MAT 1150
ARITHMÉTIQUE ET GÉOMÉTRIE CLASSIQUE

Christophe Hohlweg et François Bergeron

2 décembre 2014

UQÀM **Université du Québec à Montréal**
Département de mathématiques
Case postale 8888, Succursale Centre-Ville
Montréal (Québec) H3C 3P8

Table des matières

Introduction

En simplifiant probablement un peu trop, on peut dire que les mathématiques étudient les « *les abstractions, les structures abstraites, et leurs interactions* ». Parmi ces abstractions, et structures abstraites, celles qui relèvent de la géométrie euclidienne et de l'arithmétique classique restent encore parmi celles qui sont incontournables dans une formation mathématique. D'abord, parce que beaucoup des idées développées à partir de la Grèce Antique sont encore d'actualité à ce jour ; mais aussi parce que l'un des meilleurs moyens de s'initier au langage et au raisonnement mathématique, ainsi qu'à l'algèbre et à la géométrie moderne est de suivre (en partie) l'évolution des idées mathématiques depuis la géométrie de l'école pythagoricienne jusqu'à ce jour.

Le but de ce texte est donc de retracer une partie du développement des idées qui ont mené à la conception moderne des mathématiques, en soulignant combien l'abstraction fournit un outil extraordinairement efficace pour orienter le développement des nouveaux concepts essentiels à la pensée mathématique.

Pour bien comprendre tout le cheminent accompli par l'humanité dans ce domaine, il est important de rappeler les conditions dans lesquelles se retrouvaient les penseurs et constructeurs de l'époque. Les outils concrètement à leur disposition étaient hautement limités. En effet, pendant longtemps les seuls outils de mesures spatiales étaient la corde, la règle, et le compas. Ces limitations déterminent les questions que les mathématiciens grecs ont considérées, entre autres dans leur recherche de solutions pratiques aux problèmes concrets de constructions (en architecture, construction navale, etc.).

Nous allons donc entreprendre notre exploration en nous replaçant dans le contexte de l'époque, pour évoluer rapidement vers une approche plus moderne. Ce faisant, nous allons voir comment le besoin de rigueur dans la réflexion mathématique s'est imposé comme garant de la justesse des conclusions. De plus, nous verrons combien l'importance de définitions claires facilite grandement la réflexion. C'est d'ailleurs là une des particularités encore trop méconnues des mathématiques. En fait, après un très long cheminement pas toujours facile, les mathématiciens ont compris qu'il est impossible d'étudier correctement une notion sans en donner une définition claire et précise. Ils ont aussi constaté qu'il en résulte une surprenante efficacité.

Délaissant l'approche historique, nous survolerons ensuite plusieurs des notions mathématiques de

géométrie et d'arithmétique qui fondent la réalité mathématique moderne.

À la fin de chaque chapitre se trouve une liste d'exercices classés en trois catégories : les exercices de type A, ceux de type B, ainsi que les exercices encadrés. Les exercices de type A sont destinés à s'assurer de la bonne compréhension d'une méthode ou d'une définition. Il est donc important de savoir faire ces exercices ; des solutions complètes ou partielles sont parfois fournies à titre d'autocorrection. Les exercices de type B sont des problèmes de niveau moyen à difficile, tout comme les exercices encadrés. Toutefois, les exercices encadrés sont destinés à être traités lors des séances de travaux pratiques, contrairement aux exercices de type B. Ces derniers sont donc des exercices supplémentaires pour celles et ceux qui désirent s'entraîner davantage. Finalement, les démonstrations laissées en exercice tout au long du recueil figurent aussi dans cette liste d'exercice et portent l'étiquette « Démonstration du cours ». Ces démonstrations sont classées de la même manière que les autres exercices.

Certaines sections ou annexes apparaissent avec le symbole (*). Ces sections proposent des pistes de réflexion, ou ouvrent la porte à d'autres domaines.

Chapitre 1

Géométrie élémentaire du plan et de l'espace

L'objectif de ce chapitre est multiple. Tout d'abord, nous allons donner une idée du rôle des mathématiques en tant qu'outil conceptuel pour aborder « scientifiquement » la réalité. Bien entendu, cela n'en sera qu'une présentation très partielle, puisque le spectre des mathématiques actuelles, ainsi que leurs utilisations en science, est évidemment trop vaste pour n'être abordés que dans un seul cours. On commencera par souligner comment le développement de plusieurs outils mathématiques contemporains remonte à l'Antiquité, et plus particulièrement au temps de la Grèce Antique [1] avec le développement de la *géométrie euclidienne du plan et de l'espace*. En donner une perspective historique sera un de nos premiers objectifs. Ainsi, nous aurons l'occasion d'observer que le développement des mathématiques est intimement au développement de la culture (au sens large) et de la technologie ; et que cette relation est réciproque.

Une autre contribution fondamentale des artisans de la géométrie euclidienne, est d'avoir développé l'approche déductive en mathématique, et d'en avoir montré la puissance et la nécessité. Notre second objectif est donc de montrer cette puissance du langage et du raisonnement mathématique, ainsi que l'efficacité qui résulte d'une bonne maîtrise de ceux-ci. Ainsi, nous espérons amener le lecteur à saisir la différence entre la vérité absolue des énoncés mathématiques démontrés rigoureusement, et la vérité toute relative d'autres approches utilisées pour décrire la réalité. Bien que les résultats présentés dans ce chapitre soient parfois (sinon souvent) déjà connus du lecteur, l'accent sera mis sur l'élaboration de démonstrations de ces résultats qui deviendront de plus en plus rigoureuses. Il est remarquable qu'en un certain sens, les mathématiciens de la Grèce antique fussent déjà d'accord avec l'impression suivante d'un physicien moderne bien connu :

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

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 ? – Albert Einstein.

1.1 Introduction

Les « architectes » et ouvriers de l'époque des Grecs anciens ne disposaient que de peu d'outils pour aborder les problèmes concrets de construction auxquels ils étaient confrontés. Nous replaçant (à peu près [2]) dans leur contexte, nous allons admettre que nous ne disposons que d'outils très limités pour nous attaquer à des tâches plus complexes, comme celles de construire des triangles équilatéraux, des carrés, des cubes, des pyramides, ou encore de tracer des parallèles. Nous aurons aussi besoin de rapporter des longueurs, les additionner, les multiplier, etc.

Dans un premier temps, nous nous contenterons d'une approche assez intuitive des objets considérés tels que : points, droites, segments, angles, perpendiculaires, droites parallèles, plans, espace, longueurs ou distances. Ce faisant, nous suivrons (plus ou moins) une évolution historique des concepts de la géométrie. Des définitions plus satisfaisantes, dans le contexte de la théorie des ensembles, seront données au chapitre 3. On se permettra tout de même dès maintenant l'utilisation de certains symboles du langage mathématique moderne. Nous invitons à ce propos le lecteur à lire au préalable l'annexe A, et en nous y référant au besoin au cours de sa lecture.

Comme c'est souvent le cas en mathématiques, on commence par spécifier les notations utilisées, et définir (naïvement dans un premier temps) les objets mathématiques que nous allons manipuler.

Ainsi, on dénote
- par $\mathcal{P}$ le **plan** (pour lequel on a des notions de longueur et largeur) ;
- par $\mathcal{E}$ l'**espace** (pour lequel on a des notions de longueur, largeur et épaisseur) ;
- par $A \in \mathcal{P}$ le fait qu'on a un **point** A dans le plan $\mathcal{P}$ (le symbole « $\in$ » se lit « appartient à » ou « est élément de ») ;
- par (AB) l'unique (c'est un principe) **droite** passant par des points A et B du plan $\mathcal{P}$;
- par $[AB]$ le segment de droite allant du point A au point B ; et
- par AB la longueur du segment $[AB]$.

À partir de ces objets de base, on en construit d'autres comme les suivants.
- Un **triangle** ABC est déterminé par trois **sommets**, qui sont des points A, B et C du plan $\mathcal{P}$. Ses **côtés** sont les segments $[AB]$, $[BC]$, et $[AC]$, et ses **angles** (intérieurs) sont $\widehat{ABC} = \widehat{CBA}$, $\widehat{BAC} = \widehat{CAB}$ et $\widehat{ACB} = \widehat{BCA}$. À la Figure 1.1, ces diverses composantes sont illustrées, avec les longueurs respectives des segments $[BC]$, $[AC]$ et $[AB]$, du triangle ABC, dénotées par

2. Pour en savoir plus, et avec plus de rigueur historique, voir **ce texte** rédigé par une équipe de l'Université de Strasbourg : *Histoire des mathématiques*. Pour y accéder, consulter la page web du cours.

$a = BC$, $b = AC$, et $c = AB$.

— Si d et d' sont deux droites du plan $\mathcal{P}$, on dénote par $d \perp d'$ le fait que d soit **perpendiculaire** à d', et par $d \parallel d'$ le fait que d soit **parallèle** à d'.

— Soit O et A deux points du plan $\mathcal{P}$. Le **cercle** $\mathscr{C}$, 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

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

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

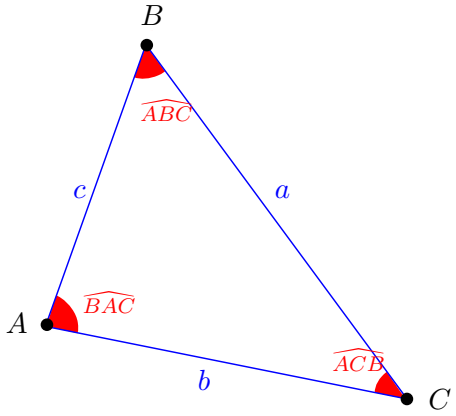


FIGURE 1.1 – Les composantes d'un triangle.

Une fois ces objets introduits, on cherche à en dégager les propriétés. Celles-ci prendront la forme d'énoncés mathématiques, pour lesquels on donnera un « certificat » de vérité, c'est-à-dire une démonstration.

Construction avec la règle et le compas. Rappelons que, dans l'antiquité, les mathématiciens n'avaient pas (loin de là) notre conception moderne des nombres, comme entités abstraites non liées à un contexte spécifique. Pour les mathématiciens grecs, les nombres (réels) se concevaient plutôt concrètement comme longueurs de segments, obtenus par des « constructions géométriques explicites». Autrement dit, un nombre n'avait de sens pour eux que s'il pouvait s'obtenir par une construction géométrique précise, basée elle-même sur d'autres longueurs (nombres) déjà déterminées. Les propriétés des nombres, et des opérations sur ceux-ci, se devaient d'être liées à une interprétation géométrique. Cette approche, qui lie les propriétés algébriques des nombres à une démarche géométrique, trouve d'ailleurs écho jusqu'à nos jours. En particulier, dans son livre classique Geometric Algebra (datant de 1957), Emil Artin montre (d'un point de vue moderne) comment de nombreuses propriétés des corps de nombres sont liées à des résultats de géométrie euclidienne. Les mathématiciens grecs n'avaient donc peut-être pas une approche si démodée que cela.

Tout cela explique beaucoup la nature de plusieurs des problèmes que les mathématiciens grecs se

sont posés. Il n'est pas inutile de souligner que certains de ces problèmes ont demandé de nombreux siècles avant de trouver réponse. Ainsi, le problème de la « quadrature du cercle» (qui consiste à déterminer s'il est possible de construire avec une règle et un compas un carré d'aire π) est resté mystérieux [3]. Jusqu'au XVIII^{e} siècle, quand on a finalement réussi à démonter qu'une telle construction est impossible. Leurs règles de construction étaient simples, et basées sur les technologies (assez rudimentaires) disponibles à l'époque, les voici :

On se donne :
- une unité (correspondant à un bout de bois par exemple) ;
- une règle non graduée (permettant de tracer des droites et segments) ;
- un compas (permettant de tracer des cercles).

On peut alors, par exemple :
- tracer avec la règle le segment $[AB]$, ayant pour extrémités des points A et B, déjà « construits » au préalable ;
- tracer avec la règle la droite (AB), passant par des points A et B, déjà « construits » ;
- tracer avec le compas le cercle de centre O et de rayon OA, pour des points O et A, déjà « construits ».

Comme on va le constater, il est intéressant d'ainsi décrire de nouvelles constructions à partir de celles mises au départ à notre disposition. On se constitue ainsi, étape par étape, un répertoire de constructions (un peu comme quand on programme avec un langage de programmation), partant des constructions très simples données au départ vers des constructions de plus en plus complexes (et de plus en plus intéressantes). Une première est la suivante.

Report de longueurs avec la règle et le compas Une première constatation est qu'on peut « reporter » des longueurs, avec les outils mis à notre disposition. Plus précisément, étant donné un segment $[AB]$ de longueur AB, et un point C, on peut facilement construire un (en fait plusieurs) segment(s) $[CD]$ de longueur AB, avec $CD = AB$? En effet, avec le compas que l'on pointe en A et que l'on ouvre jusqu'à B (en le conservant ainsi ouvert), on prend la mesure du segment AB. On trace ensuite (avec le compas tel qu'il est) le cercle de rayon AB ayant pour centre C, puis le segment $[CD]$ (tracé avec la règle). Bien évidemment [4], $CD = AB$, puisque c'est le rayon du cercle tracé.

3. Cette question est restée sans réponse pendant si longtemps, qu'on en a fait l'expression courante : « Chercher la quadrature du cercle», pour dire qu'on s'attaque à une entreprise vouée à l'échec.

4. Attention, affirmer qu'on a une évidence est souvent risqué en mathématiques.

1.2 Quelques résultats classiques

Pour mieux illustrer notre réflexion mathématique, nous allons d'abord revisiter deux résultats classiques bien connus. Nous chercherons à comprendre pourquoi ces énoncés sont « vrais », en dégageant les étapes qui en permettent la démonstration. Dans un premier temps, nos démonstrations ne seront qu'approximatives, parce que nous n'aurons pas encore bien clarifié notre démarche logique (voir Section 1.7). C'est d'ailleurs dans son livre « Les Éléments » que Euclide d'Alexandrie (cerca -325 à cerca -265) décrit cette démarche pour la première fois dans l'histoire des mathématiques.

1.2.1 Somme des angles d'un triangle

On considère l'énoncé suivant, et sa « démonstration » du point de vue des Grecs.

Proposition 1.1. *La somme des angles d'un triangle est un* **angle plat**, *c'est-à-dire de mesure* π *en radians (ou* 180 *degrés).*

Esquisse de démonstration. On raisonne comme suit. Soit ABC un triangle, et soit d l'unique (voir Section 1.2.4) droite parallèle à la droite (AB) passant par C. Plaçons des points X et Z sur d, et un point Y sur (BC) afin de former des demi-droites (voir la Figure 1.2 ci-dessous [5]). En reportant les angles, on obtient :

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

■

Cette « démonstration » suppose qu'on ai justifié au préalable certains énoncés, entre autres les suivants qui ont été invoqués dans la preuve.

des angles « opposés » sont égaux, et les angles sont invariants par « translation ».

Avant de ce faire, il est pratique de leur donner une forme mathématique plus explicite.

Énoncé 1 : Soit d et d' deux droites sécantes. Alors, les angles opposés par le point d'intersection sont égaux. Cet énoncé se « formule » plus précisément de la façon suivante. Pour

5. Il y a tellement d'imprécisions dans la phrase qui précède qu'il est nécessaire de l'expliquer par un dessin. Qu'arrive-t-il si on échange les rôles de X et de Z, ou si Y se trouve à gauche de A ?

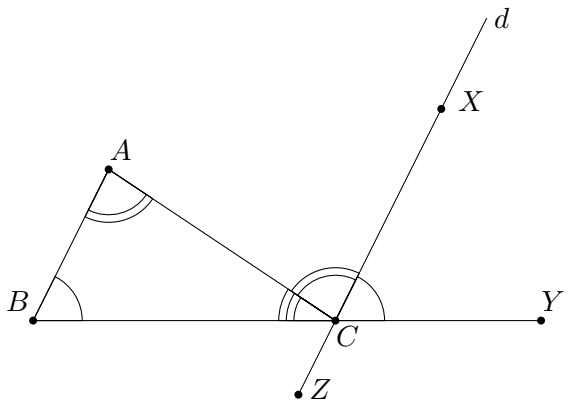


FIGURE 1.2 – La somme des angles intérieurs d'un triangle.

tout choix de deux points X et Y sur d, et de deux points X' et Y' sur d', tels que le point d'intersection A de d et d' se trouve entre X et Y et entre X' et Y', on a les égalités suivantes :

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

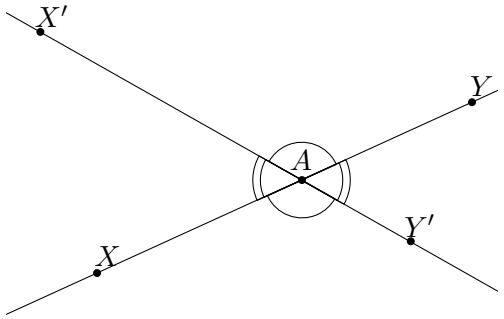


FIGURE 1.3 – Égalité d'angles opposée.

Énoncé 2 : Les angles sont invariants par translation. Autrement dit : soit d et d' deux droites parallèles, et d'' une droite sécante à d et d', en posant des points comme avant, on obtient (en se servant aussi de l'énoncé 1) :

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

Que penser de ces énoncés ? Sont-ils vrais ? Peuvent-ils se démontrer ? Si oui, on est certain que la

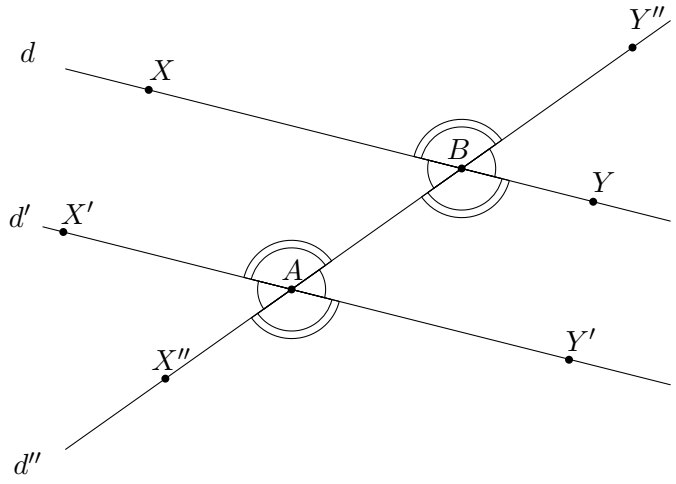


FIGURE 1.4 – Invariance d'angles par translation.

somme des angles d'un triangle est π ; si non ... on n'est certain de rien. Dans les faits :

— L'énoncé 1 peut se démontrer :

Démonstration de l'énoncé 1. $\widehat{X'AY} + \widehat{YAY'} = \pi = \widehat{X'AY} + \widehat{XAX'} \Rightarrow \widehat{YAY'} = \widehat{XAX'}$. De même pour l'autre égalité. ■

— L'énoncé 2 ne peut pas se démontrer ! C'est un **axiome**. Intuitivement, un axiome est une règle, une hypothèse, que l'on se donne et qui définit le contexte dans lequel on va produire des vérités mathématiques. En général, les axiomes ne sont pas le produit du hasard. Ils sont sélectionnés avec beaucoup de réflexion. En particulier, celui dont nous discutons est issu de la volonté des mathématiciens grecs de construire un modèle mathématique décrivant les réalités géométriques qu'ils observaient dans la nature. En quelque sorte, un axiome est une idéalisation d'une ≪loi de la nature≫ dont l'objectif est de servir de base à un modèle mathématique pour ce phénomène naturel. Nous reviendrons plus tard plus en détail sur les axiomes de la géométrie euclidienne. Donc, dans le cadre de la géométrie euclidienne où l'énoncé 2 est vrai, puis qu'il est posé en axiome, la somme des angles d'un triangle est π.

1.2.2 Triangles isométriques

Revenons aux triangles. Les triangles sont considérés par les mathématiciens grecs comme des objets élémentaires du plan : constitués de trois points distincts et non alignés, reliés par des arêtes ou

côtés, les triangles font partie d'un plan $\mathcal{P}$. Avant de passer à l'étude d'objets plus complexes (carrés, polygones, etc.), il est naturel de commencer par la comparaison de triangles afin d'en comprendre les différences et les similarités. Par exemple, on « observe » que lorsque deux triangles ont des côtés respectivement égaux, alors les angles adjacents aux côtés de même longueur paraissent aussi être égaux. Cette observation empirique n'est pas une preuve, mais ce « fait » apparent peut-il être démontré ? Commençons par le « mathématiser », en le précisant un peu plus.

Définition. Deux triangles sont dits **isométriques** (ou **congrus**) si leurs trois côtés sont respectivement isométriques (c.-à-d. de longueur égale). Voir la Figure 1.5.

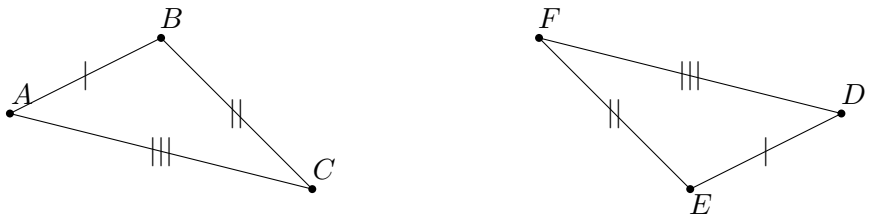


FIGURE 1.5 – Triangles isométriques

Énoncé 3 : Les énoncés suivants sont équivalents :

1. Deux triangles sont isométriques ;
2. Deux triangles ont deux côtés respectivement isométriques adjacents à un même angle. Voir Figure 1.6.

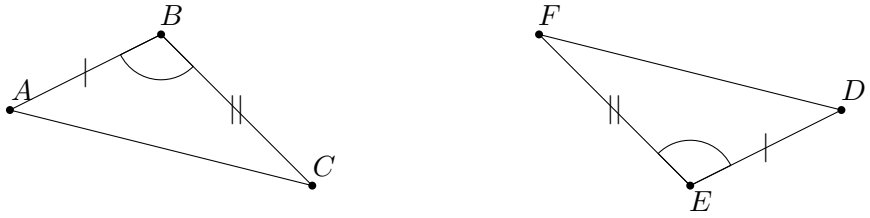


FIGURE 1.6 – Côtés isométriques adjacents à des angles égaux

3. Deux triangles ont un côté isométrique compris entre deux angles respectivement égaux. Voir Figure 1.7.

Remarque. Cette règle signifie que (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3).

Comment démontre-t-on que cet énoncé est vrai, et est-ce possible ? C'est en explorant ce genre de question que l'approche déductive des mathématiques s'est développée. Dans ce cas, et après beaucoup

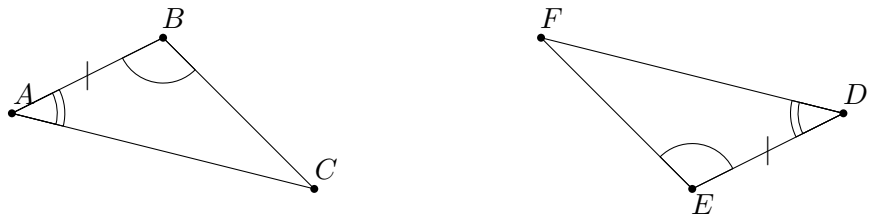


FIGURE 1.7 – Côtés isométriques adjacents à deux angles égaux

de tentatives, on est a été amené à conclure que l'énoncé 3 devrait aussi être considéré comme un axiome. Attention, il ne sera pas fréquent qu'on procède ainsi. Sinon, chaque fois qu'on est incapable de trouver une preuve, il suffirait de déclarer que l'énoncé considéré est un autre axiome. Au contraire, un des principes qui nous guideront est que le nombre d'axiomes doit rester très petit. Autrement dit, la liste des axiomes doit être maintenue au strict nécessaire [6]. Cela soulève une foule de questions profondes (et parfois même sans réponse) comme celle de savoir :

— quels sont les « bons » candidats à des axiomes ?
— quand en a-t-on assez ?
— quand en a-t-on trop ?
— sont-ils compatibles ?

Une partie des réponses vient de la pratique. On se convainc qu'on a « les bons axiomes » quand on constate qu'ils paraissent « évidents », et qu'on arrive à en déduire efficacement tous les énoncés qui nous intéressent. Par exemple, la propriété bien connue suivante se déduit de l'équivalence (1) $\Leftrightarrow$ (2), en alternant successivement les rôles de A B et C.

Corollaire 1.2. *Si deux triangles sont isométriques, alors leurs angles sont égaux.*

Remarque. On voit facilement que la réciproque de cet énoncé est fausse, c'est-à-dire que deux triangles dont les angles sont égaux ne sont pas forcément isométriques. Par exemple, on peut penser à deux triangles équilatéraux dont l'un est deux fois plus petit que l'autre. Dans le cas où deux triangles ont des angles qui sont deux à deux égaux, on dit qu'ils sont **semblables**. Ainsi donc, deux triangles isométriques sont toujours semblables, mais deux triangles semblables ne sont pas nécessairement isométriques.

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. Comme l'avons déjà souligné, le fait de clarifier les définitions facilite toujours la discussion mathématique. On rappelle donc que :

6. Il a fallu des siècles pour vérifier que l'axiome des parallèles est nécessaire en géométrie euclidienne, et beaucoup ont cru qu'il était superflu.

Définition. Un **parallélogramme** $ABCD$ est la donnée de quatre points A, B, C et D de $\mathcal{P}$ tel que $(AB) \parallel (CD)$ et $(AD) \parallel (BC)$. Voir Figure 1.8.

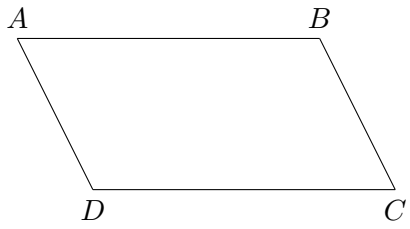


FIGURE 1.8 – Un parallélogramme $ABCD$.

Remarque. C'est un quadrilatère convexe (c.-à-d. non croisé).

Pour déterminer autrement (et plus facilement) que $ABCD$ est un parallélogramme, on a la règle suivante.

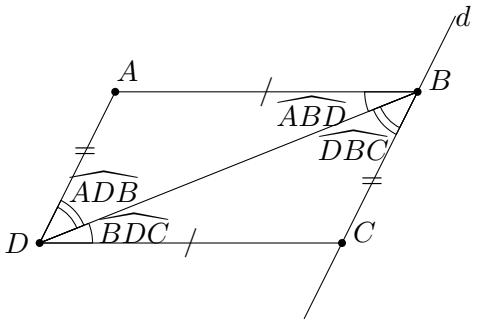
Proposition 1.3 (Règle du parallélogramme)**.** *Soit $ABCD$ un quadrilatère convexe. Les énoncés suivants sont équivalents :*

1. *$ABCD$ est un parallélogramme.*
2. *$AB = CD$ et $AD = BC$.*
3. *les diagonales de $ABCD$ se coupent en leur milieu.*
4. *$AB = CD$ et $(AB) \parallel (CD)$.*

Démonstration de la règle du parallélogramme. Montrons (1) $\Leftrightarrow$ (2) (pour le reste des équivalences, voir exercice 1).

($(1) \Longrightarrow (2)$) Afin de démontrer cette implication, il suffit de montrer que les triangles ABD et BCD sont isométriques. On a $\widehat{ADB} = \widehat{DBC}$ (en traçant la diagonale (BD)), car $(AD) \parallel (BC)$. De même, $\widehat{ABD} = \widehat{BDC}$ car $(AB) \parallel (CD)$. Ainsi, ABD et BDC sont isométriques, donc $AB = CD$ et $AD = BC$.

($(2) \Longrightarrow (1)$) L'hypothèse de départ est $AB = CD$ et $AD = BC$. On veut montrer 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 BDC 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 Construction de la parallèle à une droite donnée passant par un point donné.

On se donne une droite d et un point $A \notin d$, et on cherche à construire « l'unique » parallèle à d passant par A. Pour ce faire, on choisit deux points (distincts) C et D sur la droite d, à partir desquels

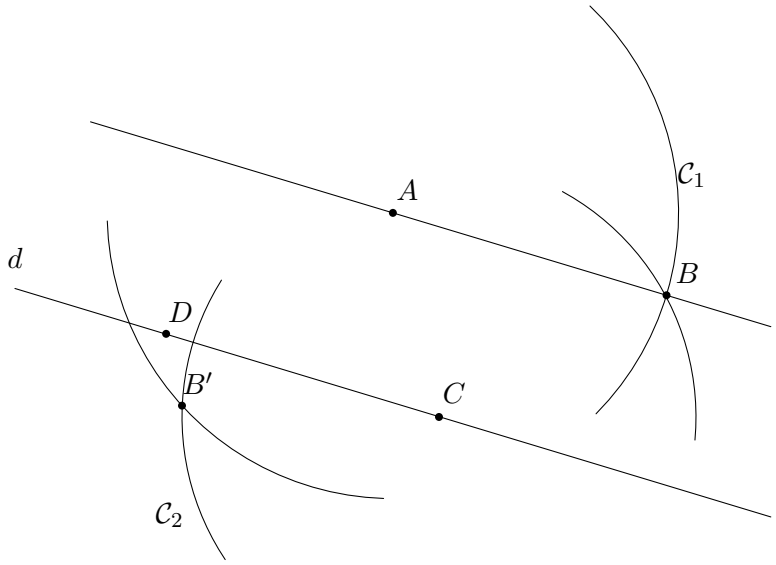


FIGURE 1.9 – Construction de la droite parallèle à d passant par A.

nous allons construire un point B de façon à ce que $ABCD$ soit un parallélogramme. Comme la règle du parallélogramme assure que $d = (CD) \parallel (AB)$, on aura ainsi construit une droite (AB) parallèle à d qui (par construction) passe par A. Le fait qu'il n'y en a pas d'autres sera discuté plus loin. Voir la figure 1.9.

Pour construire le point B tel que $AB = DC$ et $AD = BC$, on procède comme suit. 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 (soit convexe), c'est celui du même côté que A de d (sinon (AB) couperait d). Par construction du point B, les conditions 2. de la proposition sont satisfaites, et donc on a bien un parallélogramme. Il suffit alors de tracer la droite (AB), qui passant par les points A à B, pour obtenir la parallèle cherchée.

1.2.5 Première construction d'un angle droit

Pour poursuivre notre exploration, rappelons que :

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

Pour construire avec règle et compas des triangles rectangles, et incidemment des angles droits, on exploite la proposition suivante.

Proposition 1.4. *Soit $\mathcal{C}$ un cercle de centre O, soit $[BC]$ un diamètre de $\mathcal{C}$ et $A \in \mathcal{C} \setminus \{B, C\}$. Alors ABC est un triangle rectangle en A. Voir la figure 1.10.*

Démonstration de la proposition 1.4. Soit $A \in \mathcal{C}$ tel que $A \neq B, A \neq C$. 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 $[BC]$. On considère A' le seul point de la droite (AO) tel que O soit le milieu du segment $[AA']$. Forcément, A' se situe sur le cercle $\mathcal{C}$, puisque $AO = OA'$. Le quadrilatère $ACA'B$ a des diagonales qui se coupent en leur milieu O. C'est donc un parallélogramme. De plus, ces diagonales sont de même longueur ($BC = 2OB = 2OA = AA'$), c'est donc un rectangle (voir l'exercice 2). On conclu donc que ABC est un triangle rectangle en A. ■

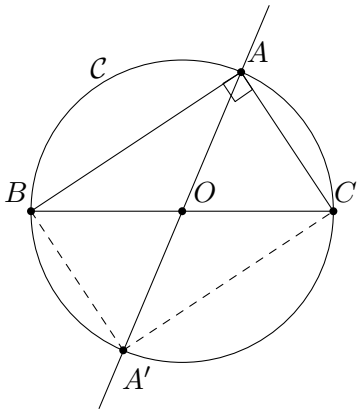


FIGURE 1.10 – Triangle rectangle inscrit dans un cercle.

Construction d'un angle droit et d'une équerre. Pour construire un angle droit, il suffit donc 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 pratiquement construire une équerre de prendre une planche de bois, d'y tracer un cercle, puis de tracer un diamètre, et enfin de choisir un point sur ce cercle qui n'est pas sur le diamètre. On découpe alors soigneusement le triangle obtenu pour obtenir un nouvel outil de précision.

1.3 Les théorèmes de Pythagore et de Thalès

Nous présentons ici les deux théorèmes qui sont sans nul doute les plus célèbres parmi ceux issus des recherches des mathématiciens grecs. Rappelons que l'aire d'un rectangle [7] est définie comme le produit des longueurs de ses côtés. Comme on montre facilement qu'un rectangle est séparé en deux triangles rectangles isométriques par une de ses diagonales, il est aussi naturel de définir l'aire d'un triangle rectangle comme étant égale à la moitié du produit de ses côtés adjacent à l'angle droit.

1.3.1 Théorème de Pythagore

Un des résultats mathématiques les plus connus de tous, mais aussi d'une grande utilité pratique et théorique, est certainement le suivant. On peut probablement parier (sans grand risque de perdre) qu'il est connu de tous les mathématiciens de l'univers (au cas où il y en ait ailleurs que sur notre planète [8]). Il est dû à Pythagore de Samos, né autour de -569 et mort autour de -475.

Théorème 1.5 (Théorème de Pythagore)**.** *Soit ABC un triangle, alors :*

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

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

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

7. Une petite question pour vos réflexions : comment définit-on l'aire en général ?
8. D'autant plus qu'il y a peu de chance qu'ils débarquent demain pour prouver que nous avons eu tort.

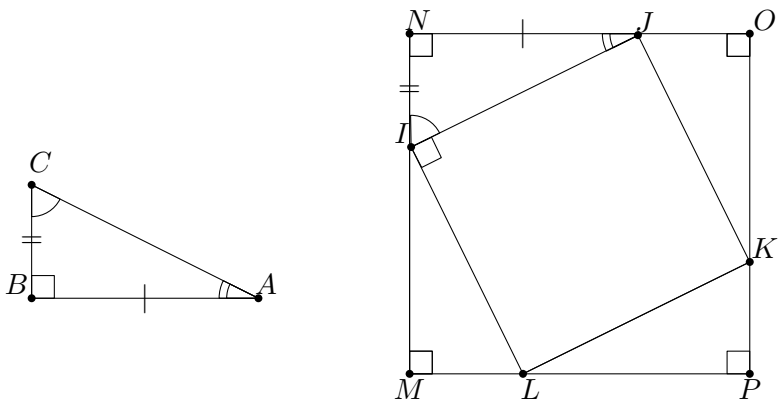


FIGURE 1.11 – Théorèm de Pythagore

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

Donc $IJKL$ est un carré. D'où $\text{Aire}(MNOP) = \text{Aire}(IJKL) + 4 \cdot \text{Aire}(ABC)$

$\implies (AB + BC)^2 = AC^2 + 4 \cdot (AB \cdot BC)/2$

$\implies AC^2 = AB^2 + BC^2$.

($\Longleftarrow$) 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), alors montrons 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 :

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

De $AB = AI + IB$ (l'autre possibilité $AI = AB + IB$ se traite façon analogue) et $AB^2 + BC^2 = AC^2$, on déduit que :

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

Donc ABC est rectangle en B. ■

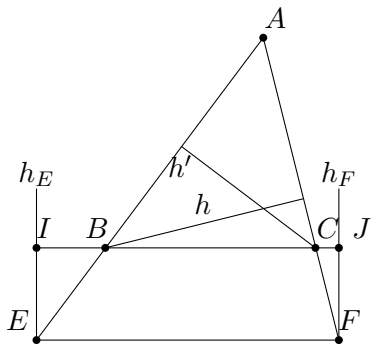


FIGURE 1.12 – Théorème de Thalès

Application. Le théorème de Pythagore permet entre autres de tester calculatoirement (par des mesures de longueur) si deux droites sont perpendiculaires. Pour cela, il suffit de nommer A le point d'intersection de ces deux droites, de prendre un point B sur la première et un point C sur la deuxième puis de calculer AB^2, AC^2 et BC^2. Si $AB^2 + AC^2 = BC^2$, 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 un autre résultat majeur issu des travaux des géomètres de la Grèce Antique, dû à Thalès de Milet, ayant vécu de -625 à -574.

Théorème 1.6 (Théorème de Thalès)**.** *Soit ABC et AEF deux triangles tels que $B \in (AE)$ et $C \in (AF)$ (voir figure 1.3.2).*

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

(ii) Réciproquement, si $AE/AB = AF/AC$, 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

$$\left.\begin{array}{l}\text{Aire}(ABC) = (AC \cdot h)/2 \\ \text{Aire}(ABF) = (AF \cdot h)/2\end{array}\right\} \quad \text{implique que} \quad AF/AC = \text{Aire}(ABF)/\text{Aire}(ABC).$$

De même, avec la hauteur h' issue de C dans ABC, on montre que

$$AE/AB = \text{Aire}(AEC)/\text{Aire}(ABC).$$

Il faut maintenant montrer que Aire(AEC) = Aire(ABF), ou encore que Aire(BCE) = Aire(BCF), puisque Aire(AEC) = Aire(ABC) + Aire(BCE) et Aire(ABF) = Aire(ABC) + Aire(BCF). Soit 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. Comme $(BC) \parallel (EF)$, alors $h_E \parallel h_F$ et donc $IJFE$ est un rectangle. Ainsi $IE = JF$ et on obtient que

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

D'où $AF/AC = AE/AB$. La preuve de l'égalité $AE/AB = EF/BC$ est laissée en exercice (exercice 8).

(ii) Soit d la parallèle à (BC) passant par E et soit F' l'intersection de d avec AF. Par (i), on a que

$$AE/AB = AF/AC = AF'/AC.$$

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

1.3.3 Les nombres constructibles

Pour étendre notre répertoire d'outils (à l'époque où ces outils n'existent pas encore) on aimerait disposer de moyens pour construire des graduations régulières sur une règle sans marques. De même, on aimerait pouvoir construire des rapporteurs d'angles gradués. Cela nous amène directement au problème de la constructibilité des nombres au moyen de la règle et du compas. À partir d'une unité donnée, on peut par exemple construire un segment de droite de longueur $\sqrt{2}$, et la question plus précise qui se pose est de savoir si

1. un segment, d'une longueur égale à n'importe quel nombre (réel, complexe) donné, peut-il être construit avec règle et compas ?
2. Si ce n'est pas le cas, quels sont les nombres pour lesquels ceci est possible ?

Des réponses à certaines des questions posées par les mathématiciens grecs ne seront obtenues que bien plus tard dans l'histoire des mathématiques. En effet, la recherche des nombres constructibles débouchera entre autres sur le développement de l'algèbre, et de la théorie de Galois [9]. Pour ne citer qu'un seul exemple célèbre, l'impossibilité de la quadrature du cercle (maintenant bien établie) se traduit par le fait que le nombre $\sqrt{\pi}$ n'est pas constructible.

Définition. On dit donc qu'un nombre réel a est dit **constructible** s'il existe des $A, B \in \mathcal{P}$ 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.

9. Evariste Galois a vécu de 1811 à 1832. Beaucoup de ces questions n'étaient donc pas encore résolues au début du 19^{e} siècle, et certaines sont encore ouvertes

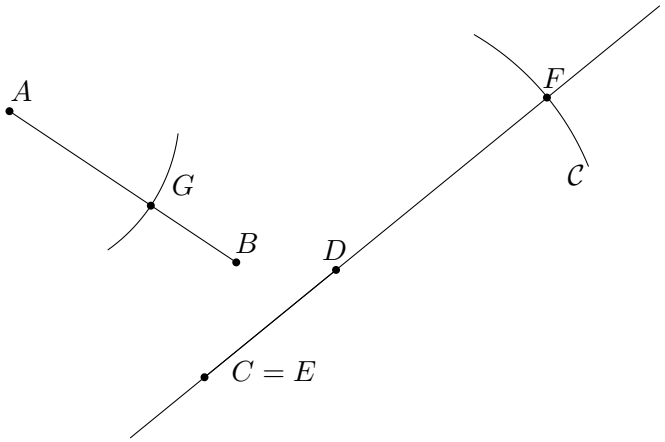


FIGURE 1.13 – Construction de la somme de deux nombres constructibles.

Nous allons voir maintenant des propriétés algébriques très agréables des nombres constructibles. Ces propriétés permettent immédiatement de déterminer une large classe de nombres constructibles, en plus de déterminer des procédures pour les construire pratiquement. En un certain sens, elles permettent de « programmer » la construction de longueurs.

i) Addition : Pour deux segments $[AB]$ et $[CD]$, on construit de la manière suivante un segment $[EF]$ tel que $EF = AB + CD$. La somme de deux nombres constructible est donc un nombre constructible. On trace le cercle $\mathcal{C}$ de centre D et de rayon AB (voir Figure 1.3.3). Alors $\mathcal{C}$ coupe (CD) en deux points, l'un deux que l'on nomme F fait en sorte que C, D et F sont alignés dans cet ordre. Il suffit donc de poser $E = C$ et on obtient :

$$EF = CD + DF = CD + AB.$$

ii) Soustraction : La différence de deux nombres constructible est un nombre constructible. Pour le voir, on considère que $AB > CD$. On trace le cercle de centre A et de rayon CD. On appelle G le point d'intersection de $[AB]$ avec le cercle. Alors.

$$AB = AG + GB \Longrightarrow GB = AB - CD, \text{ car } AG = CD.$$

iii) Multiplication : le produit de deux nombres constructible est un nombre constructible. Ceci est une conséquence du théorème de Thalès. Voir la Figure 1.3.3. On reporte la longueur CD sur la droite (AB) et on construit I tel que $AI = CD$ et $B \in [AI]$. On trace le cercle de centre B et de rayon EF. Puis on trace une droite passant par A et coupant ce cercle en F', donc $BF' = EF$.

