 Nombres complexes et géométrie : angles et rotations

Continuons à explorer le lien entre nombres complexes et géométrie. Dans le CHAPITRE 1, nous avons utilisé quelques concepts sans les définir, tels les angles, les points, les droites, etc. Nous allons voir comment bien définir ces concepts dans le plan.

5.2.1 Points, vecteurs, droites et cercles

Points et vecteurs. Un point A du plan est représenté par son affixe $a \in \mathbb{C}$. De même, si A et B sont les points d'affixes a et b, le vecteur $\overrightarrow{AB}$ est associé au nombre complexe $b - a$:

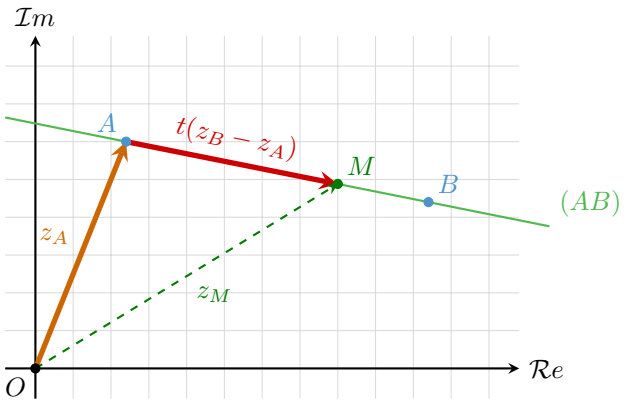


Axes, droites et cercles. On pose O comme le point de coordonnée $(0, 0)$ et les vecteurs $\vec{u}$ et $\vec{v}$ comme les vecteurs associés aux nombres complexes 1 et i. On considère le plan $\mathcal{P}$ muni d'un repère orthonormé $(O, \vec{u}, \vec{v})$. On a alors les correspondances suivantes. Soient A et B des points du plan d'affixes respectifs z_A et z_B :

- ***(i)*** l'affixe du vecteur $\overrightarrow{OA}$ est z_A et $\|\overrightarrow{OA}\| = |z_A|$;
- ***(ii)*** l'affixe du vecteur $\overrightarrow{AB}$ est $z_B - z_A$ et $\|\overrightarrow{AB}\| = |z_B - z_A|$;
- ***(iii)*** la droite (AB) passant par A et B est définie comme l'ensemble

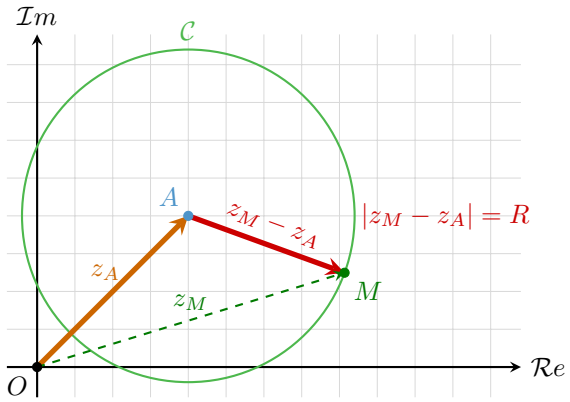
$$(AB) = \{\, M \in \mathcal{P} \mid z_M = z_A + t\,(z_B - z_A),\ t \in \mathbb{R}\,\}.$$

On appelle l'équation $z_M = z_A + t(z_B - z_A), t \in \mathbb{R}$ l'***équation paramétrique*** de la droite (AB).



(iv) le cercle $\mathcal{C}$ de centre A et de rayon R a pour équation :

$$M \in \mathcal{C} \iff |z_M - z_A| = R.$$



5.2.2 Translations et homothéties dans le plan complexe

Dans le CHAPITRE 2, il y a une notion fondamentale de géométrie que nous avons légèrement abordée au moyen des homothéties et translations : les ***transformations affines*** du plan. Ces transformations comprennent en particulier les translations, les rotations et les homothéties. Nous allons voir ici comment définir les rotations, et nous allons aussi donner les expressions complexes pour les homothéties et translations.

⚠ REMARQUE On rappelle qu'une ***transformation affine*** f s'applique aussi sur les vecteurs de la manière suivante : $f(\overrightarrow{AB}) = \overrightarrow{f(A)f(B)}$. Donc

$$z_{f(\overrightarrow{AB})} = z_{f(B)} - z_{f(A)}.$$

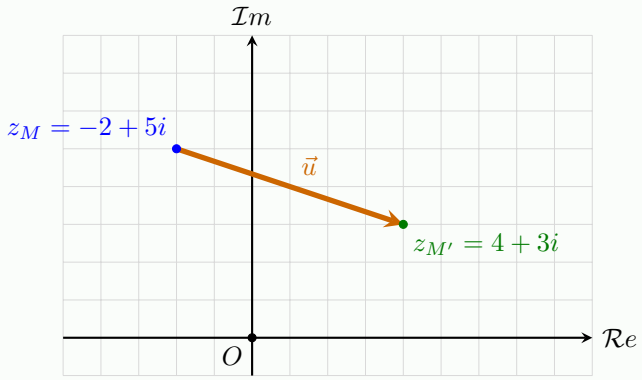
Translation dans $\mathbb{C}$. Nous savons que la translation t de vecteur $\vec{u}$ est la fonction qui envoie un point M sur un point $M' = t(M)$ tel que $\overrightarrow{MM'} = \vec{u}$. Donc, de manière équivalente, si $\vec{u}$ a pour affixe b, la transformation t envoie M d'affixe z_M sur le point $M' = t(M)$ d'affixe

$$z_{M'} = z_M + b.$$

On notera, pour simplifier les notations, $t(z_M) = z_{M'}$ lorsque nous travaillerons dans $\mathbb{C}$.

EXEMPLE

Soit t la translation de vecteur $\vec{u}$ de coordonnées $(6, -2)$. Soit M le point du plan de coordonnée $(-2, 5)$. Comment calculer les coordonnées de $M' = t(M)$? Par définition, l'affixe de M est $z_M = -2 + 5i$ et l'affixe de $\vec{u}$ est $z_{\vec{u}} = 6 - 2i$. Donc l'affixe de M' est $z_{M'} = -2 + 5i + 6 - 2i = 4 + 3i$. Les coordonnées de $M' = t(M)$ sont $(4, 3)$.



Homothétie dans $\mathbb{C}$. Nous savons que l'*homothétie h de centre A et de rapport $k \in \mathbb{R}^*$* est la fonction qui envoie un point M sur un point $M' = h(M)$ tel que $\overrightarrow{AM'} = k\,\overrightarrow{AM}$. Donc, de manière équivalente, la transformation h envoie le point M d'affixe z_M sur le point $M' = h(M)$ d'affixe

$$z_{M'} = k\,(z_M - z_A) + z_A.$$

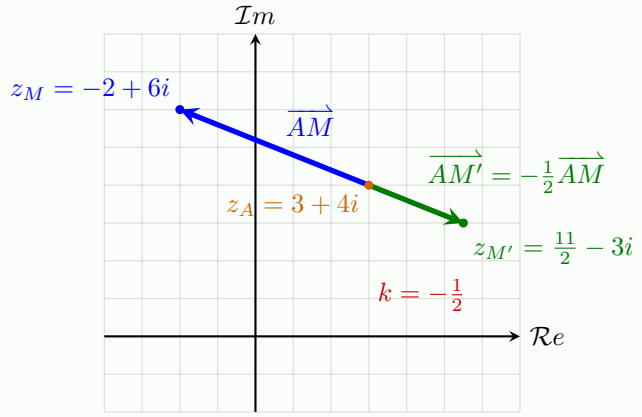
On notera $z_{M'} = h(z_M)$.

⚠ **Remarque** On vérifie très aisément avec l'expression complexe de l'homothétie que $AM' = \|\overrightarrow{AM'}\| = |k|\,\|\overrightarrow{AM}\| = |k|\,AM$ et que A, M et M' sont alignés.

Exemple

Soit h l'homothétie de centre A d'affixe $z_A = 3 + 4i$ et de rapport $k = -\frac{1}{2}$. Soit M le point du plan d'affixe $z_M - 2 + 6i$. Comment calculer l'affixe $z_{M'}$ de $M' = h(M)$? Par définition, on a

$$z_{M'} = -\frac{1}{2}\big((-2 + 6i) - (3 + 4i)\big) + 3 + 4i = \frac{11}{2} + 3i.$$

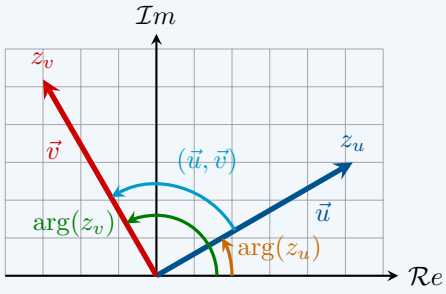


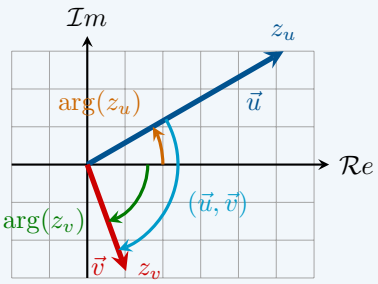
5.2.3 Angles orientés et rotation

Définition 5.1

Soient $\vec{u}, \vec{v}$ deux vecteurs non nuls du plan d'affixes respectives z_u et z_v. On définit l'***angle orienté*** entre $\vec{u}$ et $\vec{v}$ (dans cet ordre) par

$$(\vec{u}, \vec{v}) \;=\; \arg(z_v) - \arg(z_u) \qquad (\text{mod } 2\pi).$$





Remarque

(i) Au sujet des « modulo » : $\theta \equiv \eta \ (\text{mod } 2\pi)$ veut dire qu'il existe $k \in \mathbb{Z}$ tel que $\theta = \eta + 2k\pi$. Il faut donc faire attention à cela, surtout lorsque l'on divise par 2. Dans ce cas, le modulo 2π devient un modulo π.

(ii) La ***mesure principale*** d'un angle orienté est la valeur comprise dans l'intervalle $]-\pi, \pi]$.

Proposition 5.2

Soient $\vec{u}, \vec{v}$ deux vecteurs non nuls du plan d'affixes respectives z_u et z_v. On a alors l'égalité suivante :

$$(\vec{u}, \vec{v}) \quad = \quad \arg\left(\frac{z_v}{z_u}\right)$$

Démonstration Sous la forme exponentielle, on a que :

$$z_u \;=\; |z_u| e^{i \arg(z_u)} \qquad \text{et} \qquad z_v \;=\; |z_v| e^{i \arg(z_v)}.$$

Ainsi, on a

$$\frac{z_v}{z_u} \quad = \quad \frac{|z_u|}{|z_v|} \cdot e^{i\left(\arg(z_v) - \arg(z_u)\right)},$$

d'où

$$\arg\left(\frac{z_v}{z_u}\right) \quad = \quad \arg(z_v) \;-\; \arg(z_u) \quad = \quad (\vec{u}, \vec{v}).$$

■

Proposition 5.3: (Propriétés des angles orientés)

Soient $\vec{u}$, $\vec{v}$ et $\vec{w}$ trois vecteurs non nuls du plan. Alors

- ***(i)*** $(\vec{u},\vec{v})+(\vec{v},\vec{w})=(\vec{u},\vec{w})$ (***Relation de Chasles***) ;
- ***(ii)*** $(\vec{u},\vec{v})=-(\vec{v},\vec{u})$;
- ***(iii)*** pour tout réels strictement positifs α,β on a : $(\alpha\vec{u},\beta\vec{v})=(\vec{u},\vec{v})$;
- ***(iv)*** $(\vec{u},-\vec{v})=(\vec{u},\vec{v})+\pi \pmod{2\pi}$; en particulier $(-\vec{u},-\vec{v})=(\vec{u},\vec{v})$;
- ***(v)*** $\vec{u}$ et $\vec{v}$ sont colinéaires si et seulement si $(\vec{u},\vec{v})=k\pi$, $k\in\mathbb{Z}$;
- ***(vi)*** $\vec{u}\perp\vec{v}$ si et seulement si $(\vec{u},\vec{v})=\frac{\pi}{2}+k\pi$, $k\in\mathbb{Z}$.

Démonstration Les preuves de ***(i)***, ***(ii)*** et ***(iii)*** sont une conséquence immédiate de la définition. On en laisse la vérification au soin du lecteur.

Pour ***(iv)***, il suffit d'observer que si $re^{i\theta}$ est l'affixe de $\vec{m}$, alors l'affixe z' de $-\vec{m}$ est $z'=-re^{i\theta}=e^{i\pi}re^{i\theta}=re^{i(\pi+\theta)}$. D'où $\arg(z')=\theta+\pi$.

Pour ***(v)*** et ***(vi)***, on procède comme suit : soit z l'affixe de $\vec{u}$ et z' l'affixe de $\vec{v}$. On a $\vec{u}$ colinéaire à $\vec{v}$ si et seulement si $\vec{u}=k\,\vec{v}$. Autrement dit, si et seulement si $z=kz'$, avec $k\in\mathbb{Z}^*$. Si $k>0$ on peut conclure par un simple calcul d'angle ; si $k<0$, on utilise alors ***(iv)*** pour conclure.

Finalement, $\vec{u}\perp\vec{v}$ si et seulement si une droite dirigée par $\vec{u}$ est perpendiculaire à une droite dirigée par $\vec{v}$. Cela veut dire que l'angle entre ces deux droites, et donc entre ces deux vecteurs, est une angle droit qui s'écrit $\frac{\pi}{2}+k\pi$ avec $k\in\mathbb{Z}$.

■

Remarque L'angle géométrique $\widehat{ABC}$ est obtenu en prenant la valeur absolue de la mesure principale, c-à-d comprise dans l'intervalle $]-\pi,\pi]$, de l'angle orienté $(\overrightarrow{BA},\overrightarrow{BC})$.

Exemple

La somme des angles d'un triangle est plat. En effet en vertu de la proposition précédente, on a $(\overrightarrow{BC},\overrightarrow{BA})=(\overrightarrow{BC},\overrightarrow{AB})+\pi$ et $(\overrightarrow{CA},\overrightarrow{CB})=(\overrightarrow{AC},\overrightarrow{BC})$. D'où :

$$(\overrightarrow{AB},\overrightarrow{AC})+(\overrightarrow{BC},\overrightarrow{BA})+(\overrightarrow{CA},\overrightarrow{CB})=(\overrightarrow{AB},\overrightarrow{AC})+(\overrightarrow{BC},\overrightarrow{AB})+\pi+(\overrightarrow{AC},\overrightarrow{BC})=\pi+(\overrightarrow{AB},\overrightarrow{AB})=\pi\,(\mathrm{mod}\,2\pi).$$

Définition 5.4: (Rotation)

La ***rotation*** est la transformation qui déplace selon un angle θ un point M autour d'un point A, son centre. Plus précisément, la rotation $r_{A,\theta}$ de centre A et d'angle θ est la fonction qui envoie un point M sur un point $M' = r_{A,\theta}(M)$ tel que $\left(\overrightarrow{AM}, \overrightarrow{AM'}\right) = \theta$ et $AM = AM'$; ou de manière équivalente, la transformation $r_{A,\theta}$ envoie le point M d'affixe z_M sur le point $M' = r_{A,\theta}(M)$ d'affixe

$$z_{M'} = e^{i\theta}(z_M - z_A) + z_A.$$

⚠ Remarque

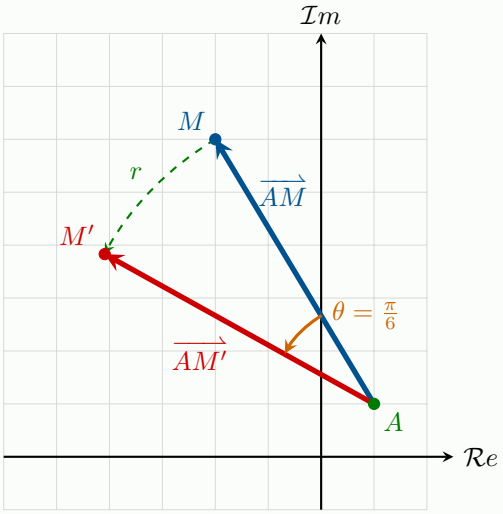
(i) On vérifie aisément que $AM' = \|\overrightarrow{AM'}\| = \|\overrightarrow{AM}\| = AM$ et que $(\overrightarrow{AM}, \overrightarrow{AM'}) = \theta$.

(ii) Soient deux points A et A' à égal distance d'un point B. Alors il existe une unique rotation r de centre B telle que $r(A) = A'$. Dans ce cas l'angle de cette rotation est $\theta = (\overrightarrow{BA}, \overrightarrow{BA'})$.

Exemple

Soit r la rotation de centre A d'affixe $z_A = 1+i$ et d'angle $\theta = \frac{\pi}{6}$. Soit M le point du plan d'affixe $z_M = -2+6i$. Comment calculer l'affixe $z_{M'}$ de $M' = r(M)$? On a :

$$\begin{aligned} z_{M'} &= e^{i\frac{\pi}{6}}\left((-2+6i) - (1+i)\right) + 1 + i \\ &= \left(\frac{\sqrt{3}}{2} + i\,\frac{1}{2}\right)(-3+5i) + 1 + i \\ &= -\frac{3\sqrt{3}+5}{2} + i\frac{5\sqrt{3}-3}{2} + 1 + i \\ &= -\frac{3\sqrt{3}+3}{2} + i\frac{5\sqrt{3}-1}{2}. \end{aligned}$$



Définition 5.5

Soit f une transformation affine.

(i) On dit que f est une ***isométrie*** si f préserve les distances, c-à-d, pour tout point A, B du plan

$$d(f(A), f(B)) \quad = \quad \|f(\overrightarrow{AB})\| \quad = \quad \|\overrightarrow{AB}\| = d(A, B).$$

(ii) On dit que f ***préserve les angles orientés*** si pour tout vecteur $\vec{u}, \vec{v}$ du plan on a

$$(f(\vec{u}), f(\vec{v})) \quad = \quad (\vec{u}, \vec{v}).$$

Théorème 5.6

(i) Les rotations et les translations préservent les distances (ce sont des isométries).

(ii) L'image d'une droite par une translation, une rotation ou une homothétie est une droite.

(iii) L'image de deux droites parallèles par une translation, une rotation ou une homothétie sont deux droites parallèles.

(iv) L'image de deux droites perpendiculaires par une translation, une rotation ou une homothétie sont deux droites perpendiculaires.

(v) Plus généralement, les translations, les rotations et les homothéties préservent les angles orientés.

Démonstration *(iii)* et *(iv)* sont des conséquence de *(v)*. En effet, si ces transformations préservent les angles géométriques, alors elles préservent le parallélisme et l'orthogonalité. Finalement *(i)*, *(ii)* et *(v)* sont laissés au lecteur en exercice. (Voir exercice 5.4)

■

Remarque Si aux translations et rotations nous ajoutons les ***réflexions***, c-à-d les transformations du plan qui fixent une droite et dont l'image d'un point hors de cette droite est le symétrique par rapport à cette droite, nous avons alors toutes les transformations du plan qui préservent les distances : ce sont les ***isométries***. La classification des isométries du plan et de l'espace est un problème qui dépasse le cadre de ce cours. Le lecteur curieux pourra se référer par exemple au livre de Michèle Audin [Audin 2006] pour y lire une démonstration.

L'***axiome des triangles isométriques*** peut alors être remplacé par le concept d'***isométrie linéaire*** : deux triangles sont isométriques si et seulement si il existe une isométrie linéaire qui envoie un de ces triangles sur l'autre.

Les homothéties de rapport $k \neq \pm 1$ ne sont pas des isométries, elles ne conservent pas les longueurs. Par contre, elles sont l'objet à ajouter aux isométries linéaires si l'on veut remplacer la propriété des « triangles semblables ». La composée d'une isométrie linéaire et des homothéties s'appelle une ***similitude*** et est l'objet de la section suivante.

5.2.4 Les similitudes (section facultative)

Définition 5.7

La ***similitude*** $s_{A,\theta,k}$ de centre A, d'angle θ et de rapport $k \in \mathbb{R}^*$ est la transformation du plan qui au point M d'affixe z_M associe le point $M' = s_{A,\theta,k}(M)$ d'affixe

$$z_{M'} = ke^{i\theta}(z_M - z_A) + z_A.$$

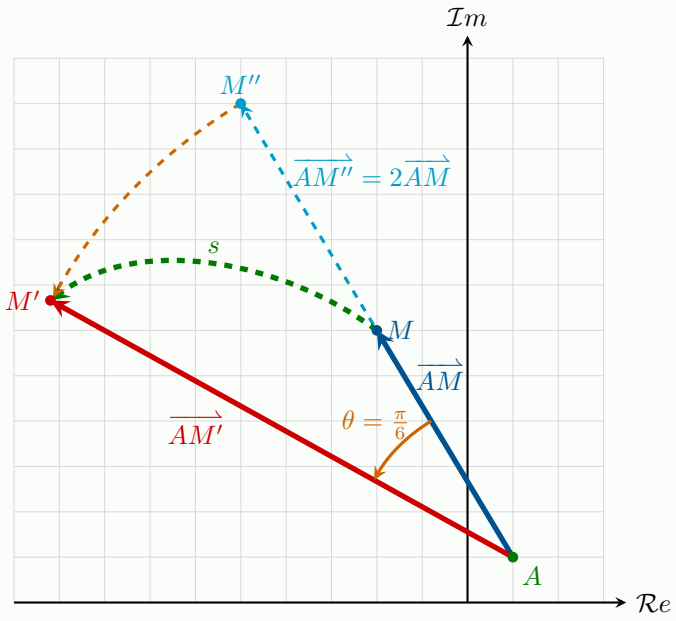
Remarque On vérifie aisément que $\|\overrightarrow{AM'}\| = |k| \, \|\overrightarrow{AM}\|$ et que $(\overrightarrow{AM}, \overrightarrow{AM'}) = \theta$.

Exemple

Soit s la similitude de centre A d'affixe $z_A = 1+i$, d'angle $\theta = \frac{\pi}{6}$ et de rapport $k = 2$. Soit M le point du plan d'affixe $z_M = -2+6i$. Comment calculer l'affixe $z_{M'}$ de $M' = s(M)$? Par définition, on a

$$\begin{aligned} z' &= 2e^{i\frac{\pi}{6}}\left((-2+6i)-(1+i)\right)+1+i \\ &= 2\left(\frac{\sqrt{3}}{2}+i\,\frac{1}{2}\right)(-3+5i)+1+i \\ &= -3\sqrt{3}-5+(5\sqrt{3}-3)i+1+i \\ &= -3\sqrt{3}-4+(5\sqrt{3}-2)i. \end{aligned}$$

Dans la figure suivante, le point M'' est la transformation de A selon la composante ***homotétie*** de s, avant d'effectuer la composante ***rotation*** :



Théorème 5.8

(i) Les rotations et les homothéties sont des similitudes.