On trace maintenant la parallèle à (BF') passant par D' et on note J son intersection avec

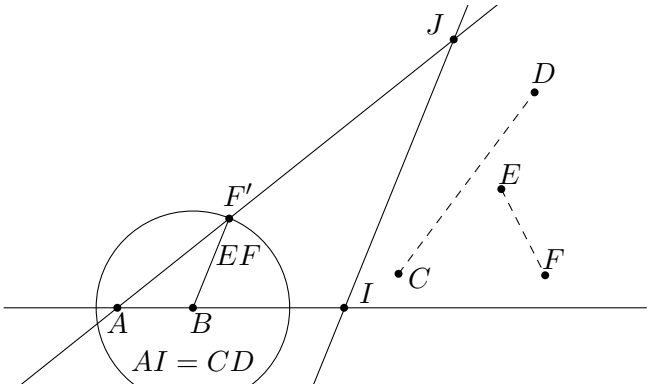


FIGURE 1.14 – Construction du produit de nombres constructibles.

(AF'). Alors, par le théorème de Thalès, on a :

$$\frac{IJ}{DF'} = \frac{AI}{AB} \Leftrightarrow \frac{IJ}{EF} = \frac{CD}{1} \Longrightarrow IJ = EF \cdot CD.$$

iv) Division : Le quotient de deux nombres constructibles (en ne divisant pas par zéro bien entendu) est un nombre constructible. À faire à l'exercice 11 (d). Il en découle, avec les propriétés ci-dessus, que tout nombre rationnel est constructible (mais ce ne sont pas les seuls).

v) Racine carrée : La racine carrée d'un nombre constructible (positif !) est constructible. C'est une conséquence des théorèmes de Pythagore et de Thalès, et nous en discuterons un peu plus loin (à la section 1.4). Voir aussi l'exercice 11 (e).

Dans un langage moderne (typique de la théorie de Galois), la conclusion est que l'ensemble des nombres constructibles forme un sous-corps du corps des nombres réels, et que ce sous-corps contient l'ensemble des nombres rationnels. En fait, il y a beaucoup d'autres nombres réels qui sont constructibles, mais il y en a aussi beaucoup (c'est une longue histoire) que ne le sont pas.

1.4 Médiatrice, et autres constructions à la règle et au compas

Une autre construction intéressante est celle de la droite perpendiculaire à une autre, et passant par un point donné.

Définition. Soit $A, B \in \mathcal{P}$ distincts. La **médiatrice** du segment $[AB]$ est la droite perpendiculaire à (AB) passant par le milieu de $[AB]$. On dit aussi qu'un point $M \in \mathcal{P}$ est **équidistant à A et B**, si $AM = BM$. 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 $[AB]$.

Proposition 1.7. *Soit $M \in \mathcal{P}$, alors M est 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

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

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

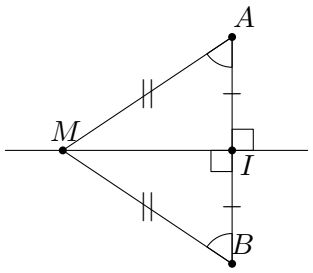


FIGURE 1.15 – Médiatrice et points équidistants de A et B.

($\Longleftarrow$) 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 :

$$\left.\begin{array}{rcl} MA &=& MB \\ AI &=& IB \\ \widehat{MAI} &=& \widehat{MBI} \end{array}\right\} \Longrightarrow \text{les triangles } MAI \text{ et } MBI \text{ sont isométriques.}$$

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

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

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

Construire le milieu d'un segment (et sa médiatrice). 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 (voir la figure 1.16). Ils se coupent en deux points C et D, et la droite (CD) est la médiatrice du segment $[AB]$. En effet, comme C et D sont

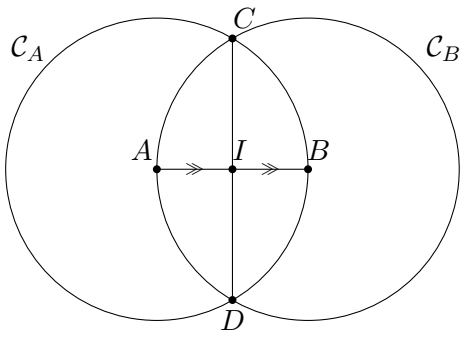


FIGURE 1.16 – Construction de la médiatrice.

équidistants de A et de B, alors C et D sont sur la médiatrice de $[AB]$. D'où (CD) est la médiatrice de $[AB]$. Le milieu de $[AB]$ est le point d'intersection I des droites (AB) et (CD).

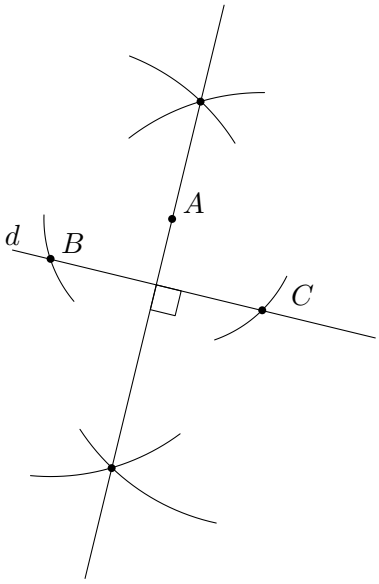


FIGURE 1.17 – Construction de la perpendiculaire à d passant par A.

Construction de la perpendiculaire à une droite passant par un point donné. On trace un cercle de centre A et de rayon suffisamment grand pour que le cercle coupe d en deux points B et C (voir la figure 1.17). Ces deux points sont équidistants de A, donc A est sur la médiatrice de $[BC]$, qui est la perpendiculaire à d passant par A. Il suffit donc de tracer la médiatrice à $[BC]$ (voir section 1.4).

Construction d'un carré dont un côté est un segment $[AB]$ **donné**. On trace la perpendiculaire à (AB) passant par A et la perpendiculaire à (AB) passant par B (voir section 1.4). Puis on reporte

la longueur AB sur ces perpendiculaires en traçant les cercles de rayon AB et de centres A et B. On obtient les points C et D (du même côté) de la droite (AB). Donc $AB = AD = BC$ et $\widehat{DAB} = \widehat{ABC} = \pi/2$: $ABCD$ est un carré !

Construire $\sqrt{2}$. On se donne un segment unité $[AB]$: $AB = 1$. On trace le carré $ABCD$ de côté $1 = AB$, puis sa diagonale $[BD]$. Alors par le théorème de Pythagore $BD = \sqrt{AB^2 + AD^2} = \sqrt{2}$. Voir l'exercice 11 (f) pour une généralisation de cette construction.

1.5 Construction de polygones réguliers

Dans cette section, on s'intéresse à la construction de certains polygones réguliers.

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

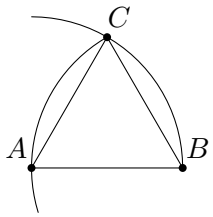


FIGURE 1.18 – Construction du triangle équilatéral

Pour construire un tel triangle (voir la figure 1.18), 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.

Construction d'un hexagone régulier

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

Pour construire un hexagone régulier, comme il est illustré à la figure 1.19, on débute avec une droite d, et un point $O \in d$. On trace un cercle $\mathcal{C}$ de centre O. On appelle A et D les points d'intersection de $\mathcal{C}$ et d. On trace les cercles $\mathcal{C}_A$ et $\mathcal{C}_D$ de centre A et D respectivement et de même rayon $OA = OD =$ rayon de $\mathcal{C}$. On note B, C, E, F les nouveaux points obtenus par l'intersection de $\mathcal{C}_A$, $\mathcal{C}_D$ et $\mathcal{C}$. Les triangles OAB et OAF sont équilatéraux, car $OB = OA = OF = AF = AB$, donc

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

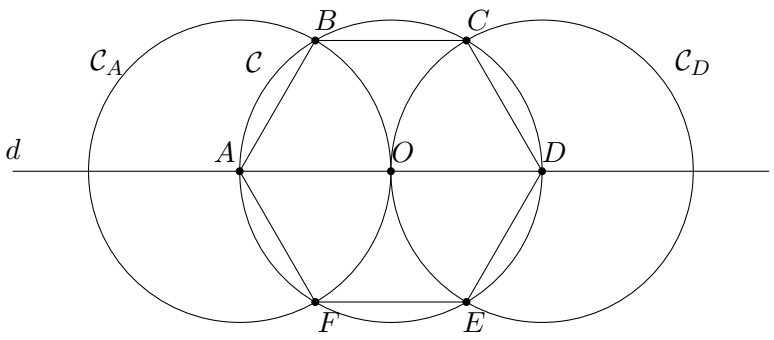


FIGURE 1.19 – Construction de l'hexagone régulier

Ainsi $ABCDEF$ est un hexagone régulier.

Remarque. Le problème général de savoir dans quels cas on peut construire un polygone régulier à n côtés a été résolu par Gauss et Wantzel (1796-1837).

Théorème 1.8. *Un polygone régulier est constructible si et seulement si son nombre de sommets* (n) *est le produit de puissance de 2 et de nombres premiers distincts de la forme* $2^{2^k}+1$ *où* $k \in \mathfrak{N}$.

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

1.6 Triangles, droites et points remarquables

1.6.1 Médiatrice et cercle circonscrit

Définition. Si ABC est un triangle, le **cercle circonscrit** à ce triangle est le cercle qui passe par A, B et C.

La proposition suivante montre qu'un tel cercle existe.

Proposition 1.9. *Soit ABC un triangle, alors ses médiatrices sont concourantes (se coupent au même point) en le centre du cercle circonscrit à ABC.*

Démonstration. Soit 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 A, B, C alignés, ce qui est impossible puisque ABC est un triangle. On a $OA = OC$, car $O \in d_B$, et $OB = OC$, car $O \in d_A$. D'où $OA = OB$. D'où $O \in d_C$, il s'en suit que $\{O\} = d_A \cap d_B \cap d_C$. ■

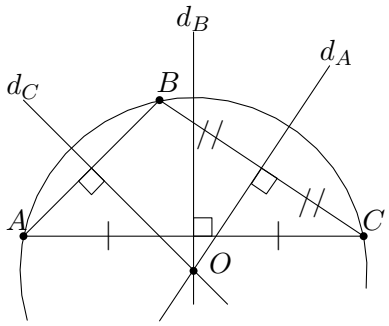


FIGURE 1.20 – Constrruction du cercle circonscrit à un triangle.

Corollaire 1.10. *Soit $A, B, C \in \mathcal{P}$ non alignés, alors il existe 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, 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 se coupent en trois points distincts, alors ils sont égaux. D'où, si deux cercles distincts se coupent, soit ils se coupent en un point (on dit alors qu'ils sont **tangents**), soit ils se coupent en deux points (on dit alors qu'ils sont **sécants**).

1.6.2 Hauteurs et orthocentre d'un triangle

Proposition 1.11. *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').

Soit 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).

Soit 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 $C_1A = BC = AB_1 \Rightarrow A$ est le milieu de $[B_1C_1]$.

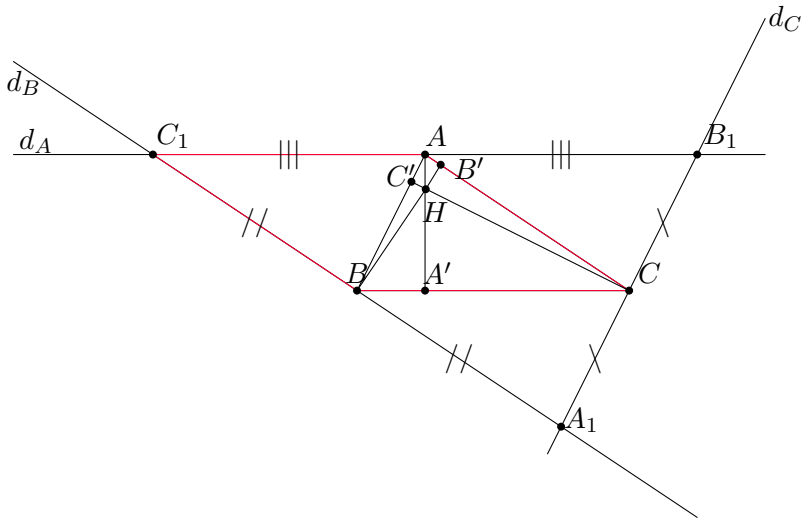


FIGURE 1.21 – Construction de l'orthocentre d'un triangle

De même, on montre que B est le milieu de $[A_1C_1]$ et que C est le point milieu de $[A_1B_1]$. Comme $(A_1C_1) \parallel (AC)$ et $(BB') \perp (AC)$, alors $(BB') \perp (A_1C_1)$. 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 $[B_1C_1]$. Les droites $(AA'), (BB')$ et (CC') sont les médiatrices du triangle $A_1B_1C_1$, et elles sont donc concourantes. ■

1.6.3 Médianes et centre de gravité

Une **médiane** d'un triangle ABC est une droite qui joint un sommet A au milieu du côté opposé.

Proposition 1.12. *Soit ABC un triangle, alors ses médianes sont concourantes au* **centre de gravité** *du triangle : ce point G est situé au $2/3$ de chaque médiane à partir du sommet correspondant.*

Démonstration. Voir exercice 21. ■

Nous allons revenir plus en détail sur la notion de centre de gravité au chapitre 2.

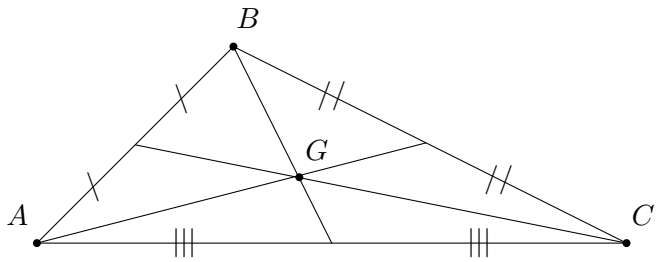


FIGURE 1.22 – Les médianes d'un triangle sont concourantes.

1.6.4 Bissectrices d'un triangle, et trisection (*)

La droite **bissectrice** d'un angle $\widehat{ABC}$ est une droite passant par B qui « coupe » l'angle en deux. Plus précisément, c'est une droite d qui contient le point B, telle que si D est un point de d distinct de B, alors l'angle $\widehat{ABD}$ est congru à l'angle $\widehat{DBC}$.

Proposition 1.13. *Un point D à égale distance des côtés d'un angle $\widehat{ABC}$ est sur la bissectrice de cet angle.*

Les **bissectrices intérieures** d'un triangle sont les bissectrices de chacun de ses angles. Une **bissectrice extérieure** d'un triangle, en un de ses sommets, est la droite passant par ce sommet qui est perpendiculaire à la bissectrice intérieure correspondante.

Proposition 1.14. *Soit ABC un triangle, alors ses bissectrices intérieures sont concourantes. De plus, deux bissectrices extérieures sont concourantes avec la bissectrice intérieure restante.*

Plutôt que de donner une démonstration de ce théorème, on donne, à la figure 1.23 l'image de trois triangles imbriqués qui illustre un joli lien entre bissectrices, hauteurs, et médiatrices. En effet, les trois droites qui sortent des triangles sont simultanément, les bissectrices du plus petit triangle, les hauteurs du triangle intermédiaire, et les médiatrices du plus grand. Une telle construction est possible dans toute situation. En effet, un peu de réflexion permet de voir qu'on peut débuter avec n'importe lequel des trois triangles (et la définition des droites associée), pour obtenir les deux autres.

La trisection de l'angle est impossible (en général) avec règle et compas. Cependant, si on accepte la possibilité de le faire (avec d'autres outils) alors de nouveaux théorèmes sont possibles. L'un des plus célèbres est le théorème de Frank Morley (datant de 1899). C'est un théorème qui en a surpris plusieurs, en partie parce qu'il est très élégant, et en partie parce qu'il n'a été découvert que très tard dans l'histoire plus que bimillénaire de la géométrie euclidienne.

Théorème 1.15 (Morley)**.** *Soit ABC un triangle quelconque. On trisecte chaque sommets pour obtenir pour chacun d'entre eux deux droites qui sont respectivement d_A, d'_A, d_B, d'_B, et d_C, d'_C comme illustré à la figure 1.24. Alors, le triangle formé des points $d_A \cap d'_B$, $d_B \cap d'_C$ et $d_C \cap d'_A$ est toujours équilatéral.*

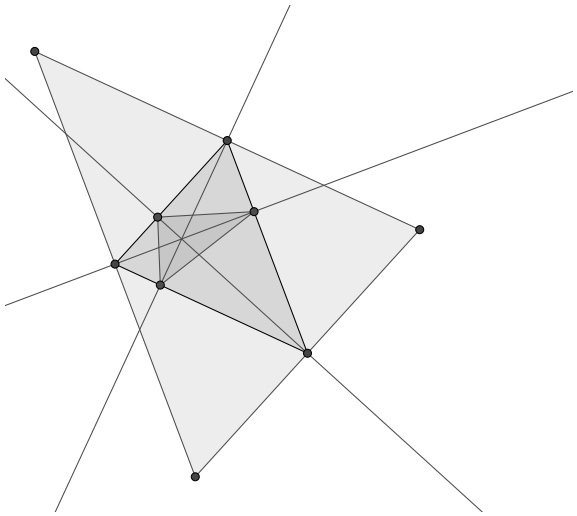


FIGURE 1.23 – Trois triangles et respectivement leurs bissectrices, hauteurs, et médiatrices

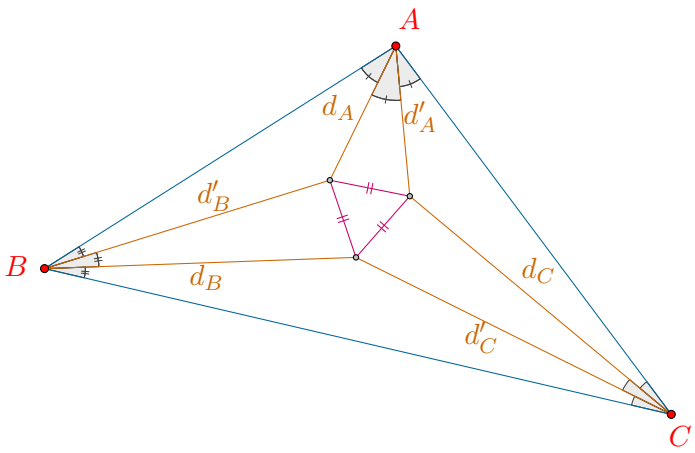


FIGURE 1.24 – Le théorème de Morley.

1.7 Axiomatisation de la géométrie euclidienne

On peut probablement croire que les mathématiciens (philosophes/physiciciens) grecs avaient l'impression de dégager les « lois de la nature » en mettant en évidence les axiomes de ce qu'ils percevaient comme étant LA géométrie. On a découvert depuis [10] qu'il y a plusieurs géométries

10. Cette aventure intellectuelle a débouché sur la théorie de la relativité d'Einstein.

intéressantes. On parle donc maintenant plutôt d'UNE géométrie. L'approche axiomatique moderne, qu'on utilise dans toutes les branches des mathématiques, correspond à décrire des « règles du jeu » qui peuvent être satisfaites dans plusieurs contextes. Cela a l'avantage de donner des théories qui peuvent s'interpréter pour l'étude d'objets différents (parfois de manière surprenante), et donc de fournir des outils conceptuels d'une plus grande capacité d'expression.

Nous n'avons discuté jusqu'ici que de deux axiomes, la règle de **l'invariance des angles par translation** et la règle des **triangles isométriques**. On a cependant déjà constaté l'importance de ces axiomes dans le processus déductif qui mène à la démonstration de résultats en géométrie. Nous allons clarifier un peu plus cette axiomatique de la géométrie. L'objectif est de se doter d'un ensemble complet de règles de base, les axiomes, à partir desquels se déduisent logiquement tous les autres faits (théorèmes) de la théorie considérée. Comme on l'a déjà souligné, un avantage de cette approche est que tout résultat démontré est automatiquement valide dans tout autre contexte dans lesquels les axiomes sont vérifiés. Nous allons présenter à la section 1.9 un petit exemple d'un contexte très différent dans lequel s'interprètent plusieurs théorèmes de géométrie (qui se déduisent à partir de certains des axiomes).

Les axiomes proposés par Euclide ont longtemps semblé adéquats, mais David Hilbert (1862-1943) a souligné qu'il y avait un certain nombre d'hypothèses implicites derrière les raisonnements typiques de la géométrie euclidienne. Il a donc proposé une liste complète d'axiomes, et montré qu'ils sont « suffisants ». Ce sont (à peu près) ceux présentés ici.

Rappelons que jusqu'ici, on a considéré le contexte suivant. On a un certain ensemble $\mathcal{E}$ (c'est l'espace) dont les éléments sont appelés **points**. Nous allons spécifier un ensemble d'axiomes à propos de certains sous-ensembles de points, et de la relation d'appartenance par rapport à ces sous-ensembles. Parmi ces sous-ensembles, certains sont appelés droites, et d'autres plans. Il y a une relation (dont les propriétés sont déterminées par les axiomes) sur les points, qui permet de dire quand un point se trouve **entre** deux autres. Si A et B sont des points distincts, et C se trouve entre A et B. On alors écrit $A < C < B$, si C est distinct de A et de B. L'ordre de gauche à droite, correspond à l'ordre dans lequel on donne les points A et B. Via cette relation on peut définir la notion de **segment** $[AB]$ d'une droite : c'est l'ensemble des points qui sont entre A et B. On a aussi la notion de demi-droite $[AB)$, c'est l'ensemble des points C, de la droite qui passe par A et B, tels que B soit entre A et C. Pour A, B, et C des points distincts, l'angle $\widehat{BAC}$ correspond à la donné (ordonnée) de deux demi-droites $[AB)$ et $[AC)$. Un triangle est simplement la donnée de trois points distincts. On a enfin des relations : de **congruence** entre segments, de **congruence** entre angles, et de **congruence** entre triangles. Choisir une géométrie consiste à choisir quels sont tous ces ensembles et relations. N'importe quel choix est acceptable, à la simple condition qu'il satisfasse les axiomes ci-dessous.

Rappelons aussi qu'on a aussi convenu de dire que : si A est un point, d est une droite, et $\mathcal{P}$ est un plan, alors

— A est sur la droite d si et seulement si $A \in d$,
— d passe par A si et seulement si $A \in d$,

— A est dans le plan $\mathcal{P}$ si et seulement si $A \in \mathcal{P}$,
— d est dans le plan $\mathcal{P}$ si et seulement si $d \subset \mathcal{P}$,
— des points sont alignés (ou colinéaires) si et seulement si ils appartiennent à une même droite.
— des points sont des dits coplanaires si et seulement si ils appartiennent à un même plan.
— des droites sont des dites coplanaires si et seulement si elles appartiennent à un même plan.

Ces objets (éléments et ensembles) satisfont les axiomes suivants.

Axiomes de la géométrie euclidienne

discutés ici

Axiome I : Soit A, B deux points dans l'espace $\mathcal{E}$, alors il existe une unique droite passant par A et B.

Axiome II : Une droite contient toujours au moins deux points distincts ; et, pour toute droite, il existe au moins un point qui n'est pas sur cette droite.

Axiome III : Par trois points non alignés passe un et un seul plan.

Axiome IV : La droite qui passe par deux points distincts d'un plan est entièrement incluse dans ce plan.

Axiome V : Il existe au moins un point de l'espace non contenu dans un plan donné, et tout plan contient au moins un point.

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

Axiome VII : (Postulat d'Euclide) Soit d une droite, et A un point qui n'est pas sur cette droite. Alors il existe un plan contenant la droite d, et le point A, et ce plan contient une et une seule droite passant par A et qui est parallèle à d.

Axiome VIII : Soit B entre A et C. Alors B est aussi entre C et A, et il existe une droite contenant les trois points A, B et C.

Axiome IX : Étant donné deux points distincts, il existe au moins un autre point qui se situe entre ces deux points.

Axiome X : Pour trois points distincts sur une même droite, il y en a un et un seul que se situe entre les deux autres.

Axiome XI : (Postulat de Pasch) Pour A, B, et C trois points non colinéaires, et d une droite dans le plan contenant A, B et C. Si d ne contient aucun des points A, B, et C, et si d contient un point du segment $[AB]$, alors d contient soit un point de $[AC]$, soit un point de $[BC]$.

Axiome XII : Les relations de congruences, entre segments, angles et triangles, sont des relations d'équivalence.

Axiome XIII : Soient A et B deux points distincts, et A' un point d'une droite d. Alors, il existe deux et exactement deux points C et D sur la droite d, avec A' entre C et D, et les segments $[A'C]$ et $[A'D]$ tous deux congrus à $[AB]$.

Axiome XIV : Soit A, B et C des points distincts avec B entre A et C, ainsi que A', B' et C' des points distincts avec B' entre A' et C'. Si $[AB]$ est congru à $[A'B']$, et $[BC]$ est congru à $[B'C']$, alors $[AC]$ est congru à $[A'C']$.

Axiome XV : Soit $\widehat{ABC}$ un angle, et soit $[B'C')$ une demi-droite. Alors il existe deux et exactement deux demi-droites $[B'D)$ et $[B'E)$ (bien entendu le choix de D et E n'est pas unique), tels que les angles $\widehat{DB'C'}$ et $\widehat{C'B'E}$ soient tous deux congrus à $\widehat{ABC}$.

Axiome XVI : Soient ABC et $A'B'C'$ deux triangles, avec $[AB]$ congru à $[A'B']$, $[BC]$ congru à $[B'C']$, et $\widehat{ABC}$ congru à $\widehat{A'B'C'}$, alors le triangle ABC est congru au triangle $A'B'C'$, $[AC]$ est congru à $[A'C']$, les angles $\widehat{BCA}$ et $\widehat{B'C'A'}$ sont congrus, et les angles $\widehat{CAB}$ et $\widehat{C'A'B'}$ sont congrus.

Axiome XVII : (Podstulat d'Archimède) Soient $[AB]$ et $[CD]$ des segments, avec A distinct de B, et C distinct de D. Alors, il existe un entier n, et une suite finie de points tels que

$$A = A_1 < A_2 < \ldots < A_{n-1} \leq B < A_n$$

tels que les segments $[A_iA_{i+1}]$ soient tous congrus à $[CD]$.

Axiome XVIII : Soient (A_i) et (B_i) deux suites de points (sur une même droite), avec

$$A_i < A_{i+1} < B_{i+1} < B_i.$$

Alors il existe au moins un point C tel que $A_i < C < B_i$ pour tout i.

Chacun de ces axiomes clarifie le contexte. Nous allons discuter plus en détail l'impact des axiomes de I à VII dans les sections qui suivent. Les axiomes de VIII à XI permettent de définir de façon précise les notions de segments, intérieur de triangles, etc. Les axiomes XII à XVI clarifient les notions de congruences. Enfin, les deux derniers axiomes permettent de montrer que toute droite (orientée) peut être confondue avec la droite « réelle ». Autrement dit, modulo le choix d'une origine et d'une unité de mesure, les points d'une droite s'identifient aux nombres réels. Comme l'a souligné René Descartes (1596-1650), c'est une idée qui a un grand impact. Nous y reviendrons au chapitre 2.

1.7.1 Discussion des axiomes sur les droites et plans

On peut déduire du seul axiome I les propriétés bien connues suivantes.

Proposition 1.16. *Soit d_1 et d_2 deux droites de l'espace, alors on a un et seulement un des cas suivants :*

1. *il existe un unique point $A \in \mathcal{E}$ tel que $d_1 \cap d_2 = \{A\}$ (on dit que d_1 et d_2 sont sécantes ou concourantes) ;*
2. *$d_1 = d_2$;*

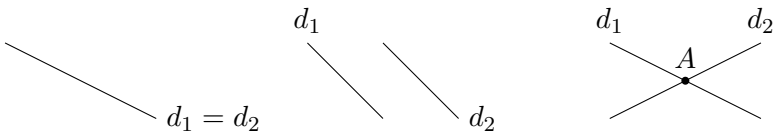


FIGURE 1.25 – Positions relatives de droites.

3. $d_1 \cap d_2 = \emptyset$.

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 $A, B \in d_2$. Le premier axiome 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.

Proposition 1.17.

1. *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.*
2. *Si $\mathcal{P}$ est un plan, alors il existe trois points non alignés A, B, C tel que $\mathcal{P} = (ABC)$.*

Démonstration. En vertu du deuxième axiome, on peut prendre deux points distincts A, B sur d. Comme $C \notin d$, A, B et C ne sont pas alignés. Le troisième axiome nous assure alors qu'il existe un unique plan $\mathcal{P} = (ABC)$. Enfin, le quatrième axiome nous assure que $d = (AB)$ est contenu dans cet unique plan $\mathcal{P}$. Ceci montre les deux énoncés cherchés. ■

Les positions relatives possibles d'un plan et d'une droite sont déterminées par la proposition suivante.

Proposition 1.18. *Soit d une droite et $\mathcal{P}$ un plan, alors on a un des cas suivants :*

1. *d coupe $\mathcal{P}$ en un point.*
2. *$d \subset \mathcal{P}$.*
3. *$d \cap \mathcal{P} = \emptyset$.*

Démonstration. Si $d \cap \mathcal{P} = \emptyset$, on a la situation (3). Si $d \cap \mathcal{P} \neq \emptyset$ on a deux cas possibles :
— $d \cap \mathcal{P} = \{A\}$, donc on est dans la situation (1)

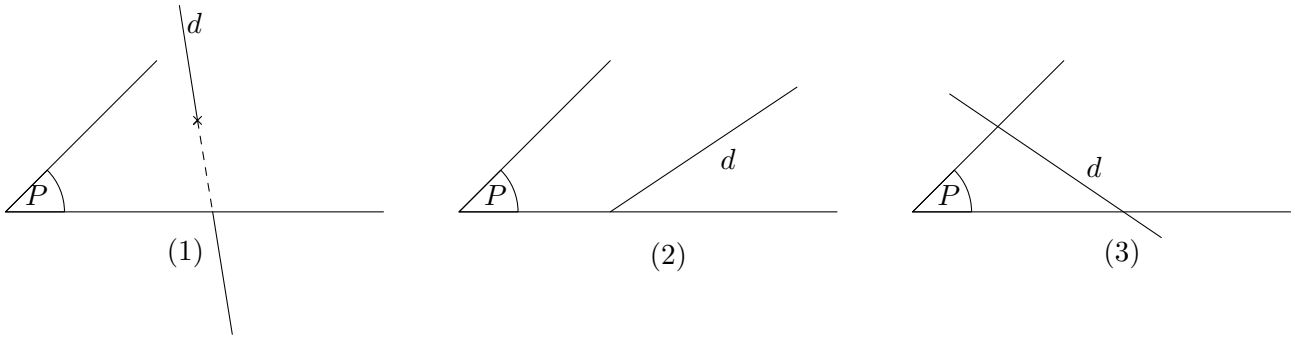


FIGURE 1.26 – Positions relatives d'une droite et un plan.

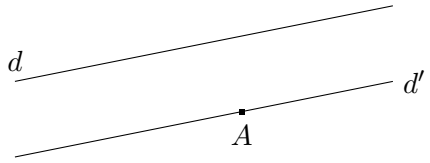
— d coupe $\mathcal{P}$ en au moins deux points distincts A et B. En vertu du quatrième axiome on obtient $d = (AB) \subseteq \mathcal{P}$, car $A, B \in \mathcal{P}$. On est donc dans la situation (2).

■

Définition. On dit que deux droites d'un même plan sont **parallèles** si elles ne se croisent pas ou si elles sont confondues. On note encore $d \parallel d'$ le fait que des droites soient parallèles dans l'espace.

On reformule comme suit la proposition 1.16 pour un plan quelconque de l'espace.

Proposition 1.19. *Soit 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 est un point : les droites sont sécantes (elles se coupent en un point).*



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.

Proposition 1.20. *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
— *$d_1 \parallel d_1$ (réflexive).*
— *$d_1 \parallel d_2 \Longrightarrow d_2 \parallel d_1$ (symétrique).*
— *$d_1 \parallel d_2$ et $d_2 \parallel d_3 \Longrightarrow d_1 \parallel d_3$ (transitive).*

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 23 (2) (ce résultat nécessite l'axiome d'Euclide). ■

Pour l'espace, la situation est un peu plus complexe. Nous avions fait la remarque plus haut que deux droites de l'espace d'intersection vide ne sont pas forcément parallèles. Plus précisément, on a la situation décrite ci-dessous, après l'introduction d'un peu de terminologie.

Définition. Rappelons qu'on dit que

1. des points sont **coplanaires** s'ils sont contenus dans le même plan.
2. des droites sont **coplanaires** si elles sont contenues dans un même plan.
3. 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 des axiomes les faits suivants :

1. dans l'espace, il existe au moins 4 points non coplanaires ;
2. deux droites non sécantes et non coplanaires ne sont pas parallèles ; et
3. il existe un unique plan contenant deux droites parallèles distinctes (pourquoi ?).

On peut maintenant reformuler de manière plus précise la proposition 1.16

Proposition 1.21. *Soit d_1 et d_2 deux droites de l'espace, alors on a l'un des cas suivants :*

1. *d_1 et d_2 sont sécantes (et donc coplanaires) ;*
2. *$d_1 \parallel d_2$ (et donc coplanaires) ;*
3. *$d_1 \cap d_2 = \emptyset$ et ne sont pas coplanaires.*

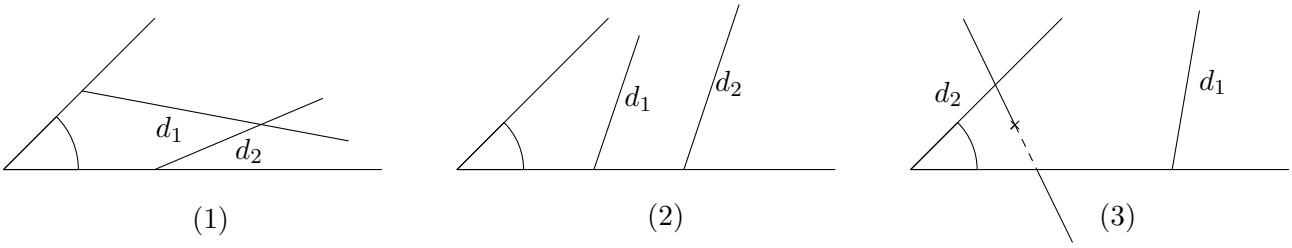


FIGURE 1.27 – Positions relatives de droites dans l'espace à 3 dimensions

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.

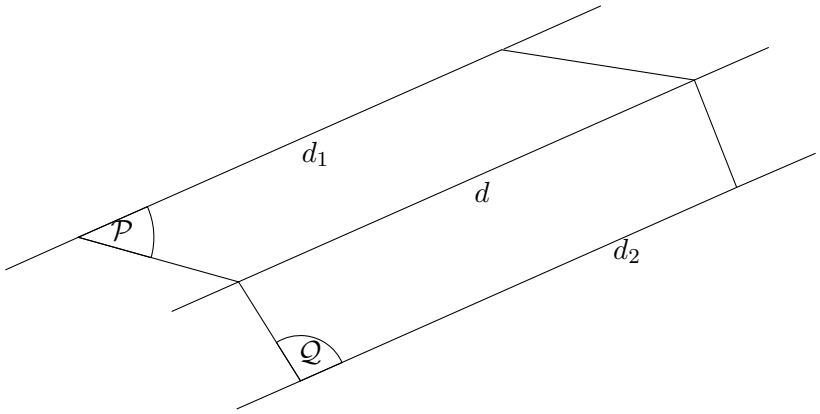


FIGURE 1.28 – Transitivité du parallélisme dans l'espace à 3 dimensions.

Théorème 1.22 (du toit)**.** *Soit $\mathcal{P}$ 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 ($d_1 \parallel d_2$). Alors $A \in \mathcal{R} \cap \mathcal{P}$ et $A \in \mathcal{R} \cap \mathcal{Q}$, car $A \in d_1 \cap d \subset \mathcal{R} \cap \mathcal{Q} \cap \mathcal{P}$. Donc $\mathcal{R}$ est l'unique plan contenant d_2 et $A \in d$, ainsi $\mathcal{R} = \mathcal{Q}$. Donc 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 d_2. ∎

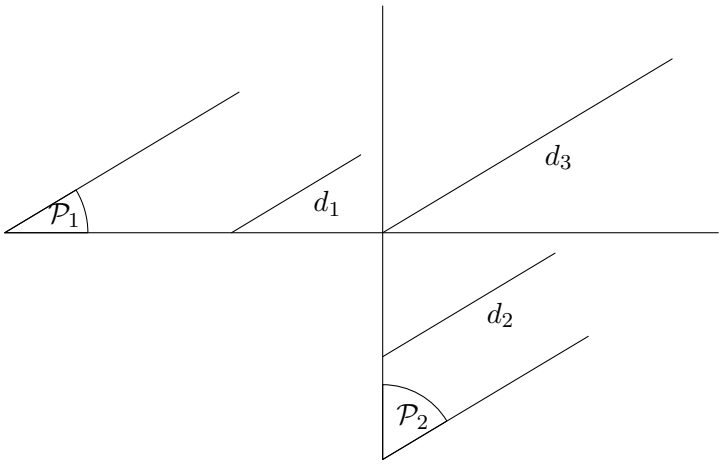
Corollaire 1.23. *La relation « être parallèle dans l'espace » pour les droites est une relation d'équivalence, c'est-à-dire : si d_1, d_2, d_3 sont trois droites de $\mathcal{E}$, on a*

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

[**Preuve de la propriété de transitivité.** 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 $d_3 (d_2 \parallel d_3)$. Par le théorème du toit, on obtient que $d' = \mathcal{P}_1 \cap \mathcal{P}_2$ est parallèle à d_1 et à d_2, car $d_1 \parallel d_2$. Or,

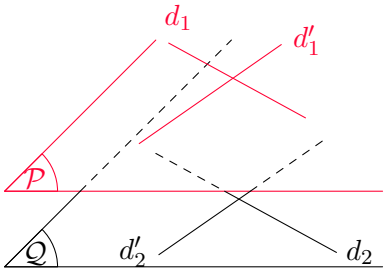
$$\left.\begin{array}{c} d' \parallel d_2 \\ d_3 \parallel d_2 \\ A \in d_3 \cap d' \end{array}\right\} \Longrightarrow d_3 = d' \parallel d_1.$$

∎

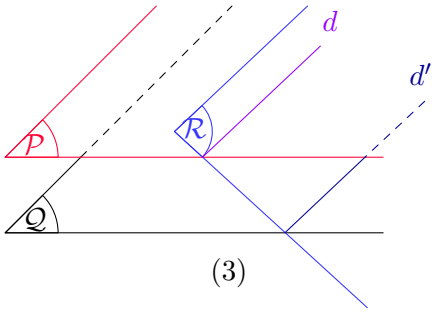


1.7.2 Plans parallèles

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



(1)



(3)

Proposition 1.24. *Soit $\mathcal{P}, \mathcal{Q}$ et $\mathcal{R}$ trois plans alors :*

1. *Si deux droites sécantes de $\mathcal{P}$ sont parallèles à deux droites sécantes de $\mathcal{Q}$ alors $\mathcal{P} \parallel \mathcal{Q}$.*
2. *La relation « être parallèle dans l'espace » pour les plans est une relation d'équivalence, c'est-à-dire :*
   - *$\mathcal{P} \parallel \mathcal{P}$ (réflexive).*
   - *$\mathcal{P} \parallel \mathcal{Q} \Longrightarrow \mathcal{Q} \parallel \mathcal{P}$ (symétrique).*
   - *$\mathcal{P} \parallel \mathcal{Q}$ et $\mathcal{Q} \parallel \mathcal{R} \Longrightarrow \mathcal{P} \parallel \mathcal{R}$ (transitive).*
3. *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.

1. 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 $\mathcal{P} = \mathcal{Q}$.
2. 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). Pour conclure, 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 $\mathcal{P} \parallel \mathcal{R}$.
3. 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, entraîne 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'une parallèle à un plan donné passant par une droite donnée ne nécessite pas de nouvel axiome.

Corollaire 1.25. *Soit $\mathcal{P}$ un plan et $A \notin \mathcal{P}$, il existe 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 (3) on a que $\mathcal{R} \cap \mathcal{P} = d'$ une droite, ce qui 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

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. Deux droites d et d' sont dites **orthogonales** si elles sont parallèles à deux droites perpendiculaires (i.e à deux droites qui se coupent en angle droit). Notation : $d \perp d'$.
2. Une droite d et un plan $\mathcal{P}$ sont **orthogonaux** si d est orthogonale à toutes les droites de $\mathcal{P}$. Notation : $d \perp \mathcal{P}$.
3. Deux plans sont **perpendiculaires** si l'un d'eux contient une droite orthogonale à l'autre plan. Notation : $\mathcal{P} \perp \mathcal{Q}$.

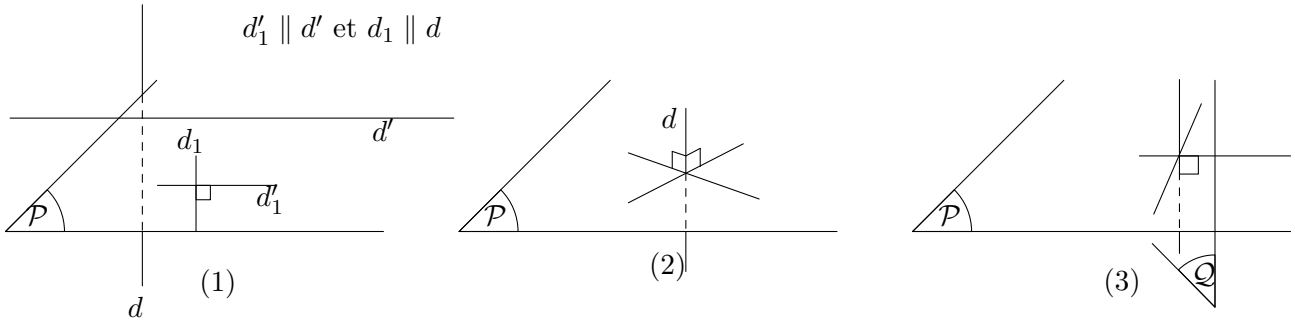


FIGURE 1.29 – Diverses formes d'orthogonalité.

Proposition 1.26. *Si $d \parallel d'$ et $d \perp d''$ alors $d' \perp d''$*

Démonstration. Voir exercice 24 (1). ■

Théorème 1.27. *Si une droite est orthogonale à deux droites sécantes d'un plan, alors elle est orthogonale à ce plan.*

Idée de la preuve. Donnée : $(B'B) \perp (AD)$ et $(BB') \perp (AC)$. Est-ce que $(BB') \perp d$? On choisit B, B' tels que A soit 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.

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

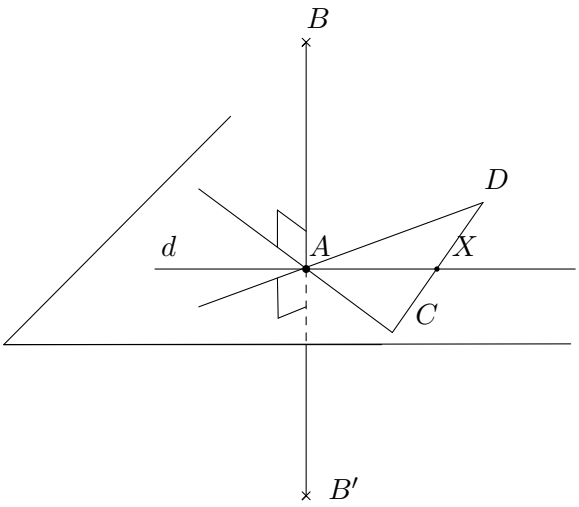


FIGURE 1.30 – Condition d'orthogonalité d'une droite à un plan.

$\Longrightarrow$ 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 1.28.

(1) *Si deux droites sont parallèles, alors un plan orthogonal à l'une l'est aussi à l'autre.*
(2) *Si deux plans sont parallèles, alors toute droite orthogonale à l'un l'est aussi à l'autre.*
(3) *Par un point de l'espace, il ne passe qu'un unique plan orthogonal à une droite donnée.*

Démonstration. Voir exercice 25. ■

On termine cette section en donnant la définition du plan médiateur, qui joue le rôle dans l'espace que la médiatrice jouait dans le plan.

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

Proposition 1.29. *M est dans le plan médiateur de $[AB]$ $\Leftrightarrow$ $AM = BM$.*

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

1.8.2 Application : le cube

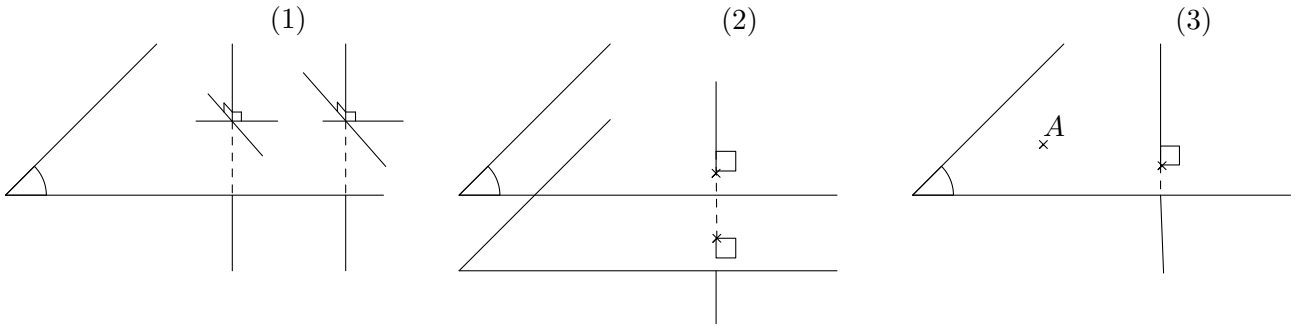
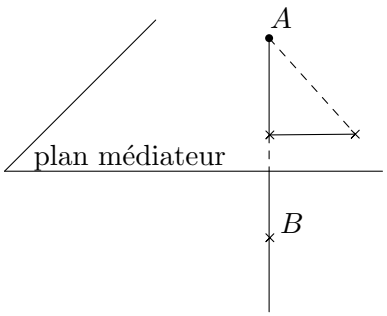
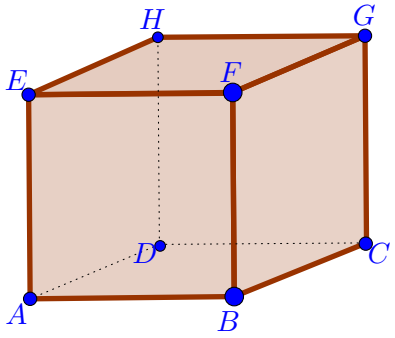


FIGURE 1.31 – Orthogonalités droites-plans.





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

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

Proposition 1.30. *Le cube $ABCDEFGH$ a les propriétés suivantes :*

1. *les droites définies par les arêtes des faces opposées $ABCD$ et $EFGH$ sont tels que $(AB) \parallel (DC) \parallel (EF) \parallel (HG)$ et $(AD) \parallel (BC) \parallel (EH) \parallel (FG)$;*
2. *les plans définis par les faces opposées sont parallèles ;*
3. *les droites définies par les arêtes de la face $ABCD$ sont orthogonales aux droites (AE) et (FB) de la face $AEFB$;*
4. *les plans définis par des faces adjacentes sont perpendiculaires.*

Démonstration. 1. Montrons par exemple que $(AB) \parallel (HG)$. Comme $ABCD$ est un carré, $(AB) \parallel (DD)$. 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.

2. Montrons par exemple que $(AEF) \parallel (DHG)$. On sait que les deux droites sécantes (AE) et (EF) sont respectivement parallèles aux deux droites sécantes (DH) et (HG), car $ADEH$ et $HEFG$ sont des carrés. En vertu de la proposition 1.24 (1) on en déduit que $(AEF) \parallel (DHG)$.

3. 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.

4. Montrons par exemple que $(AEF) \perp (ABC)$. Comme (AEF) contient la droite (AE) qui est perpendiculaire aux droites sécantes (AB) et (AD), on déduit du théorème 1.27 que $(AE) \perp (ABC)$ et donc que $(AEF) \perp (ABC)$.

■

1.9 Plan projectif à 7 points (*)

Pour mieux appréhender le rôle abstrait des axiomes en mathématiques, nous discutons ici un exemple qui permet d'illustrer ce fait. Le **plan projectif** est un espace géométrique constitué de points et de droites satisfaisant les axiomes suivants.

Axiome I : Par deux points distincts passe une et une seule droite.

Axiome II : Deux droites distinctes se croisent en un et un seul point.

Axiome III : Il existe au moins quatre points, tels que trois d'entre eux ne sont jamais colinéaires.

Rien n'exige qu'il y ait un nombre infini de points. En fait, le plus petit contexte dans lequel ces axiomes sont satisfaits est le **plan de Fano**[11] dont la description suit. Le plan $\mathcal{P}$ est constitué de 7 points et 7 droites. Comme on va le voir, il est pratique d'identifier ces points à des triplets de 0 et de 1. L'espace $\mathcal{P}$ est

$$\mathcal{P} := \{001, 010, 100, 110, 101, 011, 111\}.$$

Les 7 droites de $\mathcal{P}$ sont chacune constituée de trois points. Ce sont les sous-ensembles :

$$\{\{001, 010, 011\},\ \{100, 010, 110\},\ \{100, 001, 101\},\\ \{100, 011, 111\},\ \{010, 101, 111\},\ \{001, 110, 111\},\\ \{110, 101, 011\}\}.$$

Les quatre points 100, 101, 110 et 111 mettent en évidence le fait que le troisième axiome est satisfait. Chaque droite $\{X, Y, Z\}$ est telle que $X + Y + Z = 000$, où on calcule la somme de deux points comme

11. Portant le nom de Gino Fano (1871-1952).

suit :

$$(a_1, b_1, c_1) + (a_2, b_2, c_2) = (a_1 + a_2, b_1 + b_2, c_1 + c_2),$$

avec les règles de calcul habituelles $0 + 0 = 0$, $0 + 1 = 1$, $1 + 0 = 1$, mais surtout $1 + 1 = 0$. Toujours avec ces règles, on trouve que $Z = X + Y$. Autrement dit, le premier axiome est satisfait, puisque l'unique droite qui contient les points X et Y est $\{X, Y, X + Y\}$. On peut vérifier directement que le second axiome est satisfait, en calculant les intersections des droites deux à deux. Bien entendu, il y a des méthodes plus élégantes pour faire cela, mais c'est une autre histoire.

1.10 Exercices du chapitre 1

Quelques résultats classiques

Exercice 1 **(Démonstration du cours)** (Proposition 1.3) 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 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 ont même longueur.

Exercice 3 (B) Montrer que la somme des angles intérieurs d'un quadrilatère convexe est 2π.
Petit défi : montrer que la somme des angles intérieurs d'un polygone convexe (une définition ?) à n côtés est $(n - 2)\pi$.

Exercice 4 (B) Soit $\mathscr{C}$ un cercle de centre O et $\mathscr{C}'$ un cercle de centre O'. On suppose que $\mathscr{C}$ et $\mathscr{C}'$ sont sécants en A et B. On note E le point diamétralement opposé à B sur $\mathscr{C}$ et F le point diamétralement opposé à B sur $\mathscr{C}'$. Montrer que A, E et F sont alignés.

Les théorèmes de Pythagore et de Thalès

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

Exercice 6 Un avion vole au-dessus de Montréal, il doit atterrir dans l'aéroport situé à 19 km du centre-ville. Pour descendre, il parcourt 20 km. À quelle altitude volait-il au-dessus du centre-ville ?

Exercice 7 Soit $ABCD$ un quadrilatère convexe quelconque. Soit I milieu de $[AB]$, J milieu de $[BC]$, K milieu de $[CD]$ et L milieu de $[AD]$. Montrer que $IJKL$ est un parallélogramme.

Exercice 8 (B) (Démonstration du cours) (Théorème 1.6) Soit ABC et AEF deux triangles tels que $B \in (AE)$ et $C \in (AF)$. On a déjà montré que si $(BC) \parallel (EF)$, alors $AE/AB = AF/AC$. Montrer qu'on a aussi $AE/AB = EF/BC$.

Exercice 9 (B) (a) Le mathématicien Thalès sait qu'il mesure $1,80\,m$. Il se place en plein soleil au pied de la grande pyramide de Kheops. 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 $1,50\,m$ pour l'ombre de Thalès et $122\,m$ 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 $130\,m$. Quelle est la mesure d'une de ses arêtes ?

Exercice 10 (B) Comme illustré à la Figure 1.32, on trace un cercle $\mathcal{C}$ de centre O, et de rayon $(r+1)/2$. Soit $[AB]$ un diamètre de $\mathcal{C}$, et D sur ce diamètre tel que la longueur de $[AD]$ soit égale à 1. On a donc que r est la longueur de $[DB]$. On construit en D une droite perpendiculaire à (AB), et alors C est un des points d'intersection (ben sûr, il y en a deux) de cette droite et du cercle. Calculez la longueur x du segment $[CD]$, en fonction de la longueur r du segment $[DB]$.

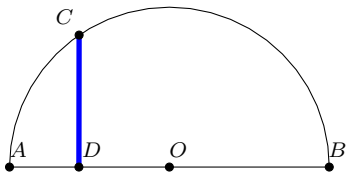


FIGURE 1.32 – Construction de l'exercice 10.

Médiatrices et autres constructions à la règle et au compas

Exercice 11 Donnez, 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 de longueur 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 $\sqrt{n}$. **Petit défi :** pouvez-vous généraliser à la construction de la racine d'un nombre constructible quelconque ?

g) Un triangle rectangle isocèle en C dont on connaît l'hypoténuse AB.

Exercice 12 **(Examen 2009)** Soient $\mathscr{C}$ et $\mathscr{C}'$ deux cercles de centre respectifs O et O' et de rayon r et r'. On suppose que $\mathscr{C}$ et $\mathscr{C}'$ sont sécants en deux points distincts A et B. Montrer que $(OO') \perp (AB)$.

Exercice 13 Soient O_1, O_2 et O_3 trois points distincts non alignés, et soit $r > 0$. Soit $\mathscr{C}_i$ $(i = 1, 2, 3)$ le cercle de centre O_i et de rayon r. On suppose que ces cercles sont sécants 2 à 2 (voir exercice 12). On note A et B les points d'intersection de $\mathscr{C}_1$ et $\mathscr{C}_2$; C et D les points d'intersection de $\mathcal{C}_1$ et $\mathscr{C}_3$; E et F les points d'intersection de $\mathscr{C}_2$ et $\mathscr{C}_3$.

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

Exercice 14 (B) **(Examen 2010)** Soient $\mathscr{C}$ et $\mathscr{C}'$ deux cercles de centre respectifs O et O' et de rayon r et r'. On suppose que $\mathscr{C}$ et $\mathscr{C}'$ sont sécants en deux points distincts A et B. Soit C et D deux points tels que $[AC]$ est un diamètre de $\mathscr{C}$ et $[AD]$ est un diamètre de $\mathscr{C}'$.

1. Faire un dessin de la situation.
2. Montrer que $(OO') \perp (AB)$.
3. Montrer que B, C et D sont alignés.
4. Montrer que $(CD) \parallel (OO')$.
5. Montrer que $CD = 2\,OO'$.

Exercice 15 (B) **Petit défi :** à partir d'un polygone régulier à n côtés déjà construit, montrer comment construire un polygone régulier à $2n$ côtés.

Exercice 16 (B) Par calcul, on trouve que

$$\sin(\pi/5) = \frac{\sqrt{2}\sqrt{5-\sqrt{5}}}{4}.$$

Petit défi : Utilisez ceci pour décrire une construction avec règle et compas du pentagone. Vous aurez besoin d'avoir d'abord relevé le défi de l'exercice 11 (f).

Triangles, droites et points remarquables

Exercice 17 Soit 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. Soit H le projeté orthogonal de C sur (AD) et K le projeté orthogonal de D sur (AC).

1. Montrer que (CH) et (DK) se coupent en un point I.
2. Montrer que (AI) est perpendiculaire à (AB).

Exercice 18 Soit $ABCD$ un rectangle. La médiatrice de $[AC]$ coupe (AB) en I et (BC) en J. Montrer que (CI) est perpendiculaire à (AJ).

Exercice 19 (B) Soit $\mathscr{C}$ un cercle de centre O et de diamètre $[IJ]$. On note $\mathscr{C}'$ le cercle de diamètre $[OI]$. Soit M un point du cercle $\mathscr{C}$ différent de I et J . La droite (MI) coupe le cercle $\mathscr{C}'$ en S et la droite (MO) coupe le cercle $\mathscr{C}'$ en T. La droite perpendiculaire à (IJ) passant par M coupe la droite (IT) en P .

1. Faire un dessin de la situation.
2. Montrer que (OP) est une hauteur du triangle IPM.
3. Déduire de la question précédente que les points P, O et S sont alignés.
4. En utilisant le théorème de Thalès, démontrer que S est le milieu du segment $[IM]$.
5. Quelle est la nature du triangle IPM ? Justifier votre réponse.

Exercice 20 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.

1. 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).
2. Montrer que les bissectrices de ABC sont concourantes.
3. Construire les bissectrices de ABC à la règle et au compas (justifier la construction).

Exercice 21 (B) (Démonstration du cours) (Proposition 1.12) 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 $2/3$ 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'). Soit G le point d'intersection de (AA') et (BB').

1. Faire un dessin de la situation.

2. Montrer que A_1BGC, AB_1CG et $BGAC_1$ sont des parallélogrammes.
3. Montrer que ABA_1B_1 est un parallélogramme.
4. Montrer que G est le milieu de $[A_1\,A]$.
5. 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.
6. Montrer que $AG = \frac{2}{3}AA'$, $BG = \frac{2}{3}BB'$ et $CG = \frac{2}{3}CC'$.

Exercice 22 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 23 Soient d, d' et d'' trois droites distinctes d'un même plan.

1. Montrer que si d et d' parallèles et si d'' coupe d, alors d'' coupe aussi d'.
2. Montrer que si $d \parallel d'$ et $d' \parallel d''$ alors $d \parallel d''$ (**Démonstration du cours** - Proposition 1.20).

Orthogonalité dans l'espace

Exercice 24 (B) Soit d, d', d'' trois droites distinctes de l'espace, montrer que

1. Si $d \perp d'$ et $d' \parallel d''$ alors $d \perp d''$ (**Démonstration du cours** - Proposition 1.26).
2. Si $d \perp d'$, $d' \perp d''$ et si d et d'' sont coplanaires, alors $d \parallel d''$.

Exercice 25 (B) (Démonstration du cours) (Corollaire 1.28) Démontrer les propositions suivantes :

1. Si deux droites sont parallèles, alors un plan orthogonal à l'une l'est aussi à l'autre.
2. Si deux plans sont parallèles, alors une droite orthogonale à l'un l'est aussi à l'autre.
3. Par un point de l'espace, il ne passe qu'un unique plan orthogonal à une droite donnée.

Exercice 26 (B) Démontrer les propositions suivantes :

1. Par un point de l'espace, il passe une et une seule droite orthogonale à un plan donné.
2. Soit P_1 et P_2 des plans perpendiculaires, alors P_1 et P_2 sont sécants.
3. Soit 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.
4. Deux droites orthogonales à un même plan sont parallèles.

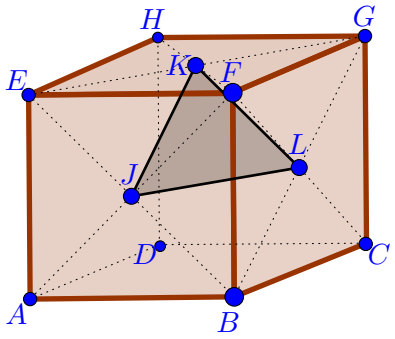
Exercice 27 (B) (Examen 2009) On considère un parallélogramme $ABCD$ de centre O (l'intersection des diagonales) et I l'orthocentre du triangle OBC.

1. Montrer que les droites (OI) et (BC) sont perpendiculaires.
2. Soit K l'orthocentre du triangle OAD.
   (a) Montrer que les points K, O et I sont alignés.
   (b) Montrer que (AK) et (IC) sont parallèles.
   (c) Montrer que $OK = OI$.
   (d) En déduire que O est le milieu de $[IK]$.
3. Soient les points J et L, orthocentres respectifs des triangles OCD et AOB. Quelle est la nature du quadrilatère $IJKL$?

Exercice 28 Soit $ABCDEFGH$ un cube (un solide dont les faces sont toutes des carrés de même coté et tel que les faces opposées soient parallèles).

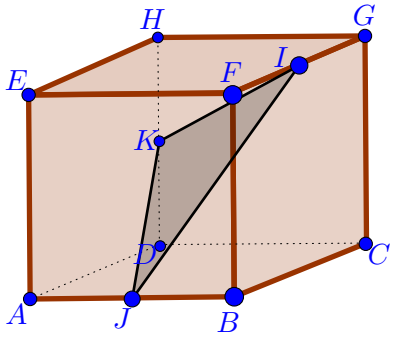
1. Montrer que les faces adjacentes sont perpendiculaires.
2. Montrer que $ABGH$ est un rectangle. Calculer AG en fonction de AB.
3. Montrer que $[AG]$ et $[BH]$ se coupent en leur milieu. Notons ce milieu O.
4. Les diagonales d'un cube sont-elles perpendiculaires ?

Exercice 29 On considère un cube $ABCDEFGH$, où les points J, K et L sont les centres respectifs des faces $(ABEF)$, $(EFGH)$, et $(BCGF)$ (voir la figure ci-contre).



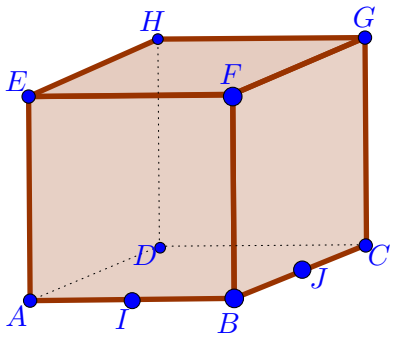
1. Quelle est la nature du triangle JKL ? (Justifiez)
2. Démontrer que F est équidistants des points J, K et L.
3. Démontrer que D est équidistants des points J, K et L.
4. En déduire que la droite (FD) est orthogonale au plan (JKL).

Exercice 30 On considère un cube $ABCDEFGH$, où les points I, J et K sont les milieux respectifs des côtés $[FG]$, $[AB]$ et $[DH]$ (voir la figure ci-contre).



1. Démontrer que la droite (EC) est orthogonale au plan (IJK).
2. Démontrer que IJK est un triangle équilatéral.

Exercice 31 Soit $ABCDEFGH$ un cube. Soit I le milieu de $[AB]$ et J le milieu de $[BC]$ (voir la figure ci-contre).



1. Quelle est la droite parallèle à (HF) passant par B.
2. Donner le tracer de la droite parallèle à (EG) passant par I. (en justifiant)
3. (IJ) et (EG) sont-elles parallèles ? Si c'est le cas, expliquer pourquoi. Sinon justifier.

Exercice 32 (B) Soit $ABCDE$ une pyramide de base $ABCD$ et dont tous les côtés sont de longueur 7 mètres. Soit O l'intersection des diagonales du carré $ABCD$, la hauteur de la pyramide est la longueur du segment $[OE]$. Calculer la hauteur de la pyramide. En déduire que la hauteur de la pyramide multipliée par la longueur de la diagonale de la base est égale à 49 mètres.

Exercice 33 (B) Soit $SABC$ un tétraèdre. La droite (SA) est orthogonale au plan (ABC) et le triangle ABC est rectangle en B.

1. Le but de cette question est de montrer que SBC est rectangle en B.
   (a) Démontrer que (BC) et (SA) sont orthogonales.
   (b) Démontrer que le triangle SBC est rectangle en B.
2. 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.
   (a) Démontrer que les droites (HI) et (BC) sont parallèles.
   (b) En déduire que les droites (HI) et (KJ) sont parallèles.
   (c) Démontrer que les droites (KH) et (SA) sont parallèles.
   (d) En déduire que les droites (HK) et (IJ) sont parallèles.
   (e) Démontrer que $HIJK$ est un rectangle.
3. On suppose à présent que $AB = 1$ et que $SA = BC = 2$. On pose $AH = x$.
   (a) Démontrer, en utilisant le théorème de Thalès dans le triangle ABC, que $HI = 2x$.
   (b) Démontrer, en utilisant le théorème de Thalès dans le triangle SAB, que $HK = 2(1 - x)$.
   (c) Calculer l'aire du rectangle HIJK en fonction de x. On note $A(x)$ cette aire.
4. Le but de cette question est de déterminer la nature de $HIJK$.
   (a) Démontrer que $4x(1 - x) = 1 - (1 - 2x)^2$.
   (b) Pour quelle valeur de x l'aire $A(x)$ est-elle maximale ?
   (c) Quelle est alors la position du point H sur $[AB]$.
   (d) Quelle est alors la nature du quadrilatère $HIJK$?

1.11 Pour vos réflexions

Le but de cette section (comme les autres similaires dans ces notes) est de soulever des questions qui provoquent une réflexion, et pas nécessairement d'y répondre complètement. Parfois, les réponses dépassent de loin le contexte de ce cours. Après une bonne période de réflexion, consulter la toile internet sera peut-être une bonne idée.

1. Dans l'esprit des Grecs, on peut considérer que l'aire d'une région du plan est définie (quand c'est possible) de façon telle qu'on ait les propriétés suivantes.
   — L'aire d'un rectangle est le produit de la longueur de ses côtés.
   — Si une région s'obtient en « recollant » deux régions plus petites, alors l'aire de la grande région est la somme des aires des petites.

   Des questions se posent
   — Comment définit-on correctement la notion de recollement ?
   — Quelles sont les régions pour lesquelles on arrive à calculer l'aire ?
   — Par exemple, quand pouvez-vous calculer (seulement avec ces hypothèses, et les constructions par la règle et le compas) l'aire d'un polygone régulier ?
   — En utilisant vos connaissances plus modernes, pouvez-vous répondre à la question précédente ?
2. Pouvez trouvez touts les triplets d'entiers positifs non nuls (a, b, c), tels que $a^2 + b^2 = c^2$? On dit que ce sont des triplets pythagoriciens. Bien entendu, vaut mieux réfléchir un peu avant d'aller chercher une réponse toute faite sur la toile.

Chapitre 2

Introduction à la géométrie vectorielle

L'approche à la géométrie à la manière des Grecs de l'Antiquité rend parfois difficile le raisonnement avec des concepts géométriques comme le parallélisme, la coplanarité ou l'orthogonalité. Sautant quelques siècles de raffinement de ces concepts, nous abordons dans ce chapitre de meilleurs outils : les vecteurs, qui permettent une approche algébrique à la manipulation de constructions géométriques. On peut ainsi mener par calculs les raisonnements géométriques. Introduisant de meilleures abstractions (des notions plus efficaces), le concept de vecteur permet de simplifier, de clarifier et d'unifier les énoncés géométriques. On appréhende alors plus facilement le « pourquoi » de leur véracité. Un des aspects marquants de cette nouvelle approche est qu'elle élimine en grande partie la différence entre la géométrie du plan, et celle de l'espace. Ainsi, les théorèmes s'énoncent d'une façon indépendante de la dimension. De ce fait, on ouvre la porte à la géométrie dans l'espace à n dimension.

La notion de vecteur, et les constructions qui s'y rattachent, sont le fruit du travail de plusieurs mathématiciens du début du XIX^{e} siècle (Bernard Bolzano, Michel Chasles, etc.). Cette démarche trouve aussi sa source dans les idées de René Descartes au XVII^{e}, qui semble avoir été le premier à établir un lien explicite entre l'algèbre et la géométrie.

2.1 Les vecteurs

Notre contexte est encore l'espace $\mathcal{E}$ à trois dimensions (ou parfois le plan $\mathcal{P}$ « inséré » dans l'espace).

Définition. Un **vecteur** u est la donnée
— d'une **longueur** (qu'on appelle aussi sa norme) ;
— d'une **direction**[1] ;

1. C'est une classe d'équivalence de droites pour la relation de parallélisme.

— d'un **sens** (de déplacement le long d'une droite).

Un peu plus techniquement, il peut se représenter (de plusieurs façons !) par une « flèche » allant d'un point A à un point B, et on écrit $u = \overrightarrow{AB}$. La direction de $\overrightarrow{AB}$ correspond à la droite (AB) (ou toute droite qui lui est parallèle) ; son sens correspond à aller de A vers B le long de cette droite, et sa longueur est celle du segment $[AB]$. On dit de cette longueur que c'est la **norme** du vecteur, et on la note $||u|| = AB$.

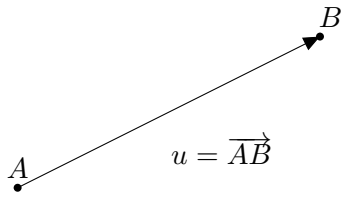


FIGURE 2.1 – Le vecteur allant de A vers B.

On verra ci-dessous qu'un vecteur correspond à une « translation » de l'espace qui déplace A vers B. La définition de vecteurs permet une première réinterprétation (reformulation [2]) des notions géométriques. Par exemple, deux droites (AB) et (CD) sont parallèles si et seulement si les vecteurs $\overrightarrow{AB}$ et $\overrightarrow{CD}$ ont même direction.

Un même vecteur admet plusieurs « descriptions » (équivalentes), et cet aspect de la question est rendu précis via la définition suivante.

Égalité de vecteurs. On dit (décrète [3]) que $\overrightarrow{AD}$ et $\overrightarrow{BC}$ sont **égaux** si et seulement si on a que : soit $ABCD$ est un parallélogramme (ces points sont donc coplanaires), autrement dit

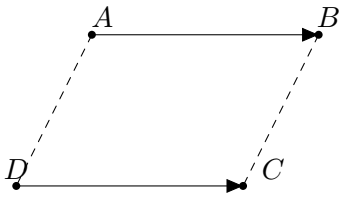
$$ABCD \text{ est un parallélogramme} \quad \Rightarrow \quad \overrightarrow{AD} = \overrightarrow{BC} ;$$

soit les points A, D, B et C sont colinéaires, les segments $[AD]$ et $[BC]$ sont d'égale longueur, et les demi-droites $[AD)$ et $[BC)$ s'intersectent en une demi-droite. Autrement dit, le vecteur $\overrightarrow{BC}$ s'obtient en « glissant » $\overrightarrow{AD}$ sur la droite qui le supporte. Les propriétés des parallélogrammes permettent de montrer facilement que l'égalité est bien définie (c'est une relation d'équivalence).

Remarque. Comme $ABCD$ est un parallélogramme, il en est de même avec $BCDA$, $CDAB$ et $DABC$. D'où

2. D'autres viendront dans les chapitres subséquents.

3. Ceci correspond à identifier $\overrightarrow{AD}$ et $\overrightarrow{BC}$, via une relation d'équivalence, dans l'ensemble quotient associé (voir annexe B).



$$\begin{aligned}\overrightarrow{AD} = \overrightarrow{BC} \\ \Rightarrow \overrightarrow{BA} = \overrightarrow{CD} \\ \Rightarrow \overrightarrow{CB} = \overrightarrow{DA} \\ \Rightarrow \overrightarrow{AB} = \overrightarrow{DC}.\end{aligned}$$

Représentation d'un vecteur : La définition ci-haut permet de fixer un point O comme « origine » de tous les vecteurs. Autrement dit, tout vecteur u (certains dénotent $\vec{u}$ les vecteurs) peut s'écrire sous la forme $u = \overrightarrow{OA}$, pour un certain point A.

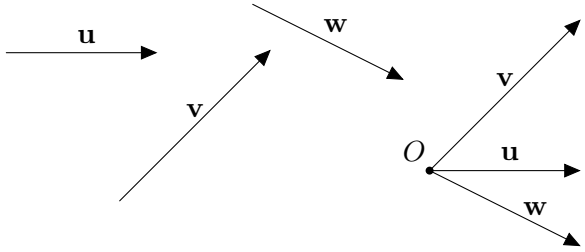


FIGURE 2.2 – Des vecteurs « flottants », et leur réalisation issue de O.

Cette façon de considérer les vecteurs nous amène naturellement à la définition suivante.

Définition (translation). La **translation** $\mathcal{T}_{\mathbf{u}}$ est la transformation de l'espace (ou du plan) qui déplace tous les points dans la direction, le sens et la longueur du vecteur $\mathbf{u}$. Plus précisément, la translation $\mathcal{T}_{\mathbf{u}} : \mathcal{E} \to \mathcal{E}$ est la fonction qui envoie un point M sur le seul point $\mathcal{T}_{\mathbf{u}}(M) = M'$, qui soit tel que $\overrightarrow{MM'} = \mathbf{u}$.

Comme nous allons le montrer, une translation est us cas particulier de ce que l'on appelle une transformation **affine**. Les transformations affines $\mathcal{A} : \mathcal{E} \to \mathcal{E}$ de l'espace envoient les points de l'espace sur des points de l'espace, les droites sur des droites, les plans sur des plans, en respectant les relations d'incidence. En particulier, elles respectent la notion de parallélisme. On peut donc les appliquer aux vecteurs de la manière suivante :

$$\mathcal{A}(\overrightarrow{AB}) = \overrightarrow{\mathcal{A}(A)\mathcal{A}(B)}.$$

Remarque. En un certain sens, la définition de vecteur correspond au fait qu'une translation est entièrement caractérisée par l'image d'un seul point. Autrement dit, si A et B sont deux points donnés alors il existe une unique translation $\mathcal{T}$ telle que $\mathcal{T}(A) = B$. Bien entendu, c'est la translation de vecteur $\overrightarrow{AB}$.

Proposition 2.1. *Soit $\mathcal{T}$ une translation.*

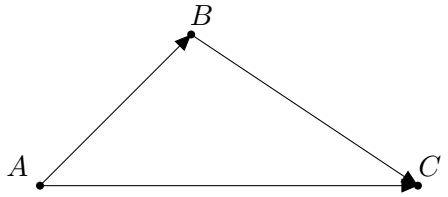
1. *Si d est une droite, alors $\mathcal{T}(d)$ est une droite*[4] *et $\mathcal{T}(d) \parallel d$.*
2. *L'image par $\mathcal{T}$ d'un cercle de centre O, et de rayon R, est un cercle de centre $\mathcal{T}(O)$, et de rayon R.*

Démonstration. Voir exercice 1. ■

2.1.1 Addition de vecteurs, et triangle

L'addition des vecteurs se définit via la « relation de Chasles ». On peut la considérer comme une interprétation algébrique de la notion de triangle.

Définition (Relation de Chasles). Quelque soient A, B, et C dans $\mathcal{E}$, on pose $\overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$, pour tout $A, B, C \in \mathcal{E}$. Comme ceci est compatible[5] avec la notion d'égalité entre représentations de vecteurs, on obtient une notion d'**addition** de vecteurs.



« Partir de A pour aller directement à C, revient au même que de partir de A pour aller en B, pour ensuite aller à C. »

FIGURE 2.3 – Addition géométrique de vecteurs.

Vecteur nul et opposé : Le vecteur $\overrightarrow{AA}$ est appelé le **vecteur nul**, et il est noté $\overrightarrow{0}$ pour aider à le distinguer du nombre 0. Pour tout point on a bien entendu, $\overrightarrow{AA} = \overrightarrow{BB} = \overrightarrow{CC} = \ldots = \overrightarrow{0}$. De plus si $\overrightarrow{AM} = \overrightarrow{0}$, alors $A = M$. Le vecteur $\overrightarrow{BA}$ est le **vecteur opposé** de $\overrightarrow{AB}$ et il est noté $\overrightarrow{BA} = -\overrightarrow{AB}$.

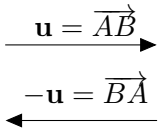


FIGURE 2.4 – Vecteur opposé.

4. On désigne par $\mathcal{T}(d)$ l'ensemble $\{\mathcal{T}(A) | \ A \in d\}$.

5. Techniquement, ceci signifie que : si $\overrightarrow{AB} = \overrightarrow{A'B'}$ et $\overrightarrow{BC} = \overrightarrow{B'C'}$, alors $\overrightarrow{AC} = \overrightarrow{A'C'}$. Attention, ces égalités doivent s'interpréter au sens de la définition plus haut. Elles ne sont donc pas de simples « évidences ».

Proposition 2.2. *Pour tout vecteurs u, v et w, on a les propriétés*

(a) $\mathbf{u} + \overrightarrow{0} = \mathbf{u}$ (élément neutre) ;

(b) $\mathbf{u} + (-\mathbf{u}) = \overrightarrow{0}$ (inverse additif) ;

(c) $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$ (Commutativité) ;

(d) $\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$ (Associativité).

On définit la **soustraction** en posant $\mathbf{u} - \mathbf{v} := \mathbf{u} + (-\mathbf{v})$.

Démonstration. Tout vecteur s'écrit en terme de points : $\mathbf{u} = \overrightarrow{AB}$.

(a) On a $\mathbf{u} + \overrightarrow{0} = \overrightarrow{AB} + \overrightarrow{BB} = \overrightarrow{AB} = \mathbf{u}$.

(b) On a $\mathbf{u} + (-\mathbf{u}) = \overrightarrow{AB} + (-\overrightarrow{AB}) = \overrightarrow{AB} + \overrightarrow{BA} = \overrightarrow{AA} = \overrightarrow{0}$.

(c) Si $\mathbf{u} = \overrightarrow{AB}$ et $\mathbf{v} = \overrightarrow{BC}$, alors $\mathbf{u} + \mathbf{v} = \overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$. Soit D le point tel que $\overrightarrow{AD} = \mathbf{v} = \overrightarrow{BC}$, on obtient donc que $ABCD$ est un parallélogramme. Donc $\overrightarrow{AB} = \overrightarrow{DC} = \mathbf{u}$. On en déduit que $\mathbf{v} + \mathbf{u} = \overrightarrow{AD} + \overrightarrow{DC} = \overrightarrow{AC} = \mathbf{u} + \mathbf{v}$.

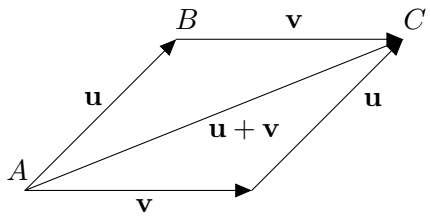


FIGURE 2.5 – Commutativité de l'addition de vecteurs.

(d) On pose $\mathbf{u} = \overrightarrow{AB}, \mathbf{v} = \overrightarrow{BC}, \mathbf{w} = \overrightarrow{CD}$

$$\Rightarrow \begin{cases} \mathbf{u} + (\mathbf{v} + \mathbf{w}) = \overrightarrow{AB} + (\overrightarrow{BC} + \overrightarrow{CD}) = \overrightarrow{AB} + \overrightarrow{BD} = \overrightarrow{AD} \\ (\mathbf{u} + \mathbf{v}) + \mathbf{w} = (\overrightarrow{AB} + \overrightarrow{BC}) + \overrightarrow{CD} = \overrightarrow{AC} + \overrightarrow{CD} = \overrightarrow{AD} \end{cases}$$

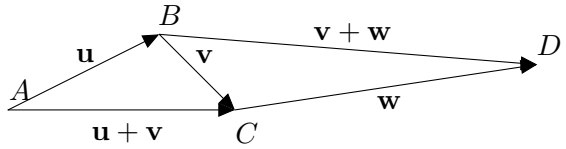


FIGURE 2.6 – Associativité de l'addition de vecteurs.

Une autre façon « classique » de décrire l'addition de vecteurs est la suivante.

Proposition 2.3 (Règle du parallélogramme)**.** *$ABCD$ est un parallélogramme* $\Leftrightarrow$ $\overrightarrow{AB} + \overrightarrow{AD} = \overrightarrow{AC}$.

Démonstration. ($\Leftarrow$)

$$\begin{aligned} \overrightarrow{AC} = \overrightarrow{AB} + \overrightarrow{AD} &\Rightarrow \overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AB} + \overrightarrow{AD} \\ &\Rightarrow \overrightarrow{BC} = \overrightarrow{AD} \text{ (en soustrayant } \overrightarrow{AB}) \\ &\Rightarrow ABCD \text{ est un parallélogramme.} \end{aligned}$$

($\Rightarrow$) $ABCD$ est un parallélogramme $\Rightarrow \overrightarrow{AD} = \overrightarrow{BC} \Rightarrow \overrightarrow{AB} + \overrightarrow{AD} = \overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$.

2.1.2 Multiplication d'un vecteur par un réel

Définition. Soit $\mathbf{u}$ un vecteur, et k un nombre réel (on dit parfois que c'est un **scalaire**, le vecteur $k \cdot \mathbf{u}$ est défini par le fait

- sa longueur est $||k \cdot \mathbf{u}|| = |k| \cdot ||\mathbf{u}||$ c.-à-d. si $\mathbf{u} = \overrightarrow{AB}$, alors $||k \cdot \mathbf{u}|| = |k| \cdot ||\overrightarrow{AB}||$,
- il a la même direction que $\mathbf{u}$, et
- si $k > 0$ il a le même sens que $\mathbf{u}$, et si $k < 0$ il a le sens opposé.

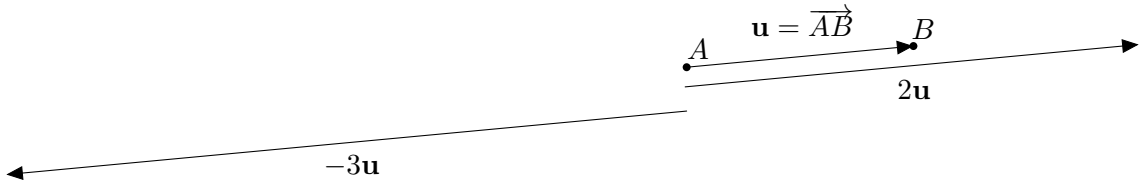


FIGURE 2.7 – Multiplication d'un vecteur par un scalaire.