(ii) L'image d'une droite par une similitude est une droite.

(iii) L'image de deux droites parallèles par une translation ou une similitude sont deux droites parallèles.

(iv) L'image de deux droites perpendiculaires par une translation ou une similitude sont deux droites perpendiculaires.

(v) Plus généralement, les translations et les similitudes de rapport positif préservent les angles orientés. Si le rapport de la similitude est négatif, elle transforme un angle orienté en son opposé.

Démonstration Voir l'exercice 5.5.

5.2.5 Exemple d'application

Soient A et B les points du plan d'affixes respectives $a = 1+i$ et $b = 2-3i$. On veut déterminer l'ensemble des points M d'affixe z du plan tels que ABM soit un triangle équilatéral.

On sait que ABM est équilatéral si et seulement si $AB = \|\overrightarrow{AB}\| = \|\overrightarrow{AM}\| = AM$ et $\widehat{BAM} = \frac{\pi}{3}$. En d'autres termes, ABM est équilatéral si et seulement si $|b-a| = |z-a|$ et si $\left(\overrightarrow{AB}, \overrightarrow{AM}\right) = \pm\frac{\pi}{3}$.

On va tout d'abord montrer le résultat suivant :

Lemme 5.9

Le triangle ABM est équilatéral si et seulement si M est l'image de B par une rotation de centre A et d'angle $\pm\frac{\pi}{3}$.

Démonstration Tout d'abord, si M est l'image de B par une rotation de centre A et d'angle $\pm\frac{\pi}{3}$, on montre que ABM est un triangle équilatéral. En effet, dans ce cas, $AM = AB$ et l'angle géométrique $\widehat{BAM} = \frac{\pi}{3}$ ce qui fait du triangle ABM un triangle isométrique à un triangle équilatéral : ABM est donc équilatéral.

Supposons maintenant que ABM est un triangle équilatéral. Il y a deux cas possible $\left(\overrightarrow{AB}, \overrightarrow{AM}\right) = \frac{\pi}{3}$ ou $\left(\overrightarrow{AB}, \overrightarrow{AM}\right) = -\frac{\pi}{3}$. Supposons d'abord que $\left(\overrightarrow{AB}, \overrightarrow{AM}\right) = \frac{\pi}{3}$. Comme $AB = AM$ on a que

$$\frac{z-a}{b-a} = \frac{|z-a|}{|b-a|} e^{i \arg\left(\frac{z-a}{b-a}\right)} = \frac{AM}{AB} e^{i\left(\overrightarrow{AB}, \overrightarrow{AM}\right)} = e^{i\frac{\pi}{3}}.$$

Donc $z - a = e^{i\frac{\pi}{3}}(b-a)$ ce qui peut se réécrire

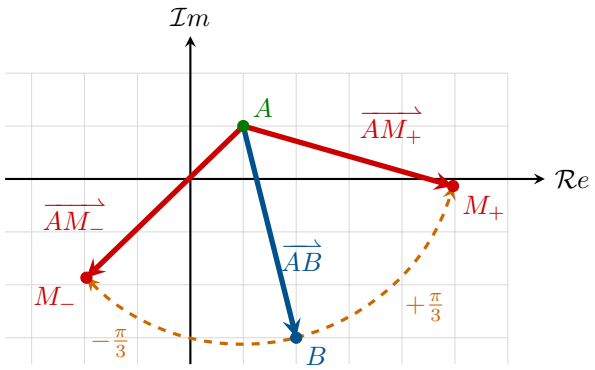
$$z = e^{i\frac{\pi}{3}}(b-a) + a.$$

Donc z est l'affixe de l'image de B par la rotation r de centre A et d'angle $\frac{\pi}{3}$. Le cas restant se résout de manière similaire à l'aide de la rotation r' de centre A et d'angle $-\frac{\pi}{3}$.

On peut donc conclure, après calcul, que

$$\begin{aligned}
\{\, M \in \mathcal{P} \mid ABM \text{ équilatéral} \,\} &= \{\, M \in \mathcal{P} \mid M = r_{A,\pi/3}(B) \text{ ou } M = r_{A,-\pi/3}(B) \,\} \\
&= \{\, M \in P \mid z_M = e^{\pm i\pi/3}(b-a) + a \,\} \\
&= \left\{ M \in \mathcal{P} \mid z_M = \tfrac{3}{2} + 2\sqrt{3} + i\left(\tfrac{\sqrt{3}}{2} - 1\right) \right. \\
&\qquad \left. \text{ou } z_M = \tfrac{3}{2} - 2\sqrt{3} - i\left(\tfrac{\sqrt{3}}{2} + 1\right) \right\}.
\end{aligned}$$

$\{ M \in \mathcal{P} \mid ABM \text{ est équilatéral} \} = \{M_-, M_+\}$:



5.3 Les polynômes

Le but de cette section est d'apprendre des techniques de factorisation des polynômes ainsi qu'à résoudre des équations polynomiales. Pour cela, on va « algébriser » le langage : au lieu de chercher les solutions d'une équation polynomiale du type $P(x) = 0$, on va étudier la divisibilité du polynôme P.

5.3.1 Polynômes à coefficients réels et complexes

On se place ici dans $\mathbb{C}$ (on rappelle que $\mathbb{R} \subseteq \mathbb{C}$).

Définition 5.10

(i) Un ***monôme*** M de degré $n \in \mathbb{N}$ est une fonction de la forme $M(X) = aX^n$, avec $a \in \mathbb{C}$. Ici X est une indéterminée ;

(ii) Si $a = 0$, on dit que le monôme est le ***polynôme nul***, noté 0, et qu'il est de degré $-\infty$;

(iii) Un ***polynôme à coefficients complexes*** P de degré $n \in \mathbb{N}$ est la fonction définie par une somme finie de monômes dont le plus grand degré est n :

$$P(X) = \sum_{i=0}^{n} a_i X^i = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0, \quad a_n \neq 0.$$

Si $a_i \in \mathbb{R}$ pour tout i, on dit que le polynôme est ***à coefficients réels*** ;

(iv) On note $\deg(P)$ le degré de P ;

(v) On note $\mathbb{C}[X]$ l'ensemble des polynômes à coefficients complexes ;

(vi) On note $\mathbb{R}[X]$ l'ensemble des polynômes à coefficients réels.

Remarque

(i) $P = Q$ si et seulement si leurs coefficients sont tous égaux (***identification des polynômes***) ;

(ii) Il est clair que $\mathbb{R}[X] \subseteq \mathbb{C}[X]$;

(iii) Les polynômes constants non nuls (appelés ***constantes***) sont les éléments de $\mathbb{C} \setminus \{0\}$; ils ont pour degré 0 ;

(iv) Par convention, on définit le degré du polynôme nul comme étant $-\infty$: $\deg(0) = -\infty$. Comme ceci, le seul polynôme de degré strictement négatif est le polynôme nul.

Addition des polynômes : Commençons par un calcul. Pour additionner des polynômes, on aimerait utiliser des règles de calculs similaires à celles existantes dans $\mathbb{R}$ (et $\mathbb{C}$) :

Exemple

Soient

$$P = 2X^2 - 4X + i \quad \text{et} \quad Q = X^3 + iX - 1.$$

Si X était un réel ou un complexe, on obtiendrait alors

$$P + Q \quad = \quad X^3 + 2X^2 + (i-4)X + i - 1.$$

Munissons $\mathbb{C}[X]$ d'une addition inspirée par cet exemple : Soient

$$P = \sum_{i=0}^{n} a_i X^i \quad \text{et} \quad Q = \sum_{j=0}^{m} b_j X^j,$$

deux polynômes à coefficients complexes. Supposons que $n \geq m$ et posons $b_{m+1} = b_{m+2} = \cdots = b_n = 0$. On a alors, pour tout entier $1 \leqslant i \leqslant n$, que $a_i + b_i \in \mathbb{C}$ (et si $a_i, b_i \in \mathbb{R}$, alors $a_i + b_i \in \mathbb{R}$). On définit alors

$$P + Q = \sum_{i=0}^{n} (a_i + b_i) X^i$$

qui est un polynôme de degré au plus $\max(\deg P, \deg Q)$. On note aussi

$$-P = \sum_{i=0}^{n} (-a_i) X^i$$

.

Proposition 5.11

L'addition des polynômes vérifie les propriétés suivantes.

Soient $P, Q, R \in \mathbb{C}[X]$. Alors :

(i) $P + Q = Q + P$ (***commutativité***) ;

(ii) $P + (Q + R) = (P + Q) + R$ (***associativité***) ;

(iii) $P + 0 = P$ (***élément neutre***) ;

(iv) $P + (-P) = 0$ (***opposé***) ;

(v) $\deg(P + Q) \leqslant \max(\deg(P), \deg(Q))$;

(vi) si $P, Q \in \mathbb{R}[X]$, alors $P + Q \in \mathbb{R}[X]$.

Démonstration La démonstration est laissée en exercices (voir exercice 5.12).

Multiplication des polynômes : Commençons à nouveau par un calcul. Pour multiplier des polynômes, on aimerait utiliser des règles de calculs similaires à celles existantes dans $\mathbb{R}$ (et $\mathbb{C}$) :

Exemple

Soient

$$P = 2X^2 - 4X + i \quad \text{et} \quad Q = X^3 + iX - 1.$$

Alors si X était un réel ou un complexe, on obtiendrait :

$$\begin{aligned} P \cdot Q &= (2X^2 - 4X + i)(X^3 + iX - 1) \\ &= 2X^2(X^3 + iX - 1) - 4X(X^3 + iX - 1) + i(X^3 + iX - 1) \\ &= 2X^5 + 2iX^3 - 2X^2 - 4X^4 - 4iX^2 + 4X + iX^3 - X - i \\ &= 2X^5 - 4X^4 + 3iX^3 - (2 + 4i)X^2 + 3X - i. \end{aligned}$$

On munit alors $\mathbb{C}[X]$ d'une multiplication inspirée de cet exemple : Soient

$$P = \sum_{i=0}^{n} a_i X^i \quad \text{et} \quad Q = \sum_{j=0}^{m} b_j X^j$$

deux polynômes à coefficients complexes. Posons pour tout $k \in \mathbb{N}$

$$c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0 = \sum_{i+j=k} a_i b_j \in \mathbb{C}.$$

On définissons alors

$$P \cdot Q = \sum_{k=0}^{n+m} c_k X^k$$

qui est un polynôme de degré $n + m = \deg(P) + \deg(Q)$ (car $c_{n+m} = a_n b_m \neq 0$).

Proposition 5.12

La multiplication des polynômes vérifie les propriétés suivantes.

Soient $P, Q, R \in \mathbb{C}[X]$. Alors :

- ***(i)*** $PQ = QP$ (***commutativité***) ;
- ***(ii)*** $P(QR) = (PQ)R$ (***associativité***) ;
- ***(iii)*** $1 \cdot P = P$ (***élément neutre***) ;
- ***(iv)*** $0 \cdot P = 0$;
- ***(v)*** $\deg(PQ) = \deg(P) + \deg(Q)$;
- ***(vi)*** si $P, Q \in \mathbb{R}[X]$, alors $PQ \in \mathbb{R}[X]$;
- ***(vii)*** $P(Q + R) = PQ + PR$ (***distributivité***).

Démonstration La vérification est laissée en exercice au lecteur (voir exercice 5.13).

⚠ Remarque

(i) En général, un polynôme n'a pas d'inverse : on ne peut pas diviser un polynôme par un autre polynôme afin d'obtenir un nouveau polynôme. Par exemple, $\frac{X+1}{X+2}$ ne peut pas être écrit sous la forme d'un polynôme. Supposons par contradiction qu'il existe un polynôme P tel que $(X+2)P = (X+1)$. Alors

$$\begin{aligned} \deg\big((X+2)P\big) &= \deg(X+1) \\ \deg(X+2)+\deg(P) &= 1 \\ 1+\deg(P) &= 1 \\ \deg(P) &= 0. \end{aligned}$$

Ceci signifie que $P = a \in \mathbb{C}^*$ est une constante non nulle (on rappelle que le degré de 0 est $-\infty$). On obtient finalement par identification :

$$\begin{aligned} (X+2)a &= X+1 \\ aX+2a &= X+1 \quad \Rightarrow \quad 2a = 1 = a \end{aligned}$$

Ceci est absurde. On peut par contre toujours diviser un polynôme par une constante non nulle. L'objet $\frac{X+1}{X+2}$ est appelée une ***fraction rationnelle***. Les fractions rationnelles sont aux polynômes ce qu'est $\mathbb{Q}$ à $\mathbb{Z}$.

(ii) Multiplier un polynôme P par une constante $c \in \mathbb{C}$, c'est-à-dire un polynôme de degré 0, revient à multiplier tous ses coefficients par c.

5.3.2 Racine d'un polynôme

Définition 5.13

(i) Soient $P \in \mathbb{C}[X]$ et $x \in \mathbb{C}$. Alors $P(x) \in \mathbb{C}$ est appelée l'***évaluation de P en x*** et est obtenue en remplaçant X dans P par x.

(ii) Une ***racine complexe d'un polynôme P*** est un nombre $\alpha \in \mathbb{C}$ tel que $P(\alpha) = 0$. On dit ***racine réelle*** si $\alpha \in \mathbb{R}$.

Pour résoudre une équation polynomiale, il suffit de trouver les racines du polynôme associé. L'existence d'au moins une racine est assurée par le résultat suivant :

Théorème 5.14: (Théorème fondamental de l'algèbre)

Tout polynôme à coefficients complexes de degré $\geqslant 1$ admet au moins une racine $\alpha \in \mathbb{C}$.

Démonstration Ce résultat est admis sans démonstration dans le cadre de ce cours.

⚠ Remarque Ce résultat n'est pas valide dans $\mathbb{R}$. En effet, l'équation $P(x) = x^2+1 > 0$ n'a pas de solution réelle, mais admet bien les solutions $\alpha = \pm i$ dans $\mathbb{C}$.

5.3.3 Factorisation des polynômes de degré 2 sur $\mathbb{C}$

La méthode pour factoriser un polynôme de degré 2 à coefficients complexes est exactement la même que celle pour ceux à coefficients réels, à un détail près : alors que la racine carrée d'un discriminant strictement négatif n'existe pas dans $\mathbb{R}$, la racine carrée d'un discriminant complexe existe toujours dans $\mathbb{C}$.

Soit $P = aX^2 + bX + c \in \mathbb{C}[X]$ un polynôme à coefficients complexes avec $a \neq 0$. On calcule le ***discriminant du polynôme*** :

$$\Delta = b^2 - 4ac \in \mathbb{C}.$$

Dans $\mathbb{R}$, il faudrait maintenant regarder le signe de Δ pour savoir si oui ou non il y a des racines. Dans $\mathbb{C}$, il y en a toujours. Les racines complexes du polynôme P sont

$$z_1 = \frac{-b + \sqrt{\Delta}}{2a} \quad \text{et} \quad z_2 = \frac{-b - \sqrt{\Delta}}{2a}.$$

Le polynôme P admet alors la factorisation suivante :

$$P = a(X - z_1)(X - z_2).$$

On invite le lecteur à vérifier ces affirmations. Il faut aussi noter que bien que la racine carrée de tout nombre complexe existe, elle n'est pas toujours facile à calculer. Pour cela, il faudra passer à la forme exponentielle dudit nombre complexe.

Exemple

Prenons $P = X^2 + i$. Le discriminant est $\Delta = 0 - 4i = -4i = 4$. On obtient

$$\sqrt{\Delta} = \Delta^{\frac{1}{2}} = (-4i)^{\frac{1}{2}} = \left(4e^{-i\frac{\pi}{2}}\right)^{\frac{1}{2}} = 2e^{-i\frac{\pi}{4}} = \sqrt{2} - i\sqrt{2}.$$

D'où

$$P = \left(X - e^{-i\frac{\pi}{4}}\right)\left(X + e^{-i\frac{\pi}{4}}\right).$$

Pour les polynômes de degrés supérieurs à 2, la résolution par calcul de racine carrée n'est pas un problème facile. La ***résolution des équations polynomiales par radicaux***, nom donné à cette méthode, n'est pas généralisable au-delà du degré 4. Ce résultat est dû à Évariste Galois, mathématicien français du début du XIX^{e} siècle.

5.3.4 Division euclidienne des polynômes

On a vu que l'on ne peut pas diviser un polynôme par un autre. Pour contourner ce problème, nous nous dotons d'un nouvel outil : la ***division euclidienne des polynômes***.

Théorème 5.15: (Division euclidienne)

Soient $A, B \in \mathbb{C}[X]$ (resp. à coefficients réels) de degrés respectifs n et m. Si $0 \leqslant m \leqslant n$, alors il existe une unique décomposition

$$A = BQ + R$$

où $Q, R \in \mathbb{C}[X]$ (resp. à coefficients réels) tels que $\deg(R) < m = \deg(B)$.

Définition 5.16

Soient $A, B, Q, R \in \mathbb{C}[X]$ tels que $A = BQ + R$. On dit que Q est le ***quotient*** de la division euclidienne de A par B, et que R est le ***reste*** de la division euclidienne de A par B.

Remarque

(i) Si $m = 0$, alors $\deg(R) = -\infty$, ce qui implique que $R = 0$. De plus, on peut noter que $A = A \cdot 1 + 0$.

(ii) Le degré de Q est forcément $\deg(Q) = \deg(A) - \deg(B)$. ***Pourquoi ?***

(iii) Si $R = 0$, on dit que B ***divise*** A ***dans*** $\mathbb{C}[X]$;

Exemple

Soient $A = X^3 - 1$ et $B = X^2 + 1$. Alors

$$A \quad = \quad X(X^2+1) + (-X-1) \quad = \quad XB + (-X-1).$$

Comme $\deg(-X-1) = 1 < 2$, on a que $Q = X$ et $R = -X - 1$ sont respectivement le quotient et le reste de la division euclidienne de A par B.

Démonstration (Division euclidienne)

Nous démontrons séparément l'existence et l'unicité de la décomposition.

- **Existence.**

  Nous raisonnons par récurrence forte sur $n = \deg(A) \geqslant 0$.

  - **Étape initiale.**

    Si $n = 0$, alors

    $$0 = \deg(A) \geqslant \deg(B) \geqslant 0.$$

    Ainsi, A et B sont des polynômes constants non nuls. Il suffit de prendre $Q = A/B$ et $R = 0$.

- **Récursion.**

  Soit $n \geqslant 1$. Supposons le résultat établi pour tout polynôme de degré strictement inférieur à n, et écrivons

  $$A = a_n X^n + \cdots, \qquad B = b_m X^m + \cdots,$$

  où $a_n \neq 0$, $b_m \neq 0$ et $m \leqslant n$. Posons

  $$Q_1 = \frac{a_n}{b_m} X^{n-m} \qquad \text{et} \qquad R_1 = A - BQ_1.$$

  Les termes de degré n s'annulent, donc $R_1 = 0$ ou $\deg(R_1) < n$.

  Si $R_1 = 0$ ou $\deg(R_1) < m$, la décomposition $A = BQ_1 + R_1$ convient déjà. Sinon,

  $$m \leqslant \deg(R_1) < n.$$

  L'hypothèse de récurrence appliquée à R_1 donne alors des polynômes Q' et R' tels que

  $$R_1 = BQ' + R' \qquad \text{et} \qquad \deg(R') < m.$$

  Par conséquent,

  $$A \quad = \quad BQ_1 + R_1 \quad = \quad BQ_1 + BQ' + R' \quad = \quad B(Q_1 + Q') + R'.$$

  Il suffit donc de prendre $Q = Q_1 + Q'$ et $R = R'$.

Par récurrence forte, la décomposition existe pour tout $n \in \mathbb{N}$.

- **Unicité.**

  Supposons que A possède deux décompositions

  $$A = BQ_1 + R_1 = BQ_2 + R_2,$$

  où $\deg(R_1) < m$ et $\deg(R_2) < m$. On obtient

  $$B(Q_1 - Q_2) = R_2 - R_1.$$

  Si $Q_1 - Q_2$ était non nul, alors

  $$\deg\big(B(Q_1 - Q_2)\big) = m + \deg(Q_1 - Q_2) \geqslant m,$$

  tandis que

  $$\deg(R_2 - R_1) \leqslant \max\big(\deg(R_1), \deg(R_2)\big) < m,$$

  ce qui est impossible. Ainsi, $Q_1 = Q_2$, puis l'égalité précédente donne $R_1 = R_2$. La décomposition est donc unique.

■

Corollaire 5.17

Soient $P \in \mathbb{C}[X]$ et $\alpha \in \mathbb{C}$ une racine de P. Alors P se factorise par $(X-\alpha)$: il existe $S \in \mathbb{C}[X]$ tel que

$$P = (X-\alpha)S \quad \text{et} \quad \deg(S) = \deg(P) - 1.$$

Démonstration En vertu de la division euclidienne des polynômes, il existe $R, S \in \mathbb{C}[X]$ tels que $\deg(R) < 1$ et

$$P \;=\; (X-\alpha)S + R.$$

Comme $\deg(R) < 1$, on sait que R est une constante éventuellement nulle. On évalue maintenant P en α :

$$0 \;=\; P(\alpha) \;=\; (\alpha-\alpha)S(\alpha) + R(\alpha) \;=\; R(\alpha).$$

Donc $R(\alpha) = 0$. Et comme R est une constante, R s'écrit : $R = a \in \mathbb{C}$. On obtient alors $0 = R(\alpha) = a = R$.

■

Corollaire 5.18

Si $P = a_n X^n + \cdots + a_0 \in \mathbb{C}[X]$ avec $n \geq 1$, il existe $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ tels que

$$P(X) = a_n(X-\alpha_1)\cdots(X-\alpha_n).$$

On dit que l'on a ***factorisé*** P sur $\mathbb{C}$ En particulier, P admet au plus n racines ***distinctes*** dans $\mathbb{C}$.

Démonstration La preuve se fait par récurrence sur $n = \deg(P)$ en utilisant le corollaire 5.17 (voir exercice 5.19).

■

Exemple

Factorisons le polynôme $P = X^3 + 2X^2 + 2X + 1$ sur $\mathbb{C}$. On voit que $P(-1) = 0$, donc

$$P = (X+1)Q$$

où Q est de la forme $aX^2 + bX + c$. Par identification des coefficients après développement, on obtient

$$P \;=\; (X+1)(X^2 + X + 1).$$

Le discriminant de $X^2 + X + 1$ est $\Delta = 1^2 - 4 = -3$. Comme $\sqrt{\Delta} = i\sqrt{3}$, les racines de $X^2 + X + 1$ sont

$$z_1 \;=\; \frac{-1 + i\sqrt{3}}{2} \quad \text{et} \quad z_2 = \frac{-1 - i\sqrt{3}}{2} = \overline{z_1}.$$

Ainsi, P se factorise comme suit :

$$P \;=\; (X-1)(X-z_1)(X-\overline{z_1}) \;=\; (X+1)\left(X - \tfrac{-1+i\sqrt{3}}{2}\right)\left(X - \tfrac{-1-i\sqrt{3}}{2}\right).$$

Les solutions de l'équation polynomiale $P(X) = 0$ sont $1, z_1, \overline{z_1}$.

Dans l'exemple précédent, nous avons eu de la chance en trouvant rapidement une racine de P, permettant de trouver facilement un polynôme qui divise P. Il existe toutefois une méthode plus générale qui reprend exactement l'idée de la division d'entiers apprise à la petite école. Illustrons la démarche à l'aide d'un exemple :

Exemple

Divisons le polynôme $A = 2X^4 + X^2 + 3$ par le polynôme $B = X^2 - 2$:

$$\begin{array}{rrrrr|rrr}
2X^4 & + & X^2 & + & 3 & X^2 & - & 2 \\
\cline{6-8}
-\,2X^4 & + & 4X^2 & & & 2X^2 & + & 5 \\
\cline{1-3}
 & & 5X^2 & + & 3 & & & \\
 & - & 5X^2 & + & 10 & & & \\
\cline{2-5}
 & & & & 13 & & &
\end{array}$$

On commence par diviser le terme dominant de A par celui de B. Le quotient obtenu est $2X^2$, qui devient le premier terme du quotient. On multiplie alors B par $2X^2$ et on soustrait le résultat au polynôme initial, ce qui élimine le terme en X^4.

On recommence ensuite avec le polynôme obtenu, $5X^2 + 3$. La division de son terme dominant par celui de B donne cette fois 5, que l'on ajoute au quotient. En soustrayant $5B$ au polynôme intermédiaire, il ne reste que 13.

Comme 13 est un polynôme de degré strictement plus petit que celui de B, il constitue le reste de la division. On obtient donc :

$$2X^4 + X^2 + 3 \;=\; (X^2 - 2)\big(2X^2 + 5\big) \;+\; 13.$$

5.3.5 Factorisation d'un polynôme à coefficients réels

On a vu que les polynômes à coefficients réels ne pouvaient pas forcément se factoriser en produit de polynômes de degré 1 ***à coefficients réels***. Par exemple :

$$X^2 + 1 = (X - i)(X + i)$$

n'est pas un produit de polynômes à coefficients réels de degré 1.

Théorème 5.19

Soit $P(X) = a_n X^n + \cdots + a_0 \in \mathbb{R}[X]$ de degré $n \geq 1$.

(i) Si α est une racine complexe de P, alors $\overline{\alpha}$ est aussi une racine de P.

(ii) P a au plus n racines réelles et P peut se décomposer sur $\mathbb{R}$ comme suit :

$$P(X) = a_n(X - \alpha_1)\dots(X - \alpha_k)Q_1 \dots Q_\ell,$$

où $\alpha_1, \dots, \alpha_k \in \mathbb{R}$ et $Q_1, \dots, Q_\ell \in \mathbb{R}[X]$ sont des polynômes de degré 2 qui n'ont pas de racine réelle.

Démonstration

(i) Il suffit d'observer que $\overline{P(\alpha)} = P(\overline{\alpha})$. Comme $P(\alpha) = 0$, on conclut que $P(\overline{\alpha}) = 0$, et donc que $\overline{\alpha}$ est une racine de P.

(ii) Nous allons esquisser un plan de la preuve. Les détails sont laissés en exercice (voir exercice 5.20). Tout d'abord, en vertu du corollaire 5.18, on écrit :

$$P = a_n(X - \alpha_1)\cdots(X - \alpha_k)(X - z_1)\cdots(X - z_\ell),$$

où $\alpha_i \in \mathbb{R}$ et $z_i \in \mathbb{C} \setminus \mathbb{R}$.

Maintenant, on utilise le point ***(i)*** pour montrer que, quitte à renuméroter les racines,

$$(X - z_1)\cdots(X - z_\ell) = (X - z_1)(X - \overline{z_1})\cdots(X - z_j)(X - \overline{z_j}),$$

avec $j = \frac{\ell}{2}$.

Enfin, si $z \in \mathbb{C} \setminus \mathbb{R}$, on observe que :

$$(X - z)(X - \overline{z}) = X^2 - (z + \overline{z})X + z\overline{z} = X^2 - 2\,\mathrm{Re}(z)X + |z|^2 \in \mathbb{R}[X],$$

qui est un polynôme de degré 2 n'ayant pas de racine réelle. La conclusion est une conséquence immédiate de ces trois observations.

■

5.4 Exercices

Nombres complexes et géométrie

Exercice 5.1 Les questions ci-dessous sont indépendantes.

(a) Déterminer l'ensemble des points M du plan dont l'affixe z vérifie $\overline{z}z = 4$;

(b) On considère le point A d'affixe $z_A = (2 + 3i)$. Déterminer l'ensemble des points M d'affixe z tels que $|z - z_A| = 5$.

Réponse : (a) $\{M \mid |z| = 2\}$, c'est-à-dire les points M du plan qui appartiennent au cercle de centre $(0, 0)$ et de rayon $R = 2$. (b) $\{M \mid |z - z_A| = 5\}$, c'est-à-dire les points M du plan qui appartiennent au cercle de centre $(2, 3)$ et de rayon $R = 5$.

Exercice 5.2 (Examen 2012) Soit f la transformation du plan complexe qui à M d'affixe z associe $M' = f(M)$ d'affixe z' tel que :

$$z' = az + 3i, \quad a \in \mathbb{C}.$$

(a) Montrer que si $a = 2$, f est une homothétie et déterminer le centre et le rapport de f ;

(b) Montrer que si $a = -i$, f est une rotation et déterminer le centre et l'angle de f.

Exercice 5.3 Donner l'écriture complexe des transformations suivantes :

(a) La translation de vecteur $\vec{u}$ de coordonnées $(1, 2)$;

(b) L'homothétie de centre A de coordonnées $(-1, 1)$ et de rapport -3 ;

(c) La rotation de centre B d'affixe $2 - 4i$ et d'angle $\dfrac{\pi}{3}$.

Exercice 5.4 (Démonstration du théorème 5.6) Démontrer les propriétés suivantes :

(a) Les rotations et les translations préservent les distances (ce sont des isométries).

(b) L'image d'une droite par une translation, une rotation ou une homothétie est une droite.

(e) Plus généralement, les translations, les rotations et les homothéties de rapport positif préservent les angles orientés. Si le rapport d'une homothétie est négatif, elle transforme un angle orienté en son opposé.

Exercice 5.5 (Démonstration du théorème 5.8) Démontrer les propriétés suivantes :

(a) Les rotations et les homothéties sont des similitudes.

(b) L'image d'une droite par une similitude est une droite.

(c) L'image de deux droites parallèles par une translation ou une similitude sont deux droites parallèles.

(d) L'image de deux droites perpendiculaires par une translation ou une similitude sont deux droites perpendiculaires.

(e) Plus généralement, les translations et les similitudes de rapport positif préservent les angles orientés. Si le rapport de la similitude est négatif, elle transforme un angle orienté en son opposé.

Exercice 5.6 Montrer que l'image d'un cercle par une rotation est un cercle dont on déterminera à chaque fois le rayon et le centre.

Exercice 5.7

(a) Soient $z_1 = 4 + 4i$ et $z_2 = 4 - 4i$. Écrire z_1 et z_2 sous forme algébrique et exponentielle ;

(b) Soit le nombre complexe $4e^{i\frac{\pi}{3}}$. Donner sa forme algébrique ;

(c) Soient K, L, M les points du plan d'affixes respectives :

$$z_K = 4 + 4i \; ; \quad z_L = 4 - 4i \; ; \quad z_M = 2 + 2i\sqrt{3}.$$

Montrer que le triangle KLM est rectangle.

Exercice 5.8 On considère la translation t de vecteur $\vec{w}$ et d'affixe $c = 2 + i$, l'homothétie h de centre A d'affixe $a = 2 + 4i$ et de rapport $-\dfrac{3}{2}$ ainsi que la rotation r de centre B d'affixe $b = 1 - i$ et d'angle $\dfrac{\pi}{3}$.

Soit M le point d'affixe z.

(a) Soit M_1 le point d'affixe z_1, l'image de M par t. Donner l'expression de z_1 en fonction de z. En déduire l'affixe du vecteur $\overrightarrow{MM_1}$;

(b) Soit M_2 le point d'affixe z_2, l'image de M par h. Donner l'expression de z_2 en fonction de z. En déduire une expression du vecteur $\overrightarrow{AM_2}$ en fonction du vecteur $\overrightarrow{AM}$;

(c) Soit M_3 le point d'affixe z_3, l'image de M par r. Déterminer le module et l'argument de $\dfrac{z_3 - b}{z - b}$. En déduire $\dfrac{BM_3}{BM}$ et $\left(\overrightarrow{BM}, \overrightarrow{BM_3}\right)$.

(d) Déterminer l'image du point O d'affixe 0 par h, t et r.

Exercice 5.9 (Examen 2011) Soit ABC un triangle quelconque (en sens direct). On notera a (resp. b, c) l'affixe de A (resp. B, C). On construit les points A' (resp. B' et C') extérieurement à ABC tels que le triangle BCA' (resp. CAB' et ABC') soit rectangle isocèle en A' (resp. B' et C'). On notera a', b' et c' les affixes de A', B' et C'.

(a) En choisissant judicieusement une rotation dont on donnera le centre et l'angle, montrer que :

$$a' = \frac{b - ic}{1 - i}.$$

En déduire que $a' - a = i(c' - b')$;

(b) En déduire que $(AA') \perp (B'C')$ et $AA' = B'C'$, puis que (AA'), (BB') et (CC') sont concourantes.

Exercice 5.10

Partie A. Soit O le centre d'un cercle passant par deux points A et B. M est un point du cercle, distinct de A et B. Soit M' le point diamétralement opposé à M.

(a) Quelle est la nature du triangle AOM ? En déduire que :

$$2\left(\overrightarrow{MA}, \overrightarrow{MO}\right) = \left(\overrightarrow{OA}, \overrightarrow{OM'}\right) \pmod{2\pi};$$

(b) Évaluer de la même manière $2\left(\overrightarrow{MB}, \overrightarrow{MO}\right)$;

(c) En déduire que $2\left(\overrightarrow{MA}, \overrightarrow{MB}\right) = \left(\overrightarrow{OA}, \overrightarrow{OB}\right) \pmod{2\pi}$;

(d) A-t-on $\left(\overrightarrow{MA}, \overrightarrow{MB}\right) = \frac{1}{2}\left(\overrightarrow{OA}, \overrightarrow{OB}\right) \pmod{2\pi}$? Justifier la réponse.

Partie B. On dit que quatre points A, B, C et D sont cocycliques s'il existe un cercle $\mathcal{C}$ tel que $A, B, C, D \in \mathcal{C}$.

(a) Montrer que A, B, C, D sont cocycliques si et seulement si D est un point du cercle circonscrit au triangle ABC.

(b) Montrer que A, B, C, D sont cocycliques si et seulement si

$$\left(\overrightarrow{AB}, \overrightarrow{AC}\right) = \left(\overrightarrow{DB}, \overrightarrow{DC}\right) \pmod{\pi}.$$

Exercice 5.11 Dans le plan orienté identifié à $\mathbb{C}$, on considère un carré direct $ABCD$ de centre O. Soit I le milieu de $[CD]$ et on construit le carré direct $DIJK$.

(a) Faire une figure en choisissant $AB = 6$.

(b) On considère la similitude S de centre D qui transforme A en B.

(i) Déterminer les éléments caractéristiques de S, c'est-à-dire l'angle et le rapport.

(ii) Déterminer l'image du point I par la similitude S.

(c) *(i)* Soit $\mathcal{C}$ le cercle circonscrit au carré $ABCD$ et E le point d'intersection des droites (AI) et (BJ). Montrer que E appartient à $\mathcal{C}$. (Indication : on pourra utiliser l'exercice précédent.)

(ii) Montrer que les droites (ED) et (BJ) sont orthogonales.

Polynômes

Exercice 5.12 (Démonstration de la proposition 5.11) Soient $P, Q, R \in \mathbb{C}[X]$. Montrer que :

(a) $P + Q = Q + P$ (commutativité) ;

(b) $P + (Q + R) = (P + Q) + R$ (associativité) ;

(c) $P + 0 = P$ (élément neutre) ;

(d) $P + (-P) = 0$ (opposé) ;

(e) $\deg(P + Q) \leqslant \max\big(\deg(P), \deg(Q)\big)$;

(f) si $P, Q \in \mathbb{R}[X]$, alors $P + Q \in \mathbb{R}[X]$.

Exercice 5.13 (Démonstration de la proposition 5.12) Soient $P, Q, R \in \mathbb{C}[X]$, montrer que :

(a) $PQ = QP$ (commutativité) ;

(b) $P(QR) = (PQ)R$ (associativité) ;

(c) $1 \cdot P = P$ (élément neutre) ;

(d) $0 \cdot P = 0$;

(e) $\deg(PQ) = \deg(P) + \deg(Q)$;

(f) si $P, Q \in \mathbb{R}[X]$, alors $PQ \in \mathbb{R}[X]$;

(g) $P(Q + R) = PQ + PR$ (distributivité).

Exercice 5.14 (Examen 2010) Dans l'ensemble $\mathbb{C}$ des nombres complexes, i désigne le nombre de module 1 et d'argument $\frac{\pi}{2}$.

(a) Montrer que $(1+i)^6 = -8i$;

(b) En déduire une racine du polynôme $P = X^3 + 8i$;

(c) On considère le point A d'affixe $2i$ et la rotation r de centre O (d'affixe 0) et d'angle $\frac{2\pi}{3}$.

- ***(i)*** Déterminer l'affixe b du point B, image de A par r, ainsi que l'affixe c du point C, image de B par r ;
- ***(ii)*** Montrer que b et c sont aussi des racines de P ;
- ***(iii)*** En déduire une factorisation de P sur $\mathbb{C}$;

(d) Dans le plan rapporté à un repère orthonormé, représenter les points A, B et C ;

(e) Quelle est la nature du triangle formé par les racines du polynôme P ? (Justifier)

EXERCICE 5.15 (Pentagone régulier) Dans le plan complexe, on considère le pentagone régulier standard, dont les sommets sont les racines cinquièmes de l'unité :

$$1,\ \xi = e^{i\frac{2\pi}{5}},\ \xi^2,\ \xi^3 = \xi^{-2},\ \xi^4 = \xi^{-1} = \overline{\xi}.$$

(a) Montrer que $1 + \xi + \xi^2 + \xi^3 + \xi^4 = 0$;

(b) Montrer que les sommets autres que 1 du pentagone sont toutes les racines du polynôme

$$P(X) = X^4 + X^3 + X^2 + X + 1,$$

c'est-à-dire que

$$P(X) = (X-\xi)(X-\xi^2)(X-\xi^3)(X-\xi^4);$$

(c) Soient $\alpha = \xi + \xi^{-1}$ et $\beta = \xi^2 + \xi^{-2}$.

- ***(i)*** Montrer que α et β sont les racines du polynôme $X^2 + X - 1$;
- ***(ii)*** Calculer $\alpha + \beta$ et $\alpha\beta$;
- ***(iii)*** En déduire les valeurs de $\cos\frac{2\pi}{5}$ et de $\cos\frac{4\pi}{5}$;

(d) On trace le cercle $\mathcal{C}$ de centre d'affixe $-\frac{1}{4}$ passant par le point d'affixe $\frac{i}{2}$.

- ***(i)*** Écrire l'équation de $\mathcal{C}$ en termes d'affixes ;
- ***(ii)*** Montrer que $\mathcal{C}$ coupe l'axe des réels aux points d'affixe $\frac{\alpha}{2}$ et $\frac{\beta}{2}$;
- ***(iii)*** En déduire une construction du pentagone régulier à la règle et au compas.

EXERCICE 5.16

(a) Effectuer la division euclidienne du polynôme P par le polynôme Q dans les cas suivants :

- ***(i)*** $P = 2X^3 + 5X^2 - X - 6$ et $Q = X - 1$;
- ***(ii)*** $P = 2X^4 + X^2 + 3$ et $Q = X^2 - 2$;
- ***(iii)*** $P = X^4 - X^3 + 2X^2 - X + 1$ et $Q = X^2 + 1$.

(b) Dans le cas où le reste de cette division est nul, donner les factorisations et les racines de ces polynômes sur $\mathbb{C}$ et $\mathbb{R}$.

Réponse : 1(a) $P(X) = (2X^2+7X+6)Q(X)$; 1(b) $P(X) = (2X^2+5)Q(X)+13$; 1(c) $P(X) = (X^2 - X + 1)Q(X)$.

Exercice 5.17 Montrer que si $P \in \mathbb{R}[X]$ est de degré impair $n > 0$, alors P admet au moins une racine réelle.

Exercice 5.18 Décomposer les polynômes suivants dans $\mathbb{R}$ et dans $\mathbb{C}$:

$$P(X) = X^2 + iX - 2, \quad Q(X) = X^2 + \sqrt{3}X + \tfrac{1}{2}, \quad R(X) = X^4 + 4X^2 + 3.$$

Exercice 5.19 (Démonstration du corollaire 5.18) Soit $P = a_n X^n + \cdots + a_0 \in \mathbb{C}[X]$ de degré $n \geq 1$. Montrer qu'il existe $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ tels que

$$P(X) = a_n(X - \alpha_1) \ldots (X - \alpha_n).$$

Exercice 5.20 (Démonstration du théorème 5.19) Démontrer la deuxième partie de ce théorème :
Soit $P(X) = a_n X^n + \cdots + a_0 \in \mathbb{R}[X]$ de degré $n \geq 1$.

(a) Si α est une racine complexe de P, alors $\overline{\alpha}$ est aussi une racine de P.

(b) P a au plus n racines réelles et P peut se décomposer sur $\mathbb{R}$ comme suit :

$$P(X) = a_n(X - \alpha_1) \cdots (X - \alpha_k) Q_1 \cdots Q_l$$

où $\alpha_1, \ldots, \alpha_k \in \mathbb{R}$ et $Q_1, \ldots, Q_l \in \mathbb{R}[X]$ sont des polynômes de degré 2 sans racine réelle.

Exercice 5.21 (Examen 2012) Soit $P \in \mathbb{C}[X]$ le polynôme défini par

$$P = X^3 - (6 + 2i)X^2 + (12 + 12i)X - 24i.$$

(a) Montrer que $2i$ est une racine de P ;

(b) Montrer qu'il existe $Q \in \mathbb{R}[X]$ de degré 2 tel que $P = (X - 2i)Q$;

(c) Résoudre, dans l'ensemble $\mathbb{C}$, l'équation suivante :

$$z^3 - (6 + 2i)z^2 + (12 + 12i)z - 24i = 0.$$

On en donnera les solutions sous forme algébrique.

Chapitre 6

Arithmétique

6.1 Arithmétique dans $\mathbb{Z}$

Les nombres entiers furent étudiés depuis la nuit des temps. Vers le IIIe siècle, le mathématicien grec Diophante d'Alexandrie proposa dans son traité d'arithmétique une méthode pour répondre à la question suivante :

On considère l'équation

$$6x + 9y = 12.$$

Admet-elle des solutions entières ? Si oui, lesquelles ?

Diophante d'Alexandrie

De manière générale on cherche à calculer les solutions entières $x, y \in \mathbb{Z}$ de ***l'équation linéaire du premier ordre*** :

$$ax + by = c, \quad a, b, c \in \mathbb{Z}$$

Nous allons expliquer dans ce qui suit comment résoudre ce problème, tout en posant les bases de ce qu'on appelle l'***arithmétique***, c'est-à-dire, la « science des nombres ». Pour ce faire, il va nous falloir développer une notion de ***division d'entiers*** dont le résultat est entier. Puis, en se servant de cette notion, nous allons étudier les conditions sous lesquelles cette équation admet au moins une solution et enfin nous allons apprendre à calculer ces solutions.

6.1.1 La division euclidienne

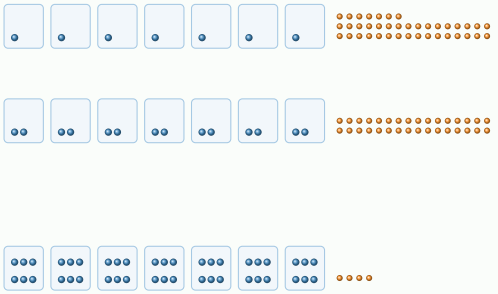
Comment savoir si une proportion est entière ou non ?

Exemple: (La division de 46 par 7)

Est-il possible de séparer 46 étudiants dans 7 classes différentes contenant le même nombre d'étudiants ? Nous savons que le résultat de la division de 46 par 7 n'est pas entier, mais comment exprimer ce fait en n'utilisant que

des nombres entiers ? On peut observer que 42 est divisible par 7 avec quotient 6, et qu'il reste alors $46 - 42 = 4$. On peut donc écrire

$$\begin{aligned} 46 &= 7 + 39 \\ &= 2 \cdot 7 + 32 \\ &\vdots \\ &= 6 \cdot 7 + 4 \end{aligned}$$



On dit que le ***quotient*** de la ***division euclidienne*** de 46 par 7 est 6, et que le ***reste*** est 4.

Ce procédé fonctionne de manière générale de la façon suivante :

Théorème 6.1: (Division euclidienne)

Soient $a, b \in \mathbb{N}$ avec $b \neq 0$. Alors il existe $q, r \in \mathbb{N}$ avec $0 \leqslant r < b$ tels que

$$a = bq + r.$$

Les nombres q et r sont déterminés de manière unique par ces conditions. Le nombre q est appelé le ***quotient*** de la division euclidienne de a par b, et r en est le ***reste***.

Démonstration C'est un énoncé du type « existence » (il faut montrer que q et r existent) et « unicité » (il faut montrer que q et r sont uniques). Les deux démonstrations se font séparément.

Existence : Nous démontrons l'existence de q et r par récurrence sur a (b étant fixé).

- **Étape initiale.**

  Si $a = 0$, nous pouvons prendre $q = r = 0$ et on a bien $0 \leqslant r < b$, puisque $b \geqslant 1$.