Proposition 2.4. *Soit $x, y \in \mathbb{R}$, et $\mathbf{u}$, $\mathbf{v}$ des vecteurs, alors on a les propriétés suivantes*

(a) $1 \cdot \mathbf{u} = \mathbf{u}$, $x \cdot \overrightarrow{0} = \overrightarrow{0}$ *et* $0 \cdot \mathbf{u} = \overrightarrow{0}$ *;*

(b) $x \cdot (y \cdot \mathbf{u}) = (x \cdot y) \cdot \mathbf{u}$ *;*

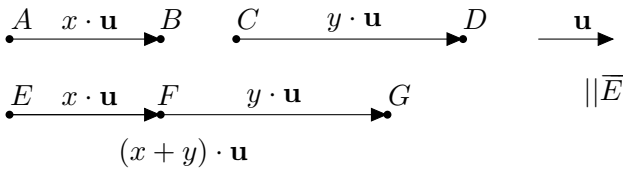
(c) $(x + y) \cdot \mathbf{u} = x \cdot \mathbf{u} + y \cdot \mathbf{u}$ (distributivité) *;*

(d) $x \cdot (\mathbf{u} + \mathbf{v}) = x \cdot \mathbf{u} + x \cdot \mathbf{v}$ (Théorème de Thalès).

Idée de la preuve. On rappelle que pour montrer l'égalité entre deux vecteurs on peut soit construire un parallélogramme, soit montrer que ces deux vecteurs ont même norme, sens et direction.

(a) et (b) sont conséquence du fait que $||k \cdot \mathbf{u}|| = |k| \cdot ||\mathbf{u}||$.

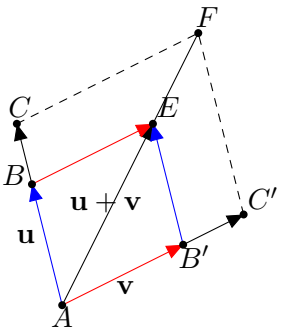
(c) Supposons que $x \cdot \mathbf{u}$, $y \cdot \mathbf{u}$ et $(x+y) \cdot \mathbf{u}$ ont le même sens, c'est-à-dire que $x, y > 0$ ou $x, y < 0$. Le dessin ci-dessous illustre comment montrer que les deux vecteurs $(x+y) \cdot \mathbf{u}$ et $x \cdot \mathbf{u} + y \cdot \mathbf{u}$ ont même norme, même direction et même sens.



$$||\overrightarrow{EG}|| = (|x| + |y|)||\cdot \mathbf{u}|| = ||x \cdot \mathbf{u} + y \cdot \mathbf{u}||,$$

FIGURE 2.8 – La distributivité $(x+y) \cdot \mathbf{u} = x \cdot \mathbf{u} + y \cdot \mathbf{u}$.

Dans le cas où $x \cdot \mathbf{u}$, $y \cdot \mathbf{u}$ et $(x+y) \cdot \mathbf{u}$ n'ont pas le même sens, c'est-à-dire que $x < 0 < y$ ou $y < 0 < x$, il suffit alors de soustraire les longueurs des segments, car le point E se trouvera entre les points F et G.



(d) On suppose $k > 0$ (sinon il suffit de prendre $(-k)(-\mathbf{u})$). Cette propriété est une conséquence du théorème de Thalès. On pose $\mathbf{u} = \overrightarrow{AB}, k \cdot \mathbf{u} = \overrightarrow{AC}, \mathbf{v} = \overrightarrow{AB'}$ et $k \cdot \mathbf{v} = \overrightarrow{AC'}$. Par la règle du parallélogramme, on a $\mathbf{u} + \mathbf{v} = \overrightarrow{AE}$ avec $ABEB'$ parallélogramme. Soit $F \in (AE)$ tel que $AF/AE = k$,

(i) la parallèle à (BE) passant par C coupe (AE) en F. En effet, $AC/AB = k = AF/AE$ donc par la réciproque du théorème de Thalès on obtient que $(CF) \parallel (BE)$.

(ii) De même, la parallèle à $(B'E)$ passant par C' coupe (AE) en F.

(iii) Donc $ACFC'$ est un parallélogramme et $k \cdot \mathbf{u} + k \cdot \mathbf{v} = \overrightarrow{AC} + \overrightarrow{AC'} = \overrightarrow{AF}$. Comme $\overrightarrow{AF} = k \cdot (\mathbf{u} + \mathbf{v})$, on obtient $k \cdot \mathbf{u} + k \cdot \mathbf{v} = k \cdot (\mathbf{u} + \mathbf{v})$ ■

Remarque. On constate qu'on a « traduit » les principaux objets de la géométrie en propriété algébrique : *bref, l'algèbre linéaire est née !* Nous invitons le lecteur à consulter un livre de géométrie moderne, par exemple [Audin 2006], pour mieux apprécier l'importance de l'algèbre linéaire pour la géométrie.

Exemple : la multiplication par un scalaire d'un vecteur, alliée à l'addition de vecteurs, permet de définir le milieu d'un segment de plusieurs façons. Par exemple, le milieu du segment $[AB]$ est l'unique point I tel que $\overrightarrow{AI} = \frac{1}{2} \cdot \overrightarrow{AB}$. Ou encore, c'est l'unique point I tel que $\overrightarrow{IA} + \overrightarrow{IB} = \overrightarrow{0}$.

2.1.3 Homothétie

Nous avons souligné au début de ce chapitre que la définition même de vecteur pouvait être considérée comme une transformation de l'espace : la *translation*. Il en est de même avec la multiplication d'un vecteur par un scalaire.

Définition (homothétie). L'homothétie de centre O, et de facteur r, est la transformation (affine) qui rapproche (ou éloigne) un point M de l'origine O, selon une proportion r. Plus précisément, **l'homothétie** $\mathcal{H}_{O,k}$, de centre O et de rapport $r \in \mathbb{R}^*$, est la fonction qui envoie tout point M de l'espace sur l'unique point $M' = \mathcal{H}_{O,r}(M)$ qui soit tel que $\overrightarrow{OM'} = r \cdot \overrightarrow{OM}$.

Remarque. Une homothétie est caractérisée par le choix de son centre, d'un point, et de l'image de ce point. Plus précisément, si O, A et B sont trois points distincts alignés, alors il existe une unique homothétie $\mathcal{H}$ de centre O tel que $\mathcal{H}(A) = B$. Le rapport $\mathcal{H}$ est $r = \pm OB/OA$; le signe est positif si et seulement si $\overrightarrow{OA}$ et $\overrightarrow{OB}$ ont même sens.

Proposition 2.5. *Soit $\mathcal{H}$ une homothétie de centre A et de rapport r non nul.*

1. *Si $r \neq 1$, A est l'unique point fixe de $\mathcal{H}$.*
2. *Pour tout point M, on a que A, M et $\mathcal{H}(M)$ sont alignés.*
3. *Si d est une droite alors $\mathcal{H}(d)$ est une droite et $\mathcal{H}(d) \parallel d$.*
4. *L'image par $\mathcal{H}$ d'un cercle de centre O et de rayon R est un cercle de centre $\mathcal{H}(O)$ et de rayon $R \cdot |r|$.*

Démonstration. Voir exercice 2. ■

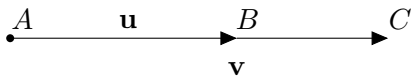
2.2 Vecteurs colinéaires, droites et parallélisme

Définition. Deux vecteurs non nuls $\mathbf{u}$ et $\mathbf{v}$ sont **colinéaires** si et seulement si $\mathbf{u} = \overrightarrow{AB}$, $\mathbf{v} = \overrightarrow{AC}$, et A, B et C sont alignés.

Remarque. Bien entendu $\mathbf{u}$ et $\mathbf{u}$ sont colinéaires.

Proposition 2.6. *$\mathbf{u}$ et $\mathbf{v}$ non nuls sont colinéaires $\Leftrightarrow$ $\exists\, r \neq 0$ tel que $\mathbf{u} = r \cdot \mathbf{v}$*

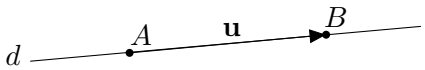
Démonstration.



($\Rightarrow$) On pose $\mathbf{u} = \overrightarrow{AB}, \mathbf{v} = \overrightarrow{AC}$ et A, B et C alignés distincts. On pose $r = \frac{||\mathbf{u}||}{||\mathbf{v}||}$ $\left(||\mathbf{v}|| \neq 0, \text{ car } \overrightarrow{AC} \neq \overrightarrow{0}\right)$. Comme $r = AB/AC$, on a bien que $AB = \frac{AB}{AC} \cdot AC$. On en déduit que $||r \cdot \mathbf{v}|| = ||\mathbf{u}||$. De plus, $r \cdot \mathbf{v}$ et $\mathbf{u}$ ayant le même sens et la même direction ($r > 0$), on conclut que $r \cdot \mathbf{v} = \mathbf{u}$.

($\Leftarrow$) Soit A, B, et C tels que $\mathbf{u} = \overrightarrow{AB}$ et $\mathbf{v} = \overrightarrow{AC}$. Comme $\mathbf{u} = r \cdot \mathbf{v}$, $\mathbf{u}$ et $\mathbf{v}$ ont même direction et il s'en suit que A, B et C sont alignés.

Définition. Soit d une droite. On dit qu'un vecteur $\mathbf{u} = \overrightarrow{AB}$ est un **vecteur directeur** de d, si A et B sont distincts et $d = (AB)$. Autrement dit, A et B sont incidents à d.



- Le couple $(A, \mathbf{u})$ constitue un repère (affine) de la droite d.
- Un point $M \in d$ est **repéré** par sa coordonnée x telle que $\overrightarrow{AM} = x \cdot \mathbf{u}$. Il est uniquement caractérisé par x.

Corollaire 2.7.

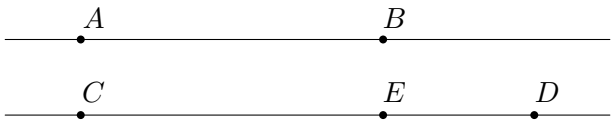
(i) *Soit A, B, et C trois points distincts alors : A, B, et C sont alignés $\Leftrightarrow$ $\overrightarrow{AB}$ et $\overrightarrow{AC}$ sont colinéaires.*

(ii) *Soit A, B, C, et D quatre points distincts, alors : $(AB) \parallel (CD)$ $\Leftrightarrow$ $\overrightarrow{AB}$ et $\overrightarrow{CD}$ colinéaires.*

Démonstration.

(i) Immédiat par définition.

(ii) On a la figure suivante



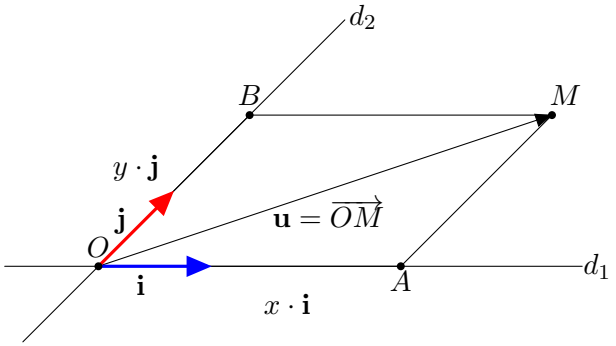
($\Rightarrow$) Soit E tel que $\overrightarrow{AB} + \overrightarrow{AC} = \overrightarrow{AE}$. Alors $ABEC$ est un parallélogramme. Donc $(CE) \parallel (AB)$, d'où $E \in (CD)$, car (CD) est l'unique parallèle à (AB) passant par C. Il s'ensuit que $\overrightarrow{AB} = \overrightarrow{CE}$ est colinéaire à $\overrightarrow{CD}$.

($\Leftarrow$) On sait que $\overrightarrow{AB} = r \cdot \overrightarrow{CD}$, pour un certain $r \neq 0$ et $\overrightarrow{AB}$ et $\overrightarrow{CD}$ sont des vecteurs directeurs de (AB) et (CD). Il faut montrer que A, B, et C et D sont coplanaires, et que soit $(AB) = (CD)$, soit $(AB) \cap (CD) = \emptyset$.
Si E est tel que $\overrightarrow{CE} = r \cdot \overrightarrow{CD}$. En vertu de (i) les points C, D et E sont alignés. Donc pour montrer que A, B, et C et D sont coplanaires, il suffit de montrer que A, B, et C et E sont coplanaires. Comme $\overrightarrow{AB} = r \cdot \overrightarrow{CD} = \overrightarrow{CE}$, on a que $ABEC$ est un parallélogramme. En particulier, A, B, et C et E sont coplanaires
Supposons que $(AB) \cap (CD) \neq \emptyset$, c'est-à-dire qu'il existe $F \in (AB) \cap (CD)$. Alors $M \in (AB)$ s'écrit $\overrightarrow{FM} = x \cdot \overrightarrow{AB} = x \cdot r \cdot \overrightarrow{CD}$. De ce fait, tout point M de (AB) est aussi un point de (CD). Autrement dit $(AB) = (CD)$.

2.3 Repère affine du plan

Une des idées qui a grandement modifié la relation entre la géométrie et l'algèbre, due à René Descartes, se base sur l'utilisation de **coordonnées** pour désigner un point de l'espace (ou du plan). Cela permet autant de définir et manipuler efficacement les objets géométriques par des calculs algébriques, que de donner un sens géométrique à des questions d'algèbre. Cette idée est tellement bien imbriquée dans notre culture, qu'on oublie souvent ce qu'elle a eu de révolutionnaire en son temps. Elle a ouvert la porte à l'émergence de plusieurs nouveaux domaines des mathématiques : géométrie algébrique, algèbre géométrique, théorie des invariants, etc. Les quatre sections qui suivent en développent la base.

Dans le plan $\mathcal{P}$, on se donne deux vecteurs non colinéaires $\mathbf{i}$ et $\mathbf{j}$, et un point O qui jouera le rôle d'origine.



Soit d_1 la droite passant par O et de vecteur directeur $\mathbf{i}$ et d_2 celle de vecteur directeur $\mathbf{j}$.

Pour un point M du plan, on procède à la construction suivante.

— On trouve A, le point d'intersection entre la droite d_1 et la parallèle à d_2 passant par M ;

— ainsi que B le point d'intersection entre la droite d_2 et la parallèle à d_1 passant par M.

On observe que $\mathbf{j}$ et $\overrightarrow{OB}$ sont colinéaires, ainsi que $\mathbf{i}$ et $\overrightarrow{OA}$. Il existe donc d'uniques scalaires x et y, tels que

$$\overrightarrow{OM} = \overrightarrow{OA} + \overrightarrow{OB} = x \cdot \mathbf{i} + y \cdot \mathbf{j}.$$

Afin de transformer cette propriété en proposition, on se donne la définition suivante.

Définition. On dit d'un triplet $(O, \mathbf{i}, \mathbf{j})$ satisfaisant les conditions ci-haut que c'est un **repère affine** du plan.

Proposition 2.8.

(i) *Pour tout point M du plan, il existe un unique couple (x, y) tel que*

$$\overrightarrow{OM} = x \cdot \mathbf{i} + y \cdot \mathbf{j}.$$

Le couple (x, y) correspond aux **coordonnées** *de M dans le repère $(O, \mathbf{i}, \mathbf{j})$.*

(ii) *Pour tout vecteur $\mathbf{u}$ du plan, il existe un unique couple (x, y) tel que*

$$\mathbf{u} = x \cdot \mathbf{i} + y \cdot \mathbf{j},$$

Le couple (x, y) correspond aux coordonnées du vecteur $\mathbf{u}$ dans le repère $(O, \mathbf{i}, \mathbf{j})$.

Démonstration. Comme tout vecteur $\mathbf{u}$ peut s'écrire sous la forme $\overrightarrow{OM}$, (ii) est une conséquence de (i) qui a été prouvée en prélude à cette proposition. ∎

Remarque.

(i) $\overrightarrow{OO} = \overrightarrow{0}$, donc O a pour coordonné $(0, 0)$.

(ii) $\mathbf{i}$ a pour coordonnée $(1, 0)$ et $\mathbf{j}$ a pour coordonnée $(0, 1)$.

(iii) Si les coordonnées de A sont (x_A, y_A), et celles de B sont (x_B, y_B), alors le vecteur $\overrightarrow{AB}$ a pour coordonnée $(x_B - x_A, y_B - y_A)$, 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 coordonnée $((x_B + x_A)/2, (y_B + y_A)/2)$, car

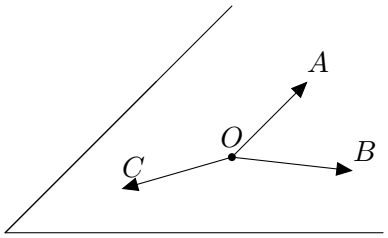
$$\overrightarrow{OI} = \overrightarrow{OA} + \overrightarrow{AI} = \overrightarrow{OA} + \frac{1}{2}\overrightarrow{AB} = \frac{1}{2}\overrightarrow{OA} + \frac{1}{2}\overrightarrow{OB}.$$

2.4 Vecteurs coplanaires

Nous venons de voir que dans le plan, tout point est entièrement déterminé par ses coordonnées par rapport au choix d'une origine, et de deux vecteurs non colinéaires. Autrement dit, les points du plan sont entièrement déterminés par la donnée d'un repère affine (du plan). Sur un plan de l'espace, cette propriété demeure vraie : c.-à-d. que tous les points de l'espace plan sont entièrement déterminés par la donnée d'un repère affine de ce plan, à savoir la donnée d'un point du plan (servant d'origine dans ce plan), et de deux vecteurs non colinéaires de ce plan.

Définition. Trois vecteurs $\mathbf{u}, \mathbf{v}, \mathbf{w}$ sont **coplanaires** dans $\mathcal{E}$ s'il existe quatre points coplanaires O et A, B, C tels que

$$\mathbf{u} = \overrightarrow{OA}, \ \mathbf{v} = \overrightarrow{OB}, \quad \text{et} \quad \mathbf{w} = \overrightarrow{OC}$$



Remarque. Si $\mathbf{u}, \mathbf{v}, \mathbf{w}$ sont colinéaires, ils sont évidement coplanaires.

Corollaire 2.9. *Soit* $\mathbf{u}, \mathbf{v}$ *et* $\mathbf{w}$ *trois vecteurs, avec* $\mathbf{u}$ *et* $\mathbf{v}$ *non colinéaires. Alors* $\mathbf{u}, \mathbf{v}$ *et* $\mathbf{w}$ *sont coplanaires* $\Leftrightarrow$ *il existe* x, y *réels tels que* $\mathbf{w} = x \cdot \mathbf{u} + y \cdot \mathbf{v}$. *On dit que* $\mathbf{w}$ *est une combinaison linéaire de* $\mathbf{u}$ *et* $\mathbf{v}$.

Démonstration. $\mathbf{u} = \overrightarrow{AB}, \mathbf{v} = \overrightarrow{AC}$ avec A, B, et C trois points non alignés, car $\mathbf{u}, \mathbf{v}$ sont non colinéaires. Alors (ABC) est un plan et $(A, \mathbf{u}, \mathbf{v})$ est un repère de $\mathcal{P}$. Le corollaire s'en suit. ■

Nous pouvons maintenant simplifier l'énoncé, et la preuve, de la proposition 1.24.

Proposition 2.10 (Critère de parallélisme des plans de l'espace)**.** $(ABC) \parallel (EFG) \Leftrightarrow \overrightarrow{AB}, \overrightarrow{AC}, \overrightarrow{EF}$ *et* $\overrightarrow{EG}$ *sont coplanaires.*

Démonstration. Soit (ABC) et (EFG) deux plans de l'espace. Alors $(A, \overrightarrow{AB}, \overrightarrow{AC})$ et $(E, \overrightarrow{EF}, \overrightarrow{EG})$ sont des repères de (ABC) et (EFG).

($\Rightarrow$) Si $(ABC) \parallel (EFG)$, alors il existe deux droites sécantes (EF') et (EG') respectivement parallèles à (AB) et (AC). On peut choisir $F', G' \in (EFG)$ tel que $\overrightarrow{AB} = \overrightarrow{EF'}$ et $\overrightarrow{AC} = \overrightarrow{EG'}$. Donc $(E, \overrightarrow{EF'}, \overrightarrow{EG'})$ est un repère de (EFG)

$$\Rightarrow \begin{cases} \overrightarrow{EF} = x \cdot \overrightarrow{EF'} + y \cdot \overrightarrow{EG'} = x \cdot \overrightarrow{AB} + y \cdot \overrightarrow{AC} \\ \overrightarrow{EG} = x' \cdot \overrightarrow{EF'} + y' \cdot \overrightarrow{EG'} = x' \cdot \overrightarrow{AB} + y' \cdot \overrightarrow{AC} \end{cases} \Rightarrow \overrightarrow{AB}, \overrightarrow{AC}, \overrightarrow{EF} \text{ et } \overrightarrow{EG} \text{ coplanaires.}$$

($\Leftarrow$) Si $\overrightarrow{AB}, \overrightarrow{AC}, \overrightarrow{EF}$ et $\overrightarrow{EG}$ sont coplanaires, alors $\overrightarrow{EF} = x \cdot \overrightarrow{AB} + y \cdot \overrightarrow{AC}$ et $\overrightarrow{EG} = x' \cdot \overrightarrow{AB} + y' \cdot \overrightarrow{AC}$. Soit B' et C' dans (ABC) tels que

$$\begin{cases} \overrightarrow{AB'} = x \cdot \overrightarrow{AB} + y \cdot \overrightarrow{AC} \\ \overrightarrow{AC'} = x' \cdot \overrightarrow{AB} + y' \cdot \overrightarrow{AC}, \end{cases}$$

alors $(AB') \parallel (EF)$, $(AC') \parallel (EG)$, (AB') et (AC') sécantes, et (EF) et (EG) sécantes

$$\Rightarrow (ABC) \parallel (EFG).$$

■

2.5 Repère de l'espace

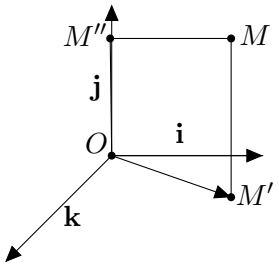
Définition. Dans $\mathcal{E}$ on se donne trois vecteurs non coplanaires $\mathbf{i}$, $\mathbf{j}$ et $\mathbf{k}$ et un point (origine) O. On dit alors que le quadruplet $(O, \mathbf{i}, \mathbf{j}, \mathbf{k})$ est un **repère affine** de $\mathcal{E}$.

Proposition 2.11. *Pour tout point M du plan, il existe un unique triplet (x, y, z) tel que*

$$\overrightarrow{OM} = x \cdot \mathbf{i} + y \cdot \mathbf{j} + z \cdot \mathbf{k}.$$

On dit alors que le triplet (x, y, z) corresponds aux **coordonnés** *de M selon le repère $(O, \mathbf{i}, \mathbf{j}, \mathbf{k})$.*

Démonstration. Soit M' le point d'intersection entre la droite passant par M et de vecteur directeur $\mathbf{j}$ et le plan $(O, \mathbf{i}, \mathbf{k})$. Soit M'' le point d'intersection entre la droite $(O, \mathbf{j})$ et le plan $(M, \mathbf{i}, \mathbf{k})$ (parallèle à $(O, \mathbf{i}, \mathbf{k})$). Alors $\overrightarrow{OM''} = y \cdot \mathbf{j}$ et $\overrightarrow{OM'} = x \cdot \mathbf{i} + z \cdot \mathbf{k}$. Or, $\overrightarrow{OM} = \overrightarrow{OM'} + \overrightarrow{OM''} = x \cdot \mathbf{i} + y \cdot \mathbf{j} + z \cdot \mathbf{k}$. $((OM''MM')$ est un parallélogramme dans le plan (OMM'), car $(OM'') \subseteq (OMM'))$. ■

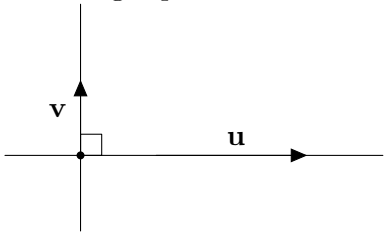


2.6 Orthogonalité, et produit scalaire

2.6.1 Repères orthonormés

Définition.

— On dit que deux vecteurs $\mathbf{u}$ et $\mathbf{v}$ sont **orthogonaux** (ce fait est noté $\mathbf{u} \perp \mathbf{v}$) si la droite dirigée par $\mathbf{u}$ est perpendiculaire à la droite dirigée par $\mathbf{v}$.



— Un repère $(O, \mathbf{i}, \mathbf{j})$ du plan est dit **orthogonal** si et seulement si $\mathbf{i} \perp \mathbf{j}$. De façon similaire, un repère $(O, \mathbf{i}, \mathbf{j}, \mathbf{k})$ de l'espace est dit **orthogonal** si et seulement si on a respectivement $\mathbf{i} \perp \mathbf{j}$,

$\mathbf{i} \perp \mathbf{k}$ et $\mathbf{j} \perp \mathbf{k}$. De plus, ces repères sont dits **orthonormés** si $||\mathbf{i}|| = 1$, $||\mathbf{j}|| = 1$, et (au besoin) $||\mathbf{k}|| = 1$.

2.6.2 Produit scalaire, et théorème de Pythagore

Définition. Soit $(O, \mathbf{i}, \mathbf{j}, \mathbf{k})$ un repère orthonormé. Soit $\mathbf{u} = x \cdot \mathbf{i} + y \cdot \mathbf{j} + z \cdot \mathbf{k}$ et $\mathbf{v} = x' \cdot \mathbf{i} + y' \cdot \mathbf{j} + z' \cdot \mathbf{k}$. Le **produit scalaire** de $\mathbf{u}$ et $\mathbf{v}$ est le nombre réel :

$$\langle \mathbf{u}, \mathbf{v} \rangle = x \cdot x' + y \cdot y' + z \cdot z'.$$

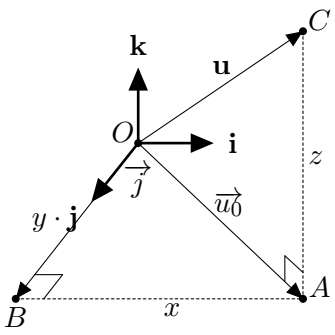
On écrit aussi $\langle (x, y, z), (x', y', z') \rangle = x \cdot x' + y \cdot y' + z \cdot z'$.

Proposition 2.12. *Pour tout vecteur* $\mathbf{u} = x \cdot \mathbf{i} + y \cdot \mathbf{j} + z \cdot \mathbf{k}$ *on a :*

$$||\mathbf{u}||^2 = \langle \mathbf{u}, \mathbf{u} \rangle = x^2 + y^2 + z^2.$$

Démonstration. On considère d'abord le cas du plan en supposant que $z = 0$. Soit A et B les points tels que $\overrightarrow{OB} = y \cdot \mathbf{j}$ et $\overrightarrow{OA} = \mathbf{u} = x \cdot \mathbf{i} + y \cdot \mathbf{j}$. Alors $\overrightarrow{AB} = -\overrightarrow{OA} + \overrightarrow{AB} = x \cdot \mathbf{i}$. Donc $\overrightarrow{AB} = x \cdot \mathbf{i}$ est orthogonal à $y \cdot \mathbf{j} = \overrightarrow{OB}$. De ce fait, OBA est un triangle rectangle en B. En vertu du théorème de Pythagore, on en déduit que :

$$||\mathbf{u}||^2 = OA^2 = OB^2 + BA^2 = ||y \cdot \mathbf{j}||^2 + ||x \cdot \mathbf{i}||^2 = x^2 + y^2 + 0 \cdot 0 = \langle \mathbf{u}, \mathbf{u} \rangle.$$



Cas général : Soit $\mathbf{u}_0 = x \cdot \mathbf{i} + y \cdot \mathbf{j}$. Donc $\mathbf{u} = \mathbf{u}_0 + z \cdot \mathbf{k}$. Soit A et C des points tels que $\overrightarrow{OA} = \mathbf{u}_0$ et $\overrightarrow{OC} = \mathbf{u}$. Alors $\overrightarrow{AC} = -\overrightarrow{OA} + \overrightarrow{AC} = z \cdot \mathbf{k}$. Donc $\overrightarrow{AC} = z \cdot \mathbf{k}$ est orthogonal à $x \cdot \mathbf{i} + y \cdot \mathbf{j} = \mathbf{u}_0 = \overrightarrow{OA}$. De ce fait, OAC est un triangle rectangle en A. En vertu du théorème de Pythagore et du cas où $z = 0$, on en déduit que :

$$||\mathbf{u}||^2 = OC^2 = OA^2 + AC^2 = ||\mathbf{u}_0||^2 + ||z \cdot \mathbf{k}||^2 = x^2 + y^2 + z^2 = \langle \mathbf{u}, \mathbf{u} \rangle.$$

■

Par simple calcul de produit scalaire, en utilisant la proposition ci-dessus, on déduit ce qui suit.

Corollaire 2.13. *On a pour tout vecteur* $\mathbf{u}$, $\mathbf{v}$ *et* $\mathbf{w}$ *les énoncés suivants :*

1. $\langle \mathbf{u}, \mathbf{v} \rangle = \frac{1}{2}(||\mathbf{u}+\mathbf{v}||^2 - ||\mathbf{u}||^2 - ||\mathbf{v}||^2)$;
2. $\langle \mathbf{u}, (\mathbf{v}+\mathbf{w}) \rangle = \langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{u}, \mathbf{w} \rangle$ *(distributivité) ;*
3. $\lambda \cdot (\langle \mathbf{u}, \mathbf{v} \rangle) = \langle (\lambda \cdot \mathbf{u}), \mathbf{v} \rangle = \langle \mathbf{u}, (\lambda \cdot \mathbf{v}) \rangle$ *pour tout scalaire* $\lambda \in \mathbb{R}$;
4. $\langle \mathbf{u}, \mathbf{v} \rangle = \langle \mathbf{v}, \mathbf{u} \rangle$ *(commutativité).*

Nous sommes maintenant en mesure de « traduire » le théorème de Pythagore en forme algébrique. Soit $\mathbf{u}$ et $\mathbf{v}$ deux vecteurs. Soit A, B et C trois points tels que $\overrightarrow{AB} = \mathbf{u}$ et $\overrightarrow{BC} = \mathbf{v}$ et donc $\mathbf{u}+\mathbf{v} = \overrightarrow{AC}$. Alors on a que

$$AC^2 = ||\mathbf{u}+\mathbf{v}||^2 = ||\mathbf{u}||^2 + ||\mathbf{v}||^2 = AB^2 + BC^2.$$

si et seulement si le triangle ABC est rectangle en B, en vertu du théorème de Pythagore. En d'autres termes, ces égalités sont vraies si et seulement si $\mathbf{u} \perp \mathbf{v}$. Nous obtenons donc le résultat suivant.

Théorème 2.14 (Théorème de Pythagore)**.** *Soit* $\mathbf{u}$ *et* $\mathbf{v}$ *deux vecteurs, les énoncés suivants sont équivalents :*

(a) $||\mathbf{u}+\mathbf{v}||^2 = ||\mathbf{u}||^2 + ||\mathbf{v}||^2$;

(b) $\mathbf{u} \perp \mathbf{v}$;

(c) $\langle \mathbf{u}, \mathbf{v} \rangle = 0$.

Démonstration. (b) $\Leftrightarrow$ (c) est une conséquence de la première formule du corollaire ci-dessus. ■

2.7 Barycentres

En physique, surtout en mécanique, la notion de « point d'équilibre » ou « centre de masse » est fondamentale. Par exemple, on considère un polygone, à n-sommets, aux sommets duquel on attache des poids respectifs a_1, …, a_n. On cherche par quel point « retenir » le polygone pour avoir équilibre. La notion mathématique correspondante est la notion de « barycentre ». Elle met en évidence le fait que le calcul de vecteurs permet d'obtenir facilement ce centre de masse.

Définition. Soit $A_1, A_2, \ldots, A_n \in \mathcal{E}$ et $a_1, \ldots, a_n$ des réels (incluant des valeurs négatives). On dit que le n-uplet $((A_1, a_1), \ldots, (A_n, a_n))$ est un **système de points pondérés**.

Proposition 2.15. *Soit* $((A_1, a_1), \ldots, (A_n, a_n))$ *un système de points pondérés tel que* $\sum_{i=1}^{n} a_i = a_1 + a_2 + \ldots + a_n \neq 0$*, alors il existe un unique point* G *tel que*

$$\sum_{i=1}^{n} a_i \cdot \overrightarrow{GA_i} = \overrightarrow{0}.$$

De plus, pour tout point $M \in \mathcal{E}$, on a

$$\sum_{i=1}^{n} a_i \cdot \overrightarrow{MA_i} = (\sum_{i=1}^{n} a_i) \cdot \overrightarrow{MG}.$$

Remarque. Si $a_1 = a_2 = \ldots = a_n$, on dit que G est le **centre de gravité** des points $A_1, \ldots, A_n$.

Exemple.

1. I est le milieu de $[AB] \Leftrightarrow$ I centre de gravité de A et B. En effet,
$$\begin{aligned} \overrightarrow{IA} = \overrightarrow{BI} &\Leftrightarrow \overrightarrow{IA} - \overrightarrow{BI} = \overrightarrow{IA} + \overrightarrow{IB} = \overrightarrow{0} \\ &\Leftrightarrow I \text{ centre de gravité de } A \text{ et } B. \end{aligned}$$

2. Soit ABC un triangle. On attache à A le poids 2, à B le poids 3 et à C le poids -1 (on peut imaginer qu'au lieu d'un poids, quelqu'un tire vers haut sur le sommet C). Voici comment trouver et placer le barycentre G de $(A, 2)$, $(B, 3)$ et $(C, -1)$. On a pour tout point M l'équation suivante, car $2 + 3 + (-1) = 4 \neq 0$:
$$4\overrightarrow{MG} = 2\overrightarrow{MA} + 3\overrightarrow{MB} - \overrightarrow{MC}.$$
En posant le cas particulier $M = C$ par exemple on obtient :
$$\overrightarrow{CG} = \frac{1}{2}\overrightarrow{CA} + \frac{3}{4}\overrightarrow{CB}.$$
Comme les points A, B et C sont donnés, G est donc bien défini par l'équation vectorielle ci-dessus.

Démonstration de la Proposition 2.15.

Existence : $\sum_{i=1}^{n} a_i \cdot \overrightarrow{MA_i}$ est un vecteur. Posons $\mathbf{u} = \sum_{i=1}^{n} a_i \cdot \overrightarrow{MA_i}$. Il existe donc un point B tel que $\mathbf{u} = \overrightarrow{MB}$. Comme $\sum_{i=1}^{n} a_i \neq 0$, on peut poser G le point tel que $\overrightarrow{MG} = \frac{1}{\sum_{i=1}^{n} a_i}\overrightarrow{MB}$. D'où $\sum_{i=1}^{n} a_i \cdot \overrightarrow{MA_i} = (\sum_{i=1}^{n} a_i) \cdot \overrightarrow{MG}$. En posant $M = G$, on retrouve la première formule.

Unicité : Soit G' tel que $\sum_{i=1}^{n} a_i \cdot \overrightarrow{G'A_i} = \overrightarrow{0}$, alors comme précédemment, il existe un point G tel que $\overrightarrow{0} = \sum_{i=1}^{n} a_i \cdot \overrightarrow{G'A_i} = (\sum_{i=1}^{n} a_i) \cdot \overrightarrow{G'G}$. D'où comme $\sum_{i=1}^{n} a_i \neq 0$, on a $\overrightarrow{G'G} = \overrightarrow{0} \Rightarrow G = G'$. ■

Proposition 2.16 (Associativité du barycentre)**.** *Soit G le barycentre de $((A, a), (B, b), (C, c))$, avec $a + b + c \neq 0$. Supposons que $b + c \neq 0$ et notons K le barycentre de $((B, b), (C, c))$. Alors G est le barycentre du système pondéré $((A, a), (K, b + c))$.*

Démonstration. Il suffit de montrer que $a \cdot \overrightarrow{GA} + (b + c) \cdot \overrightarrow{GK} = \overrightarrow{0}$. Comme K est le barycentre de $((B, b), (C, c))$, on a que $b \cdot \overrightarrow{MB} + c \cdot \overrightarrow{MC} = (b + c) \cdot \overrightarrow{MK}$ pour tout point M. En particulier on a avec $M = G$:
$$a \cdot \overrightarrow{GA} + (b + c) \cdot \overrightarrow{GK} = a \cdot \overrightarrow{GA} + b \cdot \overrightarrow{GB} + c \cdot \overrightarrow{GC} = \overrightarrow{0},$$

car G est le barycentre de $((A,a),(B,b),(C,c))$. ■

2.8 Espaces à n dimensions (*)

Avec l'introduction de repères orthonormés, on constate qu'on a unifié l'étude de la géométrie du plan et de la géométrie de l'espace. Cela suggère de poursuivre avec l'étude de la géométrie de l'espace à n dimension. Il suffit en effet de remplacer les vecteurs de dimension 2 ou 3, par des vecteurs de dimension n ; à savoir des vecteurs dont les coordonnées sont $(x_1, x_2, \ldots, x_n)$. Les constructions géométriques se généralisent de manière naturelle, et se manipulent facilement. Par exemple, on peut définir dans l'espace à 4 dimensions la notion d'hypercube, dont les sommets sont les 16 vecteurs $(\pm 1, \pm 1, \pm 1 \pm 1)$, avec un segment qui joint deux sommets si et seulement si ils diffèrent seulement en une de leurs coordonnées. Cet objet abstrait peut ensuite être projeté dans l'espace à 3 dimensions, pour obtenir l'objet représenté à la figure 2.9. Dans l'espace à 4 dimensions, toutes les faces sont congrues, et tous les angles sont droits.

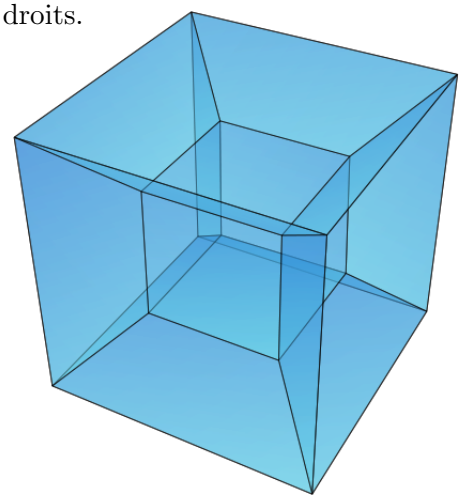


FIGURE 2.9 – Une projection à 3 dimensions de l'hypercube.

En plus d'être d'un grand intérêt pour les mathématiques, la géométrie à n dimension est extrêmement utile en génie, en physique, ou pour le graphisme sur ordinateur. Par exemple, elle permet décrire de manière efficace et claire l'évolution d'un mécanisme complexe. Le contexte naturel est alors un espace qui a autant de dimensions qu'il y a de paramètres nécessaires à la description des états de ce mécanisme. Pour avoir une idée de comment l'étude de l'espace à n dimension s'est développée au départ, on peut lire le texte de Camille Jordan (1838-1922), *Essai sur la géométrie à n dimensions*, dans le Bulletin de la Société Mathématique de France, tom 3 (1875), p 103–174 (qu'on peut télécharger gratuitement ici).

2.9 Exercices du chapitre 2

Homothétie et translation

Exercice 1 (B) (Démonstration du cours) (Proposition 2.1) Soit $\mathcal{T}$ une translation, montrer que :

1. Si d est une droite alors $\mathcal{T}(d)$ est une droite et $\mathcal{T}(d) \parallel d$.
2. L'image par $\mathcal{T}$ d'un cercle de centre O et de rayon R est un cercle de centre $\mathcal{T}(O)$ et de rayon R.

Exercice 2 (B) (Démonstration du cours) (Proposition 2.5) Soit $\mathcal{H}$ une homothétie de centre A et de rapport r non nul, montrer que :

1. Si $r \neq 1$, A est l'unique point fixe de $\mathcal{H}$., c.-à-d. que $A = \mathcal{H}(A)$.
2. Pour tout point M, on a que A, M et $\mathcal{H}(M)$ sont alignés.
3. Si d est une droite alors $\mathcal{H}(d)$ est une droite et $\mathcal{H}(d) \parallel d$.
4. L'image par $\mathcal{H}$ d'un cercle de centre O et de rayon R est un cercle de centre $\mathcal{H}(O)$ et de rayon $R \cdot |r|$.

Exercice 3 Montrer que les images respectives de deux droites perpendiculaires, par une homothétie ou une translation, sont deux droites perpendiculaires.

Exercice 4 (B) 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 5 (B) (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 $\mathcal{H}$ de centre O qui transforme A en B.

1. Montrer que $\mathcal{H}(C) = D$.
2. Montrer que $\mathcal{H}(E) = F$.

Exercice 6 Soit ABC un triangle, $\mathscr{C}$ son cercle circonscrit et O le centre de $\mathscr{C}$. Soit J le milieu de $[BC]$ et D le point de $\mathscr{C}$ diamétralement opposé à A. Soit $B' = \mathcal{H}_{B,-1}(A)$ le symétrique de A par rapport à B et $C' = \mathcal{H}_{C,-1}(A)$ 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 (c.-à-d. 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, J et K sont alignés. Pour cela, on considère l'homothétie $\mathcal{H}$ de centre A, qui transforme B en B'.

1. Tracer une figure qui représente le contexte.
2. Quel est le rapport de $\mathcal{H}$?

3. Déterminer les images par $\mathcal{H}$ des points O et C, puis l'image du segment $[BC]$.
4. Soit $\mathscr{C}'$ l'image du cercle $\mathscr{C}$ par $\mathcal{H}$. Quel est le centre de $\mathscr{C}'$? Montrer que $\mathscr{C}'$ passe par B' et C'.
5. Montrer que (DK) est médiatrice de $[B'C']$. En déduire que $K = \mathcal{H}(J)$ puis que les points A, J et K sont alignés.

Repères du plan, et de l'espace

Exercice 7 Soit $ABCD$ un parallélogramme. Soit E le milieu de $[AD]$ et le point F tel que $\overrightarrow{AF} = \frac{1}{3}\overrightarrow{AC}$.

1. Exprimer $\overrightarrow{BE}$ et $\overrightarrow{BF}$ en fonction de $\overrightarrow{AB}$ et $\overrightarrow{AD}$.
2. Montrer que B, E et F sont alignés.

Exercice 8 Montrer qu'une droite d et un plan $\mathcal{P}$ ne se coupent 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 9 Soit $ABCDEFGH$ un cube. Soit I et J les points définis par $\overrightarrow{DI} = \frac{1}{4}\overrightarrow{DC}$ et $\overrightarrow{BJ} = \frac{3}{4}\overrightarrow{BC}$.

1. Exprimer $\overrightarrow{HF}, \overrightarrow{HJ}$ et $\overrightarrow{EI}$ dans le repère $(D, \overrightarrow{DA}, \overrightarrow{DB}, \overrightarrow{DH})$.
2. Peut-on écrire $\overrightarrow{EI}$ comme combinaison linéaire de $\overrightarrow{HF}$ et $\overrightarrow{HJ}$?
3. Montrer que l'intersection du plan (HEI) et du plan (FHJ) n'est pas vide.

Exercice 10 (B) (Examen 2009) Soit $ABCDEFGH$ un cube. Soit P et Q les points définis par $\overrightarrow{DP} = \frac{1}{4}\overrightarrow{DC}$ et $\overrightarrow{BQ} = \frac{3}{4}\overrightarrow{BC}$.

1. Peut-on écrire $\overrightarrow{PH}$ dans le repère $(E, \overrightarrow{GE}, \overrightarrow{GQ})$ du plan (EGQ).
2. Montrer que l'intersection de la droite (HP) et du plan (EGQ) est vide.

Exercice 11 (B) On considère un tétraèdre $ABCD$. On appelle I, J, K et L les points définis respectivement par :

$$\overrightarrow{AI} = \frac{2}{3}\overrightarrow{AB} \ ; \ \overrightarrow{BJ} = \frac{1}{3}\overrightarrow{BC} \ ; \ \overrightarrow{CK} = \frac{2}{3}\overrightarrow{CD} \ ; \ \overrightarrow{DL} = \frac{1}{3}\overrightarrow{DA}.$$

1. Exprimer $\overrightarrow{IJ}$ en fonction de $\overrightarrow{AB}$ et $\overrightarrow{BC}$, puis en fonction de $\overrightarrow{AC}$.
2. 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.
3. Montrer que la droite (BD) ne coupe pas le plan $(IJKL)$.

Exercice 12 Soit $ABCDEFGH$ un parallélépipède rectangle. Soit I le milieu du rectangle $ADHE$ et J celui du rectangle $BCGF$.

1. Montrer que $\overrightarrow{IF} = \overrightarrow{DJ}$.
2. Justifier que D, J, F et I sont coplanaires. Quel est la nature de $DJFI$?

3. Montrer que $\overrightarrow{IJ}$, $\overrightarrow{BD}$ et $\overrightarrow{GF}$ sont coplanaires.

Exercice 13 (B) (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

$$\overrightarrow{AJ} = \frac{3}{4}\overrightarrow{AE}, \quad \overrightarrow{DI} = \frac{3}{4}\overrightarrow{DE}, \quad \overrightarrow{BK} = \frac{3}{4}\overrightarrow{BE}.$$

1. Donner les coordonnées des points I, J et K dans le repère $(A, \overrightarrow{AB}, \overrightarrow{AD}, \overrightarrow{AE})$.
2. Montrer les plans (IJK) et (ABC) sont parallèles.
3. Montrer que la droite $d = (ABE) \cap (CDE)$ est parallèle à la droite (AB).
4. Montrer que $\overrightarrow{JK}$ est un vecteur directeur de d.
5. Montrer que la droite d ne coupe pas le plan (IJK).

Exercice 14 (B) (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

$$\overrightarrow{SK} = \frac{1}{3}\overrightarrow{SD}, \quad \overrightarrow{SL} = \frac{2}{3}\overrightarrow{SD}.$$

1. Donner les coordonnées des points O et J dans le repère $(S, \overrightarrow{SB}, \overrightarrow{SC}, \overrightarrow{SD})$.
2. Montrer que les vecteurs $\overrightarrow{BK}$, $\overrightarrow{SB}$ et $\overrightarrow{SD}$ sont coplanaires.
3. Exprimer le vecteur $\overrightarrow{BJ}$ comme combinaison linéaire des seuls vecteurs $\overrightarrow{SB}$ et $\overrightarrow{SD}$.
4. Montrer que les points B, K et J sont alignés.
5. Montrer que la droite (OL) est parallèle à la droite (BK).

Produit scalaire

Exercice 15 Soit $ABCDEFGH$ un cube de côté de longueur 1. On se place dans le repère orthonormé $(A, \overrightarrow{AB}, \overrightarrow{AD}, \overrightarrow{AE})$.

1. Donner les coordonnées des points A, F, C et G.
2. Calculer le produit scalaire $\overrightarrow{AF} \cdot \overrightarrow{CH}$. Les droites (AF) et (CH) sont-elles orthogonales ?
3. Calculer $\overrightarrow{EC} \cdot \overrightarrow{FD}$. Les droites (EC) et (FD) sont-elles orthogonales ?

Exercice 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 17 (B) (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.

1. Montrer que $\overrightarrow{CQ} \cdot \overrightarrow{PR} = \overrightarrow{CQ} \cdot (\overrightarrow{AR} - \overrightarrow{AP})$.
2. Montrer que les droites (CQ) et (PR) sont perpendiculaires.

Barycentres

Exercice 18

1. 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 $((B,b),(C,c))$.
2. Soit G le barycentre de $((A,1),(B,1),(C,1))$. Soit A' le milieu de $[BC]$. Montrer que les médianes du triangle 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 19 (B) Soit BCD un triangle.

1. Soient A le barycentre du système pondéré $((B,1),(C,-1),(D,1))$. Montrer que $ABCD$ est un parallélogramme.
2. 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 20 (B) **(Examen 2010)** Soit ABC un triangle et r un réel non nul, on définit les points D et E par les relations :

$$\overrightarrow{AD} = r \cdot \overrightarrow{AB} \quad \text{et} \quad \overrightarrow{CE} = r \cdot \overrightarrow{CA}.$$

1. Montrer que D est le barycentre de $((A,1-r),(B,r))$.
2. Montrer que E est le barycentre de $((C,1-r),(A,r))$.
3. En déduire que pour tout point M du plan, on a :
$$\overrightarrow{MD} + \overrightarrow{ME} = \overrightarrow{MA} + \overrightarrow{MC} + r \cdot \overrightarrow{CB} = 2(\overrightarrow{MB'} + r \cdot \overrightarrow{B'C'})$$
où B' et C' sont les milieux respectifs de $[AC]$ et $[AB]$.
4. Soit I le milieu de $[DE]$, montrer que I, B' et C' sont alignés.

Exercice 21 Soit ABC un triangle. Soit H le point défini par $\overrightarrow{AH} = \frac{1}{3}\overrightarrow{AC}$ et K le point défini par $\overrightarrow{AK} = \frac{1}{4}\overrightarrow{AB} + \frac{1}{4}\overrightarrow{AC}$.

1. Exprimer H comme le barycentre des points A et C.
2. Exprimer K comme le barycentre des points A, B et C.
3. En déduire que B, H et K sont alignés.

Exercice 22 (B) 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 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 $[AG]$.

1. Montrer que pour tout point M du plan on a $3\overrightarrow{MA} + \overrightarrow{MB} + 2\overrightarrow{MJ} = 6\overrightarrow{MI}$.
2. En déduire que I est le barycentre de $((K,4),(J,2))$.
3. Montrer que I, J et K sont alignés.

Exercice 24 (B) **(Examen 2011)** Soit $ABCD$ un parallélogramme de centre de gravité O (l'intersection de ses diagonales) et $r \neq -1$ un réel non nul. Soit I le barycentre de (A,r), $(B,1)$ et J le barycentre de (C,r), $(D,1)$.

1. Montrer que les droites (AC), (BD) et (IJ) sont concourantes.
2. Soit E le barycentre de $(A,2-r)$, $(I,r+1)$, $(D,1)$.
   (a) Montrer que pour tout point M du plan, on a :
   $$2\overrightarrow{MA} + \overrightarrow{MB} + \overrightarrow{MD} = 4\overrightarrow{ME}.$$
   (b) En déduire que E est le milieu de $[AO]$.
   (c) Pour quelle valeur de r les points D, I et E sont-ils alignés ? Justifier.

Exercice 25 (B) **(La droite et le cercle d'Euler)** Dans le plan $\mathcal{P}$, on considère un triangle ABC. Soient G, O et L respectivement : son centre de gravité, le centre du cercle qui lui est circonscrit, et son orthocentre.

1. Soit $A'B'C'$ le triangle formé des parallèles aux côtés de ABC passant par ses sommets.
   (a) Montrer que L est le centre du cercle circonscrit à $A'B'C'$.
   (b) Montrer que G est le centre de gravité de $A'B'C'$.
   (c) Montrer que l'homothétie $\mathcal{H}$ de centre G et de rapport $-1/2$ envoie $A'B'C'$ sur ABC.
2. Montrer que $\overrightarrow{GO} = -\overrightarrow{GL}/2$. En déduire que G, O et L sont alignés (c'est la droite d'Euler).
3. **Petit défi** : Soit I,J et K les milieux de $[BC]$, $[AC]$ et $[AB]$ et soit $\mathscr{C}$ le cercle circonscrit à IJK. Montrer que $\mathscr{C}$ passe aussi par les pieds des hauteurs de ABC et par les milieux de $[AL]$, $[BL]$ et $[CL]$; c'est le cercle des neuf points d'Euler (indication : on pourra considérer l'homothétie $\mathcal{H}$ ainsi que l'homothétie $\mathcal{H}'$ de centre L et de rapport $1/2$).

Chapitre 3

Nombres complexes, polynômes et géométrie

Les chapitres précédents nous ont mené de la géométrie telle que pratiquée par les mathématiciens de l'Antiquité jusqu'à la création de l'algèbre linéaire. Par ce biais, les questions de géométrie classique se trouvent souvent traduites sous forme d'équations que l'on cherche à "résoudre". C'est ce problème de résolution d'équations qui lui-même donné lieu à l'apparition des nombres complexes. C'est donc la prochaine étape de notre étude.

3.1 Motivation

Le problème de trouver des méthodes de résolutions d'équations est au coeur d'un grand nombre de problématiques mathématiques. Le cas particulier des **équations polynomiales**, c'est-à-dire les équations du type

$$a_n x^n + a_{n-1} x^{n-1} \dots a_1 x + a_0 = 0, \qquad \text{où } a_i \in \mathbb{R} \quad \text{et} \quad n \in \mathbb{N}, \tag{3.1}$$

est parmi le premier à avoir été étudiés. Dans un premier temps, on en cherche les solutions (on dit plus souvent les **racines**) réelles. Bien sûr, le cas le plus simple est le cas des équations du premier degré :

$$ax + b = 0, \ a, b \in \mathbb{R}, \ a \neq 0,$$

pour lequel on n'a qu'une seule racine qui est $x = -b/a$. Viennent ensuite les équations du second degré, c'est-à-dire de la forme

$$ax^2 + bx + c = 0, \ a, b, c \in \mathbb{R}, \ a \neq 0.$$

Leur résolution est aussi classique. On calcule d'abord le *discriminant* $\Delta = b^2 - 4ac$, pour déterminer la nature des solutions possibles. En effet, pour avoir des racines réelles, il faut et il suffit que $\Delta \geq 0$. Les racines sont alors données par les formules

$$x_1 = \frac{-b + \sqrt{\Delta}}{2a} \quad \text{et} \quad x_2 = \frac{-b - \sqrt{\Delta}}{2a},$$

où l'on prend la racine carrée (positive) du discriminant. Si $\Delta = 0$, on dit que la racine est **double**. L'équation peut encore s'écrire sous la forme $a\,(x - x_1)(x - x_2) = 0$, $a \neq 0$, ce qui souligne que $x - x_1 = 0$, soit $x - x_2 = 0$. Autrement dit, la *factorisation*

$$ax^2 + bx + c = 0 = a\,(x - x_1)(x - x_2),$$

ramène à le problème de résoudre l'équation à celui de résoudre deux équations de premier degré.

De manière générale, la résolution d'une équation polynomiale $P(x) = 0$, est équivalente à la recherche de la **factorisation** du polynôme $P(x) = a_n x^n + a_{n-1}x^{n-1} \ldots a_1 x + a_0$ $(a_n \neq 0)$:

$$P(x) = a_n\,(x - x_n)(x - x_{n-1}) \ldots (x - x_1).$$

Les x_i sont alors les racines de l'équation 3.1.

Nombres complexes

Revenons aux cas des équations du second degré. Lorsque le discriminant Δ est négatif, on peut démontrer que l'équation $ax^2 + bx + c = 0$ n'a pas de racines réelles. Par exemple, le polynôme $x^2 + 1$ ne peut pas se factoriser sous la forme

$$x^2 + 1 = (x - x_1)(x - x_2),$$

avec les x_i des nombres réels. Autrement dit, -1 n'admets pas de racine carrée si on se restreint au domaine $\mathbb{R}$ des nombres réels.

Ce phénomène est général pour les équations polynomiales de degré supérieur à 1. Plus précisément, pour tout degré pair [1] non nul ($n = 2, 4, 6, \ldots$), il existe [2] des polynômes qui n'ont aucune racine réelle. Par exemple, on observe (pour l'instant ce n'est pas tout-à-fait évident à trouver) que

$$x^4 + 1 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1),$$

et résoudre revient à factoriser chacune de ces équations de second degré. Aucune des deux n'a de solution réelle. Donc, $x^4 + 1$ n'a pas de racine réelle.

Une des plus belles découvertes des mathématiques est que la difficulté de la factorisation des polynômes de degré 2 est la seule « obstruction » à toute factorisation. Autrement dit, on sait (en

1. Dans le cas impair, un joli argument permet de voir qu'il y a toujours au moins une racine réelle.
2. En fait, c'est presque toujours le cas.

principe[3]) factoriser complètement tout polynôme, si on sait le faire pour des polynômes de degré 2. C'est le théorème fondamental de l'algèbre (voit Théorème 3.14). Concrètement, c'est encore plus impressionnant, il suffit simplement de pouvoir factoriser le seul polynôme x^2+1, pour pouvoir factoriser n'importe quel autre polynôme. À cette fin, on introduit un nouveau nombre i tel que $i^2 = -1$. C'est là l'origine des nombres dits « complexes ».

Un aspect inattendu de cette extension des nombres réels aux nombres complexes est l'incroyable efficacité qu'ils introduisent dans un grand nombre de questions mathématiques, qui sont sans liens directs avec la factorisation de polynômes. Cela va de la théorie générale des fonctions, à la théorie des nombres, en passant par une foule d'autres domaines des mathématiques.

3.2 L'ensemble des nombres complexes

On obtient l'ensemble des **nombres complexes** en ajoutant aux nombres réels le seul nombre i, avec tout ce qu'on peut obtenir par calcul de sommes, différences, multiplications et divisions. Après avoir travaillé un peu, on s'aperçoit qu'on peut formellement tout exprimer comme en terme des éléments de l'ensemble

$$\mathbb{C} = \{a + b\,i \,|\, a, b \in \mathbb{R}\}.$$

L'écriture $a + b\,i$ est *formelle* : c.-à-d. que la lettre i désigne simplement un « objet abstrait ». Par définition, les éléments de $\mathbb{C}$ sont les « nombres complexes ». Pour un nombre complexe $z = a+b\,i$ dans $\mathbb{C}$, on dit que a est sa **partie réelle**, et on la note $\mathrm{Re}(z)$; le nombre réel b est la **partie imaginaire** de z, et elle se note $\mathrm{Im}(z)$. Par définition, deux nombres complexes sont égaux si et seulement si ils ont la même partie réelle et la même partie imaginaire. Donc,

$$a + b\,i = c + d\,i, \qquad \text{ssi} \qquad (a = b, \quad \text{et} \quad c = d).$$

Un nombre complexe z dont la partie réelle est nulle est dit **imaginaire**, et donc $z = b\,i$. Un nombre complexe dont la partie imaginaire est nulle s'écrit $z = a$, c'est un réel. On a donc une inclusion naturelle $\mathbb{R} \subseteq \mathbb{C}$, de l'ensemble des nombres réels $\mathbb{R}$ dans l'ensemble des nombres complexes $\mathbb{C}$.

On calcule avec les nombres complexes de la manière décrite dans ce qui suit. Il s'agit simplement de préciser comment manipuler des sommes, différences, produits et divisions d'élément de $\mathbb{C}$, en expliquant chaque fois comment s'exprime le résultat en terme d'éléments de $\mathbb{C}$.

Addition sur $\mathbb{C}$. Étant donnés deux nombres complexes $z = a + b\,i$ et $z' = a' + ib'$, l'addition est simplement l'opération définie par

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

3. Cependant, cette factorisation peut être très difficile à obtenir explicitement. C'est la raison d'être de la théorie de Galois.

Elle admet $0 = 0 + 0 \cdot i$ comme élément neutre, et on a l'inverse additif $-z = (-a) + (-b)i$. L'addition complexe vérifie les propriétés usuelles suivantes.

Proposition 3.1. *Quelque soit z, z', et z'' dans $\mathbb{C}$, on a :*

(i) $z + z' = z' + z$ (commutativité) ;

(ii) $z + (z' + z'') = (z + z') + z''$ (associativité) ;

(iii) $0 + z = z + 0 = z$ (élément neutre) ;

(iv) $z + (-z) = 0$ (inverse additif).

Démonstrations. Voir exercice 2. ■

Produit sur $\mathbb{C}$. On étend à $\mathbb{C}$ le produit dans $\mathbb{R}$, en ajoutant la contrainte $i^2 = -1$. Utilisant (sans se questionner) les règles de calculs usuelles, on trouve, pour $z = a + b\,i$ et $z' = a' + b'\,i$ que

$$\begin{aligned} z \cdot z' = (a + b\,i) \cdot (a' + b'\,i) &= aa' + bb'\,i^2 + ab'\,i + a'b\,i \\ &= (aa' - bb') + (ab' + a'b)\,i. \end{aligned}$$

Ceci suggère d'adopter comme définition (abstraite) de la **multiplication** dans $\mathbb{C}$ la formule ainsi trouvée. On pose donc

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

Ce n'est plus le résultat d'un calcul, c'est devenu une définition abstraite (un point de départ). Il reste maintenant à vérifier qu'en démarrant la réflexion ainsi, on trouve une opération qui a de bonnes propriétés.

Exemple. Si $z = 3 + 2i$ et $z' = -2/3 - 5\,i$ alors :

$$z \cdot z' = (3 + 2\,i)(-2/3 - 5\,i) = -2 - 15\,i - (4/3)\,i + 10 = 8 - (49/3)\,i.$$

Cette multiplication admet comme élément neutre le nombre complexe $1 = 1 + i \cdot 0$. La multiplication complexe vérifie les propriétés usuelles de la multiplication réelle.

Proposition 3.2. *Soit $z, z', z'' \in \mathbb{C}$, alors :*

(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).

Démonstrations. Voir exercice 3. ■

Remarque.

1) La définition abstraite de « corps » (discutée plus en détail dans les cours d'algèbre) s'applique à la situation considérée ici : on a un ensemble $\mathbb{C}$ muni de deux opérations (l'addition et la multiplication) satisfaisant les bonnes conditions (Propositions 3.1 et 3.2). On obtient le **corps des nombres complexes**.

2) L'inverse (multiplicatif) d'un nombre complexe non nul se « calcule » de la façon suivante

$$(a+b\,i)^{-1} = \frac{1}{a+b\,i} = \left(\frac{a}{a^2+b^2} + i\frac{-b}{a^2+b^2}\right).$$

Observez que $a^2+b^2 \neq 0$ lorsque $z \neq 0$. On vérifie par calcul, pour $z \in \mathbb{C}^* = \mathbb{C} \setminus \{0\}$, que

$$z \cdot \left(\frac{a}{a^2+b^2} + i\frac{-b}{a^2+b^2}\right) = \left(a\frac{a}{a^2+b^2} - b\frac{-b}{a^2+b^2}\right) + i\left(\frac{a}{a^2+b^2}b + a\frac{-b}{a^2+b^2}\right) = 1,$$

d'où le résultat annoncé.

3.2.1 Module et conjugué d'un nombre complexe

Pour simplifier les calculs, il est intéressant de considérer les notions suivantes.

Définition. Soit $z = a + b\,i$ un nombre complexe.

1) Le **module** de z est le nombre $|z| = \sqrt{a^2+b^2}$.

2 On dit du nombre complexe $\overline{z} = a - ib$ que c'est le **conjugué** de z.

L'inverse d'un nombre complexe $z \in \mathbb{C}$ s'exprime alors comme

$$z^{-1} = \frac{1}{z} = \frac{\overline{z}}{|z|^2}.$$

Exemple. Si $z = 3 - 4i$ alors $|z| = 5$ et $\overline{z} = 3 + 4i$. On calcule que

$$z\overline{z} = (3-4i)(3+4i) = (9+16) + i(12-12) = 25 = |z|^2.$$

Proposition 3.3. *Soit $z, z' \in \mathbb{C}$, alors*

(i) $z\overline{z} = |z|^2 \in \mathbb{R}$;

(ii) $z + \overline{z} = 2\,\mathrm{Re}(z)$;

(iii) $z - \overline{z} = 2\,\mathrm{Im}(z)$;

(iv) $|zz'| = |z||z'|$ *et* $|\overline{z}\,| = |z|$;

(v) $z \in \mathbb{R} \;\Leftrightarrow\; \mathrm{Im}(z) = 0 \;\Leftrightarrow\; \overline{z} = z$.

Démonstrations. Voir exercice 4. ■

Remarque. On exploite ces propriétés pour écrire en terme de parties réelles et imaginaires le résultat d'un calcul. Par exemple, pour écrire z/z' sous la forme $a + b\,i$, il suffit de multiplier le numérateur et le dénominateur de la fraction par $\overline{z'}$ pour obtenir

$$\frac{z}{z'} = \frac{z\overline{z'}}{z'\overline{z'}} = \frac{\mathrm{Re}(z\overline{z'})}{|z'|^2} + \frac{\mathrm{Im}(z\overline{z'})}{|z'|^2}\, i.$$

3.2.2 Forme trigonométrique, forme exponentielle, et formule de De Moivre

Comme on introduit les nombres complexes afin de résoudre des équations polynomiales, il est naturel de chercher à simplifier l'écriture des puissances $z^n = (a + b\,i)^n$ d'un nombre complexe $z = a + b\,i \in \mathbb{C}$. À cette fin, on exploite une interprétation géométrique des nombres complexes. Plus précisément, on identifie les points du plan $\mathcal{P}$, muni d'un repère orthonormé $(O, \mathbf{u}, \mathbf{v})$, avec les nombres complexes, en interprétant le nombre complexe $z = a + b\,i$ comme « correspondant » au point M de coordonnées (a, b). Ceci semble naturel si on observe que l'addition dans $\mathbb{C}$ coïncide avec l'addition de vecteurs dans le plan.

Remarque. De plus, on constate que

1) Le segment OM est de longueur $|z|$, c.-à-d. $OM = ||\overrightarrow{OM}|| = |z|$.
2) Soit M' le symétrique de M par rapport à l'axe des abscisses. M' a donc pour coordonnée $(a, -b)$ et correspond donc à $\overline{z}$.

Dorénavant, on identifie z au point M, et on obtient la notion suivante.

Définition. Le points (a, b) du **plan des complexes** s'identifient au nombre complexe $a+b\,i$. L'origine de ce plan est le nombre complexe $0 = 0 + 0\,i$, et on a le repère orthonormé constitué du triplet de nombres complexes $(0, 1, i)$. Autrement dit, les nombres complexes $1 = 1 + 0\,i$ et $i = 0 + 1\,i$ s'identifient respectivement aux vecteurs de coordonnées $(1, 0)$ et $(0, 1)$. L'addition vectorielle correspond à l'addition de nombres complexes, et la norme d'un vecteur au module du nombre complexe correspondant.

Afin de donner une interprétation géométrique au produit de nombres complexes, on commence par considérer le cas où $|z| = 1$. Le point correspondant se trouve alors sur le cercle de centre 0, et de rayon 1. En vertu des définitions usuelles des fonctions *cosinus* et *sinus*, il existe un unique angle $\theta \in [0, 2\pi[$ tel que

$$z = a + b\,i = \cos(\theta) + i\sin(\theta),$$

et tout nombre complexe de cette forme est de module 1, car $\cos(\theta)^2 + \sin(\theta)^2 = 1$.

Proposition 3.4. *Soit $z \in \mathbb{C}$, il existe un unique $\theta \in [0, 2\pi[$ tel que $z = |z|(\cos(\theta) + i\sin(\theta))$. Le nombre θ est appelé* l'argument de z *et est noté* $\arg(z)$.

Démonstrations. Voir exercice 8. ■

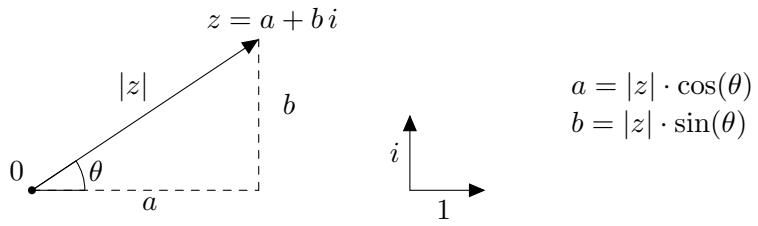


FIGURE 3.1 – Repésentation géométrique d'un nombre complexe.

Définition. L'écriture $z = a + b\,i$ de $z \in \mathbb{C}$ est la *forme algébrique de* z, tandis que $z = |z|(\cos(\theta) + i\sin(\theta))$ est sa *forme trigonométrique de* z.

Exemple. On considère $z = 2 + 2i$. 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 $z = |z|(\cos\theta + i\sin\theta)$, on obtient que $\cos\theta = \sin\theta = \sqrt{2}/2$. On en déduit donc que $\theta = \arg(z) = \pi/4$.

L'argument de z est l'angle « orienté » (voir section 3.4.2) entre le vecteur 1 de coordonnées $(1, 0)$ et le vecteur $z = \overrightarrow{OM}$. Le résultat suivant sera démontré à la section 3.3.1. Il met en évidence que l'utilisation de nombres complexes permet de simplifier grandement les calculs trigonométriques. Pour se convaincre, il suffit de tenter de trouver le développement de $\sin(n\,\theta)$ (pour n assez grand) en terme de $\sin(\theta)$ et $\cos(\theta)$ avec les outils usuels de la trigonométrie, et de comparer ce calcul à l'approche permise par la formule de De Moivre.

Proposition 3.5 (Formule de De Moivre)**.** *Pour tout* $n \in \mathbb{N}$*, on a*

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

En comparant les développements en séries selon la variable θ de chaque membre de l'équation suivante, on se convainc qu'il n'est pas trop étonnant de poser

$$e^{i\theta} := \cos\theta + i\sin\theta \tag{3.2}$$

(ceci reçoit sa justification complète dans un cours d'analyse), et la formule de De Moivre s'écrit alors encore plus simplement :

$$(e^{i\theta})^n = e^{in\,\theta}.$$

Forme exponentielle d'un nombre complexe. On est maintenant en mesure de simplifier la forme trigonométrique d'un nombre complexe considérée dans la proposition 3.4. En effet, tout nombre complexe peut s'écrire sous **forme exponentielle** comme $z = re^{i\theta}$, où $r = |z|$ est le module de z, et θ

est son argument. On dit que le couple (r, θ) donne les **coordonnées polaires** de z. Cette notation exponentielle permet de donner une interprétation géométrique au produit de deux nombres complexes, et en facilite grandement le calcul. Le produit de deux nombres complexes $z = re^{i\theta}$ et $z' = r'e^{i\theta'}$ se multiplient en effet selon la formule :

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

En particulier

$$\arg(zz') = \arg(z) + \arg(z') \quad \text{et} \quad \arg\left(z/z'\right) = \arg(z) - \arg(z')$$

puisque $1/z = (1/r)\, e^{(-i\theta)}$. En fait, on a plus généralement $(re^{i\theta})^n = r^n\, e^{in\,\theta}$ pour tout entier n. Ceci suggère qu'on devrait avoir $\sqrt{re^{i\theta}} = (re^{i\theta})^{1/2} = \sqrt{r}\, e^{i\,\theta/2}$ (comme $r \geq 0$, la racine carré (positive) $\sqrt{r}$ existe). On a en fait deux racines quadratiques [4] qui sont $\pm\sqrt{r}\, e^{i\,\theta/2}$, comme c'est le cas dans les réels.

Exemple. On trouve facilement que $x^4 + 1 = (x^2 - i)(x^2 + i)$. On observe que

$$i = e^{i\,\pi/2} \quad \text{et} \quad -i = e^{-i\,\pi/2}.$$

D'où

$$x^4 + 1 = (x^2 - e^{i\,\pi/2})(x^2 - e^{-i\,\pi/2}) = (x - e^{i\,\pi/4})(x + e^{i\,\pi/4})(x - e^{-i\,\pi/4})(x + e^{-i\,\pi/4}).$$

Posons $z = e^{i\,\pi/4}$, alors $\overline{z} = e^{-i\,\pi/4}$. L'équation ci-dessus se réécrit alors

$$x^4 + 1 = (x - z)(x - \overline{z}\,)(x + \overline{z}\,)(x + z) = (x^2 - (z + \overline{z}\,)x + z\overline{z}\,)(x^2 + (z + \overline{z}\,)x + z\overline{z}\,).$$

Comme $z\overline{z} = |z|^2 = 1$ et $z + \overline{z} = 2\,\mathrm{Re}(z) = \sqrt{2}$, on obtient que :

$$x^4 + 1 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1).$$

Ce phénomène est plus profond, comme nous le verrons dans la suite de ce chapitre.

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 3.6. *Toute racine de l'unité a pour module* 1.

Démonstrations. Soit $z = re^{i\theta}$ une racine de l'unité, alors $z^n = 1$. Or $z^n = r^n e^{ii\,n\,\theta}$ et $1 = 1 \cdot e^{0i}$. Par identification, on obtient que $r^n = 1$. Comme $r > 0$, on a $|z| = r = 1$, car la fonction $r \mapsto r^n$ est strictement croissante sur $\mathbb{R}^+$. ∎

4. Le problème du calcul de la racine n^{e} d'un nombre complexe est très intéressant, et d'un grand intérêt pour plusieurs domaines des mathématiques. On trouve n telles racines, et elles se trouvent aux sommets d'un certain polygone régulier à n côtés.

3.3 Les preuves par récurrence

Afin de démontrer la formule de De Moivre, ou d'autres formules dépendant d'un entier n, on se dote d'un des outils les plus utiles pour les démonstrations de ce genre : le raisonnement par récurrence. La récurrence est une notion centrale en mathématiques. Elle est l'un des outils majeurs pour définir de nouvelles notions mathématiques. L'une des façon de mettre ce fait en évidence est de souligner qu'on peut grossièrement identifier un ordinateur à un appareil qui permet des calculs récursifs [5]. Or, comme on le discute dans le document Calcul Formel, disponible en ligne, les systèmes de calculs formels permettent de manipuler un large pan des concepts mathématiques. Cela est essentiellement possible parce que ceux-ci sont largement construits de manière récursive.

Bon ordre

Pour démarrer la discussion de la notion de récursivité, et l'asseoir sur des fondements clairs, on introduit d'abord le concept suivant. Le fait d'être muni d'un **bon ordre** est une des propriétés de base de l'ensemble des entiers naturels. Cela en est un axiome. Elle s'exprime comme suit : *tout sous-ensemble non vide de* $\mathbb{N}$ *contient un plus petit élément*. De façon plus technique : soit $A \subseteq \mathbb{N}$, alors il existe $n \in A$ tel que $n \leq x$ pour tout $x \in A$. Par exemple, pour l'ensemble des nombres impairs, 1 est le plus petit élément.

Preuve par récurrence. Pour discuter le mécanisme d'une preuve par récurrence, on considère la démonstration de la proposition [6] suivante. Après l'énoncé de la proposition comme telle, on présente la preuve comme telle, pour ensuite en décortiquer le mécanisme.

Proposition 3.7. *Soit $n \in \mathbb{N}$, alors la somme de tous les entiers de 0 à n est égale à $n(n+1)/2$.*

Démonstration. On cherche à prouver que pour tout $n \in \mathbb{N}$, l'énoncé

$$\sum_{i=0}^{n} i = 0 + 1 + 2 + 3 + \ldots + (n-1) + n = \frac{n(n+1)}{2},$$

est vrai. La preuve par récurrence nécessite deux étapes.

Étape 1. On montrer (c'est souvent une simple vérification facile) que l'énoncé considéré est vrai lorsque $n = 0$. Dans notre cas, cela consiste à vérifier que

$$\sum_{i=0}^{0} i = 0 = \frac{0 \times 1}{2},$$

5. À ce propos, voir la Thèse de Church.

6. Une anecdote bien connue prétend que le jeune Carl-Friederich Gauss (1777-1855) aurait retrouvé cette formule à l'école primaire pour calculer presque instantanément le cas $n = 100$, évitant ainsi le calcul direct assigné par l'enseignant comme une longue tâche.

ce qui est bien le cas.

Étape 2. Supposant que l'énoncé est vrai pour l'entier naturel n (c'est ce qu'on appelle l'hypothèse de récurrence), on montre qu'on en déduit qu'il est vrai aussi pour $n+1$ en calculant comme suit. L'hypothèse de récurrence affirme donc que la somme des entiers de 0 à n est bien $n(n+1)/2$, on a donc le calcul

$$\begin{aligned}\sum_{i=0}^{n+1} i &= \sum_{i=0}^{n} i + (n+1)\\ &= \frac{n(n+1)}{2} + (n+1)\\ &= \frac{(n+1)(n+2)}{2},\end{aligned}$$

ce qui démontre que l'énoncé de la proposition est aussi vrai pour $n+1$. Ceci achève la preuve par récurrence. ■

Accepter qu'une telle preuve par récurrence soit légitime (et complète) demande une justification. La situation générale prend la forme suivante. On a un **énoncé** à propos des entiers naturels qui prend la forme abstraite $P(n)$, où P désigne une certaine propriété, et on écrit $P(n)$ pour

$$P(n) = n \text{ possède la propriété } P.$$

On cherche à montrer que tous les énoncés

$$P(0),\ P(1),\ P(2),\ P(3), \ldots$$

sont vrais. C'est là une infinité d'affirmations. Dans la preuve ci-dessus, on a montré, pour la propriété

$$P(n) = \left(\sum_{i=0}^{n} i = 0+1+2+3+\ldots+(n-1)+n = \frac{n(n+1)}{2} \right),$$

que

(i) $P(0)$ est vraie, et

(ii) si $P(n)$ est vraie, alors $P(n+1)$ est vraie.

On aimerait conclure que $P(n)$ est vrai pour tout n, parce que c'est là l'énoncé de la Proposition. C'est ce que nous permet le principe de la preuve par récurrence.

Proposition 3.8 (Principe de la preuve par récurrence)**.** *Pour une propriété $P(n)$, formulée pour des entiers n, si on peut montrer que*

(i) *$P(0)$ est vrai, et que*

(ii) *$P(n) \Longrightarrow P(n+1)$ est vrai,*

alors on peut conclure que $P(n)$ est vraie pour tout $n \in \mathbb{N}$.

Démonstration. Soit $A := \{n \in \mathbb{N} \mid P(n) \text{ est faux}\}$. On aimerait montrer que $A = \emptyset$ (ce qui revient à dire que $P(n)$ vrai pour tous les entiers). On procède par l'absurde, en supposant que ce n'est pas le cas, c.à-d. que $A \neq \emptyset$. Autrement dit, on suppose qu'il y a certains entiers pour lesquels la propriété P ne tient pas. Ce sont les éléments de A.

Comme A est un sous-ensemble non vide de $\mathbb{N}$, l'axiome du bon ordre assure que A contient un plus petit élément ; appelons-le m. On observe que $m > 0$, puisque que la partie (i) des hypothèses assure que $P(0)$ est vrai. De plus, comme m est le plus petit élément de A, l'entier $m - 1 \geq 0$ n'est pas dans A. Autrement dit $P(m-1)$ est vrai. D'autre part, comme $m \in A$, on a que $P(m)$ est faux. En résumé, $P(m-1)$ est vrai et $P(m)$ est faux.

Hors, on déduit logiquement aussi que $P(m)$ doit être vrai. En effet, on a $P(m-1)$ vrai et $P(m-1) \Longrightarrow P(m)$ par (ii). Il s'ensuit que $P(M)$ est à la fois vrai et faux, de là une contradiction. Cela montre que l'hypothèse que A $\not\emptyset$ mène à une absurdité. L'hypothèse doit donc être rejetée. ■

Remarque. Pour une preuve par récurrence, il est essentiel de vérifier les deux composantes : le cas 0, et l'hypothèse de récurrence. Par exemple, sans vérification du cas 0, on peut facilement démontrer (essayez pour voir) que tout nombre dans $\mathbb{Z}$ est positif, ce qui n'est manifestement pas le cas.

3.3.1 Démonstration de la formule de De Moivre

Nous allons montrer par récurrence, la *formule de De Moivre* :

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

Soit θ un nombre réel. L'étape initiale consiste à considérer $n = 0$. On a bien l'affirmation considérée, puisque $(\cos\theta + i\sin\theta)^0 = 1 = 1 + 0\cdot i = \cos(0\cdot\theta) + i\sin(0\cdot\theta)$.

Supposons maintenant que la *formule de De Moivre* est vraie pour $n \in \mathbb{N}$ fixé :

$$(\cos\theta + i\sin\theta)^n = \cos(n\,\theta) + i\sin(n\,\theta).$$

Montrons qu'elle l'est aussi au rang $n+1$, c'est-à-dire que

$$(\cos\theta + i\sin\theta)^{n+1} = \cos((n+1)\theta) + i\sin((n+1)\theta).$$

Développons l'expression $(\cos(\theta) + i\sin\theta)^{n+1}$ en utilisant l'hypothèse de récurrence :

$$\begin{aligned}
(\cos\theta + i\sin\theta)^{n+1} &= (\cos\theta + i\sin\theta)^n(\cos\theta + i\sin\theta) \\
&= (\cos(n\,\theta) + i\sin(n\,\theta))(\cos\theta + i\sin\theta) \\
&= \cos(n\,\theta)\cos\theta - \sin(n\,\theta)\sin\theta + i\,(\sin(n\theta)\cos\theta + \cos(n\theta)\sin\theta) \\
&= \cos((n+1)\theta) + i\sin((n+1)\theta).
\end{aligned}$$

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 $n \in \mathbb{N}$.

3.4 Nombres complexes et transformations affines

Dictionnaire de traduction. Poursuivons l'idée, sous-jacente à tout ce chapitre, qui consiste à identifier le plan à l'ensemble des nombres complexes $\mathbb{C}$, avec le repère orthonormé $(O, \mathbf{u}, \mathbf{v}) = (0, 1, i)$. Rappelons que cela permet d'identifier le nombre complexe $z = x + y\,i$ au point A du plan, ayant coordonnées (x, y) où x et y sont des nombres réels. Cette « traduction » se transpose aussi aux vecteurs, en identifiant le nombre complexe $w - z$ au vecteur $\overrightarrow{AB}$, pour des points A et B correspondant respectivement aux nombres complexes z et w. Cela mène au dictionnaire de traduction suivant, qui reformule tout en terme de nombres complexes.