- **Récursion.**

  Hypothèse de récurrence : Supposons que $a = bq + r$ avec $0 \leqslant r < b$ pour un certain $a \geqslant 0$.

  Prouvons maintenant l'existence de q' et r' tels que $a + 1 = bq' + r'$ avec $0 \leqslant r' < b$.

  Par hypothèse de récurrence, nous avons :

  $$a + 1 = bq + r + 1$$

  Dans le cas où $r + 1 < b$, remarquons que si $q' = q$ et $r' = r + 1$, nous avons $a + 1 = bq' + r'$ avec $0 \leqslant r' < b$.

  Si l'on n'a pas $r + 1 < b$, on doit avoir $r + 1 \geqslant b$; mais comme $r < b$, la seule possibilité est $r + 1 = b$, d'où

  $$a + 1 = bq + r + 1 = bq + b = b(q + 1).$$

On a bien $a+1 = bq' + r'$ avec $r' = 0 < b$ et $q' = q+1$. Ceci achève la preuve de l'existence.

Unicité : Supposons que a admette deux écritures

$$a \quad = \quad bq_1 + r_1 \quad = \quad bq_2 + r_2,$$

avec $0 \leqslant r_1 < b$ et $0 \leqslant r_2 < b$. Montrons que ces deux écritures sont nécessairement identiques.

- **Les quotients sont égaux.**

  Puisque $0 \leqslant r_1 < b$ et $0 \leqslant r_2 < b$, la différence des deux restes vérifie

  $$-b < r_1 - r_2 \quad < \quad b,$$

  et donc

  $$|r_1 - r_2| \quad < \quad b.$$

  D'autre part, l'égalité des deux écritures de a donne

  $$bq_1 + r_1 \;=\; bq_2 + r_2 \quad \Longrightarrow \quad b(q_1 - q_2) \;=\; r_2 - r_1.$$

  En prenant les valeurs absolues, nous obtenons

  $$b\,|q_1 - q_2| \quad = \quad |r_2 - r_1| \quad < \quad b.$$

  Comme $b > 0$, nous pouvons diviser par b et conclure que

  $$|q_1 - q_2| \quad < \quad 1.$$

  Or $q_1 - q_2$ est un entier. Sa valeur absolue est donc un entier naturel strictement inférieur à 1 ; elle vaut nécessairement 0. Ainsi,

  $$q_1 \quad = \quad q_2.$$

- **Les restes sont égaux.**

  En remplaçant q_2 par q_1 dans l'égalité des deux écritures de a, nous obtenons

  $$bq_1 + r_1 = bq_1 + r_2 \quad \Longrightarrow \quad r_1 = r_2.$$

  Les deux écritures ont donc le même quotient et le même reste. Ceci prouve l'unicité.

■

⚠ **REMARQUE** La division euclidienne peut aussi se formuler ainsi :

Soient $a, b \in \mathbb{Z}$ avec $b \neq 0$. Alors il existe $q, r \in \mathbb{Z}$ avec $0 \leqslant r < |b|$ tels que

$$a \quad = \quad bq + r.$$

Les nombres q et r sont déterminés de manière unique par ces conditions.

La preuve de cet énoncé est très similaire à celui que nous venons juste de prouver : on procède par récurrence sur $|a|$. Il faut toutefois faire attention et procéder à la preuve par récurrence dans chacun des cas suivants : $a \leqslant 0$ (en se ramenant de a-1 à a) et $a > 0$.

6.1.2 Divisibilité dans $\mathbb{Z}$

Définition 6.2

Soient $d, n \in \mathbb{Z}$, où $d \neq 0$. On dit que d ***divise*** n (dans $\mathbb{Z}$), et on note $d|n$, s'il existe $q \in \mathbb{Z}$ tel que $n = dq$. Dans ce cas, on dit que d est un ***diviseur*** de n, et n un ***multiple*** de d. On notera $d \nmid n$ si d ***ne divise pas*** n.

Exemple

Est-ce que 3 divise 10 ? En fait, $3 \nmid 10$; pourquoi ? On va raisonner par contradiction.Supposons que $3|10$, alors il existe $q \in \mathbb{Z}$ tel que $10 = 3q$. Or $10 = 3 \cdot 3 + 1$ donc $3q = 3 \cdot 3 + 1$. Donc 1 est le reste de la division euclidienne de $3q$ par 3, ce qui est une contradiction car $3|3q$.

Il est important de noter que cette notion de divisibilité ne fait pas appel à l'existence des nombres rationnels : le fait que votre calculatrice affiche que $10/3 = 3,333\ldots$ n'explique pas pourquoi 3 ne divise pas 10 dans $\mathbb{Z}$.

⚠ Remarque

(i) Il faut bien comprendre que la divisibilité est un concept qui existe uniquement dans $\mathbb{Z}$. La fraction $\frac{a}{b} \in \mathbb{Q}$ est une écriture symbolique construite pour décrire les nombres rationnels et n'a rien à voir avec la notation $b|a$.

(ii) Avec le quantificateur $\exists$, qui signifie « il existe » en français, on peut réécrire la définition de divisibilité comme suit : $d, n \in \mathbb{Z} \setminus \{0\}$, $d|n \iff \exists\, q \in \mathbb{N},\ n = dq$.

(iii) On peut toujours se ramener aux entiers naturels. En effet, si $d, n \in \mathbb{Z}$ sont non nuls, alors d divise n si et seulement si $|d|$ divise $|n|$. Ici $|d|$ est la valeur absolue de d. On laisse en exercice au lecteur le fait de vérifier cette affirmation. (Voir exercice 6.4)

(iv) Le seul diviseur entier naturel de 1 est 1, i.e., si $k|1$ et $k \geqslant 1$ alors $k = 1$. En effet, si k est un diviseur entier naturel de 1 alors $1 = kp$ avec $p \in \mathbb{N}^*$; donc $k \leqslant 1$.

(v) Soient $d, n \in \mathbb{N}^*$, alors d divise n si et seulement si le reste de la division euclidienne de n par d est 0. En effet, il faut montrer une équivalence, c'est-à-dire qu'il faut montrer deux implications : supposons que $d|n$, alors il existe $q \in \mathbb{Z}$ tel que $n = dq = dq + 0$. Donc par unicité du quotient et du reste dans la division euclidienne, le reste est 0 ; la réciproque, c'est-à-dire l'implication inverse, se montre avec les mêmes arguments.

Exemple

1. $3|12$, car $12 = 3 \cdot 4$.
2. Est-ce que -7 divise 147 ? La réponse est oui, car la division euclidienne de 147 par 7 donne

$$147 = 7 \cdot 21 + 0.$$

Donc $147 = (-7) \cdot (-21)$, d'où $-7|147$.

Proposition 6.3

La divisibilité vérifie les propriétés suivantes : soient n, m, p des entiers non nuls,

- ***(i)*** 1 et -1 divisent n ;
- ***(ii)*** $n|n$ (***réflexivité***) ;
- ***(iii)*** $n|m \ \wedge \ m|p \Longrightarrow n|p$ (***transitivité***) ;
- ***(iv)*** $p|n \Longrightarrow p|nm$;
- ***(v)*** $p|n \ \wedge \ p|m \Longrightarrow p|n+m$ et $p|n-m$;
- ***(vi)*** plus généralement : $p|n \ \wedge \ p|m \Longrightarrow p|an+bm$ pour tous $a, b \in \mathbb{Z}$.

Démonstration

- ***(i)*** $1|n$, car $n = 1 \cdot n$. De même, $-1|n$, car $n = (-1) \cdot (-n)$.
- ***(ii)*** $n|n$, car $n = n \cdot 1$.
- ***(iii)*** On a

$$\begin{aligned} n|m \ \wedge \ m|p \quad &\Longrightarrow \quad \exists\, q, q' \in \mathbb{Z},\ m = nq \ \wedge \ p = mq' \\ &\Longrightarrow \quad p = (nq)q' = n(qq') \\ &\Longrightarrow \quad n|p, \text{ car } qq' \in \mathbb{Z}. \end{aligned}$$

Le reste de la preuve est laissé en exercice. (Voir exercice 6.5)

■

6.1.3 Multiples et idéaux

Au lieu de parler de division dans $\mathbb{Z}$, nous pourrions parler de l'étude des multiples de nombres entiers. En effet, soit $n \in \mathbb{Z}$ et notons ***l'ensemble des multiples de*** n par :

$$n\mathbb{Z} = \{kn \,|\, k \in \mathbb{Z}\}$$

(aussi parfois noté (n) dans d'autres ouvrages). Il est alors clair que « n divise m si et seulement si m est un multiple de n » :

$$m|m \quad \Longleftrightarrow \quad m \in n\mathbb{Z} \quad \Longleftrightarrow \quad m\mathbb{Z} \subseteq n\mathbb{Z}.$$

Exemple

1. $0\mathbb{Z} = \{0\}$;
2. $1\mathbb{Z} = \mathbb{Z}$;
3. $2\mathbb{Z} = \{2k \,|\, k \in \mathbb{Z}\} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$. C'est l'ensemble des ***nombres pairs***. L'ensemble des ***nombres impairs*** s'écrit $2\mathbb{Z} + 1$.

On remarque facilement que la somme de deux multiples de n est un multiple de n et que le produit d'un multiple de n avec un entier quelconque est à nouveau un multiple de n. Cependant, ces propriétés ne sont pas propres qu'aux

ensembles de multiples. En effet, l'ensemble $\{6a+4b \,|\, a,b \in \mathbb{Z}\}$ par exemple possède lui aussi ces propriétés ; il est intéressant de remarquer que si nous notons

$$6\mathbb{Z}+4\mathbb{Z} \quad := \quad \{6a+4b \,|\, a,b \in \mathbb{Z}\},$$

alors

$$6\mathbb{Z}+4\mathbb{Z} \quad = \quad 2\mathbb{Z}.$$

On peut donc en déduire que pour que l'équation $6x+4y=c$ admette au moins une solution, il est nécessaire (et suffisant ?) que c soit un multiple de 2, i.e. $c \in 2\mathbb{Z}$. L'étude des multiples va nous amener à donner une condition nécessaire et suffisante sur c pour que l'équation $ax+by=c$ ait une solution.

Faisons maintenant un premier pas en algèbre en regardant tous les sous-ensembles de $\mathbb{Z}$ qui ont les mêmes propriétés que les ensembles de multiples.

Définition 6.4: (Idéal)

Un sous-ensemble non vide $I \subseteq \mathbb{Z}$ est un ***idéal de*** $\mathbb{Z}$ si pour toute paire d'entiers $n, m \in \mathbb{Z}$ on a

- ***(i)*** $n, m \in I \Longrightarrow n+m \in I$;
- ***(ii)*** $m \in I \Longrightarrow nm \in I$.

On remarque que $0 \in I$, car si $n \in I$, alors par ***(ii)*** : $-n = -1 \cdot n \in I$; et donc par ***(i)*** : $0 = n + (-n) \in I$.

Exemple

1. $I = \{6a+4b \,|\, a,b \in \mathbb{Z}\}$ est un idéal (exercice 6.6) ;
2. $1 \in I \iff I = \mathbb{Z}$ (exercice 6.6) ;
3. L'ensemble des nombres impairs n'est pas un idéal, car la somme de deux nombres impairs est paire ; de plus, 0 n'est pas un nombre impair. On rappelle qu'un entier n est impair s'il peut s'écrire $n = 2k+1$, avec $k \in \mathbb{Z}$.

La notion d'idéal dans le contexte des anneaux est du ressort d'un cours d'algèbre, elle y sera fondamentale. Dans $\mathbb{Z}$, les multiples et les idéaux sont intimement liés comme le montre la proposition suivante :

Proposition 6.5

Soit I un idéal de $\mathbb{Z}$. Alors il existe $n \in \mathbb{Z}$ tel que $I = n\mathbb{Z}$. En fait, on peut toujours prendre $n \in \mathbb{N}$.

Démonstration

- **Cas trivial.**

  Si $I = \{0\}$, il suffit de prendre $n = 0$. Supposons désormais que $I \neq \{0\}$.

- **Choix du générateur.**

Considérons l'ensemble des éléments strictement positifs de I :

$$I^+ \quad := \quad \{x \in I \mid x > 0\} \subseteq \mathbb{N}.$$

Cet ensemble est non vide. En effet, I contient un élément non nul x ; si $x < 0$, alors $-x = (-1)x \in I$. Par la propriété de bon ordre de $\mathbb{N}$, l'ensemble I^+ possède donc un plus petit élément, que nous notons n.

Montrons que

$$I = n\mathbb{Z}$$

en établissant les deux inclusions.

- $n\mathbb{Z} \subseteq I$

Soit $x \in n\mathbb{Z}$. Il existe $k \in \mathbb{Z}$ tel que $x = kn$. Puisque $n \in I$ et que I est un idéal, on obtient

$$x \quad = \quad kn \in I.$$

Ainsi, $n\mathbb{Z} \subseteq I$.

- $I \subseteq n\mathbb{Z}$

Soit $x \in I$. Comme I est un idéal, on a aussi $|x| \in I$. Effectuons la division euclidienne de $|x|$ par n :

$$|x| \ = \ nq + r, \qquad 0 \leqslant r < n.$$

Puisque $|x| \in I$ et $nq \in I$, leur différence appartient à I :

$$r \quad = \quad |x| - nq \in I.$$

Si $r > 0$, alors $r \in I^+$, ce qui contredit la minimalité de n puisque $r < n$. Par conséquent, $r = 0$. Ainsi, n divise $|x|$, donc aussi x, et

$$x \in n\mathbb{Z}.$$

Nous avons donc $I \subseteq n\mathbb{Z}$.

Les deux inclusions donnent finalement $I = n\mathbb{Z}$.

■

Corollaire 6.6

La somme de deux idéaux est un idéal. Autrement dit, soient $n, m \in \mathbb{Z}$, alors l'ensemble $n\mathbb{Z} + m\mathbb{Z} = \{nx + my \mid x, y \in \mathbb{Z}\}$ est un idéal.

Démonstration D'après la proposition précédente, tout idéal de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$. Soient donc $n, m \in \mathbb{Z}$ et posons

$$S \quad := \quad n\mathbb{Z} + m\mathbb{Z} = \{nk + ml \mid k, l \in \mathbb{Z}\}.$$

- **S est non vide.**

En effet,

$$0 \quad = \quad n \cdot 0 + m \cdot 0 \in S.$$

- **S est stable par addition.**

  Soient $x = nk + ml$ et $y = nk' + ml'$ deux éléments de S. Alors

  $$x + y \quad = \quad n(k + k') + m(l + l') \in S,$$

  puisque $k + k'$ et $l + l'$ sont des entiers.

- **S est stable par multiplication par un entier.**

  Soient $p \in \mathbb{Z}$ et $x = nk + ml \in S$. On a

  $$px \quad = \quad p(nk + ml) \quad = \quad n(pk) + m(pl) \in S,$$

  puisque pk et pl sont des entiers.

Ainsi, $S = n\mathbb{Z} + m\mathbb{Z}$ est un idéal de $\mathbb{Z}$.

■

Idéaux et équations diophantiennes. Il existe un lien étroit entre l'équation $ax + by = c$ qui nous intéresse depuis le début de ce chapitre et les idéaux. Posons $I = a\mathbb{Z} + b\mathbb{Z} = \{ax + by \,|\, x, y \in \mathbb{Z}\}$, on a alors que I est un idéal. Donc en vertu de la proposition ci-dessus, il existe $n \in \mathbb{N}$ tel que $I = n\mathbb{Z}$. On en déduit alors que l'équation $ax + by = c$ admet au moins une solution si et seulement si $c \in n\mathbb{Z}$ c'est-à-dire si et seulement si n divise c. Il reste maintenant à déterminer le n en question : c'est l'objet de la partie suivante.

6.1.4 Plus grand commun diviseur (PGCD)

Un ***diviseur commun*** à n et m est un entier d qui divise à la fois n et m. Comme l'ensemble des diviseurs communs à m et n est borné par $|n|$ (ou $|m|$ au choix), il existe un unique plus grand élément dans cet ensemble. C'est-à-dire qu'il existe un plus grand commun diviseur à n et m.

Définition 6.7

Soient $n, m \in \mathbb{Z}$, non tous deux nuls. Le ***plus grand commun diviseur*** de n et m est le plus grand entier naturel qui divise n et m ; on le note $\mathsf{pgcd}(n, m)$. En particulier, $\mathsf{pgcd}(n, 0) = |n|$.

Exemple

1. $\mathsf{pgcd}(n, m) = \mathsf{pgcd}(m, n)$.
2. L'ensemble des diviseurs communs à 4 et 6 est

   $$\{\pm 1, \pm 2\} = \{-2, -1, 1, 2\},$$

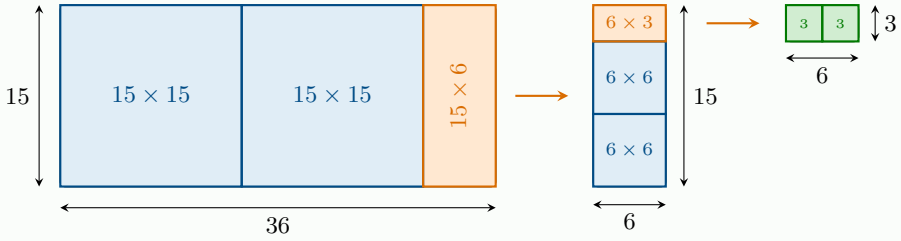
   et $\mathsf{pgcd}(4, 6) = 2$.
3. $\mathsf{pgcd}(n, m) = n \iff n \mid m$ (exercice 6.9).

6.1.4.1 Algorithme d'Euclide : calcul du pgcd

Commençons par un problème de carrelage.

Exemple: (Le carrelage d'un plancher)

On veut recouvrir, sans découpe ni chevauchement, un plancher de dimensions 36×15 avec des tuiles carrées identiques. Quelle est la plus grande longueur entière possible pour leur côté ?
Plaçons successivement les plus grands carrés possibles. Deux carrés de côté 15 laissent un rectangle 6×15 ; deux carrés de côté 6 y laissent un rectangle 6×3, que deux carrés de côté 3 recouvrent exactement.



Des tuiles de côté 3 recouvrent donc tout le plancher. On peut démontrer qu'aucune tuile carrée plus grande ne convient. La plus grande tuile carrée possible a donc un côté de longueur 3.

Remarque Dans l'exemple précédent, les dimensions des rectangles successifs sont $(36, 15)$, $(15, 6)$ et $(6, 3)$. Si l'on pouvait démontrer que le passage d'un rectangle au reste non couvert ne change pas le PGCD de ses dimensions, on obtiendrait

$$\mathsf{pgcd}(36, 15) \quad = \quad \mathsf{pgcd}(15, 6) \quad = \quad \mathsf{pgcd}(6, 3) \quad = \quad 3.$$

Nous aurions alors un algorithme pour calculer $\mathsf{pgcd}(36, 15)$. Le même procédé pourrait ensuite être appliqué à toute paire d'entiers.

Proposition 6.8: (Invariance du PGCD par division euclidienne)

Soient $a, b \in \mathbb{N}^*$ avec $a \geqslant b$, et écrivons la division euclidienne de a par b sous la forme

$$a = bq + r, \qquad 0 \leqslant r < b.$$

Alors

$$\mathsf{pgcd}(a, b) \quad = \quad \mathsf{pgcd}(b, r).$$

Démonstration Pour deux entiers x et y, non tous deux nuls, notons

$$\mathcal{D}(x, y) \quad := \quad \left\{ d \in \mathbb{Z} \;\middle|\; d|x \ \wedge \ d|y \right\}$$

l'ensemble de leurs diviseurs communs. Montrons que $\mathcal{D}(a, b) = \mathcal{D}(b, r)$ par double inclusion.

- $\mathcal{D}(a, b) \subseteq \mathcal{D}(b, r)$

Soit $d \in \mathcal{D}(a,b)$. Alors $d|a$ et $d|b$. Comme $r = a - bq$, on obtient

$$d|r.$$

Ainsi, d divise à la fois b et r, donc $d \in \mathcal{D}(b,r)$.

- $\mathcal{D}(b,r) \subseteq \mathcal{D}(a,b)$

  Soit $d \in \mathcal{D}(b,r)$. Alors $d|b$ et $d|r$. Comme $a = bq + r$, on obtient

  $$d|a.$$

  Ainsi, d divise à la fois a et b, donc $d \in \mathcal{D}(a,b)$.

Par conséquent,

$$\mathcal{D}(a,b) \quad = \quad \mathcal{D}(b,r).$$

Ces deux ensembles ont donc le même plus grand élément. Ainsi,

$$\mathsf{pgcd}(a,b) \quad = \quad \mathsf{pgcd}(b,r).$$

■

La proposition précédente permet de remplacer le couple (a,b) par le couple (b,r), où r est le reste de la division euclidienne de a par b, sans changer leur PGCD. Si $r \neq 0$, nous pouvons recommencer en divisant b par r, puis répéter le même procédé avec les nouveaux restes. C'est précisément l'idée de l'algorithme d'Euclide.

Théorème 6.9: (Algorithme d'Euclide)

Soient $a, b \in \mathbb{N}^*$ avec $a \geqslant b$. Posons $r_0 = a$ et $r_1 = b$, puis effectuons les divisions euclidiennes successives suivantes :

$$\begin{aligned}
r_0 &= q_1 \cdot r_1 + r_2, && 0 \leqslant r_2 < r_1,\\
r_1 &= q_2 \cdot r_2 + r_3, && 0 \leqslant r_3 < r_2,\\
&\vdots\\
r_{N-2} &= q_{N-1} \cdot r_{N-1} + r_N, && 0 < r_N < r_{N-1},\\
r_{N-1} &= q_N \cdot r_N + 0.
\end{aligned}$$

Ce procédé s'arrête toujours après un nombre fini d'étapes. Le dernier reste non nul est le PGCD de a et b :

$$\mathsf{pgcd}(a,b) \quad = \quad r_N.$$

Démonstration

- **Terminaison.**

  À chaque division euclidienne, si le nouveau reste est non nul, alors

  $$0 < r_{i+1} < r_i.$$

  Les restes non nuls forment donc une suite strictement décroissante d'entiers naturels. Une telle suite ne peut pas être infinie. Le procédé atteint ainsi nécessairement un premier reste nul, que nous notons $r_{N+1} = 0$.