- des nombres complexes z et w correspondent à des **points** A et B ;
- le nombre complexe $w - z$ correspond au **vecteur** $\overrightarrow{AB}$, et $|w - z| = ||\overrightarrow{AB}||$;
- la **distance** entre z et w, est $d(z, w) := |w - z|$;
- la **droite** d passant par z et w est l'ensemble

$$d = \{z + t(w - z) \mid \ t \in \mathbb{R}\}. \tag{3.3}$$

  On dit de l'équation $z + t(w - z),\ t \in \mathbb{R}$ que c'est **l'équation paramétrique** de la droite (AB) ;
- le **segment** $[AB]$ est l'ensemble des nombres complexes $\{t\,z + (1 - t)\,w \mid 0 \leq t \leq 1\}$.
- l'ensemble des nombres complexes sur le **cercle** $\mathscr{C}$ de centre A et de rayon r est :

$$\mathscr{C} = \{w \in \mathbb{C} \mid r = |w - z|\}.$$

Bref, dorénavant on peut se permettre de remplacer toute question géométrique concernant les points et vecteurs, par une question concernant les nombres complexes.

3.4.1 Translations et homothéties dans le plan complexe

Une notion fondamentale de géométrie, partiellement abordée chapitre 2, est celle de transformations affines du plan. En effet, on y a vu les homothéties et les translations, qui sont deux cas particuliers. Nos allons y ajouter ici les rotations.

Remarque. Une **transformation affine** $\mathcal{A}$ de $\mathbb{C}$, est une fonction (voir l'annexe A.3) $\mathcal{A} : \mathbb{C} \to \mathbb{C}$, telle que

$$\mathcal{A}(w) = \mathcal{M}(w) + z,$$

où $z \in \mathbb{C}$ est fixé, et où $\mathcal{M} : \mathbb{C} \to \mathbb{C}$ est une **transformation linéaire**, c'est-à-dire que :

1) pour tout w_1 et w_2 dans $\mathbb{C}$, on a $\mathcal{M}(w_1 + w_2) = \mathcal{M}(w_1) + \mathcal{M}(w_2)$, et
2) pour tout w dans $\mathbb{C}$ et r dans $\mathbb{R}$, on a $\mathcal{M}(r \cdot w) = r \cdot \mathcal{M}(w)$.

De façon équivalente, $\mathcal{A}$ est une transformation affine si et seulement si on a

$$\mathcal{A}(w_1) - \mathcal{A}(w_2) = \mathcal{M}(w_1 - w_2),$$

pour tout w_1 et w_2 dans $\mathbb{C}$. D'un point de vue géométrique, ce sont des transformations qui envoient les droites dans des droites (comme on le vérifie facilement en utilisant la caractérisation des droites en 3.3).

Translation dans $\mathbb{C}$. Dans le contexte des complexes, les **translations** correspondent simplement à l'addition par un nombre complexe fixé. Ainsi, ce sont les fonctions $\mathcal{T}$ telles que, pour tout w dans $\mathbb{C}$, on ait

$$\mathcal{T}(w) := w + z,$$

pour z fixé.

Exemple. Soit $\mathcal{T}$ la translation selon un vecteur de coordonnées $(2, -1)$, correspond à additionner $z = 2 - i$, et donc

$$\mathcal{T}(w) = w + (2 - i), \qquad \text{ou encore} \quad \mathcal{T}(x + y\,i) = (x + 2) + (y - 1)\,i - i.$$

Homothétie dans $\mathbb{C}$. De façon similaire, une **homothétie** $\mathcal{H}$, de centre z et de rapport $r \in \mathbb{R}^*$, prend simplement la forme

$$\mathcal{H}(w) := r\,(w - z) + z.$$

Exemple. Ainsi l'homothétie de centre $1 + i$ et de rapport $-1/2$ est donnée par la formule

$$\mathcal{H}(w) = -1/2\,(w - (1 + i)) + 1 + i.$$

Si $w = x + y\,i$, alors ceci correspond à

$$\mathcal{H}(x + y\,i) = (-x + 3)/2 + i\,(-y + 3)/2.$$

3.4.2 Angles orientés et rotations

Définition. Soit z et w deux nombres complexes. L'**angle orienté** entre z et w (dans cet ordre, voir figure 3.2) est

$$(\widehat{z, w}) := \arg(w/z) \equiv \arg(w) - \arg(z) \pmod{2\,\pi}.$$

On écrit aussi $\angle(z, w)$, surtout quand l'expression pour z et w est grande.

Remarque.

1) L'usage de « $\equiv$ » et de « $\pmod{2\,\pi}$ » dans l'expression $\theta \equiv \eta \pmod{2\,\pi}$ signifie qu'il existe $k \in \mathbb{Z}$ tel que $\theta = \eta + 2k\pi$. Il faut donc faire attention lorsqu'on manipule ces expressions, surtout lorsque l'on divise par 2. Dans ce cas, le modulo 2π devient un modulo π.
2) La **mesure principale** d'un angle orienté est la valeur comprise dans l'intervalle $]-\pi, \pi]$.

Proposition 3.9. *Soit z_1, z_2 et z_3 trois nombres complexes non nuls, alors*

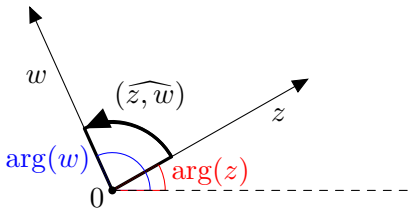


FIGURE 3.2 – L'angle entre deux nombres complexes.

(i) $(\widehat{z_1,z_2})+(\widehat{z_2,z_3})=(\widehat{z_1,z_3})$ *(Relation de Chasles) ;*

(ii) $(\widehat{z_1,z_2})=-(\widehat{z_2,z_1})$ *;*

(iii) *Pour tout réel strictement positif* α*,et* β *on a :* $(\widehat{\alpha\, z_1,\beta\, z_2})=(\widehat{z_1,z_2})$ *;*

(iv) $(\widehat{z_1,-z_2})=(\widehat{z_1,z_2})+\pi$ *(modulo* 2π*) ; en particulier* $(\widehat{-z_1,-z_2})=(\widehat{z_1,z_2})$ *;*

(v) z_1 *et* z_2 *sont colinéaires si et seulement si* $(\widehat{z_1,z_2})=k\pi$*,* $k\in\mathbb{Z}$ *;*

(vi) $z_1\perp z_2$ *si et seulement si* $(\widehat{z_1,z_2})=\pi/2+k\pi$*,* $k\in\mathbb{Z}$*.*

Démonstrations. 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

$$-re^{i\theta}=e^{i\pi}re^{i\theta}=re^{i(\pi+\theta)}.$$

Pour (v) et (vi) on procède comme suit. Les nombres complexes $z_1=r_1e^{i\,\theta_1}$ et $z_2=r_2e^{i\,\theta_2}$ sont colinéaires si et seulement si $z_1=s\,z_2$, avec $s\in\mathbb{R}^*$. Si $s>0$ on peut conclure par un simple calcul d'angle ; si $s<0$, on utilise alors (iv) pour conclure. Finalement, $z_1\perp z_2$ si et seulement si la droite dirigée par z_1 est perpendiculaire à la droite dirigée par z_2. Cela veut dire que l'angle entre ces deux droites, et donc entre ces deux nombres complexes, est un angle droit qui s'écrit $\pi/2+k\pi$ avec $k\in\mathbb{Z}$. ■

Définition (rotation). La **rotation** est la transformation affine qui déplace les points du plan d'un angle θ, en tournant autour d'un centre de rotation A. Profitant du point de vue complexe, pour être plus précis, une telle rotation $\mathcal{R}$ prend la forme

$$\mathcal{R}(w)=e^{i\theta}\,(w-z)+z,$$

avec z désignant le **centre de rotation**, et θ l'**angle de rotation**.

Remarque.

1) On vérifie aisément que $|\mathcal{R}(w)-z|=|w-z|$ et que $\angle(w-z,\mathcal{R}(w)-z)=\theta$.
2) Soit deux nombres complexes w_1 et w_2 sont à égale distance de z. Alors il existe une unique rotation $\mathcal{R}$ de centre z tel que $\mathcal{R}(w_1)=w_2$. Dans ce cas l'angle de rotation est $\theta=\angle(w_1-z,w_2-z)$.

Exemple. Soit $\mathcal{R}$ la rotation de centre $1+i$ et d'angle $\pi/6$. L'image de $w=-2+6i$ par la rotation (voir figure 3.3) est :

$$\begin{aligned}\mathcal{R}(w) &= e^{i\pi/6}(-2+6i-(1+i))+1+i\\ &= \left(\frac{\sqrt{3}}{2}+i\frac{1}{2}\right)(-3+5i)+1+i\\ &= -\frac{3\sqrt{3}+5}{2}+i\frac{5\sqrt{3}-3}{2}+1+i\\ &= -\frac{3\sqrt{3}+3}{2}+i\frac{5\sqrt{3}-1}{2}.\end{aligned}$$

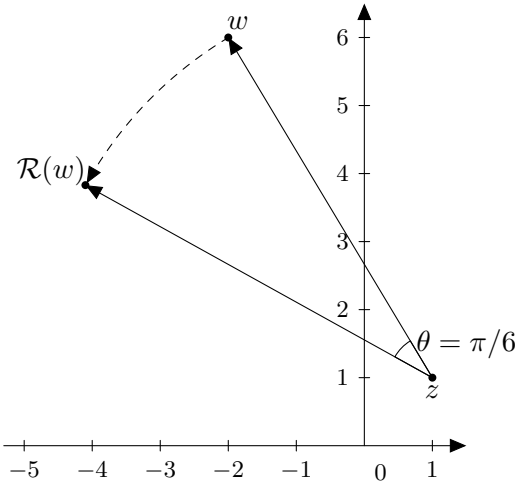


FIGURE 3.3 – La rotation d'angle $\pi/6$, de centre $(1+i)$.

Définition. Soit $\mathcal{A}$ une transformation affine.

1) On dit que $\mathcal{A}$ est une **isométrie**, si $\mathcal{A}$ préserve les distances, c.-à-d. pour tous points z et w du plan
$$d(\mathcal{A}(z),\mathcal{A}(w)) = d(z,w).$$

2) On dit que $\mathcal{A}$ **préserve les angles orientés** si pour tout complexes z, et w du plan on a
$$\angle(\mathcal{A}(z),\mathcal{A}(w)) = \widehat{(z,w)}.$$

Théorème 3.10.

(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 donne deux droites parallèles.*

(iv) *L'image de deux droites perpendiculaires par une translation, une rotation ou une homothétie donne deux droites perpendiculaires.*

(v) *Plus généralement, les translations, les rotations et les homothéties préservent les angles orientés.*

Démonstrations. (iii), (iv) sont des conséquences 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 19) ■

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 $r \neq \pm 1$ ne sont pas des isométries, elles ne conservent pas les longueurs. Par contre, les ajouter aux isométries linéaires de dégager des propriétés de « triangles semblables », ou autres objets semblables. Les composées d'isométries linéaires et d'homothéties sont les similitudes. Nous en discutons à la section suivante.

3.4.3 Les similitudes

Définition. La **similitude** $\mathcal{S}$ de centre z, d'angle θ et de rapport $z \in \mathbb{R}^*$, est la transformation (affine) du plan telle que

$$\mathcal{S}(w) := re^{i\theta}(w - z) + z.$$

Exemple. Soit $\mathcal{S}$ la similitude de centre $1 + i$, d'angle $\pi/6$ et de rapport 2. L'image par $\mathcal{S}$ de $-2 + 6i$ est

$$\begin{aligned}
\mathcal{S}(-2 + 6\,i) &= 2e^{i\pi/6}(-2 + 6i - (1 + i)) + 1 + i \\
&= 2\left(\frac{\sqrt{3}}{2} + i\frac{1}{2}\right)(-3 + 5i) + 1 + i \\
&= -3\sqrt{3} - 5 + (5\sqrt{3} - 3)i + 1 + i \\
&= -3\sqrt{3} - 4 + (5\sqrt{3} - 2)i.
\end{aligned}$$

Théorème 3.11.

(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 donne deux droites parallèles.*

(iv) *L'image de deux droites perpendiculaires par une translation ou une similitude donne 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.*

Démonstrations. Voir exercice 20. ■

Exemple. On considère les complexes $z_1 = 1 + i$ et $z_2 = 2 - 3i$. On veut déterminer l'ensemble des complexes z_3 tels que z_1, z_2 et z_3 forment un triangle équilatéral. On sait que le triangle est équilatéral si et seulement si $|z_3 - z_1| = |z_2 - z_1|$ et si $\angle(z_3 - z_1, z_2 - z_1) = \pm\frac{\pi}{3}$.

Le triangle est équilatéral si et seulement si z_3 est l'image de z_2 par une rotation de centre z_1 et d'angle $\pm\frac{\pi}{3}$. En effet, si z_3 est l'image de z_2 par une rotation de centre z_1 et d'angle $\pm\frac{\pi}{3}$, le triangle est bien équilatéral. En effet, on a, $|z_3 - z_1| = |z_2 - z_1|$ et l'angle entre les deux vecteurs $z_3 - z_1$ et $z_2 - z_1$ est $\pm\frac{\pi}{3}$ par construction.

D'autre part, si le triangle équilatéral, alors il y a deux cas possibles. Soit $\theta := \angle(z_3 - z_1, z_2 - z_1) = \frac{\pi}{3}$ ou $\theta := \angle(z_3 - z_1, z_2 - z_1) = -\frac{\pi}{3}$. Supposons d'abord que c'est le premier cas. Comme $|z_3 - z_1| = |z_2 - z_1|$ on a que

$$\frac{z_3 - z_1}{z_2 - z_1} = \frac{|z_3 - z_1|}{|z_2 - z_1|} e^{i \arg\left(\frac{z_3 - z_1}{z_2 - z_1}\right)} = e^{i\frac{\pi}{3}}.$$

Donc $z_3 - z_1 = e^{i\frac{\pi}{3}}(z_2 - z_1)$ ce qui peut se réécrire

$$z_3 = e^{i\frac{\pi}{3}}(z_3 - z_1) + z_1$$

Donc z_3 est l'image de z_2 par la rotation $\mathcal{R}$ de centre z_1 et d'angle $\frac{\pi}{3}$. Le cas restant se résout de manière similaire à l'aide de la rotation $\mathcal{R}'$ de centre z_1 et d'angle $-\frac{\pi}{3}$. Ce qui donne

$$z_3 = e^{-i\frac{\pi}{3}}(z_3 - z_1) + z_1$$

Autrement formulé,

$$\begin{aligned} z_3 &= \frac{3}{2} + 2\sqrt{3} + i\left(\frac{\sqrt{3}}{2} - 1\right), \qquad \text{ou} \\ z_3 &= \frac{3}{2} - 2\sqrt{3} - i\left(\frac{\sqrt{3}}{2} + 1\right). \end{aligned}$$

Ceci termine notre exemple.

3.5 Les polynômes

Le but de cette section est d'amorcer l'étude des polynômes en une variable, ainsi que des équations polynomiales correspondantes. Cette étude ouvre la porte à plusieurs domaines des mathématiques modernes, entre autres à la géométrie algébrique et à la théorie de Galois. C'est un très vaste sujet, qui sera étudié plus à fond dans des cours à venir. Aujourd'hui encore, il y a beaucoup de recherches sur des questions liées aux polynômes.

3.5.1 Polynômes à coefficients réels et complexes

On se place ici dans le contexte des nombres complexes, $\mathbb{C}$, en rappelant que $\mathbb{R} \subseteq \mathbb{C}$.

Définition.

1) Un **monôme** M, de **degré** $n \in \mathbb{N}$, est une expression de la forme $M(x) = a\,x^n$, avec $a \in \mathbb{C}$ où $a \neq 0$. On dit que x est une **variable**, et que a est le **coefficient** du monôme.
2) Un **polynôme à coefficients complexes** $P = P(x)$, de degré $n \in \mathbb{N}$, est une somme finie de monôme dont le plus grand degré est n :
$$P(x) = \sum_{k=0}^{n} a_k x^k = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, \qquad a_n \neq 0.$$
Si $a_k \in \mathbb{R}$, pour tout $1 \leq k \leq n$, on dit que le polynôme est à **coefficients réels**.
3) On considère aussi le polynôme **nul**, noté 0, qu'on considère comme ayant degré $-\infty$.

On dénote par $\deg(P)$ le degré de P ; par $\mathbb{C}[x]$ l'ensemble des polynômes à coefficients complexes ; et par $\mathbb{R}[x]$ l'ensemble des polynômes à coefficients réels.

Remarque. On a les propriétés suivantes.

1) Deux polynômes sot égaux, $P = Q$, si et seulement si ils ont même degré et leurs coefficients sont tous égaux (**identification des polynômes**).
2) Puisque $\mathbb{R} \subseteq \mathbb{C}$, l'ensemble $\mathbb{R}[x]$ est contenu dans $\mathbb{C}[x]$. Autrement dit, un polynôme à coefficients réels est aussi un polynôme à coefficients complexes.
3) Les polynômes **constants** non nuls, aussi appelés **constantes**, sont les éléments de $\mathbb{C} \setminus \{0\}$. Ils ont degré 0.

Addition de polynômes. L'addition de polynômes suit des règles de calcul semblables à celles pour $\mathbb{R}$ (et $\mathbb{C}$). Soit donc
$$P = \sum_{i=0}^{n} a_k x^k \quad \text{et} \quad Q = \sum_{j=0}^{m} b_j x^j$$

deux polynômes à coefficients complexes. Si $n \geq m$, on pose $b_{m+1} = b_{m+2} = \ldots = b_n = 0$. Si par contre $m > n$, on prend la convention similaire pour les a_k. On peut donc considérer la somme $a_k + b_k$, pour tout entier $1 \leq k \leq \max(m, n)$. Bien entendu $a_k + b_k \in \mathbb{C}$ (ou $a_k + b_K \in \mathbb{R}$, si a_k et b_k sont dans $\mathbb{R}$). Ceci permet de définir la **somme** :

$$P + Q = \sum_{k=0}^{n} (a_k + b_k)\, x^k.$$

C'est un polynôme de degré au plus $\max(\deg(P), \deg(Q))$. On pose aussi

$$-P = \sum_{k=0}^{n} (-a_k) x^k$$

Proposition 3.12. *La somme de polynômes vérifie les propriétés suivantes. Soit P, Q, et R dans $\mathbb{C}[x]$, 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) $\deg(P + Q) = \max(\deg(P), \deg(Q))$;
(vi) *si P, et Q sont dans $\mathbb{R}[x]$, alors $P + Q \in \mathbb{R}[x]$.*

Démonstrations. La vérification est laissée en exercice au lecteur (voir exercice 27). ■

Multiplication de polynômes La multiplication de polynômes suit elle aussi des règles de calcul similaire à celles pour $\mathbb{R}$ (et $\mathbb{C}$). On munit $\mathbb{C}[x]$ d'une multiplication : Soit

$$P = \sum_{i=0}^{n} a_i x^i \quad \text{et} \quad Q = \sum_{j=0}^{m} b_i x^i$$

deux polynômes à coefficients complexes. Pour $k \in \mathbb{N}$, on pose

$$c_k = a_0 b_k + a_1 b_{k-1} + \ldots + a_k b_0 = \sum_{i+j=k} a_i b_j \in \mathbb{C}.$$

On définit alors le **produit** de polynômes comme

$$P \cdot Q := \sum_{k=0}^{n+m} c_k x^k.$$

C'est un polynôme de degré $n + m = \deg(P) + \deg(Q)$ (car $c_{n+m} = a_n b_m \neq 0$).

Proposition 3.13. *La multiplication des polynômes vérifie les propriétés suivantes.*

Soit P, Q, et R dans $\mathbb{C}[x]$, alors :

(i) $P \cdot Q = Q \cdot P$ *(commutativité) ;*

(ii) $P \cdot (Q \cdot R) = (P \cdot Q) \cdot R$ *(associativité) ;*

(iii) $1 \cdot P = P$ *(élément neutre) ;*

(iv) $0 \cdot P = 0$ *;*

(v) $\deg(P \cdot Q) = \deg(P) + \deg(Q)$ *;*

(vi) *si* P *et* Q *sont dans* $\mathbb{R}[x]$*, alors* $P \cdot Q \in \mathbb{R}[x]$ *;*

(vii) $P \cdot (Q + R) = P \cdot Q + P \cdot R$ *(distributivité).*

Démonstrations. La vérification est laissée en exercice au lecteur. (Voir exercice 28) ■

Remarque.

1) En général, un polynôme n'a pas d'inverse multiplicatif. Autrement dit, le résultat de la division d'un polynôme par un autre polynôme n'est pas un polynôme. Par exemple, $(x+1)/(x+2)$ ne peut pas s'écrire sous la forme d'un polynôme. En effet, supposons par contradiction qu'il existe un polynôme P tel que $(x+2)P = (x+1)$. Alors $1 = \deg(x+1) = \deg(x+2)+\deg(P) = \deg(x+2)$. Donc $\deg(P) = 0$ ce qui 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 : $2a = a$. D'où $a = 0$ ce qui est absurde, car P est une constante non nulle. L'expression $(x+1)/(x+2)$ n'est donc pas un polynôme, c'est une **fraction rationnelle**. Les fractions rationnelles sont aux polynômes ce que $\mathbb{Q}$ est à $\mathbb{Z}$.

2) Multiplier un polynôme P par une constante $c \in \mathbb{C}$, c'est-à-dire un polynôme de degré 0, revient à multiplier les coefficients de P par c. On peut donc diviser un polynôme par une constante c non nulle (bien entendu en multipliant par $1/c$).

3.5.2 Racine d'un polynôme

Définition.

1) Soit $P \in \mathbb{C}[x]$ et $\alpha \in \mathbb{C}$, alors le nombre complexe $P(\alpha)$ est obtenu en remplaçant chacun des x dans P par le nombre complexe α. On dit que $P(\alpha)$ est l'**évaluation de P en α**.

2) Une **racine complexe d'un polynôme P** est un nombre $\alpha \in \mathbb{C}$ tel que $P(\alpha) = 0$. On dit qu'on a une **racine réelle** si $\alpha \in \mathbb{R}$.

Résoudre une équation polynomiale consiste à trouver toutes les racines du polynôme associé. L'existence de racine est assurée par le théorème fondamental de l'algèbre dont nous admettrons la démonstration [7].

7. Il y en a plusieurs, mais cela relève de cours plus avancées.

Théorème 3.14 (Théorème fondamental de l'algèbre)**.** *Tout polynôme à coefficients complexes, de degré* ≥ 1*, admet au moins une racine* $\alpha \in \mathbb{C}$*.*

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 i et $-i$ dans $\mathbb{C}$.

3.5.3 Factorisation des polynômes de degré 2 sur $\mathbb{C}$

La factorisation d'un polynôme de degré 2 à coefficients complexes procède exactement de la même façon que dans le cas réels, au détail près qu'on admet maintenant de calculer la racine carrée d'un nombre négatif. Soit donc $P = ax^2 + bx + c \in \mathbb{C}$ un polynôme à coefficients complexes avec $a \neq 0$. On calcule le **discriminant du polynôme**

$$\Delta = b^2 - 4ac \in \mathbb{C}.$$

Les racines complexes du polynôme P sont alors

$$z_1 = \frac{-b + \sqrt{\Delta}}{2a} \quad \text{et} \quad z_2 = \frac{-b - \sqrt{\Delta}}{2a}.$$

Le polynôme P admet donc toujours la factorisation :

$$P = a(x - z_1)(x - z_2).$$

Notons qu'on peut calculer la racine carrée de tout nombre complexe. Elle se calcule via la forme exponentielle de ce nombre complexe.

Exemple. Prenons $P = x^2 + i$. Le discriminant est $\Delta = 0 - 4i = -4i$. On obtient

$$\sqrt{\Delta} = \Delta^{1/2} = (-4i)^{1/2} = (4e^{-\pi/2})^{1/2} = 2e^{-\pi/4} = \sqrt{2} - i\sqrt{2}.$$

D'où

$$P = (x - e^{-i\pi/4})(x + e^{-i\pi/4}).$$

Pour les polynômes de degré supérieur à 2, le calcul de racines 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 XIXe siècle.

3.5.4 Division euclidienne des polynômes

On a vu que l'on ne peut pas toujours diviser (sans reste) un polynôme par un autre. Cependant, la **division euclidienne** (la division avec reste), qui est toujours possible, est très intéressante.

Théorème 3.15. *Soit $A, B \in \mathbb{C}[x]$ (resp. à coefficients réels) de degrés respectifs n et m. Si $0 \leq m \leq n$, alors il existe une unique décomposition*

$$A = BQ + R$$

où $Q, R \in \mathbb{C}[x]$ (resp. à coefficients réels) tel que $\deg(R) < m = \deg(B)$. On dit que Q est le **quotient** *(euclidien) de A par B, et que R est le* **reste**.

Remarque.

(i) Si $m = 0$, alors $\deg(R) = -\infty$ ce qui implique que $R = 0$. La division euclidienne correspondante est $A = A \cdot 1 + 0$.

(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. Soit $A = x^3 - 1$ et $B = x^2 + 1$. Alors

$$A = x(x^2 + 1) + (-x - 1) = x\,B + (-x - 1).$$

Comme $\deg(-x-1) = 1 < 2 = \deg(B)$, 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 du théorème 3.15**] 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 choses se font séparément.

Existence. On démontre l'existence de Q et R par récurrence sur $n = \deg(A) \geq 0$.

Étape initiale $n = 0$: On a par hypothèse que $0 = \deg(A) \geq \deg(B) \geq 0$. Donc $\deg(B) = 0$ et A et B sont des constantes *non nulles*. Il suffit de prendre $Q = A/B$ et $R = 0$. La propriété est donc vraie au premier rang.

Supposons maintenant la propriété vraie jusqu'au rang $n-1$. On peut toujours écrire $A = BQ_1 + R_1$ avec $Q_1, R_1 \in \mathbb{C}[x]$ tel que $\deg(R_1) < n$. Comme $\deg(R_1) < n$, l'hypothèse de récurrence (deuxième forme) implique qu'il existe un unique couple $Q', R' \in \mathbb{C}$ tel que $\deg(R') < m$ et $R_1 = BQ' + R'$. Ceci entraîne que

$$A = Q_1 B + R_1 = Q_1 B + BQ' + R' = B(Q_1 + Q') + R'.$$

Il suffit de prendre $Q = Q_1 + Q'$ et $R = R'$. On vient de montrer que la propriété se transmet de rang en rang, elle est donc vraie pour tout $n \in \mathbb{N}^*$.

Unicité. Supposons que $A = BQ_1 + R_1 = BQ_2 + R_2$ avec $\deg(R_1), \deg(R_2) < m$. En réécrivant cette égalité, on trouve

$$B(Q_1 - Q_2) = R_2 - R_1.$$

Ce qui entraîne que $\deg(R_2 - R_1) = \deg(B) + (\deg(Q_1 - Q_2))$. Comme

$$\deg(R_1 - R_2) = \max(\deg(R_1), \deg(R_2)) < m,$$

on obtient l'inégalité suivante

$$m > \deg(B) + \deg(Q_1 - Q_2) = m + \deg(Q_1 - Q_2).$$

Il s'en suit que $\deg(Q_1 - Q_2) < 0$. Ce qui veut dire que $\deg(Q_1 - Q_2) = -\infty$ et donc que $Q_1 - Q_2 = 0$. En revenant à l'égalité, on se rend alors compte que $\deg(R_1 - R_2) = -\infty$. En d'autres termes $R_2 - R_1 = 0$ et donc $R_1 = R_2$. D'où l'unicité. ■

Corollaire 3.16. *Soit $P \in \mathbb{C}[x]$ et α une racine de P, alors P se factorise par $(x - \alpha)$: il existe $S \in \mathbb{C}[x]$ tel que*

$$P = (x - \alpha)\, S \text{ et } \deg(S) = \deg(P) - 1.$$

Démonstrations. La division euclidienne des polynômes assure l'existence de $R, S \in \mathbb{C}[x]$ tel que $\deg R < 1$ et

$$P = (x - \alpha)S + R.$$

Comme $\deg R < 1$, R est une constante. c.-à.-d. que $R(x) = a$ pour a dans $\mathbb{C}$. On évalue maintenant P en α

$$0 = P(\alpha) = (\alpha - \alpha)S(\alpha) + R(\alpha) = R(\alpha).$$

Donc $a = R(\alpha) = 0$, et donc $R(x)$ est le polynôme nul. ■

Corollaire 3.17. *Soit $P = a_n x^n + \ldots + a_0 \in \mathbb{C}[x]$ de degré $n \geq 1$. Il existe $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ tel que $P(x) = a_n(x - \alpha_1)\ldots(x - \alpha_n)$. On dit que l'on a* **factorisé** *P sur $\mathbb{C}$. En particulier, P admet au plus n racines distinctes dans $\mathbb{C}$.*

Démonstrations. La preuve se fait par récurrence sur $\deg(P)$ en utilisant le corollaire précédent (voir exercice 34). ■

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

$$z_1 = \frac{-1 + i\sqrt{3}}{2} \quad \text{et} \quad z_2 = \frac{-1 - i\sqrt{3}}{2} = \overline{z}_1.$$

D'où P se factorise comme suit :

$$P = (x - 1)(x - z_1)(x - \overline{z}_1).$$

Les solutions de l'équation polynomiale $P(x) = 0$ sont $1, z_1, \overline{z}_1$.

3.5.5 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. Cependant, on a le résultat suivant.

Théorème 3.18. *Soit $P(x)=a_nx^n+\ldots+a_0\in\mathbb{R}[x]$ 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 :*

$$P(x)=a_n(x-\alpha_1)\ldots(x-\alpha_k)\,Q_1\ldots Q_j.$$

où $\alpha_1,\ldots,\alpha_k\in\mathbb{R}$ et $Q_1,\ldots,Q_j\in\mathbb{R}[x]$ sont des polynômes de degré 2 qui n'ont pas de racine réelle.

Démonstrations.

(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 35). Tout d'abord, en vertu du corollaire 3.17, on écrit

$$P=a_n(x-\alpha_1)\ldots(x-\alpha_k)(x-z_1)\ldots(x-z_\ell)$$

où $\alpha_i\in\mathbb{R}$ et $z_i\in\mathbb{C}\setminus\mathbb{R}$. On utilise ensuite (i) pour montrer que, quitte à renuméroter les racines, $(x-z_1)\ldots(x-z_\ell)=(x-z_1)(x-\overline{z}_1)\ldots(x-z_j)(x-\overline{z}_j)$ avec $j=\ell/2$. Enfin, si $z\in\mathbb{C}\setminus\mathbb{R}$, on observe que $(x-z)(x-\overline{z}\,)=x^2-(z+\overline{z}\,)x+z\overline{z}=x^2-2\,\mathrm{Re}(z)x+|z|^2\in\mathbb{R}[x]$ est un polynôme de degré 2 qui n'a pas de racine réelle. La conclusion est une conséquence immédiate de ces trois observations.

■

3.6 Exercices du chapitre 3

Les nombres complexes

Exercice 1 (A) Écrire les nombres complexes suivants sous la forme $a+b\,i$:

(a) $1+3i+9i^2+27i^3+81i^4+243i^5$; (b) $\frac{-7-3i}{1+5i}$; (c) $i^{1000}+i^{123}$.

Réponses : (a) $73+219i$; (b) $-\frac{11}{13}+\frac{16}{13}i$; (c) $1-i$.

Exercice 2 (A) (Démonstration du cours) (Proposition 3.1) Soit $z,z',z''\in\mathbb{C}$, 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 (A) (Démonstration du cours) (Proposition 3.2) Soit $z,z',z''\in\mathbb{C}$, 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 4 (A) (Démonstration du cours) (Proposition 3.3) Soit $z,z'\in\mathbb{C}$, montrer que :
(i) $z\overline{z}=|z|^2\in\mathbb{R}$;
(ii) $z+\overline{z}=2\,\mathrm{Re}(z)$;
(iii) $z-\overline{z}=2\,\mathrm{Im}(z)$;
(iv) $|zz'|=|z||z'|$ et $|\overline{z}|=|z|$;
(v) $z\in\mathbb{R}\ \Leftrightarrow\ \mathrm{Im}(z)=0\ \Leftrightarrow\ \overline{z}=z$.

Exercice 5 Montrer que si z est un nombre complexe de module 1, son inverse est $\overline{z}$.

Exercice 6 (A) (a) Calculer le module des nombres complexes suivants :

$$z_1=(7+35i)(3+2i)\quad ;\quad z_2=\frac{7-35i}{3-2i}\quad ;\quad z_3=\frac{(5+3i)(1+i)}{4+i}.$$

(b) Mettre sous forme algébrique les nombres complexes suivants : z_1 ; z_2 ; z_3 ; z_1+z_2 ; z_2-z_3 ; z_1z_2 ; z_1z_3.

Réponses : (a) $|z_1|=91\sqrt{2}$; $|z_2|=7\sqrt{2}$; $|z_3|=2$.
(b) $z_1+z_2=-42+112i$; $z_2-z_3=\frac{103}{17}-i\frac{149}{17}$; $z_1z_2=490+1176i$; $z_1z_3=\frac{-4354}{17}+i\frac{434}{17}$.

Exercice 7 (Démonstration du cours) Montrer que si $z,z'\in\mathbb{C}^*$, alors $\frac{z}{z'}=\frac{\mathrm{Re}(z\overline{z'})}{|z'|^2}+i\frac{\mathrm{Im}(z\overline{z'})}{|z'|^2}$.

Exercice 8 (B) (Démonstration du cours) (Proposition 3.4) Soit $z\in\mathbb{C}$, montrer qu'il existe un unique $\theta\in[0,2\pi[$ tel que $z=|z|(\cos(\theta)+i\sin(\theta))$. Le nombre θ est appelé *l'argument de* z et est noté $\arg(z)$.

Exercice 9 (A) Écrire les nombres complexes suivants sous forme exponentielle :
(a) $z_1=1+i$; (b) $z_2=\sqrt{3}+i$; (c) $1-i\sqrt{3}$.

Réponses : (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 10 (A) Soit $j=-\frac{1}{2}+\frac{\sqrt{3}}{2}i$.
(a) Calculer $|j|$; (b) Démontrer que $j^2=\overline{j}$; (c) En déduire que j est une racine $3^{\text{ème}}$ de l'unité.

Réponses : (a) $|j| = 1$; (b) $j^2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i = \overline{j}$; (c) $j^3 = j^2 \cdot j = \overline{j} \cdot j = |j|^2 = 1^2 = 1$.

Exercice 11 **(Examen 2011)**

On considère les deux nombres complexes suivants : $z_1 = 1 + i\sqrt{3}$ et $z_2 = 1 - i$.

1. Écrire z_1 et z_2 sous forme exponentielle ;
2. Donner la forme algébrique et exponentielle de $z_1 z_2$;
3. En déduire la valeur exacte de $\cos \frac{\pi}{12}$ et de $\sin \frac{\pi}{12}$.

Raisonnement par récurrence

Exercice 12 (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 $\binom{n}{i} = \frac{n!}{i!(n-i)!}$.

Exercice 13 Montrer par récurrence les formules suivantes :

$$(a)\ \sum_{k=0}^{n} k(k+1) = \frac{1}{3}n(n+1)(n+2); \quad (b)\ \sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6};$$

$$(c)\ \sum_{k=1}^{n} k^3 = \left(\sum_{i=1}^{n} i\right)^2; \quad (d)\ \sum_{i=0}^{n} 2^i = 2^{n+1} - 1; \quad (e)\ 2^n > n.$$

Exercice 14 (B) **(Examen 2010)**

1. Vérifier que $3^{2n+4} = 7 \cdot 3^{2n+2} + 2 \cdot 3^{2n+2}$.
2. Démontrer par récurrence que pour tout entier $n \geq 1$, 7 divise $3^{2n+2} - 2^{n+1}$.

Exercice 15 (B) **(Examen 2011)**

Montrer la formule suivante par récurrence :

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = 1 - \frac{1}{n+1}, \quad \forall n \in \mathbb{N}^*.$$

Nombres complexes et géométrie

Exercice 16 (A) Les questions ci-dessous sont indépendantes.

(a) Déterminer l'ensemble des points z vérifie $z\overline{z} = 4$.

(b) On considère le point $(2+3i)$. Déterminer l'ensemble des points z tels que $|z-(2+3i)| = 5$.

Réponses :

(a) $\{z \mid |z| = 2\}$, c.-à-d. les z qui appartiennent au cercle de centre $(0,0)$ et de rayon $R = 2$.

(b) $\{z \mid |z - z_A| = 5\}$, c.-à-d. les z qui appartiennent au cercle de centre $(2,3)$ et de rayon $R = 5$.

Exercice 17 (B) (Examen 2012) Soit $\mathcal{A}$ la transformation du plan complexe qui associe à z la valeur

$$\mathcal{A}(z) = a\,z + 3\,i, \quad a \in \mathbb{C}.$$

1. Montrer que si $a = 2$, $\mathcal{A}$ est une homothétie et déterminer le centre et le rapport de $\mathcal{A}$.
2. Montrer que si $a = -i$, $\mathcal{A}$ est une rotation et déterminer le centre et l'angle de $\mathcal{A}$.

Exercice 18 Donner l'écriture complexe des transformations suivantes :

1. La translation de vecteur $\mathbf{u}$ de coordonnées $(1,2)$;
2. L'homothétie de centre $(-1,1)$ et de rapport -3 ;
3. La rotation de centre $2-4i$ et d'angle $\pi/3$.

Exercice 19 (B) (Démonstration du cours) (Théorème 3.10) Démontrer les propriétés suivantes :

1. Les rotations et les translations préservent les distances (ce sont des **isométries**).
2. L'image d'une droite par une translation, une rotation ou une homothétie est une droite.
3. 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 20 (B) (Démonstration du cours) (Théorème 3.11) Démontrer les propriétés suivantes :

(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 donne deux droites parallèles.

(iv) L'image de deux droites perpendiculaires par une translation ou une similitude donne 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.

Exercice 21 Montrer que l'image d'un cercle par une rotation est un cercle dont l'on déterminera à chaque fois le rayon et le centre.

Exercice 22

1. Soit $z_1 = 4 + 4i$ et $z_2 = 4 - 4i$. Écrire z_1 et z_2 sous forme algébrique et exponentielle.
2. Soit le nombre complexe $4e^{i\pi/3}$. Donner sa forme algébrique.
3. Montrer que le triangle de sommets $4 + 4i$, $4 - 4i$, $2 + 2i\sqrt{3}$ est rectangle.

Exercice 23 On considère la translation $\mathcal{T}$ par $c = 2 + i$, l'homothétie $\mathcal{H}$ de centre $a = 2 + 4i$ et de rapport $-3/2$, ainsi que la rotation $\mathcal{R}$ de centre $b = 1 - i$ et d'angle $\pi/3$.

1. Soit z_1 l'image de z par $\mathcal{T}$. Donner l'expression de z_1 en fonction de z.
2. Soit z_2 l'image de z par $\mathcal{H}$. Donner l'expression de z_2 en fonction de z. En déduire une expression du vecteur $z_2 - a$ en fonction du vecteur $z_1 - a$.
3. Soit z_3 l'image de z par $\mathcal{R}$. Déterminer le module et l'argument de $(z_3 - b)/(z - b)$. En déduire
$$\frac{z_3 - b}{z - b} \quad \text{et} \quad \angle(z - b, z_3 - b).$$
4. Déterminer l'image de 0 par $\mathcal{T}$, $\mathcal{H}$ et $\mathcal{R}$.

Exercice 24 **(Examen 2011)**

Soit ABC un triangle quelconque (en sens direct), on notera a (resp. b, c) le nombre complexe correspondant à A (resp. B, C). On construit les points A' (resp. B' et C') extérieurement à ABC tel que le triangle BCA' (resp. CAB' et ABC') soit rectangle isocèle en A' (resp. B' et C'). On notera a', b' et c' les complexes correspondant à A', B' et C'.

1. En choisissant judicieusement une rotation dont on donnera le centre et l'angle, montrer que :
$$a' = \frac{b - ic}{1 - i}.$$
En déduire que $a' - a = i(c' - b')$.
2. En déduire que $(AA') \perp (B'C')$ et $AA' = B'C'$, puis que (AA'), (BB') et (CC') sont concourantes.

Exercice 25 **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 de B. Soit M' est le point diamétralement opposé à M.

1. Quelle est la nature du triangle AOM. En déduire que :
$$2\angle(\overrightarrow{MA}, \overrightarrow{MO}) \equiv \angle(\overrightarrow{OA}, \overrightarrow{OM'}) \pmod{2\pi}.$$
2. Evaluer de la même manière $2\angle(\overrightarrow{MB}, \overrightarrow{MO})$.
3. En déduire que $2\angle(\overrightarrow{MA}, \overrightarrow{MB}) \equiv \angle(\overrightarrow{OA}, \overrightarrow{OB}) \pmod{2\pi}$.
4. A-t-on $\angle(\overrightarrow{MA}, \overrightarrow{MB}) \equiv \angle(\overrightarrow{OA}, \overrightarrow{OB})/2 \pmod{2\pi}$. Justifier la réponse.

Partie B. On dit que quatre points A, B, C et D sont cocyclique s'il existe un cercle $\mathscr{C}$ tel que $A, B, C, D \in \mathscr{C}$.

1. Montrer que A, B, C, D sont cocycliques si et seulement si D est un point du cercle circonscrit au triangle ABC.
2. Montrer que A, B, C, D sont cocycliques si et seulement si
$$\angle(\overrightarrow{AB}, \overrightarrow{AC}) \equiv \angle(\overrightarrow{DB}, \overrightarrow{DC}) \pmod{\pi}.$$

Exercice 26 (B) Dans le plan orienté identifié à $\mathbb{C}$, on considère un carré direct $ABCD$ de centre O. Soit I le milieu de $[CD]$. On construit le carré direct $DIJK$.

1. Faire une figure en choisissant $AB = 6$.
2. On considère la similitude $\mathcal{S}$ et de centre D qui transforme A en B.
   a) Déterminer les éléments caractéristiques de $\mathcal{S}$, c'est-à-dire l'angle et le rapport.
   b) Déterminer l'image du point I par la similitude $\mathcal{S}$.
3. a) Soit $\mathscr{C}$ le cercle circonscrit au carré $ABCD$ et E le point d'intersection des droites (AI) et (BJ). Montrer que E appartient à $\mathscr{C}$. (Indication : on pourra utiliser l'exercice précédent).
   b) Montrer que les droites (ED) et (BJ) sont orthogonales.

Polynômes

Exercice 27 (A) (Démonstration du cours) (Proposition 3.12) Soit $P, Q, R \in \mathbb{C}[x]$, montrer que :

(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) $\deg(P + Q) = \max(\deg(P), \deg(Q))$;
(vi) si $P, Q \in \mathbb{R}[x]$, $P + Q \in \mathbb{R}[x]$.

Exercice 28 (A) (Démonstration du cours) (Proposition 3.13) Soit $P, Q, R \in \mathbb{C}[x]$, montrer que :

(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 $P, Q \in \mathbb{R}[x]$, $PQ \in \mathbb{R}[x]$;
(vii) $P(Q + R) = PQ + PR$ (distributivité).

Exercice 29 **(Examen 2010)** Dans l'ensemble $\mathbb{C}$ des nombres complexes, i désigne le nombre de module 1 et d'argument $\frac{\pi}{2}$.

1. Montrer que $(1+i)^6 = -8i$;
2. Déduire de 1) une racine du polynôme $P = x^3 + 8i$.
3. On considère le point $2i$ et la rotation $\mathcal{R}$ de centre 0, et d'angle $\frac{2\pi}{3}$.
   (a) Déterminer b l'image de a par $\mathcal{R}$, ainsi que c l'image de b par r.
   (b) Montrer que b et c sont aussi des racines de P.
   (c) En déduire une factorisation de P sur $\mathbb{C}$.
4. Dans le plan rapporté à un repère orthonormé, représenter a, b, et c.
5. Quelle est la nature du triangle formé par les racines du polynôme P ? (Justifier)

Exercice 30 **(Pentagone régulier)** Dans le plan complexe, on considère le pentagone régulier standard, dont les sommets sont les racines cinquièmes de l'unité :

$$1,\ \xi = e^{i\frac{2\pi}{5}},\ \xi^2,\ \xi^3 = \xi^{-2},\ \xi^4 = \xi^{-1} = \overline{\xi}\,.$$

1. Montrer que $1 + \xi + \xi^2 + \xi^3 + \xi^4 = 0$.
2. 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
$$P(x) = (x-\xi)(x-\xi^2)(x-\xi^3)(x-\xi^4).$$
3. Soit $\alpha = \xi + \xi^{-1}$ et $\beta = \xi^2 + \xi^{-2}$.
   (a) Montrer que α et β sont les racines du polynôme $x^2 + x - 1$.
   (b) Calculer $\alpha + \beta$ et $\alpha\beta$.
   (c) En déduire les valeurs de
$$\cos\frac{2\pi}{5} \quad \text{et} \quad \cos\frac{4\pi}{5}$$
4. On trace le cercle $\mathscr{C}$ de centre $-\frac{1}{4}$ passant par le point $\frac{i}{2}$.
   (a) Ecrire l'équation de $\mathscr{C}$.
   (b) Montrer que $\mathscr{C}$ coupe l'axe des réels aux points $\alpha/2$ et $\beta/2$.
   (c) En déduire une construction du pentagone régulier à la règle et au compas.

Exercice 31 (A) (1) Effectuer la division euclidienne du polynôme P par le polynôme Q dans les cas suivants :

(a) $P = 2x^3 + 5x^2 - x - 6$ et $Q = x - 1$;

(b) $P = 2x^4 + x^2 + 3$ et $Q = x^2 - 2$;

(c) $P = x^4 - x^3 + 2x^2 - x + 1$ et $Q = x^2 + 1$.

(2) Dans le cas où le reste de cette division est nul, donner les factorisations et les racines de ces polynômes sur $\mathbb{C}$ et $\mathbb{R}$.

Réponses : (1) (a) $P(x) = (2x^2 + 7x + 6)Q(x)$; (b) $P(x) = (2x^2 + 5)Q(x) + 13$;

(c) $P(x) = (x^2 - x + 1)Q(x)$.

Exercice 32 Montrer que si $P \in \mathbb{R}[x]$ est de degré $n > 0$ impair, alors P admet au moins une racine réelle.

Exercice 33 Décomposer les polynômes suivants dans $\mathbb{R}$ et $\mathbb{C}$:

$$P(x) = x^2 + ix - 2, \quad Q(x) = x^2 + \sqrt{3}x + \frac{1}{2}, \quad R(x) = x^4 + 4x^2 + 3.$$

Exercice 34 (B) (Démonstration du cours) (Corollaire 3.17) Soit $P = a_n x^n + \ldots + a_0 \in \mathbb{C}[x]$ de degré $n \geq 1$. Montrer qu'il existe $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ tel que $P(x) = a_n(x - \alpha_1) \ldots (x - \alpha_n)$. On dit que l'on a **factorisé** P **sur** $\mathbb{C}$. En particulier, P admet au plus n racines distinctes dans $\mathbb{C}$.

Exercice 35 (B) (Démonstration du cours) (Théorème 3.18) Démontrer la deuxième partie de ce théorème : Soit $P(x) = a_n x^n + \ldots + a_0 \in \mathbb{R}[x]$ de degré $n \geq 1$.

1. Si α est une racine complexe de P alors $\overline{\alpha}$ est aussi une racine de P.
2. P a au plus n racines réelles et P peut se décomposer sur $\mathbb{R}$ comme suit :
$$P(x) = a_n(x - \alpha_1) \ldots (x - \alpha_k)Q_1 \ldots Q_l.$$
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 qui n'ont pas de racine réelle.

Exercice 36 (B) (Examen 2012) Soit $P \in \mathbb{C}[x]$ le polynôme défini par

$$P = x^3 - (6 + 2i)x^2 + (12 + 12i)x - 24i.$$

1. Montrer que $2i$ est une racine de P.
2. Montrer qu'il existe $Q \in \mathbb{R}[x]$ de degré 2 tel que $P = (x - 2i)Q$.
3. 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 4

Arithmétique

4.1 Arithmétique dans $\mathbb{Z}$

Les nombres entiers ont été étudiés depuis la nuit des temps. Vers le IIIe siècle, le mathématicien grec Diophante d'Alexandrie (∼200 à ∼284) propose dans son traité d'arithmétique une méthode pour répondre à la question suivante : on considère l'équation $6x + 9y = 12$, est-ce qu'il y a des solutions entières ? Si oui, lesquelles ?

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 ». Un des éléments clés de cette démarche est la « division euclidienne » d'entiers, qui est très similaire à celle des polynômes.

4.1.1 La division euclidienne

Dès l'école primaire, on apprend à trouver par exemple que 13 est le quotient de 91 par 7, avec reste 4. On écrit ceci

$$95 = 13 \cdot 7 + 4.$$

En général, on a

Théorème 4.1 (Division euclidienne)**.** *Soit $a, b \in \mathbb{Z}$ avec $b \neq 0$. Alors il existe $q, r \in \mathbb{Z}$ avec $0 \leq r < |b|$ tels que*

$$a = b\,q + r.$$

Les nombres q et r sont déterminés de manière unique par ces conditions. On dit que q est le **quotient** *de a par b, et que r est le* **reste**.

[**Démonstration**.] Nous n'allons donner la preuve que dans le cas où tous les nombres sont positifs. La situation générale est similaire.

Existence. L'existence de q et r se montre par récurrence sur a (b étant fixé).

Si $a = 0$, on prend $q = r = 0$, et on a bien $0 \leq r < b$, puisque $b \geq 1$. Supposons maintenant prouvée l'existence de q et r pour a (hypothèse de récurrence), et prouvons l'existence d'un q', r' tels que $a + 1 = bq' + r'$ avec $0 \leq r' < b$. Nous avons $a = bq + r$ avec $0 \leq r < b$. Par conséquent, $a + 1 = bq + r + 1$.

Dans le cas où $r + 1 < b$, nous avons $a + 1 = bq' + r'$ avec $0 \leq r' < b$ et $q' = q$, $r' = r + 1$. Si l'on n'a pas $r + 1 < b$, on doit avoir $r + 1 \geq b$; 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 $a = bq_1 + r_1 = bq_2 + r_2$, avec $0 \leq r_1 < b$ et $0 \leq r_2 < b$. Alors $-b < -r_2 \leq 0$, d'où par addition des inégalités : $-b < r_1 - r_2 < b$. Comme $b > 0$, on a : $|r_1 - r_2| < b$. Maintenant, nous avons aussi $b(q_1 - q_2) = r_2 - r_1$, d'où en valeurs absolues $|r_2 - r_1| = |b| \cdot |q_1 - q_2|$. Ce qui donne, puisque b est positif, $b > |r_2 - r_1| = b \cdot |q_1 - q_2|$, et donc que $|q_1 - q_2| < 1$. Puisque $|q_1 - q_2| \in \mathbb{N}$, on a forcément $q_1 - q_2 = 0$. D'où $q_1 = q_2$ et par suite $r_1 = r_2$. ■

4.1.2 Divisibilité dans $\mathbb{Z}$

Définition. Soit $d, n \in \mathbb{Z}$, 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.

1. Il faut bien comprendre que la divisibilité est un concept qui existe uniquement dans $\mathbb{Z}$. La fraction $a/b \in \mathbb{Q}$ est une écriture symbolique construite pour décrire les nombres rationnels et n'a rien à voir avec la notation $b|a$.
2. Avec le quantificateur $\exists$, qui signifie « il existe » en français, on peut réécrire la définition de divisibilité comme suit : $d, n \in \mathbb{Z} \setminus \{0\}$, $d|n \Leftrightarrow \exists\, q \in \mathbb{N}$, $n = dq$.

3. 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 4)

4. Le seul diviseur entier naturel de 1 est 1, c.-à-d., si $k|1$ et $k \geq 1$ alors $k = 1$. En effet, si k est un diviseur entier naturel de 1 alors $1 = kp$ avec $p \in \mathbb{N}^*$; donc $k \leq 1$.

5. Soit $d, n \in \mathbb{N}^*$, 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.

Exemples. (a) $3|12$ car $12 = 3 \cdot 4$.

(b) 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 4.2. *La divisibilité vérifie les propriétés suivantes : soit n, m, p des entiers non nuls,*

(1) *1 et -1 divisent n ;*

(2) *$n|n$ (réflexivité) ;*

(3) *$n|m$ et $m|p \Rightarrow n|p$ (transitivité) ;*

(4) *$p|n \Rightarrow p|nm$;*

(5) *$p|n$ et $p|m \Rightarrow p|n + m$ et $p|n - m$;*

(6) *plus généralement : $p|n$ et $p|m \Rightarrow p|an + bm$ pour tous $a, b \in \mathbb{Z}$.*

Démonstration.

(1) On a que $1|n$ car $n = 1 \cdot n$, et $-1|n$ car $n = (-1) \cdot (-n)$.

(2) On a $n|n$ car $n = n \cdot 1$.

(3) On a

$$\begin{aligned} (n|m \quad \text{et} \quad m|p) \quad &\Rightarrow \quad \exists\, q, q' \in \mathbb{Z},\ m = nq \quad \text{et} \quad p = mq' \\ &\Rightarrow \quad p = (nq)q' = n(qq') \\ &\Rightarrow \quad n|p,\ \text{car } qq' \in \mathbb{Z}. \end{aligned}$$

Le reste de la preuve est laissé en exercice. (Voir exercice 5)

■

4.1.3 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 » : $n|m$ si et seulement si $m \in n\mathbb{Z}$; si et seulement si $m\mathbb{Z} \subseteq n\mathbb{Z}$.

Exemples. (a) $0\mathbb{Z} = \{0\}$; (b) $1\mathbb{Z} = \mathbb{Z}$;

(c) $2\mathbb{Z} = \{2k \,|\, k \in \mathbb{Z}\} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$. C'est l'ensemble des nombres pairs. L'ensemble des *nombres impairs* s'écrit $1 + 2\mathbb{Z}$.

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

$$6\mathbb{Z} + 4\mathbb{Z} := \{6a + 4b \,|\, a, b \in \mathbb{Z}\},$$

alors

$$6\mathbb{Z} + 4\mathbb{Z} = 2\mathbb{Z}.$$

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, c.-à-d. $c \in 2\mathbb{Z}$. 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 considérant tous les sous-ensembles de $\mathbb{Z}$ qui ont les mêmes propriétés que les ensembles de multiples.

Définition. Un sous-ensemble non vide $I \subseteq \mathbb{Z}$ est un *idéal de* $\mathbb{Z}$ si pour tout entier $n, m \in \mathbb{Z}$ on a

(i) $n, m \in I \Rightarrow n + m \in I$;

(ii) $m \in I \Rightarrow nm \in I$.

On remarque que $0 \in I$, car si $n \in I$, alors par (ii) : $-n = -1 \cdot n \in I$; et donc par (i) : $0 = n + (-n) \in I$.

Exemples.

(a) $I = \{6a + 4b \,|\, a, b \in \mathbb{Z}\}$ est un idéal (Exercice 6) ;

(b) $1 \in I \;\Leftrightarrow\; I = \mathbb{Z}$ (Exercice 6) ;

(c) L'ensemble des nombres impairs n'est pas un idéal, car la somme de deux nombres impairs est paire et 0 n'est pas non plus un nombre impair. (On rappelle qu'un nombre entier n est impair si on peut l'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 4.3. *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. Si $I = \{0\}$ on peut prendre $n = 0$. Supposons $I \neq \{0\}$.

On va à nouveau utiliser la propriété de bon ordre sur $\mathbb{N}$. Soit

$$I^+ = \{x \in I \,|\, x > 0\} \subseteq \mathbb{N}.$$

Comme I est non vide et $I \neq \{0\}$, et que si $x \in I$ alors $-x \in I$, on en déduit que I^+ est non vide. Donc par propriété du bon ordre, il existe un plus petit élément $n \in I^+$ non nul. Montrons que $I = n\mathbb{Z}$. Pour cela, il faut montrer une double inclusion, c'est-à-dire, il faut montrer que $n\mathbb{Z} \subseteq I$ et $I \subseteq n\mathbb{Z}$.

Montrons que $n\mathbb{Z} \subseteq I$. Soit $x \in n\mathbb{Z}$, alors $x = kn$ avec $k \in \mathbb{Z}$. Comme I est un idéal et $n \in I$, on a $x = kn \in I$. Donc $n\mathbb{Z} \subseteq I$.

Montrons que $I \subseteq n\mathbb{Z}$. Soit $x \in I$. Pour les mêmes raisons qu'auparavant, on peut considérer $x \in I^+$ car I^+ est non vide. Donc $x \geq n$ par minimalité de n. Effectuons la division euclidienne (Théorème 4.1) de x par n : il existe un entier $q \geq 1$ et un entier $0 \leq r < n$ tel que $x = nq + r$. Comme I est un idéal et que $n, x \in I$ on a $-nq \in I$ et

$$r = x - nq = x + (-nq) \in I.$$

Or $r \geq 0$ et $r \in I$ donc soit $r = 0$, soit $r \in I^+$. Mais $r \notin I^+$ car $r < n$ et n est le plus petit élément de I^+. Donc $r = 0$ et $x = nq \in n\mathbb{Z}$. D'où la deuxième inclusion. ∎

Corollaire 4.4. *La somme de deux idéaux est un idéal. Autrement dit, soit $n, m \in \mathbb{Z}$, alors l'ensemble $n\mathbb{Z} + m\mathbb{Z} = \{nx + my \,|\, x, y \in \mathbb{Z}\}$ est un idéal.*

Démonstration. Tout idéal peut s'écrire $n\mathbb{Z}$ en vertu de la proposition précédente. Il suffit donc de montrer que $n\mathbb{Z}+m\mathbb{Z}$ est un idéal. Il est clair que $n\mathbb{Z}+m\mathbb{Z} \neq \emptyset$. De plus, si $nk+ml, nk'+ml' \in n\mathbb{Z}+m\mathbb{Z}$, alors

$$nk + ml + nk' + ml' = n(k + k') + m(l + l') \in n\mathbb{Z} + m\mathbb{Z}.$$

Finalement, si $p \in \mathbb{Z}$ et $nk + ml \in n\mathbb{Z} + m\mathbb{Z}$, on a bien $p(nk + ml) = n(pk) + m(pl) \in n\mathbb{Z} + m\mathbb{Z}$. Donc la somme $n\mathbb{Z} + m\mathbb{Z}$ 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.

4.1.4 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. Soit n, m deux entiers non nuls. Le *plus grand commun diviseur* de n et m est le plus grand entier naturel qui divise n et m. On le note $\text{pgcd}(n, m)$.

Exemples. (a) $\text{pgcd}(n, m) = \text{pgcd}(m, n)$; (b) l'ensemble des diviseurs communs à 4 et 6 est $\{\pm 1, \pm 2\} = \{-2, -1, 1, 2\}$ et $\text{pgcd}(4, 6) = 2$; (c) $\text{pgcd}(n, m) = n \Leftrightarrow n|m$ (Exercice 9).

Algorithme d'Euclide : calcul du pgcd

L'algorithme d'Euclide est un processus récursif permettant de calculer efficacement le pgcd de deux nombres, sans avoir à les factoriser. Commençons par un exemple :

Exemple. On veut calculer $\text{pgcd}(a, b)$ où $a = 45$ et $b = 14$. L'idée est de commencer par la division euclidienne de a par b, puis celle de b par le reste de cette division, etc. Posons $r_0 = a = 45$ et $r_1 = b = 14$. Les successions de division euclidienne nous donnent alors

$$\begin{array}{rcll} r_0 = 45 & = & 3 \cdot 14 + 3 = 3 \cdot r_1 + r_2 & \text{où} \quad r_2 = 3 \\ r_1 = 14 & = & 4 \cdot 3 + 2 = 4 \cdot r_2 + r_3 & \text{où} \quad r_3 = 2 \\ r_2 = 3 & = & 1 \cdot 2 + 1 = 1 \cdot r_3 + r_4 & \text{où} \quad r_4 = 1 \\ r_3 = 2 & = & 2 \cdot 1 + 0 = 2 \cdot r_4 + 0 & \text{STOP} \end{array}$$

On peut vérifier que le **dernier reste non nul est** $\text{pgcd}(a, b)$. Ici, on obtient donc que $\text{pgcd}(45, 14) = 1$.

Théorème 4.5 (Algorithme d'Euclide)**.** *Soit $a, b \in \mathbb{N}$ non nuls. Il existe un entier $N \in \mathbb{N}^*$ et des entiers naturels $r_0, \ldots, r_N$ vérifiant*

(i) (Condition initiale) *$r_0 = a$ et $r_1 = b$;*

(ii) (étape récursive) *pour $i \geq 1$*

(a) soit $r_i | r_{i-1}$ alors $N = i$ et le processus s'arrête ;

(b) sinon r_{i+1} est le reste de la division euclidienne de r_{i-1} par r_i.

On appelle ce procédé l'algorithme d'Euclide.

Dans l'exemple ci-dessus, $N = 4$.

Démonstration. Il suffit de montrer qu'il existe $N \in \mathbb{N}^*$ tel que $r_N | r_{N-1}$. La division euclidienne nous affirme que $0 \leq r_{i+1} < r_i$ pour tout $1 \leq i$. Donc $R = \{r_i \in \mathbb{N}^* \,|\, i \geq 1\}$ a un plus petit élément $r_N > 0$ car $\mathbb{N}$ est bien ordonné. Ce plus petit élément correspond bien à l'étape où $r_N | r_{N-1}$, sinon il y aurait un $r_{N+1} \in R$ avec $0 < r_{N+1} < r_N$, ce qui contredirait la minimalité de r_N. ■

Corollaire 4.6. *Avec les notations du théorème 4.5. Si $a \geq b$, alors* $\text{pgcd}(a, b) = r_N$.

Exemple. Avec $a = 12378 = r_0$ et $b = 3054 = r_1$. Appliquons successivement la division euclidienne :

$$\begin{array}{rcll} 12378 & = & 4 \cdot 3054 + 162 & \Rightarrow \quad r_2 = 162 \\ 3054 & = & 18 \cdot 162 + 138 & \Rightarrow \quad r_3 = 138 \\ 162 & = & 1 \cdot 138 + 24 & \Rightarrow \quad r_4 = 24 \\ 138 & = & 5 \cdot 24 + 18 & \Rightarrow \quad r_5 = 18 \\ 24 & = & 1 \cdot 18 + 6 & \Rightarrow \quad r_6 = 6 \\ 18 & = & 3 \cdot 6 + 0 & \Rightarrow \quad N = 6 \end{array}$$

Donc $\text{pgcd}(12378, 3054) = 6$.

Démonstration. Résultat préliminaire : Soit $n \geq m$ deux entiers non nuls, écrivons $n = mq + r$, avec $r, q \in \mathbb{Z}$. Alors si $r = 0$, on a $\text{pgcd}(n, m) = m$; si $r \neq 0$, on a $\text{pgcd}(n, m) = \text{pgcd}(m, r)$ (Exercice 10).

Rappelons-nous les notations du théorème 1.5. On sait par (a) que le reste de la division euclidienne de r_{N-1} par r_N est 0, donc $pgcd(r_{N-1}, r_N) = r_N$ en vertu de notre résultat préliminaire. De plus, par (b) on a :

$$\text{pgcd}(a, b) = \text{pgcd}(r_0, r_1) = \text{pgcd}(r_1, r_2) = \ldots = \text{pgcd}(r_{N-1}, r_N) = r_N,$$

■

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 $n = \text{pgcd}(a, b)$ et donc que l'équation $ax + by = c$ admet au moins une solution si et seulement si $\text{pgcd}(a, b)$ divise c !

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 4.7. *Soit n, m deux entiers non nuls, alors*

$$\text{pgcd}(n, m)\mathbb{Z} = n\mathbb{Z} + m\mathbb{Z} = \{nk + ml \,|\, k, l \in \mathbb{Z}\}.$$

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 $d = \text{pgcd}(n, m)$. Comme toujours, il va falloir montrer deux inclusions. Commençons par la plus facile. Si $x = nk + ml \in n\mathbb{Z} + m\mathbb{Z}$, $k, l \in \mathbb{Z}$, alors x est un multiple de d, car n et m le sont ; donc $x \in d\mathbb{Z}$.

Nous montrons maintenant l'inclusion inverse : $d\mathbb{Z} \subseteq n\mathbb{Z} + m\mathbb{Z}$. Comme $n\mathbb{Z} + m\mathbb{Z}$ est un idéal, la proposition 4.3 nous assure que $n\mathbb{Z} + m\mathbb{Z} = p\mathbb{Z}$, où $p \in \mathbb{N}$. Comme $n = n \cdot 1 + m \cdot 0 \in n\mathbb{Z} + m\mathbb{Z} = p\mathbb{Z}$, et de même $m \in n\mathbb{Z} + m\mathbb{Z} = p\mathbb{Z}$, on obtient que p divise n et m. De plus, $p \in n\mathbb{Z} + m\mathbb{Z} \subseteq d\mathbb{Z}$ comme nous l'avons vu au début de la preuve. Nous pouvons donc écrire $p = dr$, $r \in \mathbb{N}$. Mais p divise n et m, et d est le plus grand commun diviseur de n et m ; la seule possibilité est donc que $r = 1$ (sinon $p > d$). Ainsi $p = d$, d'où finalement $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$. ■

Avant de continuer notre étude, nous allons donner une dernière caractérisation très utile du *pgcd*.

Corollaire 4.8. *Soit n, m deux entiers non nuls et soit d un diviseur commun positif à m et n ; alors les conditions suivantes sont équivalentes*

1. $d = \text{pgcd}(n, m)$;
2. *Si e est un diviseur commun à n et m, alors e divise d.*

Démonstration. Il faut montrer deux implications.

Supposons premièrement que e divise d pour tout diviseur commun e à n et m. Alors en particulier, $\text{pgcd}(n, m)|d$, donc $\text{pgcd}(n, m) \leq d$ car d est positif. Comme $\text{pgcd}(m, n)$ est le plus grand commun diviseur et que d est un diviseur commun, on a l'égalité voulue.

Supposons maintenant que $d = \text{pgcd}(n, m)$. D'après le théorème 4.7, nous avons $d = nk + ml$. Soit e un commun diviseur à m et n, alors e divise $nk + ml = d$. ■

4.1.5 Plus grand commun diviseur de polynômes (*)

Il est intéressant d'observer que l'algorithme d'Euclide peut aussi s'appliquer, presque tel quel, au calcul du plus grand commun diviseur de deux polynômes dans $\mathbb{C}[x]$ (ou $\mathbb{R}(x)$). Dans ce cas, le « plus grand commun diviseur » est le polynôme de degré le plus grand (avec coefficient dominant égal à 1) qui divise sans reste chacun des polynômes considérés. Par exemple, on a

$$\text{pgcd}(x^{12} - 1, x^{15} - 1) = x^3 - 1.$$

Pour calculer le plus grand commun diviseur de deux polynômes, on remarque que l'étape principale de l'algorithme est basée sur le fait suivant.

Proposition 4.9. *Soient A et B des polynômes dans $\mathbb{C}[x]$, avec $\deg(A) \geq \deg(B)$, pour lesquels on a la division euclidienne $A = BQ + R$. Alors on a*

$$\text{pgcd}(A, B) = \text{pgcd}(B, R).$$

4.1.6 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. 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 4.10 (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 $nk + ml = 1$.*

Exemple. $4 \cdot 4 + 15 \cdot (-1) = 1$.

Démonstration. Si n et m sont premiers entre eux, le théorème 4.7 implique que $1 = nk + ml$ pour certains entiers k et l. Réciproquement, si $1 = nk + ml$, tout $e \in \mathbb{Z}$ qui divise n et m, doit diviser 1, d'où $e = 1$; donc $\text{pgcd}(n, m) = 1$. ■

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 4.11. $\sqrt{2} \notin \mathbb{Q}$.

Démonstration. On va tout d'abord montrer la propriété suivante : $2|a^2 \Rightarrow 2|a$. En raisonnant par contraposition, on montre en fait que si 2 ne divise pas a, alors 2 ne divise pas a^2. En effet, si 2 ne divise pas a, alors $a = 2k + 1$ est impair et donc $a^2 = 2(2k^2 + 2k) + 1$ est aussi impair. Donc 2 ne divise pas a^2 et alors les seuls nombres qui au carré divise 2 sont les nombres pairs qui eux-mêmes sont divisibles par 2.

On va maintenant raisonner par contradiction pour montrer la proposition. Supposons que $\sqrt{2} \in \mathbb{Q}$. Alors il existe $p, q \in \mathbb{N}^*$ tel que $\sqrt{2} = p/q$. Écrivons $p = \text{pgcd}(p, q)p'$ et $q = \text{pgcd}(p, q)q'$. Donc en vertu du Théorème de Bézout il existe $k, l \in \mathbb{Z}$ tel que $pk + ql = \text{pgcd}(p, q)$, et de ce fait, $p'l + q'b = 1$. Donc p', q' sont premiers entre eux. De ce fait, quitte à diviser par le $\text{pgcd}(p, q)$, on peut choisir p et q premiers entre eux pour écrire $\sqrt{2} = p/q$. En passant au carré, on obtient : $2q^2 = p^2$. Ainsi $2|p^2$, et donc, de ce que l'on a montré plus haut, $2|p$. écrivons alors $p = 2b$ avec $b \in \mathbb{N}$. On obtient l'équation suivante : $2q^2 = p^2 = 4b^2$, qui se simplifie en $q^2 = 2b^2$. Avec les mêmes arguments qu'auparavant on

montre que $2|q$. Donc 2 est un diviseur commun de p et de q, ce qui est une contradiction, car p et q sont premiers entre eux. ■

4.1.7 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 allons finalement donner la méthode de résolution des *équations diophantiennes linéaires du premier ordre :* déterminons les solutions entières $x, y \in \mathbb{Z}$ de l'équation diophantienne linéaire du premier ordre

$$ax + by = c, \quad a, b, c \in \mathbb{Z}.$$

Cas $c = 0$. Nous nous intéressons tout d'abord au cas $c = 0$. L'équation s'écrit alors $ax = (-b)y$. Quitte à diviser par le PGCD, on peut supposer les entiers a, b premiers entre eux. Cette équation peut alors être résolue grâce au Lemme de Gauss.

Lemme 4.12 (Lemme de Gauss)**.** *Soit 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 autres 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, $a|c$.

Revenons à notre équation $ax = -by$. Comme a et $-b$ sont premiers entre eux, on sait d'après le lemme de Gauss que a divise y et b divise x. Donc $x = bk$ et $y = -ak$, $k \in \mathbb{Z}$ sont toutes les solutions de cette équation.

Cas $c \neq 0$. Supposons maintenant $c \neq 0$

étape 1 : Existence de solutions. L'existence d'au moins une solution est garantie par le théorème 4.7 : l'équation $ax + by = c$ admet des solutions entières - nous verrons en fait qu'il en existe une infinité - si et seulement si $c \in a\mathbb{Z} + b\mathbb{Z} = \text{pgcd}(a, b)\mathbb{Z}$; c'est-à-dire, si $\text{pgcd}(a, b)|c$. D'où :

Proposition 4.13. *Soit $a, b, c \in \mathbb{Z}$, alors l'équation $ax + by = c$ admet des solutions entières si et seulement si* $\text{pgcd}(a, b)|c$.

Exemple. L'équation $12378x + 3054y = 7$ n'a pas de solution entière car $\text{pgcd}(12378, 3054) = 6 \nmid 7$.

étape 2 : 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. L'équation $14x + 45y = 6$ a au moins une solution, car 14 et 45 sont premiers entre eux. Commençons par trouver une solution particulière à l'équation $14x + 45y = 1$. On rappelle le calcul de l'algorithme d'Euclide que nous avons déjà effectué dans l'exemple qui précéde le théorème 4.5 :

$$\begin{array}{rcllll} r_0 = 45 & = & 3 \cdot 14 + 3 = 3 \cdot r_1 + r_2 & \text{où} & r_2 = 3 \\ r_1 = 14 & = & 4 \cdot 3 + 2 = 4 \cdot r_2 + r_3 & \text{où} & r_3 = 2 \\ r_2 = 3 & = & 1 \cdot 2 + 1 = 1 \cdot r_3 + r_4 & \text{où} & r_4 = 1 \\ r_3 = 2 & = & 2 \cdot 1 + 0 = 2 \cdot r_4 + 0 & \text{STOP} & \end{array}$$

On remonte maintenant l'algorithme de bas en haut à partir du pgcd et on obtient :

$$\begin{aligned} 1 = r_4 &= r_2 - 1 \cdot r_3 = 3 - 1 \cdot 2, \\ 2 = r_3 &= r_1 - 4 \cdot r_2 = 14 - 4 \cdot 3, \\ 3 = r_2 &= r_0 - 3 \cdot r_1 = 45 - 3 \cdot 14, \end{aligned}$$

En remplaçant r_3, puis r_2 dans la première équation, on obtient

$$\begin{aligned} 1 &= r_2 - 1 \cdot r_3 \\ &= r_2 - 1 \cdot (r_1 - 4 \cdot r_2) \\ &= (r_0 - 3 \cdot r_1) - 1 \cdot (r_1 - 4 \cdot (r_0 - 3 \cdot r_1)) \\ &= (45 - 3 \cdot 14) - 1 \cdot (14 - 4 \cdot (45 - 3 \cdot 14)) \end{aligned}$$

D'où

$$1 = 14 \cdot (-16) + 45 \cdot 5.$$

Une solution particulière de l'équation $14x + 45y = 1$ est donc $x_0 = -16$ et $y_0 = 5$. D'où une solution particulière à l'équation $14x + 45y = 6$ est $x_0 = 6 \cdot (-16) = -96$ et $y_0 = 6 \cdot 5 = 30$. (à noter que les plus observateurs d'entre nous pourraient aussi déterminer une solution particulière à l'œil nu !).

Les solutions de l'équation $14x + 45y = 6$ sont en fait

$$x = -96 + 45k \quad \text{et} \quad y = 30 - 14k, \text{ où } k \in \mathbb{Z}.$$

Théorème 4.14. *Soit $a, b, c \in \mathbb{Z}$ tel que a et b sont premiers entre eux. Soit x_0, y_0 une solution particulière de l'équation, c.-à-d. $ax_0 + by_0 = c$. Alors, l'équation $ax + by = c$ possède une infinité de*

solutions qui sont toutes données par

$$x = x_0 + kb \quad et \quad y = y_0 - ka, \quad k \in \mathbb{Z}.$$

Démonstration du théorème 4.14. L'existence des solutions est garantie par la proposition 4.13.

Il faut montrer une équivalence, soit deux implications : x et y sont solutions si et seulement si

$$x = x_0 + kb \quad \text{et} \quad y = y_0 - ka, \quad k \in \mathbb{Z}.$$

Soit x et y des solutions de cette équation, alors $ax + by = c = ax_0 + by_0$. En d'autres termes, $a(x - x_0) = b(y_0 - y)$, donc $a|b(y_0 - y)$. Mais comme a et b sont premiers entre eux (c'est crucial ici), par le théorème de Gauss on obtient que $a|(y_0 - y)$, c'est à dire : $y_0 - y = ka$ avec $k \in \mathbb{Z}$. De même, puisque $b|a(x - x_0)$, on peut écrire $x - x_0 = k'b$ avec $k' \in \mathbb{Z}$. Donc l'égalité $a(x - x_0) = b(y_0 - y)$ devient $abk' = abk$, ce qui implique $k = k'$. D'où

$$x = x_0 + kb \quad \text{et} \quad y = y_0 - ka, \quad k \in \mathbb{Z}.$$

La réciproque est facile et laissée en exercice au lecteur. (Voir exercice 17) ■

étape 3 : Cas général. On part de l'équation $ax + by = c$.

(i) Si $\text{pgcd}(a, b)$ ne divise pas c, on conclut immédiatement qu'il n'y a pas de solution.

(ii) Sinon, on divise a, b et c par $\text{pgcd}(a, b)$, ce qui nous donne une équation $a'x + b'y = c'$, avec a' et b' premiers entre eux. On trouve alors une solution particulière à l'équation $a'x + b'y = 1$ en remontant l'algorithme d'Euclide, puis on multiplie le résultat par c' pour obtenir une solution particulière à l'équation $a'x + b'y = c'$. Cette *équation réduite* se résout alors grâce au théorème 4.14.

(iii) Les solutions de $ax + by = c$ sont précisément les solutions de $a'x + b'y = c'$.

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

$$x = -96 + 45k \quad \text{et} \quad y = 30 - 14k, \text{ où } k \in \mathbb{Z}.$$

4.2 Nombres premiers

Malgré l'apparente simplicité de la définition des nombres premiers, ils fascinent les mathématiciens depuis toujours. Les nombres premiers sont aux nombres ce que les briques sont aux murs.

Définition. Un nombre $p \in \mathbb{N}$ est dit *premier* si $p \geq 2$ 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 4.15. *Tout entier naturel supérieur ou égal à 2 est divisible par un nombre premier.*

Démonstration. On va raisonner par récurrence (deuxième forme). Nous prenons pour $P(n)$ la propriété « n est divisible par un nombre premier ».

(i) $P(2)$ est vraie, car 2 est premier et se divise lui-même.

(ii) Supposons que $P(k)$ soit vraie pour tout $k \leq n$ (hypothèse de récurrence). Démontrons que $P(n+1)$ est aussi vraie. Si $n+1$ est premier, $P(n+1)$ est vraie, car $n+1$ se divise par lui-même. Par contre, si $n+1$ n'est pas premier, il est alors divisible par un entier naturel a tel que $2 \leq a \leq n$.

L'hypothèse de récurrence implique alors que $P(a)$ est vraie, c.-à-d. a admet un diviseur premier p : nous pouvons donc écrire $a = pq$, où q est un entier naturel, et enfin que $n+1 = ab = pqb$, où b est aussi un entier naturel. Ceci montre donc que $n+1$ est divisible par p premier, d'où $P(n+1)$ est aussi vraie.

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 de Goldbach (1742). Tout nombre entier pair non nul est 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.).

Infinité des nombres premiers

Théorème 4.16 (Euclide)**.** *Il y a une infinité de nombres premiers.*

Démonstration. Il faut montrer que l'ensemble des nombres premiers n'est pas fini. Raisonnons par contradiction :

Supposons donc qu'il n'y a qu'un nombre fini de nombres premiers ; admettons qu'il y en ait k, et notons ces nombres premiers $p_1, p_2, p_3, \ldots, p_k$. On peut faire le produit $N = p_1 p_2 \cdots p_k$, et considérer $N+1$. Ce nombre est ≥ 2, donc il admet un diviseur premier, d'après le théorème 4.15. Celui-ci se trouve parmi $p_1, \ldots, p_k$, puisque ce sont les seuls nombres premiers. Donc, il existe $1 \leq i \leq k$ tel que p_i divise $N+1$. Mais p_i divise aussi N. Donc p_i divise $(N+1) - N = 1$, ce qui est absurde, car $p_i > 1$. De ceci, nous déduisons qu'il y a une infinité de nombres premiers.

4.2.1 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 4.17. *Tout entier $n \geq 2$ est produit de nombres premiers. Plus précisément, n s'écrit*

$$n = p_1 p_2 \dots p_l,$$

où $p_1, \dots, p_l$ 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. (1) L'unicité dans le théorème veut dire que l'ordre dans lequel on écrit les p_i n'a pas d'importance, mais que $\{p_i \mid n = p_1 \dots p_l\}$ est unique et que le nombre de fois que chaque p_i apparaît dans l'écriture est aussi unique.

(2) En regroupant les nombres premiers identiques, et en les réordonnant, n s'écrit de manière unique

$$n = p_1^{n_1} \dots p_k^{n_k},$$

où $n_1, \dots, n_k$ sont des nombres entiers positifs et $p_1, \dots, p_k$ sont des nombres premiers distincts.

Avant de montrer le théorème, nous avons besoin d'une variante du théorème de Gauss.

Lemme 4.18 (Lemme d'Euclide)**.** *Soit p un nombre premier, et soit $a, b \in \mathbb{Z}$. Si $p|ab$, alors $p|a$ ou $p|b$ (notons que ce n'est pas un « ou » exclusif, c.-à-d. que p peut diviser a et b).*

Démonstration. Comme p est premier, ses diviseurs sont 1 et p. Il y a deux cas possibles : soit $p|a$ et alors la preuve est terminée, ou bien $p \nmid a$. Dans ce dernier cas, on a forcément $pgcd(a, p) = 1$ et alors p et a sont premiers entre eux, et donc par le théorème de Gauss, $p|b$. Donc $p|a$ ou $p|b$. ■

Démonstration du théorème 4.17. Il faut montrer l'existence, puis l'unicité d'une telle écriture.

Existence. Nous raisonnons par récurrence (deuxième forme) sur $n \geq 2$. Si $n = 2$, il suffit de constater que 2 est premier.

Supposons que l'existence de cette écriture soit vraie pour tout $2 \leq l \leq n$. Montrons qu'alors une telle écriture existe pour $n + 1$. Si $n + 1$ est premier, on a gagné. Sinon, nous avons $n + 1 = ab$, avec $2 \leq a, b \leq n$. Nous appliquons alors l'hypothèse de récurrence à a et à b : ils admettent une factorisation en nombres premiers. En mettant bout à bout ces deux factorisations, nous en obtenons une pour $n + 1 = ab$. Ceci achève la preuve de l'existence.

Unicité. Nous procédons à nouveau par récurrence sur n. Si $n = 2$, il n'y a rien à prouver. Supposons l'unicité prouvée pour les nombres de 2 à n, et prouvons-la pour $n+1$. Écrivons que $n+1$ a deux factorisations :

$$p_1 p_2 \dots p_l = n + 1 = q_1 q_2 \dots q_k,$$

où les $p_1, \dots, p_l$ et $q_1, \dots, q_k$ sont des nombres premiers (on ne peut pas avoir l ou k égal à 0, sinon $n+1 = 1$ et $n = 0$, contrairement à l'hypothèse $n \geq 2$). Comme p_1 divise $n+1 = q_1 q_2 \dots q_k$, alors par le lemme d'Euclide, $p_1 | q_1$ ou $p_1 | q_2$ ou $\dots$ ou $p_1 | q_k$. En d'autres termes, comme les q_j sont premiers, il existe $1 \leq i \leq k$ tel que p_1 divise q_i. Alors $p_1 = q_i$. Quitte à réordonner les q_j on peut supposer $p_1 = q_1$. Dans ce cas, on a

$$p_2 \dots p_l = q_2 \dots q_k < n$$

et donc $l = k$ et, après avoir éventuellement réordonné, $p_j = q_j$ par récurrence. Ceci termine la preuve. ■

Exemple. On a : $6 | 1620$ car $6 = 2 \cdot 3$ et $1620 = 2^2 \cdot 3^4 \cdot 5$.