- **Résultat obtenu.**

  À chaque étape, la proposition précédente donne

$$\mathsf{pgcd}(r_{i-1}, r_i) \quad = \quad \mathsf{pgcd}(r_i, r_{i+1}).$$

  En appliquant successivement cette égalité, nous obtenons

$$\mathsf{pgcd}(a,b) \quad = \quad \mathsf{pgcd}(r_0, r_1) \quad = \quad \cdots \quad = \quad \mathsf{pgcd}(r_N, 0) \quad = \quad r_N.$$

  Le dernier reste non nul est donc bien le PGCD de a et b.

■

Exemple

Posons $r_0 = a = 12378$ et $r_1 = b = 3054$. Appliquons successivement la division euclidienne :

$$\begin{aligned}
12378 &= 4 \cdot 3054 + 162 &&\Longrightarrow && r_2 = 162,\\
3054 &= 18 \cdot 162 + 138 &&\Longrightarrow && r_3 = 138,\\
162 &= 1 \cdot 138 + 24 &&\Longrightarrow && r_4 = 24,\\
138 &= 5 \cdot 24 + 18 &&\Longrightarrow && r_5 = 18,\\
24 &= 1 \cdot 18 + 6 &&\Longrightarrow && r_6 = 6,\\
18 &= 3 \cdot 6 + 0 &&\Longrightarrow && r_7 = 0.
\end{aligned}$$

Le dernier reste non nul est $r_6 = 6$. Donc

$$\mathsf{pgcd}(12378, 3054) \quad = \quad 6.$$

Algorithme d'Euclide et équation diophantienne. Rappelons que nous cherchons la façon de déterminer le n tel que $a\mathbb{Z} + b\mathbb{Z} = n\mathbb{Z}$. On va montrer que $n = \mathsf{pgcd}(a,b)$ et donc que l'équation $ax + by = c$ admet au moins une solution si et seulement si $\mathsf{pgcd}(a,b)$ divise c !

6.1.4.2 Le théorème de Bézout, première version

Nous allons maintenant énoncer un résultat surprenant : l'ensemble des multiples du pgcd de deux nombres est égal à l'ensemble des sommes des multiples de ces deux nombres.

Théorème 6.10

Soient n, m deux entiers non nuls, alors

$$\mathsf{pgcd}(n,m)\mathbb{Z} \quad = \quad n\mathbb{Z} + m\mathbb{Z} \quad = \quad \{nk + m\ell \mid k, \ell \in \mathbb{Z}\}.$$

Dans la démonstration du théorème ci-dessous, la notion d'idéal de $\mathbb{Z}$, qui semble *a priori* étrangère à celle de diviseur, joue un rôle de clarification.

Démonstration Posons $d = \mathsf{pgcd}(n,m)$ et $S = n\mathbb{Z} + m\mathbb{Z}$.

- $S \subseteq d\mathbb{Z}$

  Soit $x \in S$. Il existe $k, \ell \in \mathbb{Z}$ tels que $x = nk + m\ell$. Puisque d divise n et m, il divise aussi toute combinaison de ces deux nombres. Ainsi,

  $$d | (nk + m\ell) = x,$$

  et donc $x \in d\mathbb{Z}$.

- **Écriture de S sous la forme $p\mathbb{Z}$.**

  L'ensemble S est un idéal. La proposition 6.5 assure donc qu'il existe $p \in \mathbb{N}$ tel que

  $$S = p\mathbb{Z}.$$

  Comme $n \neq 0$ et $n = n \cdot 1 + m \cdot 0 \in S$, on a nécessairement $p \neq 0$.

- $p = d$

  Les entiers p et d sont tous deux strictement positifs. Comparons-les.

$$\left.\begin{array}{r} n = n\cdot 1 + m\cdot 0 \in p\mathbb{Z} \\ m = n\cdot 0 + m\cdot 1 \in p\mathbb{Z} \end{array}\right\} \implies p|n \wedge p|m \implies p \leqslant d$$

$$\left.\begin{array}{r} p \in p\mathbb{Z} = S \\ S \subseteq d\mathbb{Z} \end{array}\right\} \implies p \in d\mathbb{Z} \implies d|p \implies d \leqslant p$$

$$\left.\begin{array}{l} p \leqslant d \\ d \leqslant p \end{array}\right\} \implies p = d$$

Puisque $S = p\mathbb{Z}$ et $p = d$, nous obtenons finalement $S = d\mathbb{Z}$.

■

Avant de continuer notre étude, nous allons donner une dernière caractérisation très utile du pgcd.

Corollaire 6.11

Soient $n, m \in \mathbb{Z}$ deux entiers non nuls et d un diviseur commun positif de n et m. Les conditions suivantes sont équivalentes :

(i) $d = \mathsf{pgcd}(n,m)$;

(ii) tout diviseur commun de n et m divise d.

Démonstration Posons $g = \mathsf{pgcd}(n,m)$. Montrons séparément les deux implications.

- **(ii) $\implies$ (i)**

  Supposons que tout diviseur commun de n et m divise d. Puisque g est un diviseur commun, on a $g|d$. Les entiers g et d étant positifs, il s'ensuit que

  $$g \leqslant d.$$

D'autre part, d est un diviseur commun de n et m. Par définition de leur plus grand commun diviseur,

$$d \leqslant g.$$

Ainsi, $d = g = \mathsf{pgcd}(n, m)$.

- **(i) $\Longrightarrow$ (ii)**

  Supposons que $d = \mathsf{pgcd}(n, m)$. D'après le THÉORÈME 6.10, il existe $k, \ell \in \mathbb{Z}$ tels que

  $$d = nk + m\ell.$$

  Soit e un diviseur commun de n et m. Alors e divise toute combinaison de ces deux entiers ; en particulier,

  $$e | (nk + m\ell) = d.$$

  Tout diviseur commun de n et m divise donc d.

■

6.1.5 Entiers premiers entre eux, théorèmes de Bézout et lemme de Gauss

Comme nous avons à présent une condition nécessaire et suffisante nous assurant l'existence d'une solution pour l'équation $ax + by = c$, il ne reste plus qu'à établir une méthode afin de trouver cette solution, si elle existe. Pour ce faire, nous devons introduire certaines propriétés importantes.

DÉFINITION 6.12

Deux entiers non nuls sont dits ***premiers entre eux*** si leur pgcd est 1.

EXEMPLE

4 et 15 sont premiers entre eux, mais notons que 4 et 15 ont chacun d'autres diviseurs que 1.

COROLLAIRE 6.13: (THÉORÈME DE BÉZOUT)

Deux entiers non nuls n et m sont premiers entre eux si et seulement s'il existe k, ℓ dans $\mathbb{Z}$ tels que $nk + m\ell = 1$.

DÉMONSTRATION

($\Longrightarrow$) Supposons que n et m sont premiers entre eux. Alors $\mathsf{pgcd}(n, m) = 1$ et le THÉORÈME 6.10 donne

$$\mathbb{Z} = n\mathbb{Z} + m\mathbb{Z}.$$

En particulier, $1 \in n\mathbb{Z} + m\mathbb{Z}$. Il existe donc $k, \ell \in \mathbb{Z}$ tels que

$$1 = nk + m\ell.$$

($\Longleftarrow$) Supposons qu'il existe $k, \ell \in \mathbb{Z}$ tels que $1 = nk + m\ell$. Posons $d = \mathsf{pgcd}(n, m)$. Puisque d divise n et m, il divise toute combinaison de ces deux entiers. Ainsi,

$$d \mid (nk + m\ell) = 1.$$

Comme d est positif, on obtient $d = 1$. Les entiers n et m sont donc premiers entre eux.

■

Exemple: (Suite de l'exemple précédent)

L'identité

$$4 \cdot 4 + 15 \cdot (-1) = 1$$

confirme, conformément au théorème de Bézout, que 4 et 15 sont premiers entre eux.

6.1.5.1 Récréation : $\sqrt{2}$ n'est pas rationnel

Il est presque impensable d'énoncer le théorème de Bézout sans évoquer cette propriété qui jeta le trouble dans l'école pythagoricienne : les nombres ne peuvent pas tous s'exprimer comme rapport de nombres entiers, comme les mathématiciens grecs de l'Antiquité le pensaient en premier lieu. Nous allons voir que le théorème de Bézout se trouve au coeur de la démonstration du corollaire qui suit.

Corollaire 6.14

$\sqrt{2} \notin \mathbb{Q}$.

Démonstration

- **Fait préliminaire.**

  Montrons par contraposée, pour tout $a \in \mathbb{Z}$,

  $$2|a^2 \quad \Longrightarrow \quad 2|a. \qquad (\star)$$

  Si a n'est pas divisible par 2, alors a est impair. Il existe donc $k \in \mathbb{Z}$ tel que $a = 2k + 1$, et

  $$a^2 \quad = \quad (2k+1)^2 \quad = \quad 2(2k^2 + 2k) + 1.$$

  Ainsi, a^2 est lui aussi impair et n'est pas divisible par 2. La contraposition établit le fait annoncé.

- **Réduction à une fraction irréductible grâce à Bézout.**

  Supposons que $\sqrt{2} \in \mathbb{Q}$. Nous pouvons alors écrire

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

  où $p, q \in \mathbb{N}^*$. Posons $d = \mathsf{pgcd}(p, q)$, puis écrivons

  $$p = dp' \qquad \text{et} \qquad q = dq'.$$

D'après le THÉORÈME 6.10, il existe $u, v \in \mathbb{Z}$ tels que $pu + qv = d$. En substituant les expressions de p et de q, puis en divisant par d, on obtient

$$p'u + q'v = 1.$$

Le THÉORÈME DE BÉZOUT montre alors que p' et q' sont premiers entre eux. Puisque

$$\frac{p}{q} = \frac{dp'}{dq'} = \frac{p'}{q'},$$

nous pouvons donc supposer, dès le départ, que p et q sont premiers entre eux.

- **Raisonnement par contradiction.**

En élevant l'égalité $\sqrt{2} = \frac{p}{q}$ au carré, nous obtenons

$$p^2 \quad = \quad 2q^2.$$

Ainsi, $2|p^2$ et, d'après ($\star$), $2|p$. Il existe donc $b \in \mathbb{N}^*$ tel que $p = 2b$. En substituant cette expression, on trouve

$$2q^2 \quad = \quad p^2 \quad = \quad 4b^2 \quad \Longrightarrow \quad q^2 \quad = \quad 2b^2.$$

Ainsi, $2|q^2$ et, de nouveau par ($\star$), $2|q$. Le nombre 2 divise donc à la fois p et q, ce qui contredit le fait qu'ils sont premiers entre eux. Par conséquent,

$$\sqrt{2} \notin \mathbb{Q}.$$

■

6.1.6 Résolution des équations diophantiennes linéaires $ax + by = c$

Bien entendu, comme dans le cas des problèmes de division dans $\mathbb{Z}$, on peut toujours se ramener au cas où les entiers considérés sont positifs, et nous ne nous en privons pas.

Nous revenons maintenant au problème annoncé au début du chapitre : résoudre une ***équation diophantienne linéaire du premier ordre***.

Déterminer tous les couples $(x, y) \in \mathbb{Z}^2$ qui satisfont l'équation

$$ax + by = c, \qquad a, b, c \in \mathbb{Z}.$$

6.1.6.1 Le lemme de Gauss

Avant de résoudre l'équation, établissons un résultat de divisibilité qui nous permettra ensuite de décrire toutes ses solutions.

LEMME 6.15: (LEMME DE GAUSS)

Soient a, b, c des entiers non nuls. Si $a|bc$ et a et b sont premiers entre eux, alors $a|c$.

Démonstration Comme a est premier avec b, on obtient par le théorème de Bézout que : $1 = ap+bq$ avec $p, q \in \mathbb{Z}$. En multipliant par c, on obtient donc $c = acp + bcq$. D'autre part, $a|bc$ donc il existe $u \in \mathbb{Z}$ tel que $bc = au$. D'où $c = acp + bcq = acp + auq = a(cp + uq)$, ainsi $a|c$.

■

Remarque L'énoncé ci-dessus est équivalent à : si a et b n'ont pas de diviseurs communs autre que 1 et -1 et si a divise le produit bc, alors tous les diviseurs de a sont aussi des diviseurs de c. En particulier, $a|c$.

6.1.6.2 L'équation homogène $ax + by = 0$

Lorsque $c = 0$, l'équation devient

$$ax + by = 0,$$

Posons $d = \mathsf{pgcd}(a, b)$, $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$. En divisant par d, nous obtenons l'équation équivalente

$$a'x = (-b')y,$$

où a' et b' sont premiers entre eux. Le lemme de Gauss montre alors que a' divise y et que b' divise x. Il existe donc $k, \ell \in \mathbb{Z}$ tels que

$$x = b'k \qquad \text{et} \qquad y = a'\ell.$$

En substituant ces expressions dans $a'x = (-b')y$, on obtient

$$a'b'k = -a'b'\ell.$$

Comme $a'b' \neq 0$, cette égalité entraîne $\ell = -k$. En remplaçant a' et b' par $\frac{a}{d}$ et $\frac{b}{d}$, nous concluons que toutes les solutions sont données par

$$x = \frac{b}{d}k \qquad \text{et} \qquad y = -\frac{a}{d}k, \qquad k \in \mathbb{Z}.$$

Réciproquement, une substitution directe montre que chacun de ces couples est bien une solution de $ax + by = 0$.

6.1.6.3 Condition d'existence

Le théorème 6.10 permet de déterminer exactement à quelle condition l'équation $ax + by = c$ admet des solutions entières — nous verrons qu'il en existe alors une infinité.

Proposition 6.16

Soient $a, b, c \in \mathbb{Z}$, avec a et b non tous deux nuls. L'équation $ax + by = c$ admet des solutions entières si et seulement si $\mathsf{pgcd}(a, b)|c$.

Démonstration Lorsque a et b sont non nuls, le théorème 6.10 donne $a\mathbb{Z} + b\mathbb{Z} = \mathsf{pgcd}(a, b)\mathbb{Z}$. Si l'un des deux coefficients est nul, cette égalité découle directement de $\mathsf{pgcd}(n, 0) = |n|$. Ainsi, dans tous les cas,

$$ax + by = c \text{ admet une solution entière} \iff c \in a\mathbb{Z} + b\mathbb{Z} \iff c \in \mathsf{pgcd}(a, b)\mathbb{Z}.$$

Cette dernière condition équivaut à $\mathsf{pgcd}(a, b)|c$.

■

Exemple

L'équation $12378x + 3054y = 7$ n'a pas de solution entière, car $\text{pgcd}(12378, 3054) = 6 \nmid 7$.

6.1.6.4 Le cas où a et b sont premiers entre eux

Si a et b sont premiers entre eux, alors $\text{pgcd}(a, b) = 1$ et il existe donc au moins une solution à l'équation diophantienne linéaire du premier ordre. Il faut commencer par trouver une ***solution particulière*** à l'équation $ax + by = 1$, c'est-à-dire x, y qui satisfont au théorème de Bézout, puis multiplier cette solution par c. Pour trouver une telle solution, il suffit de « remonter » l'algorithme d'Euclide. Illustrons ceci par un exemple.

Exemple: (Remonter l'algorithme d'Euclide)

L'équation $14x + 45y = 6$ admet des solutions, puisque $\text{pgcd}(14, 45) = 1$. Pour en trouver une, commençons par chercher une solution particulière de $14x + 45y = 1$.

- ***Descente : l'algorithme d'Euclide.***

  Les divisions euclidiennes successives donnent

  $$\begin{aligned} 45 &= 3 \cdot 14 + 3, \\ 14 &= 4 \cdot 3 + 2, \\ 3 &= 1 \cdot 2 + 1, \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

  Le dernier reste non nul est 1 ; ainsi, $\text{pgcd}(45, 14) = 1$.

- ***Remontée : isoler puis substituer les restes.***

  Lisons maintenant les trois premières divisions de bas en haut, en isolant chaque reste :

  $$\begin{aligned} 1 &= 3 - 2 \\ 2 &= 14 - 4 \cdot 3 \\ 3 &= 45 - 3 \cdot 14. \end{aligned}$$

  En substituant successivement ces expressions, nous obtenons

  $$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - \big(14 - 4 \cdot 3\big) \\ &= 5 \cdot 3 - 14 \\ &= 5\big(45 - 3 \cdot 14\big) - 14 \\ &= 5 \cdot 45 - 16 \cdot 14. \end{aligned}$$

  Autrement dit,

  $$1 = 14 \cdot (-16) + 45 \cdot 5.$$

  Une solution particulière de $14x + 45y = 1$ est donc

  $$(x_0, y_0) = (-16, 5).$$

- ***Passage de 1 à 6.***

En multipliant l'identité précédente par 6, on trouve

$$6 \quad = \quad 14 \cdot (-96) + 45 \cdot 30.$$

Ainsi, $(x_0, y_0) = (-96, 30)$ est une solution particulière de $14x + 45y = 6$. Le théorème qui suit montrera que toutes les solutions sont

$$x = -96 + 45k \qquad \text{et} \qquad y = 30 - 14k, \qquad k \in \mathbb{Z}.$$

Théorème 6.17

Soient $a, b, c \in \mathbb{Z}$, où a et b sont non nuls et premiers entre eux, et soit $(x_0, y_0) \in \mathbb{Z}^2$ une solution particulière de l'équation

$$ax + by = c.$$

Alors cette équation possède une infinité de solutions. Plus précisément, un couple $(x, y) \in \mathbb{Z}^2$ est une solution si et seulement s'il existe $k \in \mathbb{Z}$ tel que

$$\begin{cases} x = x_0 + bk, \\ y = y_0 - ak. \end{cases}$$

Démonstration Puisque $\text{pgcd}(a, b) = 1$, la proposition 6.16 garantit l'existence d'au moins une solution particulière.

($\Longrightarrow$) Soit $(x, y) \in \mathbb{Z}^2$ une solution. Comme (x_0, y_0) est également une solution,

$$\begin{aligned} & ax + by \quad = \quad ax_0 + by_0 \\ \Longrightarrow \quad & a(x - x_0) \quad = \quad b(y_0 - y). \end{aligned}$$

Ainsi, $a | b(y_0 - y)$. Puisque a et b sont premiers entre eux, le lemme de Gauss donne

$$a | (y_0 - y).$$

Il existe donc $k \in \mathbb{Z}$ tel que $y_0 - y = ak$, c'est-à-dire $y = y_0 - ak$. En reportant cette égalité dans $a(x - x_0) = b(y_0 - y)$, nous obtenons

$$a(x - x_0) \quad = \quad abk.$$

Comme $a \neq 0$, nous pouvons simplifier par a ; ainsi, $x = x_0 + bk$. Par conséquent,

$$\begin{cases} x = x_0 + bk, \\ y = y_0 - ak. \end{cases}$$

($\Longleftarrow$) La vérification directe de la réciproque est facile et laissée en exercice. Voir l'exercice 6.16.

Enfin, comme $b \neq 0$, les valeurs $x_0 + bk$ sont distinctes lorsque k parcourt $\mathbb{Z}$. L'équation possède donc une infinité de solutions.

■

6.1.6.5 Le cas général

Le cas général se ramène au précédent en divisant l'équation par le pgcd de ses deux coefficients.

Théorème 6.18: (Résolution générale)

Soient $a, b \in \mathbb{Z}$ deux entiers non nuls, $c \in \mathbb{Z}$ et $d = \text{pgcd}(a, b)$. L'équation

$$ax + by = c$$

admet des solutions entières si et seulement si $d|c$.
Lorsque cette condition est satisfaite, si (x_0, y_0) est une solution particulière, alors toutes les solutions sont données par

$$x = x_0 + \frac{b}{d}k \qquad \text{et} \qquad y = y_0 - \frac{a}{d}k, \qquad k \in \mathbb{Z}.$$

Démonstration La proposition 6.16 montre que l'équation admet une solution si et seulement si $d|c$.

Supposons cette condition satisfaite et posons

$$a' = \frac{a}{d}, \qquad b' = \frac{b}{d}, \qquad c' = \frac{c}{d}.$$

L'équation $ax + by = c$ est alors équivalente à

$$a'x + b'y = c',$$

où a' et b' sont premiers entre eux. Le théorème 6.17 donne donc toutes ses solutions :

$$x = x_0 + b'k \qquad \text{et} \qquad y = y_0 - a'k, \qquad k \in \mathbb{Z}.$$

En remplaçant a' et b' par leurs valeurs, on obtient la forme annoncée.

■

Exemple

L'équation $28x+90y = 12$ a une infinité de solutions, car $\text{pgcd}(28, 90) = 2|12$. L'équation réduite est $14x+45y = 6$, que nous avons résolue dans l'exemple précédent. Les solutions sont donc

$$x = -96 + 45k \qquad \text{et} \qquad y = 30 - 14k, \qquad k \in \mathbb{Z}.$$

6.2 Nombres premiers

Malgré l'apparente simplicité de la définition des nombres premiers, ils fascinèrent les mathématiciens durant les âges. Explorons à notre tour les nombres premiers qui sont aux nombres relatifs ce que les briques sont aux murs.

Définition 6.19

Un nombre $p \in \mathbb{N}$ est dit ***premier*** si $p \geqslant 2$ et si les seuls diviseurs de p sont 1 et p.

Exemple

$2, 3, 5, 7, 11$ sont des nombres premiers, mais 4 n'en est pas un car $2|4$.

Théorème 6.20

Tout entier naturel supérieur ou égal à 2 est divisible par un nombre premier.

Démonstration Pour tout $n \geqslant 2$, notons $P(n)$ la propriété

$$P(n) : \quad \text{« } n \text{ est divisible par un nombre premier »}.$$

Nous démontrons $P(n)$ par récurrence forte.

- **Étape initiale.**

  La propriété $P(2)$ est vraie, puisque 2 est premier et se divise lui-même.

- **Récursion.**

  Soit $n \geqslant 2$. Supposons que $P(k)$ soit vraie pour tout entier k tel que $2 \leqslant k \leqslant n$, et montrons que $P(n+1)$ est vraie.

  - Si $n+1$ est premier, alors il se divise lui-même. La propriété $P(n+1)$ est donc vraie.
  - Si $n+1$ n'est pas premier, alors il possède un diviseur a tel que

    $$2 \leqslant a \leqslant n.$$

    Par l'hypothèse de récurrence, $P(a)$ est vraie : il existe donc un nombre premier p qui divise a. Or, a divise $n+1$; par transitivité, p divise $n+1$. La propriété $P(n+1)$ est encore vraie.

Par récurrence forte, tout entier naturel $n \geqslant 2$ est divisible par un nombre premier.

■

Voici un problème d'arithmétique qui est toujours « ouvert », c'est-à-dire qu'il n'y a pas de preuve pour cette conjecture et qu'aucun contre-exemple n'a jamais été trouvé.

Conjecture 6.21: (Goldbach (1742))

Tout entier pair strictement supérieur à 2 est la somme de deux nombres premiers.

Il y a encore à ce jour plusieurs autres problèmes ouverts concernant les nombres premiers. D'ailleurs, le ***Clay mathematical institute*** offre un million de dollars pour la solution de certains de ces problèmes (avis aux intéressés !). La

question suivante, elle, fût au contraire démontrée il y a très longtemps par Euclide dans ses ***Éléments*** (vers 300 av. J.-C.).

Théorème 6.22: (Euclide)

Il y a une infinité de nombres premiers.

Démonstration Raisonnons par contradiction.

- **Hypothèse absurde.**

  Supposons que l'ensemble des nombres premiers soit fini. Nous pouvons alors tous les énumérer :

  $$p_1, p_2, \dots, p_k.$$

- **Construction d'Euclide.**

  Formons le produit de tous ces nombres premiers, puis ajoutons 1 :

  $$N \quad = \quad p_1 p_2 \cdots p_k, \qquad M \quad = \quad N + 1.$$

  Comme $M \geqslant 2$, le théorème précédent assure que M possède un diviseur premier. Par notre hypothèse, ce diviseur doit être l'un des nombres de la liste ; il existe donc un indice $i \in \{1, \dots, k\}$ tel que $p_i | M$.

- **Contradiction.**

  Puisque p_i apparaît dans le produit définissant N, on a également $p_i | N$. Par conséquent,

  $$\left.\begin{array}{r} p_i \mid M = N + 1 \\ p_i \mid N \end{array}\right\} \quad \Longrightarrow \quad p_i \mid (M - N) = 1.$$

  Or, aucun nombre premier ne divise 1. Nous obtenons une contradiction.

L'ensemble des nombres premiers est donc infini.

■

6.2.1 Théorème fondamental de l'arithmétique

Les nombres premiers jouent un rôle fondamental pour les nombres entiers : pour connaître un entier il suffit de connaître sa décomposition en nombres premiers comme nous le montre le théorème suivant.

Théorème 6.23

Tout entier $n \geqslant 2$ est produit de nombres premiers. Plus précisément, n s'écrit

$$n \quad = \quad p_1 p_2 \dots p_\ell,$$

où $p_1, \dots, p_\ell$ sont des nombres premiers déterminés de manière unique (mais non nécessairement distincts).

Exemple

$1620 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 5 = 2^2 \cdot 3^4 \cdot 5.$

Remarque

(i) L'ordre des facteurs n'a aucune importance. L'unicité signifie que deux décompositions de n contiennent exactement les mêmes facteurs premiers, avec les mêmes multiplicités, à une permutation près.

(ii) En regroupant les facteurs premiers identiques et en les ordonnant, on obtient une écriture de la forme

$$n \quad = \quad p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

où

$$p_1 < p_2 < \cdots < p_k \qquad \text{et} \qquad \alpha_1, \ldots, \alpha_k \in \mathbb{N}^*.$$

Les nombres premiers $p_1, \ldots, p_k$ et leurs exposants $\alpha_1, \ldots, \alpha_k$ sont alors déterminés de manière unique.

Avant de montrer le théorème, nous avons besoin d'une variante du théorème de Gauss.

Lemme 6.24: (Lemme d'Euclide)

Soit p un nombre premier et soient $a, b \in \mathbb{Z}$. Alors

$$p|ab \quad \Longrightarrow \quad p|a \ \vee \ p|b.$$

Démonstration

Supposons que $p|ab$. Distinguons deux cas.

- Si $p|a$, alors la proposition $p|a \ \vee \ p|b$ est vraie.
- Si $p \nmid a$, alors $\text{pgcd}(a, p) = 1$, puisque p est premier. Le lemme de Gauss, appliqué à $p|ab$, donne alors $p|b$. La proposition $p|a \vee p|b$ est donc encore vraie.

Ainsi, dans tous les cas, $p|a \vee p|b$.

Démonstration (Théorème 6.23)

Nous démontrons séparément l'existence et l'unicité de la factorisation.

- **Existence.**

  Nous raisonnons par récurrence forte sur $n \geqslant 2$.

  - **Étape initiale.**

    L'entier 2 est lui-même premier ; il possède donc une factorisation en nombres premiers.

- **Récursion.**

  Soit $n \geqslant 2$. Supposons que tout entier m tel que $2 \leqslant m \leqslant n$ soit un produit de nombres premiers, et considérons $n+1$.

  Si $n+1$ est premier, il constitue à lui seul la factorisation recherchée. Sinon, il existe $a, b \in \mathbb{N}$ tels que

  $$n+1 = ab, \qquad 2 \leqslant a, b \leqslant n.$$

  Par l'hypothèse de récurrence, a et b sont chacun des produits de nombres premiers. En réunissant leurs facteurs, nous obtenons une factorisation de $n+1 = ab$.

Par récurrence forte, tout entier $n \geqslant 2$ est un produit de nombres premiers.

- **Unicité.**

Nous procédons de nouveau par récurrence forte sur $n \geqslant 2$.

- **Étape initiale.**

  La factorisation de 2 est unique, puisque 2 est premier.

- **Récursion.**

  Soit $n \geqslant 2$. Supposons l'unicité établie pour tout entier m tel que $2 \leqslant m \leqslant n$, et considérons $n+1$.

  Si $n+1$ est premier, sa seule factorisation est le facteur $n+1$ lui-même. Supposons donc que $n+1$ soit composé et qu'il possède deux factorisations en nombres premiers :

  $$p_1 p_2 \cdots p_\ell \quad = \quad n+1 \quad = \quad q_1 q_2 \cdots q_k.$$

  Comme $p_1 | q_1 q_2 \cdots q_k$, des applications répétées du LEMME D'EUCLIDE montrent qu'il existe un indice i tel que $p_1 | q_i$. Les nombres p_1 et q_i étant premiers, on a nécessairement $p_1 = q_i$. Après avoir réordonné les facteurs q_j, nous pouvons supposer que $p_1 = q_1$.

  En simplifiant ce facteur commun, nous obtenons

  $$p_2 \cdots p_\ell \quad = \quad q_2 \cdots q_k \quad = \quad \frac{n+1}{p_1}.$$

  Puisque $n+1$ est composé, cet entier est compris entre 2 et n. L'hypothèse de récurrence assure donc que les deux factorisations restantes coïncident à l'ordre près. Il en va de même des deux factorisations initiales de $n+1$.

L'existence et l'unicité sont ainsi démontrées.

■

EXEMPLE

On a : $6 | 1620$, car $6 = 2 \cdot 3$ et $1620 = 2^2 \cdot 3^4 \cdot 5$.

Corollaire 6.25: (Critère de divisibilité)

Soient $m, n \geqslant 2$ deux entiers. Considérons des nombres premiers distincts $p_1, \ldots, p_k$ contenant tous les facteurs premiers de m et de n, et écrivons

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \quad \text{et} \quad m = p_1^{\beta_1} \cdots p_k^{\beta_k},$$

où $\alpha_i, \beta_i \in \mathbb{N}$ pour tout $i \in \{1, \ldots, k\}$. Alors

$$m|n \iff \beta_i \leqslant \alpha_i \quad \text{pour tout } i \in \{1, \ldots, k\}.$$

Démonstration Voir exercice 6.32.

6.3 Calcul modulaire sur les entiers

Le calcul modulaire consiste à ne retenir d'un entier que son reste dans une division euclidienne donnée. Commençons par une situation familière.

Exemple: (Quel jour serons-nous ?)

Nous sommes mardi et nous voulons déterminer le jour de la semaine dans 2583 jours. Numérotons les jours en posant lundi $= 0$, mardi $= 1$, mercredi $= 2$, etc. Comme

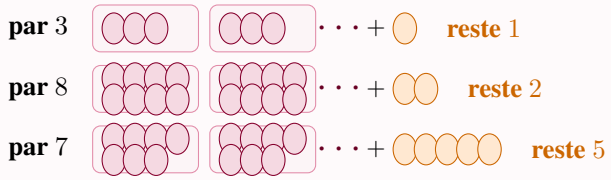
$$1 + 2583 = 2584 = 369 \cdot 7 + 1.$$

Le reste est encore 1. Après 369 semaines complètes, nous serons donc de nouveau mardi. Nous avons effectué un calcul *modulo* 7.

Le problème antique suivant demandera davantage d'outils.

Devinette 4

« Mon panier peut contenir au plus cent œufs. Si je le vide par trois œufs à la fois, il en reste un ; si je le vide par huit œufs à la fois, il en reste deux ; et si je le vide par sept œufs à la fois, il en reste cinq. Combien ai-je d'œufs ? » (Voir [Damphousse 2002].)



Nous allons définir les entiers modulaires, leurs opérations, puis les utiliser pour résoudre la devinette. Ce langage fut systématisé par Gauss au début du XIXe siècle.

6.3.1 Entiers modulaires

Définition 6.26: (Congruence modulo n)

Soit $n \in \mathbb{N}^*$. Deux entiers a et b sont ***congrus modulo*** n lorsque $n|(a-b)$. On écrit

$$a \equiv b \pmod{n}.$$

Remarque Les conditions suivantes sont équivalentes :

(i) $a \equiv b \pmod{n}$;

(ii) $n \mid (a-b)$;

(iii) $n \mid (b-a)$;

(iv) $a - b \in n\mathbb{Z}$;

(v) $\exists k \in \mathbb{Z}$ tel que $a = b + kn$.

Exemple

On a $8 \equiv 29 \pmod{7}$, car $8 - 29 = -21 = -3 \cdot 7$.

Théorème 6.27

Soit $n \in \mathbb{N}^*$. La congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$: pour tous $a, b, c \in \mathbb{Z}$,

(i) $a \equiv a \pmod{n}$ (***réflexivité***) ;

(ii) $a \equiv b \pmod{n} \implies b \equiv a \pmod{n}$ (***symétrie***) ;

(iii) $a \equiv b \pmod{n} \wedge b \equiv c \pmod{n} \implies a \equiv c \pmod{n}$ (***transitivité***).

Démonstration

- **Réflexivité.** Puisque $n|0 = a - a$, on a $a \equiv a \pmod{n}$.

- **Symétrie.** Si $n|(a-b)$, alors $n| - (a-b) = b - a$; ainsi, $b \equiv a \pmod{n}$.

- **Transitivité.** Si $n|(a-b)$ et $n|(b-c)$, alors

$$n \big| \big((a-b) + (b-c)\big) = a - c.$$

Donc $a \equiv c \pmod{n}$.

■

Une relation d'équivalence regroupe les éléments partageant une même propriété en ***classes d'équivalence***. Ici, elle regroupe les entiers ayant le même reste dans la division par n. Le lecteur pourra consulter l'annexe B pour une présentation générale des classes d'équivalence et des ensembles quotients.

6.3.1.1 Classes de congruence

Définition 6.28

Soient $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$. La ***classe de congruence modulo n de a*** est l'ensemble

$$[a]_n \quad := \quad \big\{ b \in \mathbb{Z} \;\big|\; b \equiv a \pmod{n} \big\}.$$

Exemple: (Les classes modulo 3)

Il existe exactement trois classes :

$$[0]_3 = 3\mathbb{Z},$$
$$[1]_3 = 3\mathbb{Z} + 1,$$
$$[2]_3 = 3\mathbb{Z} + 2.$$

En effet, la division euclidienne de tout entier par 3 produit un unique reste appartenant à $\{0, 1, 2\}$.

Notation

La classe de a modulo n se note $[a]_n = n\mathbb{Z} + a$. Lorsque le module n est fixé et qu'aucune confusion n'est possible, on écrit plus simplement $\overline{a}$.
Par définition,

$$b \in n\mathbb{Z} + a \iff b \equiv a \pmod{n}.$$

Définition 6.29

On note $\mathbb{Z}/n\mathbb{Z}$ l'***ensemble des classes de congruence modulo*** n. Ses éléments sont appelés ***entiers modulo*** n, ou ***entiers modulaires***.

Remarque Une classe $\overline{a} = n\mathbb{Z} + a$ est à la fois un sous-ensemble de $\mathbb{Z}$ et un élément de $\mathbb{Z}/n\mathbb{Z}$:

$$\overline{a} \subseteq \mathbb{Z} \quad \text{et} \quad \overline{a} \in \mathbb{Z}/n\mathbb{Z}.$$

Proposition 6.30

Soient $n \in \mathbb{N}^*$ et $x, y \in \mathbb{Z}$. Les conditions suivantes sont équivalentes :

- ***(i)*** $x \equiv y \pmod{n}$;
- ***(ii)*** $\overline{x} = \overline{y}$ dans $\mathbb{Z}/n\mathbb{Z}$;
- ***(iii)*** $x \in n\mathbb{Z} + y$;
- ***(iv)*** $y \in \overline{x}$;
- ***(v)*** $n\mathbb{Z} + x = n\mathbb{Z} + y$.

Démonstration Voir l'exercice 6.34.

■

6.3.1.2 Système de représentants

La division euclidienne fournit une liste finie contenant exactement un représentant de chaque classe.

Théorème 6.31

Soit $n \in \mathbb{N}^*$. Alors

(i) l'ensemble $\{0, 1, \ldots, n-1\}$ est un système de représentants des classes modulo n ; autrement dit,

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\};$$

(ii) $|\mathbb{Z}/n\mathbb{Z}| = n$.

Démonstration

- **Existence.**

  Soit $b \in \mathbb{Z}$. Sa division euclidienne par n donne $b = qn + r$, avec $0 \leqslant r < n$. Ainsi, $b \equiv r \pmod{n}$, donc $\overline{b} = \overline{r}$.

- **Unicité.**

  Soient $r, s \in \{0, \ldots, n-1\}$ tels que $\overline{r} = \overline{s}$. Alors $n|(r-s)$. Or, $|r-s| < n$; le seul multiple de n possible est donc 0. Ainsi, $r = s$.

Chaque classe possède exactement un représentant dans $\{0, \ldots, n-1\}$, qui contient n éléments.

■

Nous pouvons maintenant définir des opérations sur les classes et vérifier qu'elles ne dépendent pas du représentant choisi.

6.3.2 Addition et multiplication modulaire

Définition 6.32: (Opérations modulaires)

Soit $n \in \mathbb{N}^*$. Pour $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$, on définit

$$\begin{aligned} \overline{a} + \overline{b} &:= \overline{a+b}, \\ \overline{a} \cdot \overline{b} &:= \overline{ab}. \end{aligned}$$

Remarque Dans $\overline{a} + \overline{b} = \overline{a+b}$, l'opération à gauche se fait dans $\mathbb{Z}/n\mathbb{Z}$, tandis que celle à droite se fait d'abord dans $\mathbb{Z}$. Il en va de même pour la multiplication.

Proposition 6.33: (Compatibilité avec la congruence)

Si $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$, alors

$$\begin{aligned} a + b &\equiv a' + b' \pmod{n}, \\ ab &\equiv a'b' \pmod{n}. \end{aligned}$$

Les opérations modulaires sont donc bien définies.

Démonstration Écrivons $a' = a + kn$ et $b' = b + \ell n$, avec $k, \ell \in \mathbb{Z}$.

- Pour l'addition,
$$a' + b' = (a + b) + n(k + \ell),$$
donc $a' + b' \equiv a + b \pmod{n}$.

- Pour la multiplication,
$$a'b' = ab + n(a\ell + bk + nk\ell),$$
donc $a'b' \equiv ab \pmod{n}$.

■

Remarque

On peut indifféremment calculer avec les classes ou avec n'importe lesquels de leurs représentants, puis réduire le résultat modulo n.

Proposition 6.34: (Règles de calcul)

L'addition et la multiplication dans $\mathbb{Z}/n\mathbb{Z}$ sont commutatives et associatives ; la multiplication est distributive sur l'addition. De plus, $\overline{0}$ et $\overline{1}$ sont les éléments neutres respectifs, et l'opposé de $\overline{a}$ est $\overline{-a}$.

Démonstration Il suffit de transporter les règles de calcul de $\mathbb{Z}$ aux classes. Par exemple,
$$\overline{a}(\overline{b} + \overline{c}) = \overline{a(b + c)} = \overline{ab + ac} = \overline{a}\,\overline{b} + \overline{a}\,\overline{c}.$$
Les autres vérifications sont analogues.

■

Remarque Dans $\mathbb{Z}$, l'égalité $ax = 0$ avec $a \neq 0$ entraîne $x = 0$. Ce raisonnement échoue parfois modulo n. Par exemple, dans $\mathbb{Z}/4\mathbb{Z}$,
$$\overline{2} \cdot \overline{2} = \overline{4} = \overline{0}.$$
La proposition suivante montre que ce phénomène disparaît lorsque le module est premier.

Proposition 6.35

Soit p un nombre premier. Pour tous $\overline{x}, \overline{y} \in \mathbb{Z}/p\mathbb{Z}$,
$$\overline{x}\,\overline{y} = \overline{0} \iff (\overline{x} = \overline{0}) \vee (\overline{y} = \overline{0}).$$

Démonstration L'égalité $\overline{x}\,\overline{y} = \overline{0}$ équivaut à $p|xy$. Le lemme d'Euclide donne alors $(p|x) \vee (p|y)$, c'est-à-dire $(\overline{x} = \overline{0}) \vee (\overline{y} = \overline{0})$. La réciproque est immédiate.

■

6.3.3 Éléments inversibles

Dans $\mathbb{Z}$, seuls 1 et -1 possèdent un inverse multiplicatif entier. Modulo n, d'autres éléments peuvent devenir inversibles, mais ce n'est pas le cas de toutes les classes.

Définition 6.36

Soit $n \in \mathbb{N}^*$. Un élément $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ est ***inversible*** s'il existe $\overline{y} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{x}\,\overline{y} = \overline{1}$. Cet élément $\overline{y}$ est unique ; on l'appelle l'***inverse*** de $\overline{x}$ et on le note $\overline{x}^{-1}$.

Notation

On note $(\mathbb{Z}/n\mathbb{Z})^\times$ l'ensemble des éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$.

Exemple

1. Dans tout $\mathbb{Z}/n\mathbb{Z}$, on a $\overline{1}^{-1} = \overline{1}$.
2. Dans $\mathbb{Z}/4\mathbb{Z}$, les seuls inversibles sont $\overline{1}$ et $\overline{3}$, et chacun est son propre inverse.
3. Dans $\mathbb{Z}/11\mathbb{Z}$, les paires d'inverses sont

$$\overline{1} \leftrightarrow \overline{1}, \quad \overline{2} \leftrightarrow \overline{6}, \quad \overline{3} \leftrightarrow \overline{4}, \quad \overline{5} \leftrightarrow \overline{9}, \quad \overline{7} \leftrightarrow \overline{8}, \quad \overline{10} \leftrightarrow \overline{10}.$$

D'après l'exemple précédent, on constate par exemple que dans $\mathbb{Z}/4\mathbb{Z}$, il n'y a que deux éléments qui sont inversibles bien que cet ensemble contienne 4 éléments. En effet, la proposition suivante nous démontre que ce ne sont pas tous les éléments de $\mathbb{Z}/n\mathbb{Z}$ qui sont inversibles.

Proposition 6.37

Soient $n \in \mathbb{N}^*$ et $x \in \mathbb{Z}$. Alors

$$\overline{x} \in (\mathbb{Z}/n\mathbb{Z})^\times \iff \mathsf{pgcd}(x, n) = 1.$$

Démonstration

($\Longrightarrow$) Si $\overline{x}$ est inversible, il existe $y \in \mathbb{Z}$ tel que $\overline{x}\,\overline{y} = \overline{1}$. Ainsi, $xy \equiv 1 \pmod{n}$, donc il existe $k \in \mathbb{Z}$ tel que

$$xy + kn = 1.$$

Le théorème de Bézout entraîne alors $\mathsf{pgcd}(x, n) = 1$.

($\Longleftarrow$) Si $\text{pgcd}(x, n) = 1$, Bézout fournit $y, k \in \mathbb{Z}$ tels que $xy + kn = 1$. En réduisant cette égalité modulo n, on obtient $\overline{x}\,\overline{y} = \overline{1}$. Ainsi, $\overline{x}$ est inversible.

■

Grâce à cette proposition, nous pouvons plus particulièrement caractériser les éléments inversibles dans $\mathbb{Z}/p\mathbb{Z}$ si p est premier. On confirmera par le fait même nos observations faites dans l'exemple ci-dessus.

Corollaire 6.38

Soit p un nombre premier. Tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible. Si p est impair, les seuls éléments qui sont leurs propres inverses sont $\overline{1}$ et $\overline{-1} = \overline{p-1}$.

Démonstration Si $\overline{x} \neq \overline{0}$, choisissons son représentant $x \in \{1, \ldots, p-1\}$. Alors $\text{pgcd}(x, p) = 1$; la proposition 6.37 montre que $\overline{x}$ est inversible.

Supposons maintenant p impair et $\overline{x}^2 = \overline{1}$. Alors

$$(\overline{x} - \overline{1})(\overline{x} + \overline{1}) = \overline{0}.$$

La proposition 6.35 donne $\overline{x} = \overline{1}$ ou $\overline{x} = \overline{-1}$.

■

On peut alors déduire de ce corollaire cette caractérisation des nombres premiers, découverte par Wilson au XVIIIe siècle (et en fait, un siècle auparavant par Leibniz). On rappelle que $n! = n \cdot (n-1) \cdots (n-2) \ldots 2 \cdot 1$.

Théorème 6.39: (Wilson)

Soit $n \geqslant 2$ un entier. Alors

$$n \text{ est premier} \iff (n-1)! \equiv -1 \pmod{n}.$$

Démonstration

($\Longrightarrow$) Supposons n premier. Les classes non nulles modulo n sont inversibles. D'après le corollaire 6.38, seules $\overline{1}$ et $\overline{-1}$ sont leurs propres inverses ; les autres se regroupent en paires $\{\overline{a}, \overline{a}^{-1}\}$ dont le produit vaut $\overline{1}$. Ainsi,

$$\overline{(n-1)!} = \overline{1} \cdot \overline{-1} = \overline{-1}.$$

($\Longleftarrow$) Supposons $(n-1)! \equiv -1 \pmod{n}$. Si n était composé, il posséderait un diviseur a tel que $1 < a < n$. Alors $a|(n-1)!$ et, puisque $n|(n-1)! + 1$, on aurait aussi $a|(n-1)! + 1$. Il s'ensuivrait que $a|1$, contradiction. Donc n est premier.

■

6.3.4 Théorème des restes chinois

Nous avons maintenant tous les outils en main afin de déduire combien d'oeufs se retrouvent dans le panier de la DEVINETTE 4. Comme lors de l'étude des équations diophantiennes, nous voudrions tout de même nous assurer qu'il existe bel et bien une solution à ce problème. Le théorème suivant nous certifie précisément l'existence d'une unique solution.

THÉORÈME 6.40: (THÉORÈME DES RESTES CHINOIS)

Soient $n, m \in \mathbb{N}^*$ premiers entre eux et $k, \ell \in \mathbb{Z}$. Il existe un unique entier $x \in \{0, 1, \ldots, nm-1\}$ tel que

$$\begin{cases} x \equiv k \pmod{n}, \\ x \equiv \ell \pmod{m}. \end{cases}$$

DÉMONSTRATION

- **Existence.**

  Le THÉORÈME DE BÉZOUT fournit $\alpha, \beta \in \mathbb{Z}$ tels que $\alpha n + \beta m = 1$. Posons

  $$x_0 = \alpha n \ell + \beta m k.$$

  Réduisons l'identité de Bézout modulo chacun des deux entiers. Modulo n, le terme αn disparaît ; modulo m, c'est le terme βm qui disparaît. Ainsi,

  $$\begin{aligned} \alpha n + \beta m = 1 \quad &\Longrightarrow \quad \beta m \equiv 1 \pmod{n}, \\ \alpha n + \beta m = 1 \quad &\Longrightarrow \quad \alpha n \equiv 1 \pmod{m}. \end{aligned}$$

  Par conséquent,

  $$\begin{aligned} x_0 \equiv \beta m k \equiv k \pmod{n}, \\ x_0 \equiv \alpha n \ell \equiv \ell \pmod{m}. \end{aligned}$$

  Le représentant de $\overline{x_0}$ compris entre 0 et $nm-1$ est donc une solution.

- **Unicité.**

  Si x et x' sont deux solutions, alors $n|(x-x')$ et $m|(x-x')$. Puisque n et m sont premiers entre eux, $nm|(x-x')$ (voir l'EXERCICE 6.21). Ainsi, $x \equiv x' \pmod{nm}$. Comme $x, x' \in \{0, \ldots, nm-1\}$, le THÉORÈME 6.31 donne $x = x'$.

■

Exemple: (Le problème des œufs)

La devinette 4 revient à chercher un entier x tel que

$$0 \leqslant x \leqslant 100 \qquad \text{et} \qquad \begin{cases} x \equiv 1 \pmod 3, \\ x \equiv 2 \pmod 8, \\ x \equiv 5 \pmod 7. \end{cases}$$

Résolvons successivement ces congruences.

- La première donne $x = 3k + 1$ pour un certain $k \in \mathbb{Z}$. En réduisant cette égalité modulo 8, nous obtenons

$$3k + 1 \equiv 2 \pmod 8 \iff 3k \equiv 1 \pmod 8.$$

Or $3 \cdot 3 \equiv 1 \pmod 8$: la classe $[3]_8$ est donc son propre inverse. En multipliant la congruence $3k \equiv 1 \pmod 8$ par 3, on obtient $k \equiv 3 \pmod 8$. Ainsi, $k = 8\ell + 3$ et

$$x = 24\ell + 10.$$

- Il reste à imposer $x \equiv 5 \pmod 7$. Comme $24 \equiv 3 \pmod 7$ et $10 \equiv 3 \pmod 7$, cette condition devient

$$3\ell + 3 \equiv 5 \pmod 7 \iff 3\ell \equiv 2 \pmod 7.$$

Or $3 \cdot 5 \equiv 1 \pmod 7$: la classe $[5]_7$ est l'inverse de $[3]_7$. En multipliant la congruence $3\ell \equiv 2 \pmod 7$ par 5, on obtient $\ell \equiv 10 \equiv 3 \pmod 7$. Il existe donc $t \in \mathbb{Z}$ tel que $\ell = 7t + 3$, d'où

$$x = 168t + 82.$$

La contrainte $0 \leqslant x \leqslant 100$ force $t = 0$. Le panier contient donc exactement 82 œufs.

6.3.5 Petit théorème de Fermat

Nous terminons par un résultat fondamental d'arithmétique modulaire, formulé par Pierre de Fermat en 1640.

Théorème 6.41: (Petit théorème de Fermat)

Soient p un nombre premier et $a \in \mathbb{Z}$. Si p ne divise pas a, alors

$$a^{p-1} \equiv 1 \pmod p.$$

Démonstration Dans $\mathbb{Z}/p\mathbb{Z}$, les classes $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ sont toutes non nulles.

- **Une permutation des classes non nulles.**

Comme p ne divise pas a, la classe $\overline{a}$ est inversible. La multiplication par $\overline{a}$ permute donc les classes non nulles de $\mathbb{Z}/p\mathbb{Z}$. Par conséquent,

$$\left\{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\right\} = \left\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\right\}.$$

- **Le produit des classes.**

  En multipliant les éléments de ces deux ensembles, nous obtenons

$$\overline{a}^{\,p-1}\,\overline{(p-1)!} \quad = \quad \overline{(p-1)!}.$$

  Puisque p ne divise pas $(p-1)!$, la classe $\overline{(p-1)!}$ est inversible. Nous pouvons donc la simplifier et conclure que $\overline{a}^{\,p-1} = \overline{1}$.

■

⚠ REMARQUE

(i) Le théorème d'Euler généralise le PETIT THÉORÈME DE FERMAT aux modules qui ne sont pas nécessairement premiers.

(ii) Cette généralisation joue notamment un rôle dans le système de chiffrement à clé publique RSA, très utilisé en sécurité informatique.

(iii) L'EXERCICE 6.51 propose une autre formulation du PETIT THÉORÈME DE FERMAT, valable pour tout entier a : $a^p \equiv a \pmod{p}$.

6.4 Exercices

Arithmétique dans $\mathbb{Z}$

EXERCICE 6.1 (Division euclidienne) Écrire la division euclidienne de -514 par 35.

EXERCICE 6.2 (Divisibilité de 111111) Montrer que 111 divise 111111.

Indice : $111111 = 111000 + 111$.

EXERCICE 6.3 (Divisibilité par 11) Montrer que 572 est divisible par 11.

Indice : $572 = 550 + 22$.

EXERCICE 6.4 (Divisibilité et valeur absolue) Vérifier que, si $d, n \in \mathbb{Z}$ sont non nuls, alors d divise n si et seulement si $|d|$ divise $|n|$. Ici, $|d|$ désigne la valeur absolue de d.

EXERCICE 6.5 (Propriétés de la divisibilité) Compléter la démonstration de la PROPOSITION 6.3. Soient n, m, p des entiers non nuls. Montrer que :

(iv) $p|n \implies p|nm$;

(v) $p|n$ et $p|m \implies p|n+m$ et $p|n-m$;

(vi) plus généralement, $p|n$ et $p|m \implies p|an+bm$ pour tous $a, b \in \mathbb{Z}$.

Exercice 6.6 (Premiers exemples d'idéaux)

(a) Montrer que $I = \{6a + 4b \mid a, b \in \mathbb{Z}\}$ est un idéal.

(b) Si I est un idéal, montrer que $1 \in I \iff I = \mathbb{Z}$.

Exercice 6.7 (Le plus petit commun multiple) Soient $n, m \in \mathbb{N}^*$. Un ***multiple commun à n et m*** est un entier strictement positif qui est multiple à la fois de n et de m.

(a) Montrer qu'il existe un unique plus petit multiple commun à m et à n. On l'appelle le ***plus petit commun multiple de m et de n*** et on le note $\mathsf{ppcm}(m, n)$.

(b) Montrer que $n\mathbb{Z} \cap m\mathbb{Z} = \mathsf{ppcm}(m, n)\mathbb{Z}$.

(c) Montrer que $m|p$ et $n|p \implies \mathsf{ppcm}(n, m)|p$.

(d) Montrer que $\mathsf{ppcm}(m, n)|mn$.

Exercice 6.8 (Relation entre le PGCD et le PPCM) Montrer que si $a, b \in \mathbb{N}^*$, alors $ab = \mathsf{ppcm}(a, b) \cdot \mathsf{pgcd}(a, b)$.

Exercice 6.9 (PGCD et divisibilité) Soient $n, m \in \mathbb{N}^*$. Montrer que $\mathsf{pgcd}(n, m) = n \iff n|m$.

Exercice 6.10 (Multiplication du PGCD par un facteur) Montrer que

$$\mathsf{pgcd}(da, db) = |d| \ \mathsf{pgcd}(a, b)$$

pour tous entiers non nuls a, b et d.

Exercice 6.11 (Reconnaître un idéal principal) Pour chacun des ensembles suivants, montrer que I est un idéal et déterminer $n \in \mathbb{N}^*$ tel que $I = n\mathbb{Z}$.

(a) $I = \{52x - 2y \mid x, y \in \mathbb{Z}\}$;

(b) $I = \{3x + 9y - 15z \mid x, y, z \in \mathbb{Z}\}$;

(c) $I = \{217\ell + 34k \mid \ell, k \in \mathbb{Z}\}$.

Réponse : (a) $I = 2\mathbb{Z}$; (b) $I = 3\mathbb{Z}$; (c) $I = \mathbb{Z}$.

Exercice 6.12 (Diviseur d'une somme) Soient a, b, c des entiers non nuls. Supposons a et b premiers entre eux, et supposons que $c|a + b$. Montrer que $\mathsf{pgcd}(a, c) = 1 = \mathsf{pgcd}(b, c)$.

Exercice 6.13 (Entiers premiers entre eux) Montrer que, pour tout entier k :

(a) k et $k + 1$ sont premiers entre eux ;

(b) k et $2k + 1$ sont premiers entre eux ;

(c) $3k + 2$ et $5k + 3$ sont premiers entre eux.

Exercice 6.14 (Une équation dans $\mathbb{N}$) Soient $a, b \in \mathbb{N}^*$ premiers entre eux et tels que $a^2 + a = 7b^3$. Montrer que a divise 7, puis résoudre cette équation dans $\mathbb{N}$.

Exercice 6.15 (Réciproque du lemme de Gauss) Soient $a, b \in \mathbb{Z}$ non nuls. Supposons que, pour tout $c \in \mathbb{Z}$,

$$a|bc \quad \Longrightarrow \quad a|c.$$

Montrer que a et b sont premiers entre eux.

Exercice 6.16 (Réciproque du théorème de résolution générale) Compléter la preuve du théorème 6.18. Soient $a, b, c \in \mathbb{Z}$, où a et b sont premiers entre eux, et soit (x_0, y_0) une solution particulière de $ax + by = c$. Montrer que, pour tout $k \in \mathbb{Z}$,

$$x = x_0 + kb \qquad \text{et} \qquad y = y_0 - ka$$

définissent un couple (x, y) qui est solution de l'équation.

Exercice 6.17 (Équation diophantienne — Examen 2010) Résoudre l'équation diophantienne $26x + 57y = 1$.

Exercice 6.18 (Équation diophantienne) Résoudre l'équation diophantienne $216x + 92y = 8$.

Exercice 6.19 (Équation diophantienne — Examen 2011) Résoudre l'équation diophantienne $33x + 91y = 1$.

Réponse : $x = -11 + 91k$ et $y = 4 - 33k$, où $k \in \mathbb{Z}$.

Exercice 6.20 (Équations diophantiennes linéaires) Résoudre les équations suivantes.

(a) $12378x + 3054y = 6$;

(b) $217x + 34y = 2$;

(c) $217x + 34y = 3$;

(d) $544x - 944y = 160$.

Réponse : (a) $x = 132 + 509k$ et $y = -535 - 2063k$; (b) $x = -26 + 34k$ et $y = 166 - 217k$; (c) $x = -39 + 34k$ et $y = 249 - 217k$; (d) $x = -260 - 59k$ et $y = -150 - 34k$, où $k \in \mathbb{Z}$.

Exercice 6.21 (Produit de diviseurs — Examen 2010) Soit $n \in \mathbb{N}^*$, et soient a et b deux diviseurs de n. Montrer que, si a et b sont premiers entre eux, alors ab divise aussi n.

Exercice 6.22 (PGCD d'un produit — Examen 2011) Soient $n, m, p \in \mathbb{N}^*$. On suppose que n et p sont premiers entre eux.

(a) Soit d un diviseur de n. Montrer que d et p sont premiers entre eux.

(b) Soit d un diviseur commun à n et à mp. Montrer que d divise m.

(c) Montrer que $\mathsf{pgcd}(n, mp) = \mathsf{pgcd}(n, m)$.

Exercice 6.23 (Somme et produit — Examen 2011) Soient $a, b \in \mathbb{Z}$. Montrer que, si a et b sont premiers entre eux, alors $a + b$ et ab sont aussi premiers entre eux.

Nombres premiers

Exercice 6.24 (Deux nombres premiers à distance 15) Déterminer les couples (p_1, p_2) de nombres premiers tels que $p_1 - p_2 = 15$.

Exercice 6.25 (Un diviseur de $(n-1)!$) Montrer que tout nombre ***non premier*** $n \in \mathbb{N}$ tel que $n \geqslant 6$ divise $(n-1)!$. On rappelle que $n! = n \cdot (n-1) \cdots 2 \cdot 1$.

Exercice 6.26 (Diviseur premier d'un produit de nombres premiers) Soient $p, q_1, \ldots, q_\ell$ des nombres premiers, non nécessairement distincts. Si p divise $q_1 \cdots q_\ell$, montrer par récurrence qu'il existe $i \in \{1, \ldots, \ell\}$ tel que $p = q_i$.

Exercice 6.27 (PGCD et PPCM par factorisation) Soient n et m deux entiers supérieurs ou égaux à 2 tels que

$$n = p_1^{n_1} \cdots p_k^{n_k} \qquad \text{et} \qquad m = p_1^{m_1} \cdots p_k^{m_k},$$

où $p_1, \ldots, p_k$ sont des nombres premiers distincts.

(a) Montrer que $\mathsf{pgcd}(m, n) = p_1^{r_1} \cdots p_k^{r_k}$, où $r_i = \min(n_i, m_i)$.

(b) Montrer que $\mathsf{ppcm}(m, n) = p_1^{r_1} \cdots p_k^{r_k}$, où $r_i = \max(n_i, m_i)$.

Exercice 6.28 (Irrationalité de $\sqrt{p}$) Montrer que, pour tout nombre premier p, $\sqrt{p}$ n'est pas rationnel.

Exercice 6.29 (Propriétés élémentaires des nombres premiers)

(a) Soit p un nombre premier. Montrer que, pour tout $n \in \mathbb{N}^*$, $\mathsf{pgcd}(p, n) = 1$ ou $\mathsf{pgcd}(p, n) = p$.

(b) Soient p, q deux nombres premiers. Montrer que, pour tout $n \in \mathbb{N}^*$, $p | q^n \iff p = q$.

Exercice 6.30 (Le crible d'Ératosthène) Soit $n \in \mathbb{N}$, avec $n \geqslant 2$. La méthode suivante permet de trouver tous les nombres premiers compris entre 2 et n. Dressons la liste des entiers naturels de 2 à n. En la parcourant de gauche à droite, conservons chaque entier qui n'a pas encore été rayé, puis rayons tous ses autres multiples. Répétons ce procédé avec l'entier non rayé suivant.

(a) Montrer qu'il suffit d'effectuer les éliminations correspondant aux nombres premiers inférieurs ou égaux à $\sqrt{n}$.

(b) On note E_n l'ensemble des entiers compris entre 2 et n qui n'ont pas été rayés. Montrer qu'un entier p compris entre 2 et n est premier si et seulement si $p \in E_n$.

Exercice 6.31 (Polynômes à valeurs premières) Déterminer, pour chacune des expressions suivantes, les valeurs de $n \in \mathbb{N}$ pour lesquelles elle est un nombre premier.

(a) $2n^2 + 7n + 6$;

(b) $3n^2 + 8n + 5$.

Réponse : (a) Aucune valeur ; (b) $n = 0$.

Exercice 6.32 (Critère de divisibilité par factorisation) Compléter la preuve du corollaire 6.25. Soient n et m deux entiers supérieurs ou égaux à 2 tels que

$$n = p_1^{n_1} \cdots p_k^{n_k} \qquad \text{et} \qquad m = p_1^{m_1} \cdots p_k^{m_k},$$

où $p_1, \ldots, p_k$ sont des nombres premiers distincts. Montrer que

$$m|n \iff m_i \leqslant n_i \quad \text{pour tout } i \in \{1, \ldots, k\}.$$

Calcul modulaire sur les entiers

Exercice 6.33 (Calculer un reste) Dans chacun des cas suivants, écrire une congruence de la forme $A \equiv r \pmod{n}$, où $0 \leqslant r < n$.

(a) $A = 2^7$ et $n = 7$;

(b) $A = 231$ et $n = 7$;

(c) $A = 27x^5 - 9x^3 + 82$, où $x \in \mathbb{Z}$, et $n = 9$;

(d) n est un nombre premier qui divise A.

Réponse : (a) $A \equiv 2 \pmod{7}$; (b) $A \equiv 0 \pmod{7}$; (c) $A \equiv 1 \pmod{9}$; (d) $A \equiv 0 \pmod{n}$.

Exercice 6.34 (Caractérisations d'une classe de congruence) Compléter la preuve de la proposition 6.30. Soient $n \in \mathbb{N}^*$ et $x, y \in \mathbb{Z}$. Montrer que les énoncés suivants sont équivalents :

(i) $x \equiv y \pmod{n}$;

(ii) $\overline{x} = \overline{y}$ dans $\mathbb{Z}/n\mathbb{Z}$;

(iii) $x \in [y]_n$;

(iv) $y \in [x]_n$;

(v) $[x]_n = [y]_n$.

Exercice 6.35 (Une identité modulo 3) Montrer que, pour tout $x \in \mathbb{Z}$,

$$\overline{7x^2 + 123x} = \overline{15x^4 + x^2}$$

dans $\mathbb{Z}/3\mathbb{Z}$.

Exercice 6.36 (Bézout sous forme modulaire) Soient $a, b \in \mathbb{Z}$ non nuls. Montrer que :

(a) il existe $k \in \mathbb{Z}$ tel que $ka \equiv \mathsf{pgcd}(a, b) \pmod{b}$;

(b) il existe $\ell \in \mathbb{Z}$ tel que $\ell b \in \mathsf{pgcd}(a, b) + a\mathbb{Z}$.

Exercice 6.37 (Intersection de deux classes) Soient $n \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$. Montrer que les propositions suivantes sont équivalentes :

(i) $(a + n\mathbb{Z}) \cap (b + n\mathbb{Z}) \neq \emptyset$;

(ii) $\overline{a} = \overline{b}$ dans $\mathbb{Z}/n\mathbb{Z}$;

(iii) $a \equiv b \pmod{n}$.

Exercice 6.38 (Unicité des représentants) Soient $n \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$ tels que $0 \leqslant a, b \leqslant n-1$. Montrer que

$$a = b \iff (a + n\mathbb{Z}) \cap (b + n\mathbb{Z}) \neq \emptyset.$$

Exercice 6.39 (Déterminer les éléments inversibles) Déterminer $(\mathbb{Z}/n\mathbb{Z})^\times$ pour $n = 5$, $n = 8$, $n = 12$ et $n = 15$.

Exercice 6.40 (Produit d'éléments inversibles) Soit $n \in \mathbb{N}^*$ et $\overline{x}, \overline{y} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Montrer que $\overline{x} \cdot \overline{y} \in (\mathbb{Z}/n\mathbb{Z})^\times$ et que $(\overline{x} \cdot \overline{y})^{-1} = \overline{y}^{-1} \cdot \overline{x}^{-1}$.

Exercice 6.41 (Inverses modulo 11) Vérifier dans $\mathbb{Z}/11\mathbb{Z}$ que

$$\overline{1}^{-1} = \overline{1}, \quad \overline{2}^{-1} = \overline{6}, \quad \overline{3}^{-1} = \overline{4}, \quad \overline{5}^{-1} = \overline{9}, \quad \overline{7}^{-1} = \overline{8}, \quad \overline{10}^{-1} = \overline{10}.$$

Exercice 6.42 (Inverse modulo 997) Trouver l'inverse de $342 + 997\mathbb{Z}$ dans $\mathbb{Z}/997\mathbb{Z}$.

Exercice 6.43 (Inverse modulo 57 — Examen 2010) À la suite de l'exercice 6.17, montrer que $26 + 57\mathbb{Z}$ est inversible dans $\mathbb{Z}/57\mathbb{Z}$ et calculer son inverse.

Réponse : L'inverse de $26 + 57\mathbb{Z}$ est $11 + 57\mathbb{Z}$.

Exercice 6.44 (Inverse modulo 91 — Examen 2011) À la suite de l'exercice 6.19, montrer que $33 + 91\mathbb{Z}$ est inversible dans $\mathbb{Z}/91\mathbb{Z}$ et calculer son inverse.

Réponse : L'inverse de $33 + 91\mathbb{Z}$ est $80 + 91\mathbb{Z}$.

Exercice 6.45 (Un calendrier gigantesque) Sachant qu'aujourd'hui nous sommes lundi, quel jour de la semaine serons-nous dans $10^{1000000000}$ jours ?

Réponse : Nous serons vendredi.

Exercice 6.46 (Une suite de nombres composés) Soit $n \in \mathbb{N}$, avec $n \geqslant 2$. Montrer que les nombres $n! + 2, n! + 3, \ldots, n! + n$ ne sont pas premiers.

Exercice 6.47 (Une application du théorème de Wilson) Soit p un nombre premier tel que $p \geqslant 5$, et posons

$$N = \sum_{k=1}^{p-1} \left(\frac{(p-1)!}{k} \right)^2.$$

(a) Montrer que $N \in \mathbb{N}$ et que, dans $\mathbb{Z}/p\mathbb{Z}$,

$$\overline{N} = \sum_{k=1}^{p-1} \overline{k}^{-2} \left(\overline{(p-1)!} \right)^2.$$

(b) Montrer que $N \equiv \sum_{k=1}^{p-1} k^2 \pmod{p}$.

(c) En déduire que p divise N.

Exercice 6.48 (Résoudre une congruence linéaire) Soient $a, b \in \mathbb{Z}$, $n \in \mathbb{N}^*$ et $d = \mathsf{pgcd}(a, n)$. Montrer que la congruence $ax \equiv b \pmod{n}$ admet une solution si et seulement si $d|b$. Montrer que, dans ce cas, elle possède exactement d solutions dans $\mathbb{Z}/n\mathbb{Z}$.

Exercice 6.49 (Un système de congruences) Déterminer si le système suivant admet des solutions. Si oui, les décrire et préciser modulo quel entier elles sont déterminées de manière unique.

$$\begin{cases} 2x \equiv 3 \pmod{5}, \\ 3x \equiv 1 \pmod{4}. \end{cases}$$

Exercice 6.50 (Systèmes de congruences) Déterminer si les systèmes suivants admettent des solutions. Dans chaque cas où il en existe, les décrire et préciser modulo quel entier elles sont déterminées de manière unique.

(a) $\begin{cases} 5x \equiv 1 \pmod{7}, \\ 3x \equiv 1 \pmod{5}, \end{cases}$ (b) $\begin{cases} 2x \equiv 4 \pmod{6}, \\ 3x \equiv 3 \pmod{10}, \end{cases}$ (c) $\begin{cases} x \equiv 1 \pmod{2}, \\ x \equiv 2 \pmod{3}, \\ x \equiv 3 \pmod{4}. \end{cases}$

Réponse : (a) $x \in 17 + 35\mathbb{Z}$; (b) $x \in 11 + 30\mathbb{Z}$; (c) $x \in 11 + 12\mathbb{Z}$.

Exercice 6.51 (Une autre forme du petit théorème de Fermat) Soient $a \in \mathbb{N}$ et p un nombre premier. Montrer, par récurrence sur a, que p divise $a^p - a$.

Indice : Utiliser la formule du binôme de Newton et le fait que p divise $\binom{p}{k}$ pour $1 \leqslant k \leqslant p-1$.

Annexe A

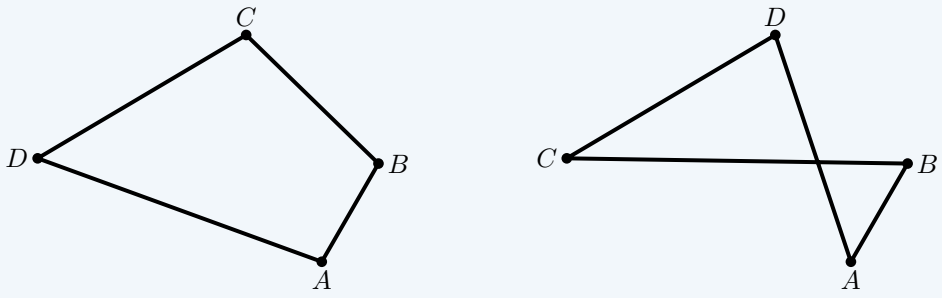
Rappels de géométrie

Ce chapitre rassemble quelques notions élémentaires de géométrie considérées comme préalables au cours. Ces notions, normalement déjà acquises, sont rappelées ici afin de fixer les définitions et les notations qui seront utilisées dans la suite, et de fournir au besoin une référence rapide.

A.1 Parallélogrammes, carrés et rectangles

Définition A.1: (Quadrilatère)

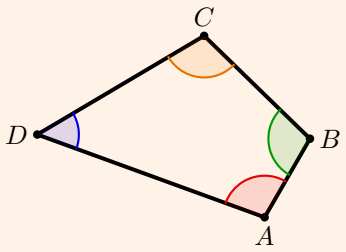
Un ***quadrilatère*** $ABCD$ est la donnée de quatre points $A, B, C, D \in \mathcal{P}$ non alignés.



Un quadrilatère est dit ***convexe*** si ses côtés ne se croisent pas (figure de gauche), et non convexe si deux de ses côtés se croisent (figure de droite).

Proposition A.2

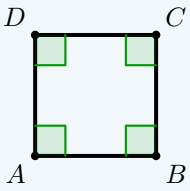
La somme des angles d'un quadrilatère convexe est de $0 \equiv 2\pi$.



$$\widehat{CBA} = \widehat{BAD} = \widehat{ADC} = \widehat{DCB} = 2\pi$$

Définition A.3: (Carré)

Un ***carré*** est un parallélogramme dont les côtés sont tous égaux et dont les angles sont égaux.



L'***aire*** d'un carré est égale à AB^2, où AB est la longueur de son côté $[AB]$.

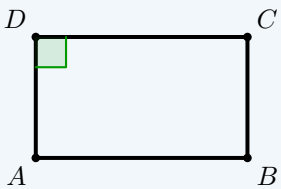
Proposition A.4

(i) Les angles d'un carré sont tous égaux à $\frac{\pi}{2}$ (angle droit) ;

(ii) $ABCD$ est un carré $\iff$ ses diagonales sont de même longueur et sont perpendiculaires.

Définition A.5: (Rectangle)

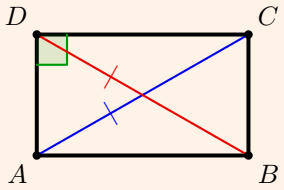
Un ***rectangle*** est un parallélogramme dont un angle est droit.



L'***aire*** d'un rectangle est égale à $AB \cdot BC$.

Proposition A.6

Un parallélogramme est un rectangle $\iff$ ses diagonales sont de même longueur.



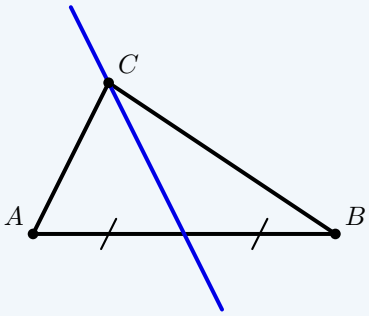
A.2 Triangles

Définition A.7: (Triangle)

Un ***triangle*** ABC est la donnée de trois points $A, B, C \in \mathcal{P}$ non alignés.

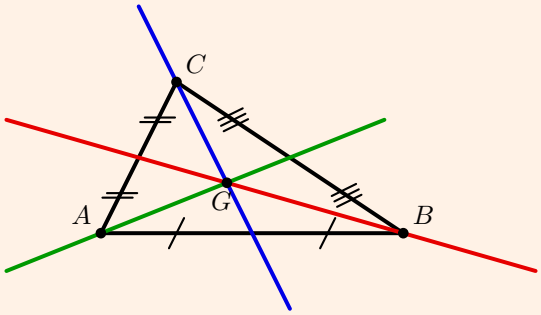
Définition A.8: (Médianes)

On appelle ***médianes*** de ABC les trois droites passant par un sommet et par le milieu du côté opposé.



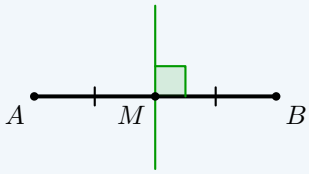
Proposition A.9

Les médianes de ABC sont concourantes (c-à-d elles se coupent toutes au même point). Ce point d'intersection est le centre de gravité de ABC, noté G



Définition A.10: (Médiatrice)

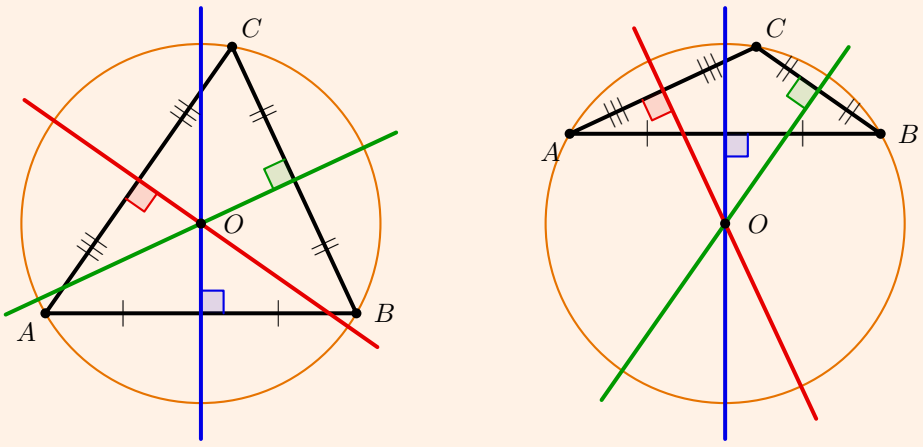
La ***médiatrice*** du segment $[AB]$ est la droite perpendiculaire à (AB) passant par le milieu de $[AB]$.



$$AM = MB$$

Proposition A.11

Les médiatrices de ABC se coupent en le centre du cercle circonscrit au triangle ABC noté O.

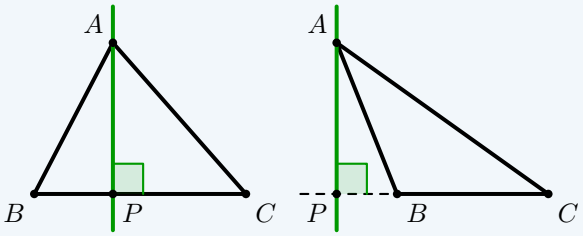


$$OA = OB = OC$$

⚠ **Remarque** Le centre du cercle circonscrit d'un triangle n'est pas forcément situé à l'intérieur du triangle, comme l'illustre la figure de droite de la proposition précédente. Cette situation a lieu dès qu'un des angles du triangle est supérieur à $\frac{\pi}{2}$.

Définition A.12: (Hauteurs d'un triangle)

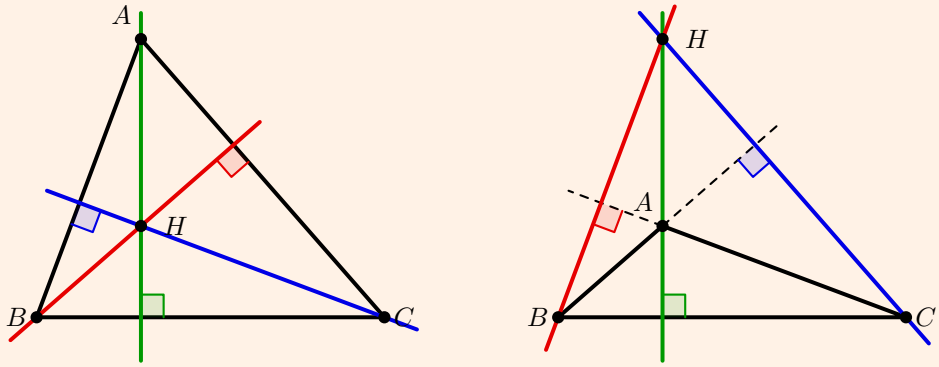
On appelle ***hauteurs*** de ABC les trois droites passant par un sommet et perpendiculaires à la droite qui supporte le côté opposé.



Dans les deux cas, la droite (AP) est la hauteur issue de A.

Proposition A.13

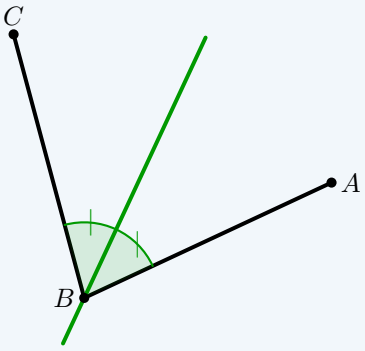
Les hauteurs de ABC sont concourantes en l'orthocentre H.



⚠ **Remarque** L'orthocentre d'un triangle n'est pas forcément situé à l'intérieur du triangle, comme l'illustre la figure de droite de la proposition précédente.

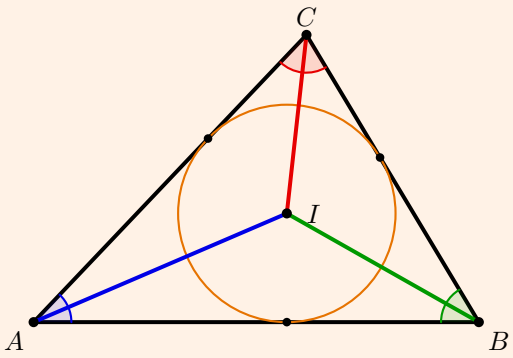
Définition A.14: (Bissectrice)

La ***bissectrice*** d'un angle est la droite issue de son sommet qui partage cet angle en deux angles de même mesure.



Proposition A.15

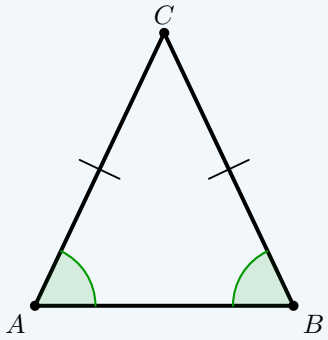
Les bissectrices de ABC sont concourantes en le centre du cercle inscrit dans ABC.



Définition A.16: (Triangle isocèle)

Soit le triangle ABC. Les trois situations suivantes sont équivalentes :

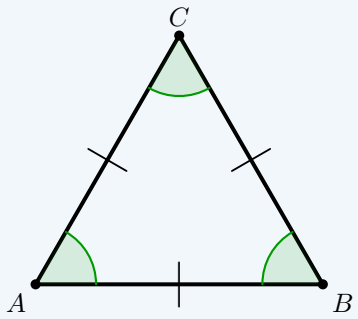
- ***(i)*** ABC est ***isocèle*** en C ;
- ***(ii)*** $AC = BC$;
- ***(iii)*** $\widehat{BAC} = \widehat{ABC}$.



Définition A.17: (Triangle équilatéral)

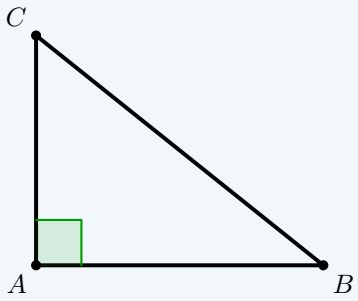
Soit le triangle ABC. Les trois situations suivantes sont équivalentes :

- ***(i)*** ABC est ***équilatéral*** ;
- ***(ii)*** $AB = BC = CA$;
- ***(iii)*** $\widehat{ABC} = \widehat{BCA} = \widehat{CAB}$.



Définition A.18: (Triangle rectangle)

Un triangle est un ***triangle rectangle*** s'il possède un angle droit. Le triangle ABC suivant est ***rectangle en*** A :



Annexe B

Relations d'équivalence

Nous allons nous intéresser ici aux relations qui servent à regrouper les éléments d'un ensemble par « familles ». On pourrait par exemple définir une relation qui regroupe les cartes d'un jeu de cartes par couleurs : c'est une relation d'équivalence.

Définition B.1: (Relation)

Soit E un ensemble. Une ***relation*** $\mathcal{R}$ sur E établit, entre certains éléments de E, un lien.
Si $x, y \in E$, on écrit

$$x \mathcal{R} y$$

pour signifier que x est en relation avec y.

Exemple

Le symbole $<$ définit une relation sur $\mathbb{R}$: deux nombres réels x et y sont en relation lorsque x est strictement plus petit que y. On écrit alors $x < y$.

Définition B.2: (Relation d'équivalence)

Soit E un ensemble. On dit que la relation $\sim$ est une ***relation d'équivalence*** si $\sim$ est :

Réflexive : $\forall x \in E, \quad x \sim x$;

Symétrique : $\forall x, y \in E, \quad x \sim y \implies y \sim x$;

Transitive : $\forall x, y, z \in E, x \sim y \wedge y \sim z \implies x \sim z$.

Exemple

Si $E = \{\text{les habitants du Québec}\}$, on peut définir la relation suivante :

$$x \sim y \iff x \text{ et } y \text{ ont le même prénom.}$$

Il s'agit bien d'une relation d'équivalence. Sans en faire une preuve rigoureuse, on remarque tout de même ceci :

- Alex Dumas $\sim$ Alex Dumas ;
- Alex Dumas $\sim$ Alex Smith $\iff$ Alex Smith $\sim$ Alex Dumas ;
- Alex Dumas $\sim$ Alex Smith $\wedge$ Alex Smith $\sim$ Alex Bouchard $\implies$ Alex Dumas $\sim$ Alex Bouchard.

Exemple

Soit E un ensemble quelconque et considérons la relation $\sim$ sur E définie par :

$$x \sim y \quad \iff \quad x = y.$$

Autrement dit, $\sim$ est l'égalité sur E. Alors $\sim$ est une relation d'équivalence :

$$x = x, \quad x = y \iff y = x, \quad \text{et si } x = y \text{ et } y = z, \text{ alors } x = z.$$

B.1 Classes d'équivalence et ensemble quotient

Plongeons un peu plus profondément dans l'abstraction.

Définition B.3

Soit E un ensemble et $\sim$ une relation d'équivalence sur E.

1. La ***classe d'équivalence de*** $a \in E$ est le sous-sensemble de E
$$[a] \quad = \quad \{x \in E \,|\, x \sim a\}.$$
2. Une ***classe d'équivalence*** de $\sim$ est un sous-ensemble A de E, tel qu'il existe $a \in E$ vérifiant $A = [a]$.
3. L'ensemble des classes d'équivalence est noté $E/\!\sim$ et est appelé ***l'ensemble quotient de*** E ***par*** $\sim$.

Remarque

- L'ensemble quotient $E/\!\sim$ est un objet de première importance en mathématiques. Il est très important de bien en comprendre la nature : les éléments de $E/\!\sim$ sont les classes d'équivalence de $\sim$, en d'autres termes, des sous-ensembles de E. Donc $E/\!\sim \subseteq \mathcal{P}(E)$.
- Une classe d'équivalence n'est jamais vide : $a \in [a]$ car $a \sim a$.

Exemple

On reprend dans l'ordre les deux exemples précédents.

- $\{$les habitants du Québec$\}/\!\sim$ est en bijection avec l'ensemble des prénoms représentés au Québec.
- Dans le cas de la relation " $=$ ", les classes d'équivalence sont les singletons de E, c'est-à-dire les sous-ensembles à un élément de E. Donc $E/\!=$ est « en bijection » avec E.

Proposition B.4

Soit $\sim$ une relation d'équivalence sur E et $x, y \in E$, alors

(i) $x \in [y] \iff [x] = [y]$;

(ii) $[x] \cap [y] \neq \emptyset \iff [x] = [y]$. Autrement dit, deux classes d'équivalence $\lambda, \lambda' \in E/\!\sim$ sont disjointes si et seulement si $\lambda \neq \lambda'$.

Démonstration

(i) $(\Longrightarrow)$ Supposons que $x \in [y]$ (c-à-d $x \sim y$). Il faut montrer une double inclusion.

$[x] \subseteq [y]$ **:** Soit $z \in [x]$. On a alors $z \sim x$ et $x \sim y$. Par transitivité de $\sim$, on obtient $z \sim y$. Ainsi $z \in [y]$ et donc $[x] \subseteq [y]$.

$[y] \subseteq [x]$ **:** Soit maintenant $z \in [y]$. On a alors $z \sim y$ et $y \sim x$. Comme auparavant, on peut conclure par transitivité de la relation $\sim$ que $z \in [x]$ et donc que $[y] \subseteq [x]$.

$(\Longleftarrow)$ La réciproque est triviale.

(ii) $(\Longrightarrow)$ Si $[x] \cap [y] \neq \emptyset$, alors il existe $z \in [x] \cap [y]$. Donc $x \sim z$ et $z \sim y$. D'où $x \sim y$. Donc $x \in [y]$ et $y \in [x]$. Par *(i)* on conclut à l'égalité.

$(\Longleftarrow)$ La réciproque est triviale.

B.2 Système de représentants des classes d'équivalence

Si on prend la relation d'équivalence sur l'ensemble d'un jeu de cartes : deux cartes sont en relation si et seulement si elles sont de même couleur. Alors les classes d'équivalences des cartes sont en bijection avec l'ensemble des couleurs : à chaque classe d'équivalence correspond une couleur. C'est là que réside l'idée de système de représentants.

Définition B.5: (Système de représentants)

Soit $\sim$ une relation d'équivalence sur E. Un sous-ensemble I de E est ***un système de représentants des classes d'équivalence*** de $\sim$ si pour tout classe d'équivalence $A \in E/\!\sim$, il existe un unique $x \in I$ tel que $A = [x]$. Les éléments de I sont les ***représentants***.

Exemple

Prenons $f : \mathbb{R} \to \mathbb{R}$ la fonction définie par $f(x) = x^2$. Regardons la relation d'équivalence sur E :

$$x \sim y \iff f(x) = f(y).$$

Alors $I = \mathbb{R}^+$ est un système de représentants des classes d'équivalence de R. En effet, dans chaque classe $A = \{-a, a\} \in E/\!\sim$ il n'y a qu'un unique élément positif $x \in I$ et on a bien $[x] = A$.

PROPOSITION B.6

Soient E un ensemble fini, $\sim$ une relation d'équivalence sur E, et I un système de représentants de $E/\!\sim$. Alors

$$\left|E/\!\sim\right| = |I|.$$

DÉMONSTRATION Notons $k = |I|$. Par définition de I, on peut alors écrire $I = \{x_1, \dots x_k\}$ avec les x_i distincts. Il s'ensuit que $E/\!\sim = \{[x_1], \dots, [x_k]\}$ et donc que $\left|E/\!\sim\right| = k = |I|$.

■

B.3 Exercices

EXERCICE B.1 Soit $\sim$ la relation sur $\mathbb{R}$ définie par :

$$x \sim y \iff |x| = |y|.$$

(a) Montrer que c'est une relation d'équivalence et déterminer son ensemble quotient $\mathbb{R}/\!\sim$.

(b) Montrer que $\mathbb{R}^+$ est un système de représentants des classes d'équivalence de $\sim$.

EXERCICE B.2 Sur l'ensemble $E = \{1, 2, 3, \dots, 30\}$, définissons la relation $\sim$ par : $i \sim j$ si tout nombre premier p qui divise i divise aussi j. Vérifier que $\sim$ est bien une relation d'équivalence, écrire l'ensemble quotient et trouver un système de représentants.

EXERCICE B.3 Soient $\sim_a$ et $\sim_b$ deux relations d'équivalence sur E. Montrer que la relation $\sim$ sur E définie par :

$$x \sim y \iff (x \sim_a y \ \wedge \ x \sim_b y)$$

est une relation d'équivalence. Décrire les classes d'équivalence de $\sim$ en fonction de celles de $\sim_a$ et de $\sim_b$.

Références

[Audin 2006] M. Audin ***Géométrie***, EDP Sciences (2006).

[Damphousse 2002] P. Damphousse, ***L'arithmétique ou l'art de compter***, Quatre à quatre, Édition le Pommier (2002).

[Hohlweg 2013] C. Hohlweg, ***MAT1006 — Arithmétique et géométrie classique***, notes de cours, UQAM, version du 13 mai 2013.

[Liret et Martinais 2003] F. Liret et D. Martinais, ***Algèbre 1re année, 2e édition***, Dunod (2003).

[Rittaud 2000] B. Rittaud, ***La géométrie classique***, Quatre à quatre, Édition le Pommier (2000).

[Smullyan 1997] R. Smullyan, ***Le livre qui rend fou***, Dunod (1997).

[XMaths] Les cours de mathématiques disponibles sur `http://xmaths.free.fr/TS/index.htm`.

[Lee] K. P. Lee, ***A Guide to Writing Mathematics***, Purdue University Calumet, sans date.

Index