Corollaire 4.19. *Soit n, m deux entiers ≥ 2 admettant les factorisations en nombres premiers*

$$n = p_1^{n_1} \dots p_k^{n_k} \quad \text{et} \quad m = p_1^{m_1} \dots p_k^{m_k}$$

où $p_1, \dots, p_k$ sont des nombres premiers distincts.

Alors $m | n$ si et seulement si : $\forall 1 \leq i \leq k,\ m_i \leq n_i$.

Démonstration. Voir exercice 33. ■

4.3 Calcul modulaire sur les entiers

Pour bien saisir l'objet de la dernière partie de ce cours, prêtons-nous à un jeu : nous sommes mardi. Quel jour serons-nous dans 2583 jours ? Un moyen de répondre joliment à cette question est de numéroter les jours : mardi = 1, mercredi = 2, etc. Maintenant, on additionne 2583 jours à 1 puisque mardi = 1, ce qui donne 2584 jours. Comme il n'y a que 7 jours dans la semaine, on peut retrancher autant de fois des multiples de 7 que l'on veut, ou autrement dit, on peut retrancher autant de semaines que l'on veut. Par la division euclidienne, on a donc que $2584 = 369 \times 7 + 1$, d'où

$$2584 \text{ "=" } 1 \text{ "=" mardi !}$$

Nous aurons donc passé 369 semaines complètes et serons de retour au jour 1. On dit ici que l'on calcule «modulo 7».

Le calcul modulaire et les *entiers modulaires* sont l'objet d'étude de cette section. Cette idée d'entier modulaire provient essentiellement de l'étude du reste de la division euclidienne que nous avons étudiée au début de ce chapitre. Comme le problème ci-dessus pourrait sembler plutôt simple à résoudre, en voici un autre, un peu plus complexe, d'origine chinoise et datant de l'Antiquité.

Probème 1. *« Mon panier peut contenir au plus cent oeufs. Si je le vide par trois oeufs à la fois, il en reste un, si je le vide par huit oeufs à la fois, il en reste deux, et si je le vide par sept oeufs à la fois, il en reste cinq. Combien ai-je d'oeufs ? » (voir [Damphousse 2002])*

Afin de pouvoir résoudre ce type de problème, nous devons introduire dans cette section les outils nécessaires pour manipuler les entiers modulaires. Nous définissons donc dans la suite une addition, une multiplication, ainsi que d'autres propriétés de ces entiers nous permettant de calculer sur cet ensemble. Ces notions et techniques qui sont présentées ont originellement été introduites par Gauss vers 1801 à l'âge de 21 ans. Finalement, nous allons résoudre le problème 1 en le réécrivant en termes mathématiques grâce aux entiers modulaires. Mais pour ce faire, commençons tout d'abord par définir ce nouvel ensemble des entiers modulaires.

4.3.1 Entiers modulaires

Définition. Soit $n \in \mathbb{N}$. La relation de *congruence modulo* n est une relation sur $\mathbb{Z}$ définie comme suit : deux entiers a et b sont *congrus modulo* n si n divise $a - b$. On écrit : $a \equiv b \pmod{n}$.

Remarque. Pour s'entraîner à jouer avec les mots mathématiques, réécrivons cette définition de plusieurs manières possibles. Les énoncés suivants sont équivalents :

1. $a \equiv b \pmod{n}$;
2. n divise $a - b$;
3. n divise $b - a$;
4. $a - b \in n\mathbb{Z}$ (c.-à-d. $a - b$ est un multiple de n) ;
5. $a = b + kn$, pour un entier k.

Exemple. $8 \equiv 29 \pmod{7}$, car 7 divise $8 - 29 = -21 = -3 \cdot 7$, ou encore, car $8 = 29 + (-3) \cdot 7$.

Théorème 4.20. *Soit $n \in N^*$. La relation de congruence modulo n est une relation d'équivalence, c'est-à-dire que pour tout entier $a, b, c \in \mathbb{Z}$ on a :*

1. $a \equiv a \pmod{n}$ *(réflexif) ;*
2. $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$ *(symétrique) ;*
3. *si* $a \equiv b \pmod{n}$ *et* $b \equiv c \pmod{n}$ *alors* $a \equiv c \pmod{n}$ *(transitif).*

Démonstration. Soit $a, b, c \in \mathbb{Z}$. La relation de congruence modulo n est

- Réflexive : n divise $0 = a - a$ donc $a \equiv a \pmod{n}$;
- Symétrique : $a \equiv b \pmod{n} \Rightarrow n|a-b \Rightarrow n|b-a \Rightarrow b \equiv a \pmod{n}$;
- Transitive : Si $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$ alors n divise $a-b$ et n divise $b-c$. Donc n divise $a-b+b-c = a-c$. D'où $a \equiv c \pmod{n}$.

La notion de relation d'équivalence permet de regrouper les éléments d'un ensemble qui sont similaires par une certaine propriété. Ces éléments forment alors un sous-ensemble qu'on appelle *classe d'équivalence* (voir Annexe C pour plus d'informations). Dans notre cas, cette propriété est celle de congruence modulo n et alors tous les éléments qui sont congrus modulo n forment la *classe de congruence modulo n*.

Classes de congruence

Définition. La *classe de congruence modulo n de $a \in \mathbb{Z}$* est l'ensemble

$$[a]_{\equiv} = \{b \in \mathbb{Z} \,|\, b \equiv a \pmod{n}\}.$$

Exemple. Prenons $n = 3$ et déterminons la classe $[0]_{\equiv}$ de 0. Par définition,

$$[0]_{\equiv} = \{a \in \mathbb{Z} \,|\, a \equiv 0 \pmod{3}\} = \{a \in \mathbb{Z} \,|\, 3 \text{ divise } a\} = 3\mathbb{Z}.$$

Ainsi la classe de 0 consiste en tous les multiples de 3. De manière analogue,

$$[1]_{\equiv} = \{a \in \mathbb{Z} \,|\, a \equiv 1 \pmod{3}\} = \{a \in \mathbb{Z} \,|\, 3 \text{ divise } a-1\} = \{a \in \mathbb{Z} \,|\, a = 1+3k,\ k \in \mathbb{Z}\} = 1+3\mathbb{Z}.$$

Donc la classe de 1 est l'ensemble $1 + 3\mathbb{Z}$ des nombres égaux à 1 plus un multiple de 3. De même, la classe de 2 est

$$[2]_{\equiv} = \{a \in \mathbb{Z} \,|\, a \equiv 2 \pmod{3}\} = \{a \in \mathbb{Z} \,|\, a = 2+3k,\ k \in \mathbb{Z}\} = 2+3\mathbb{Z}.$$

D'où la classe de 2 est l'ensemble $2 + 3\mathbb{Z}$ des nombres égaux à 2 plus un multiple de 3.

On peut observer que pour tout $a \in \mathbb{Z}$, le reste de la division euclidienne de $|a|$ par 3 sera 0, 1 ou 2. Il n'y a donc pas d'autres classes, car tout entier est soit dans $3\mathbb{Z}$, soit dans $1 + 3\mathbb{Z}$ ou soit dans $2 + 3\mathbb{Z}$. Ainsi, il y a 3 classes de congruence modulo 3.

Notation. Comme deux entiers a et b sont dans la même classe de congruence modulo n si et seulement si $b - a \in n\mathbb{Z}$, on pose les notations suivantes :

1. Soit $a \in \mathbb{Z}$, on note $a + n\mathbb{Z}$ la classe de congruence modulo n de a.
   Ainsi, on a bien que $b \in a + n\mathbb{Z} \Leftrightarrow b = a + nk,\ k \in \mathbb{Z} \Leftrightarrow b - a = nk,\ k \in \mathbb{Z} \Leftrightarrow b - a \in n\mathbb{Z}$
2. Pour simplifier les notations, on note parfois $\overline{a} = a + n\mathbb{Z}$.

Définition. On note $\mathbb{Z}/n\mathbb{Z}$ l'*ensemble des classes de congruence modulo n*. Un élément sera appelé *entier modulo n* (ou plus généralement *entier modulaire*).

Remarque. Il faut bien s'habituer à voir que $\overline{a} = a + n\mathbb{Z}$ est à la fois un sous-ensemble de $\mathbb{Z}$ et un élément de $\mathbb{Z}/n\mathbb{Z}$. Autrement dit, il faut bien comprendre que l'on peut écrire :

$$a + n\mathbb{Z} = \overline{a} \subseteq \mathbb{Z} \quad \text{et} \quad \overline{a} = a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}.$$

En particulier, on en déduit les propriétés suivantes :

Proposition 4.21. *Soit $n \in \mathbb{N}^*$ et $x, y \in \mathbb{Z}$, alors les énoncés suivants sont équivalents :*

1. $x \equiv y \pmod{n}$;
2. $\overline{x} = \overline{y}$ *dans* $\mathbb{Z}/n\mathbb{Z}$;
3. $x \in y + n\mathbb{Z}$;
4. $y \in \overline{x}$;
5. $x + n\mathbb{Z} = y + n\mathbb{Z}$.

Démonstration. Voir exercice 35. ∎

Il est difficile d'appréhender l'ensemble $\mathbb{Z}/n\mathbb{Z}$ tel que décrit précédemment. Nous aimerions donc obtenir une meilleure description de ses éléments que sont les classes de congruence. En particulier, nous aimerions montrer qu'il y a un nombre fini de classes de congruence modulo n, c'est-à-dire que l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$ est fini. Pour ce faire, donnons un système de représentant de classes de congruence.

Système de représentants des classes de congruence

Théorème 4.22. *Soit $n \in \mathbb{N}^*$, alors*

1. *l'ensemble $\{0, 1, 2, \ldots, n-1\}$ est un système de représentants des classes de congruences modulo n ; autrement dit*
$$\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\};$$
2. *l'ensemble des classes de congruence modulo n est de cardinal n : $|\mathbb{Z}/n\mathbb{Z}| = n$.*

Démonstration. Il suffit de montrer que pour toute classe de congruence $\overline{b}$, il existe un unique $a \in \{0, 1, 2, \ldots, n-1\}$ tel que $\overline{a} = \overline{b}$.

Existence. Soit $b \in \mathbb{Z}$. Alors la division euclidienne de $|b|$ par n nous donne un reste $a \in \{0, 1, \ldots, n-1\}$. Donc $|b| = qn + a$. Si $b \geq 0$, alors selon la proposition 4.21

$$b = |b| = qn + a \Rightarrow b \in a + n\mathbb{Z} \Rightarrow \overline{b} = \overline{a}.$$

Si $b < 0$, alors $b = (-q) \cdot n + (-a) = (-q-1) \cdot n + (n-a)$. On a deux cas :

Soit $a = 0$ et donc comme ci-dessus $\overline{b} = \overline{0}$;

Soit $0 < a < n$ et alors $n - a \in \{1, 2, 3, \ldots, n-1\}$ et comme auparavant $\overline{n-a} = \overline{b}$.

Unicité. Soit $a, a' \in \{0, \ldots, n-1\}$ tel que $\overline{a} = \overline{a'}$. Alors par la proposition 4.21, $a' = a + nk$ pour $k \in \mathbb{Z}$ car $a' \in a + n\mathbb{Z}$. Supposons que $a' \geq a$. On a alors $0 \leq a' \leq n-1$ et $-n+1 \leq -a \leq 0$, d'où l'inégalité $0 \leq a' - a \leq n-1$. Mais comme $a' - a = nk$, alors $0 \leq nk \leq n-1$ et donc $k = 0$. D'où $a = a'$ et il y a bien unicité. ■

Toujours dans l'idée de résoudre notre problème du nombre d'oeufs dans le panier, nous devons maintenant nous doter de règles de calcul sur les entiers modulaires. En effet, tout comme sur les entiers, nous voudrions montrer que des opérations d'addition et de multiplication sont aussi bien définies sur les classes de congruence. Comme nous avons maintenant un système de représentants simplifiant la définition de ces éléments de $\mathbb{Z}/n\mathbb{Z}$, voyons comment l'exploiter afin de définir ces deux opérations.

4.3.2 Addition et multiplication modulaire

La plus grande découverte de Gauss a été d'introduire une addition et une multiplication sur l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$, pour $n \in \mathbb{N}^*$, c'est-à-dire de *bien définir* deux opérations

$$\begin{aligned} \overline{a} + \overline{b} &:= \overline{a+b} \in \mathbb{Z}/n\mathbb{Z} \\ \overline{a} \cdot \overline{b} &:= \overline{a \cdot b} \in \mathbb{Z}/n\mathbb{Z} \end{aligned}$$

Remarque. **Attention !** Le premier «+» opère dans $\mathbb{Z}/n\mathbb{Z}$ alors que le deuxième opère dans $\mathbb{Z}$, puis le résultat est envoyé dans $\mathbb{Z}/n\mathbb{Z}$. La même remarque s'applique aux deux multiplications

Il faut donc montrer que les opérations ci-dessus existent bel et bien, en d'autres termes, qu'elles ne dépendent pas du choix d'un représentant dans une classe d'équivalence. Plus précisément, il faut montrer que, quels que soient les représentants $\alpha \in a + n\mathbb{Z}$ et $\beta \in b + n\mathbb{Z}$, on a $(a+b) + n\mathbb{Z} = (\alpha + \beta) + n\mathbb{Z}$ et $a \cdot b + n\mathbb{Z} = \alpha \cdot \beta + n\mathbb{Z}$. Pour cela, et en vertu de la proposition 4.21, il suffit de montrer que :

(1) $\alpha + \beta \in (a+b) + n\mathbb{Z}$

(2) $\alpha \cdot \beta \in (a \cdot b) + n\mathbb{Z}$.

Démonstration. (1) Comme $\alpha \in a + n\mathbb{Z}$ et $\beta \in b + n\mathbb{Z}$, alors il existe $k, l \in \mathbb{Z}$ tel que $\alpha = a + kn$ et $\beta = b + ln$. D'où

$$\alpha + \beta = (a + kn) + (b + ln) = (a+b) + n(k+l) \in (a+b) + n\mathbb{Z}.$$

(2) Comme $\alpha \in a + n\mathbb{Z}$ et $\beta \in b + n\mathbb{Z}$, alors il existe $k, l \in \mathbb{Z}$ tel que $\alpha = a + kn$ et $\beta = b + ln$. D'où

$$\alpha \cdot \beta = (a + kn) \cdot (b + ln) = a \cdot b + n(kb + la + nkl) \in (a \cdot b) + n\mathbb{Z}.$$

■

Remarque. (a) Autrement dit, comme

$$\overline{a+b} = \overline{a} + \overline{b} \quad \text{et} \quad \overline{ab} = \overline{a} \cdot \overline{b}$$

on a aussi

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z} \quad \text{et} \quad (a + n\mathbb{Z})(b + n\mathbb{Z}) = ab + n\mathbb{Z}.$$

(b) Le fait que ces opérations soient bien définies veut aussi dire que si $a, a', b, b' \in \mathbb{Z}$ tel que $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$ alors

$$a + b \equiv a' + b' \pmod{n} \quad \text{et} \quad a \cdot b \equiv a' \cdot b' \pmod{n}.$$

Voici maintenant quelques propriétés des opérations d'addition et de multiplication définies ci-haut. On remarque que d'après ces propriétés, additionner ou multiplier dans $\mathbb{Z}/n\mathbb{Z}$ est tout aussi naturel que d'additionner ou multiplier dans $\mathbb{Z}$! En effet, soit $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/n\mathbb{Z}$ alors

1. $\overline{a} + \overline{b} = \overline{b} + \overline{a}$ et $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$ (commutativité) ;
2. $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$ et $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$ (associativité) ;
3. $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$ (distributivité) ;
4. $-\overline{a} = \overline{-a}$ et $-\overline{a} + \overline{a} = \overline{0}$ (opposé) ;
5. $\overline{a} + \overline{0} = \overline{a}$; $\overline{a} \cdot \overline{1} = \overline{a}$; et $\overline{a} \cdot \overline{0} = \overline{0}$ (éléments neutres).

Attention. Pour une équation dans $\mathbb{Z}$: $ax = 0$ avec $a \neq 0$, on obtient que $x = 0$. Ici par contre, ce n'est pas vrai ; par exemple dans $\mathbb{Z}/4\mathbb{Z}$, l'équation $\overline{2}\,x = \overline{0}$ admet aussi la solution $x = \overline{2}$, car $\overline{2} \cdot \overline{2} = \overline{4} = \overline{0}$. Toutefois, dans $\mathbb{Z}/5\mathbb{Z}$ par exemple, cette même équation impliquerait nécessairement que $x = \overline{0}$ comme le montre la proposition suivante.

Proposition 4.23. *Soit p un nombre premier, alors $\overline{x} \cdot \overline{y} = \overline{0}$ dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $\overline{x} = \overline{0}$ ou $\overline{y} = \overline{0}$.*

Démonstration. Supposons $\overline{x} \neq \overline{0}$, alors on peut prendre $0 < x < p$. Donc $\operatorname{pgcd}(x, p) = 1$. Par le théorème de Bézout, on peut écrire $kx + lp = 1$ avec $k, l \in \mathbb{Z}$. Donc $\overline{k}\,\overline{x} = \overline{1}$. En multipliant par $\overline{y}$ on obtient :

$$\overline{k} \cdot \overline{x} \cdot \overline{y} = \overline{1} \cdot \overline{y} = \overline{y} \Rightarrow \overline{k} \cdot \overline{x} \cdot \overline{y} = \overline{k} \cdot \overline{0} = \overline{y} \Rightarrow \overline{y} = \overline{0}.$$

La réciproque est triviale. ■

4.3.3 Éléments inversibles

Tout entier est au moins divisible par 1 et par lui-même. Qu'en est-il des entiers modulaires dans $\mathbb{Z}/n\mathbb{Z}$? Les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont en quelque sorte l'analogue des entiers qui sont divisibles. Par contre, nous verrons que cette notion d'inversibilité ne s'applique pas à tous les éléments de $\mathbb{Z}/n\mathbb{Z}$!

Définition. Soit $n \in \mathbb{N}^*$. On dit que $\overline{x}$ est *inversible dans* $\mathbb{Z}/n\mathbb{Z}$ s'il existe $\overline{y} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{x} \cdot \overline{y} = \overline{1}$. On dit alors que $\overline{y}$ *est 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 $\mathbb{Z}/n\mathbb{Z}$.

Exemples. (a) $\overline{1} \in (\mathbb{Z}/n\mathbb{Z})^\times$, son inverse est lui-même. En effet, $\overline{1} \cdot \overline{1} = \overline{1}$

(b) Dans $\mathbb{Z}/4\mathbb{Z}$, les inversibles sont : $\overline{1}^{-1} = \overline{1}$ et $\overline{3}^{-1} = \overline{3}$ car $\overline{3} \cdot \overline{3} = \overline{9} = \overline{1}$

(c) Dans $\mathbb{Z}/11\mathbb{Z}$, les inversibles sont : $\overline{1}^{-1} = \overline{1}$, $\overline{2}^{-1} = \overline{6}$, $\overline{3}^{-1} = \overline{4}$, $\overline{5}^{-1} = \overline{9}$, $\overline{7}^{-1} = \overline{8}$ et $\overline{10}^{-1} = \overline{10}$. On remarque que seuls $\overline{1}$ et $\overline{10}$ sont leurs propres inverses (de plus, $\overline{6}^{-1} = \overline{2}$, $\overline{4}^{-1} = \overline{3}$, etc.).

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 4.24. *Soit $n \in \mathbb{N}^*$ et $x \in \mathbb{Z}$, alors $\overline{x} \in (\mathbb{Z}/n\mathbb{Z})^\times$ si et seulement si* $\text{pgcd}(x, n) = 1$.

Démonstration. Montrons d'abord l'implication directe :

$$\begin{aligned} \overline{x} \in (\mathbb{Z}/n\mathbb{Z})^\times &\Rightarrow \exists y \in \mathbb{Z},\ \overline{x} \cdot \overline{y} = \overline{1} \\ &\Rightarrow xy \in 1 + n\mathbb{Z}, \quad \text{(proposition 4.21)} \\ &\Rightarrow \exists k \in \mathbb{Z},\ xy + kn = 1 \\ &\Rightarrow \text{pgcd}(x, n) = 1, \quad \text{(théorème de Bézout).} \end{aligned}$$

La réciproque revient à emprunter le chemin inverse des implications ci-dessus. ■

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 4.25. *Soit p un nombre premier, alors tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible. De plus, $\overline{1}$ et $\overline{p-1}$ sont les seuls éléments dans $\mathbb{Z}/p\mathbb{Z}$ qui sont leurs propres inverses. En particulier, $\overline{1}^{-1} = \overline{1}$ et $\overline{p-1}^{-1} = \overline{p-1} = -\overline{1}$.*

Démonstration. On prend $x \in \mathbb{Z}/p\mathbb{Z}$ tel que $0 < x \leq p - 1$. Donc $\overline{x} \in (\mathbb{Z}/p\mathbb{Z})^\times$ si et seulement si $pgcd(x, p) = 1$. Or, comme p est premier et $0 < x \leq p - 1$, ceci est toujours vrai.

De plus, si $1 \leq x \leq p-1$ tel que $\overline{x}$ est son propre inverse, alors $\overline{x}^{\,2} = \overline{1}$. C'est-à-dire que x est solution de l'équation

$$\overline{x}^{\,2} - \overline{1} = (\overline{x} - \overline{1})(\overline{x} + \overline{1}) = \overline{0}$$

dans $\mathbb{Z}/p\mathbb{Z}$. Comme p est premier, alors $\overline{x} - \overline{1} = \overline{0}$ ou $\overline{x} + \overline{1} = \overline{0}$ par la proposition 4.23. D'où $\overline{x} = \overline{1}$ 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 4.26 (Wilson)**.** *Soit $n \in \mathbb{N}$, $n \geq 2$, alors n est premier si et seulement si*

$$(n-1)! \equiv -1 \pmod{n}.$$

En d'autres termes, n est premier si et seulement si n divise $(n-1)!+1$.

Démonstration. Montrons d'abord la réciproque : si $(n-1)! \equiv -1 \pmod{n}$ alors n divise $(n-1)!+1$. Donc, si a est un diviseur de n différent de n, donc $1 \leq a \leq n-1$, alors a divise aussi $(n-1)!+1$. D'autre part, comme $1 \leq a \leq n-1$, alors a apparaît dans le produit $(n-1)!$, et donc a divise $(n-1)!$. Puisque a divise $(n-1)!+1$ et $(n-1)!$, alors a divise 1. Ceci implique que $a = 1$ et on en déduit que les seuls diviseurs de n sont n et 1 donc n est premier.

Montrons le sens direct. Si n est premier, alors en vertu de la proposition 4.24, $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ dès que n ne divise pas a. En particulier, $\overline{1}, \overline{2}, \overline{3}, \ldots, \overline{n-1}$ sont inversibles dans $\mathbb{Z}/n\mathbb{Z}$. Par le biais de la proposition 4.24, on sait que seuls $\overline{1}$ et $\overline{p-1}$ sont leurs propres inverses dans $\mathbb{Z}/n\mathbb{Z}$. Les autres éléments $\overline{2}, \overline{3}, \ldots, \overline{n-2}$ peuvent être regroupés par paires $(\overline{a}, \overline{a}^{\,-1})$ d'inversibles. Il s'ensuit que dans le produit $\overline{2} \cdot \overline{3} \cdot \ldots \cdot \overline{n-2}$, il apparaît chaque élément et son inverse. Donc ce produit doit être $\overline{1}$, d'où

$$\overline{(n-1)!} = \overline{1} \cdot (\overline{2} \cdot \overline{3} \cdot \ldots \cdot \overline{n-2}) \cdot \overline{n-1} = \overline{1} \cdot \overline{n-1} = \overline{n-1} = -\overline{1}.$$

Donc $(n-1)! \equiv -1 \pmod{n}$. ■

4.3.4 Théorème des restes chinois

Nous avons maintenant tous les outils en main afin de déduire combien d'oeufs se retrouvent dans le panier du problème 1. 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 4.27. *Soit $n, m \in \mathbb{N}^*$ premiers entre eux. Pour $k, l \in \mathbb{Z}$, il existe un unique entier $0 \leq x \leq nm - 1$ tel que*

$$x \equiv \begin{cases} k \pmod{n} \\ l \pmod{m} \end{cases}$$

Démonstration. Comme n et m sont premiers entre eux, il existe, par le théorème de Bézout, α, β tel que $\alpha n + \beta m = 1$. Donc $\beta m \equiv 1 \pmod{n}$ et $\alpha n \equiv 1 \pmod{m}$. Posons $x = \alpha nl + \beta mk$. Alors $x \equiv \beta mk \equiv k \pmod{n}$ et $x \equiv \alpha nl \equiv l \pmod{m}$. L'existence de x est donc prouvée.

L'unicité est facile à prouver : si x, x' sont deux solutions, alors $x - x'$ est divisible à la fois par n et par m. Donc $x - x'$ est divisible par tous les diviseurs de n et tous les diviseurs de m. Ainsi $x - x'$ est divisible par nm, puisque n et m sont premiers entre eux (voir l'exercice 22). Donc $x \equiv x' \pmod{nm}$. Comme $x, x' \in \{0, 1, 2, \ldots, nm - 1\}$ sont des représentants des classes de congruences, on doit avoir $x = x'$ en vertu du théorème 4.22. ■

Exemple. Le problème 1 se traduit par la résolution du système d'équations suivant :

$$x \leq 100 \quad \text{et} \quad x \equiv \begin{cases} 1 \pmod{3} \\ 2 \pmod{8} \\ 5 \pmod{7} \end{cases}$$

où x est le nombre d'oeufs. On peut alors écrire $x = 3k + 1$ car $x \equiv 1 \pmod{3}$. Donc dans $\mathbb{Z}/8\mathbb{Z}$ on a $\overline{x} = \overline{3} \cdot \overline{k} + \overline{1} = \overline{2}$, c'est-à-dire que $\overline{3} \cdot \overline{k} = \overline{1}$. En multipliant cette expression par $\overline{3}$ qui est l'inverse de $\overline{3}$ dans $\mathbb{Z}/8\mathbb{Z}$ on obtient $\overline{k} = \overline{3}$. Donc $k = 8l + 3$ avec $l \in \mathbb{Z}$, d'où $x = 24l + 10$.

Finalement, puisque $x \equiv 5 \pmod{7}$ on a $\overline{x} = \overline{24} \cdot \overline{l} + \overline{10} = \overline{5}$ dans $\mathbb{Z}/7\mathbb{Z}$, c'est-à-dire $\overline{3} \cdot \overline{l} + \overline{3} = \overline{5}$. Donc $\overline{3} \cdot \overline{l} = \overline{2}$. Ou encore, en multipliant par $\overline{5}$ qui est l'inverse de $\overline{3}$ dans $\mathbb{Z}/7\mathbb{Z}$, on obtient $\overline{l} = \overline{10} = \overline{3}$. Donc $l = 7m + 3$ et $x = 168m + 82$. Puisque $x \leq 100$, la seule possibilité est $m = 0$ et $x = 82$.

Il y a donc 82 oeufs dans ce panier.

4.3.5 Petit théorème de Fermat

Nous terminons maintenant avec un dernier résultat d'arithmétique modulaire formulé en 1640 par Pierre de Fermat (1601-1665) dans une de ses lettres. Contrairement à ce dernier, nous en donnerons toutefois une démonstration.

Théorème 4.28 (petit théorème de Fermat)**.** *Si a n'est pas divisible par un nombre premier p alors $a^{p-1} \equiv 1 \pmod{p}$.*

Démonstration. Tout d'abord, on a que p divise toujours $a^p - a$ (voir exercice 52). Ainsi, p divise le produit $a(a^{p-1} - 1)$. Comme a et p sont premiers entre eux, p divise $a^{p-1} - 1$ en vertu du lemme de Gauss. D'où $a^{p-1} - 1 \equiv 0 \pmod{p}$. ■

4.4 Système de cryptographie RSA (*)

Pour utiliser le système de cryptographie à clé publique RSA [1] datant de 1977, on doit pouvoir calculer rapidement de grandes puissances de grands entiers, modulo un grand entier. Par « grand », on veut dire ici des entiers d'une centaine de décimales (ou plus). Heureusement, ceci est rendu possible par la méthode suivante. Pour calculer de grandes puissances modulo n, on procède comme suit. Puisque les règles de calculs pour les exposants sont aussi valables modulo n, On a les identités

$$a^{2k} \equiv (a^2)^k \pmod{n}, \qquad \text{et} \qquad a^{2k+1} \equiv (a^2)^k \cdot a \pmod{n}. \tag{4.1}$$

En cours de calcul, on remplace tout résultat intermédiaire par son reste modulo n. Illustrons ceci avec le calcul de 2^{1024} modulo 23. On a

$$2^{1024} = (2^2)^{512} = (4^2)^{256} = (16^2)^{128},$$

et donc

$$2^{1024} \equiv 3^{128} \pmod{23},$$

puisque $16^2 = 256$ et $256 \equiv 3 \pmod{23}$. On peut continuer notre calcul en remarquant que

$$3^{128} = (3^2)^{64} = (9^2)^{32},$$

et, comme $81 \equiv 12 \pmod{23}$, on a maintenant

$$2^{1024} \equiv 12^{32} \pmod{23}.$$

Le reste du calcul donne

$$\begin{aligned} 2^{1024} &\equiv (12^2)^{16} \pmod{23} \\ &\equiv (6^2)^8 \pmod{23} \\ &\equiv (13^2)^4 \pmod{23} \\ &\equiv (8^2)^2 \pmod{23} \\ &\equiv 18^2 \pmod{23} \\ &\equiv 2 \pmod{23} \end{aligned}$$

On observe qu'on n'a jamais eu à explicitement développer 2^{1024}, qui est égal au nombre astronomique :

179769313486231590772930519078902473361797697894230657273430081157732
675805500963132708477322407536021120113879871393357658789768814416622
492847430639474124377767893424865485276302219601246094119453082952085
005768838150682342462881473913110540827237163350510684586298239947245
938479716304835356329624224137216

1. Un acronyme des initiales des noms de famille de ses concepteurs : Ron Rivest, Adi Shamir et Leonard Adleman.

La prochaine étape est le théorème ci-dessous, dû à Leonhard Euler (1707-1783), qui généralise le petit théorème de Fermat. Avant de pouvoir le formuler, on a besoin de la définition de la **fonction indicatrice d'Euler**. Pour un entier n, on pose

$$\varphi(n) := \Big|\{k \mid 1 \leq k \leq n-1, \text{ et } \operatorname{pgcd}(n,k) = 1\}\Big|.$$

C'est le nombre d'entiers, entre 1 et $n-1$ qui sont **relativement premiers**[2] à n. On a les valeurs suivantes, accompagnées de la liste des entiers qui sont comptés par $\varphi(n)$.

$$\begin{array}{llllll} \varphi(2)=1, & \{1\}; & \varphi(3)=2, & \{1,2\}; & \varphi(4)=2, & \{1,3\}; \\ \varphi(5)=4, & \{1,2,3,4\}; & \varphi(6)=2, & \{1,5\}; & \varphi(7)=6, & \{1,2,3,4,5,6\}; \\ \varphi(8)=4, & \{1,3,5,7\}; & \varphi(9)=6, & \{1,2,4,5,7,8\}; & \varphi(10)=4, & \{1,3,7,9\}. \end{array}$$

Un fait marquant est que d'une part le calcul de $\varphi(n)$ est très difficile si on ne connaît pas la décomposition de n en facteurs premiers, et que d'autre part il est très facile si c'est le cas. Le système RSA est basé sur cette double réalité. En fait, on a la formule suivante. Sachant que p_1, p_2, … , p_k sont tous les nombres premiers distincts qui divise n, alors

$$\varphi(n) = n\,(1-1/p_1)(1-1/p_2)\cdots(1-1/p_k). \tag{4.2}$$

Pour élaborer le système RSA, nous n'aurons besoin que du cas où est le produit de seulement deux nombres premiers distincts, c.-à-d. que $n = p\,q$, et alors

$$\varphi(n) = (p-1)\,(q-1).$$

Le théorème central ici est le suivant. Il permet de déterminer quand deux puissances d'un même nombre sont équivalentes modulo n.

Théorème 4.29 (Euler-Fermat)**.** *Si a est relativement premier à n, alors*

$$a^k \equiv a^\ell \pmod{n}$$

exactement lorsque

$$k \equiv \ell \pmod{\varphi(n)}.$$

Dans le cas qui nous concerne, l'entier n prend la forme très particulière $n = p\,q$, avec p et q deux très grands nombres premiers distincts (ayant chacun une centaine de chiffres). L'un des exposants est aussi un grand nombre, et il est de la forme $k := e\,f$; tandis que l'autre exposant est tout simplement égal à 1, c.-à-d. que $\ell = 1$. Le théorème devient donc

$$a^{e\cdot f} \equiv a \pmod{n} \tag{4.3}$$

si et seulement si

$$e \cdot f \equiv 1 \pmod{(p-1)\cdot(q-1)}. \tag{4.4}$$

2. Deux entiers a et n sont dit relativement premiers si $\operatorname{pgcd}(a,n) = 1$.

Mise en place du système

Pour mettre en place le système RSA, chaque participant se construit une clé publique (c'est un couple (n, e)) de la façon suivante :

1. Il commence par choisir[3] en secret 2 très grands nombres premiers p et q (avec au moins 100 chiffres chacun), et il calcule $n = p \cdot q$.
2. Il est donc à même de calculer la fonction $\varphi(n) = (p-1)(q-1)$. Il choisit ensuite (au hasard) un entier e, entre 1 et $\varphi(n)$, de façon à ce que cet entier e soit relativement premier à $\varphi(n)$.
3. Il peut alors calculer (en utilisant le théorème 4.14) l'inverse multiplicatif $f = e^{-1}$, de e modulo $\varphi(n)$. C'est une solution de $f\,e + x\,\varphi(n) = 1$.
4. Enfin, le participant rend publique sa clé d'encodage, (n, e), et garde (très) secrète sa clé de décodage f.

En supposant que chaque participant ait réussi à réaliser ces étapes, on publie un annuaire donnant la clé (n, e) de chaque participant. Pour coder un message à l'intention d'un certain participant, on consulte cet annuaire de clés pour obtenir la valeur particulière de n et de e qui lui correspond. L'encodage procède de la manière suivante. On commence par découper le message à envoyer, en morceaux dont la longueur est plus petite que la moitié du nombre de chiffres dans n. On numérise un de ces morceaux en remplaçant chaque lettre par deux chiffres de la façon suivante

$$\texttt{a} \mapsto 10,\ \texttt{b} \mapsto 11, \texttt{c} \mapsto 12, \ldots$$

Par exemple, on a la numérisation

$$\texttt{bonjour} \mapsto 11242319243027.$$

Les morceaux du message sont ainsi devenus de grands entiers modulo n (parce que leur longueur est plus petite que n). L'encodage d'un morceau numérisé a se fait en calculant

$$b := (a^e \bmod n)$$

Pour décoder ce message, on cherche à récupérer a à partir de b. Comme nous allons mieux le voir plus loin, cela est une entreprise très difficile, sauf si l'on connaît f. Dans ce cas, il suffit en effet de calculer

$$\begin{aligned}(b^e \bmod n) &= ((a^e)^f \bmod n)\\ &= a,\end{aligned}$$

étant donné l'équation (4.3). On dé-numérise ensuite a pour récupérer le message envoyé.

La raison pour laquelle un « espion » n'est pas capable de décoder le message en pratique, même en connaissant le couple (n, e), dépend du fait (attention, ce n'est pas un théorème) qu'il est difficile de calculer $\varphi(n)$, et donc de calculer f. Sans connaître f, on ne peut décoder le message. Pour en savoir plus sur la cryptographie, voir les notes disponibles sur la page

3. C'est possible assez efficacement, mais nous ne discuterons pas ici de la façon de le faire.

« bergeron.math.uqam.ca »

dans la section « cours », ou suivre ce lien.

4.5 Exercices du chapitre 4

Arithmétique dans $\mathbb{Z}$

Exercice 1 (A) Écrire la division euclidienne de -514 par 35.

Exercice 2 (A) Montrer que 111 divise 111111.

Indication : $111111 = 111000 + 111$

Exercice 3 (A) Montrer que 572 est divisible par 11.

Indication : $572 = 550 + 22$

Exercice 4 (A) (Démonstration du cours) Vérifier que 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.

Exercice 5 (A) (Démonstration du cours) (Proposition 4.2) Soit n, m, p des entiers non nuls, montrer que

1. $p|n \Rightarrow p|nm$;
2. $p|n$ et $p|m \Rightarrow p|n+m$ et $p|n-m$;
3. Plus généralement : $p|n$ et $p|m \Rightarrow p|an+bm$ pour tous $a, b \in \mathbb{Z}$.

Exercice 6 (A) (Démonstration du cours) (i) Montrer que $I = \{6a + 4b \,|\, a, b \in \mathbb{Z}\}$ est un idéal ; (ii) Si I est un idéal, montrer que $1 \in I \;\Leftrightarrow\; I = \mathbb{Z}$.

Exercice 7 (PPCM- Plus petit commun multiple) Soit n, m deux entiers. Un *multiple commun à n et m* est un entier d (strictement positif) qui est multiple à la fois de n et de m.

1. Montrer qu'il existe un unique plus petit élément qui est un multiple commun à m et n. On l'appelle le *plus petit commun multiple de m et n* et on le note $\text{ppcm}(m, n)$.
2. Montrer que $n\mathbb{Z} \cap m\mathbb{Z} = \text{ppcm}(m, n)\mathbb{Z}$.
3. Montrer que $m|p$ et $n|p \Rightarrow \text{ppcm}(n, m)|p$.
4. Montrer que $\text{ppcm}(m, n)|mn$.

Exercice 8 Montrer que si $a, b \in \mathbb{N}^*$, alors $ab = \text{ppcm}(a, b) \cdot \text{pgcd}(a, b)$.

Exercice 9 (A) (Démonstration du cours) Soit n, m deux entiers non nuls. Montrer que $\text{pgcd}(n, m) = n \;\Leftrightarrow\; n|m$.

Exercice 10 **(Démonstration du cours)** Soit $n \geq m$ deux entiers non nuls et écrivons $n = mq+r$, avec $r, q \in \mathbb{Z}$. Montrer que si $r \neq 0$, on a $\text{pgcd}(n, m) = \text{pgcd}(m, r)$ (on notera que pgcd(0,m)= m).

Exercice 11 (B) Montrer que $\text{pgcd}(da, db) = d \cdot \text{pgcd}(a, b)$, pour tous entiers a, b, d non nuls.

Exercice 12 (A) Pour les ensembles suivants, montrer que I est un idéal et déterminer $n \in \mathbb{N}^*$ tel que $I = n\mathbb{Z}$:
(a) $I = \{52x - 2y \,|\, x, y \in \mathbb{Z}\}$; (b) $I = \{3x + 9y - 15z \,|\, x, y, z \in \mathbb{Z}\}$; (c) $I = \{217l + 34k \,|\, l, k \in \mathbb{Z}\}$;

Réponses : (a) $I = 2\mathbb{Z}$; (b) $I = 3\mathbb{Z}$; (c) $I = \mathbb{Z}$.

Exercice 13 Soit a, b, c des entiers non nuls tels que a et b sont premiers entre eux et $c|a + b$. Montrer que $\text{pgcd}(a, c) = 1 = \text{pgcd}(b, c)$.

Exercice 14 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 15 Soit $a, b \in \mathbb{N}^*$ premiers entre eux tels que $a^2 + a = 7b^3$. Montrer que a divise 7 et résoudre cette équation dans $\mathbb{N}$.

Exercice 16 (B) *(Réciproque du théorème de Gauss)* Soit $a, b \in \mathbb{Z}$ tel que : $\forall c \in \mathbb{Z},\ a|bc \Rightarrow a|c$. Alors a et b sont premiers entre eux.

Exercice 17 (A) (Démonstration du cours) (Théorème 4.14)
Démontrer la réciproque du Théorème 1.13 : Soit $a, b, c \in \mathbb{Z}$ tel que a et b sont premiers entre eux. Soit x_0, y_0 une solution particulière de l'équation $ax + by = c$, c.-à-d. $ax_0 + by_0 = c$. Si pour $k \in \mathbb{Z}$ on a que $x = x_0 + kb$ et $y = y_0 - ka$, alors x et y sont solutions de l'équation $ax + by = c$.

Exercice 18 **(Examen 2010)**
Résoudre l'équation diophantienne $26x + 57y = 1$.

Exercice 19 Résoudre l'équation diophantienne $216x + 92y = 8$.

Exercice 20 (A) **(Examen 2011)**
Résoudre l'équation diophantienne $33x + 91y = 1$.

Réponse : $x = -11 + 91k$ et $y = 4 - 33k$ où $k \in \mathbb{Z}$

Exercice 21 (A) Résoudre les équations diophantiennes linéaires du premier ordre suivantes :
(a) $12378x + 3054y = 6$; (b) $217x + 34y = 2$; (c) $217x + 34y = 3$; (d) $544x - 944y = 160$.

Réponses : (a) $x = 132 + 509k$ et $y = -535 - 2063k$ où $k \in \mathbb{Z}$

(b) $x = -26 + 34k$ et $y = 166 - 217k$ où $k \in \mathbb{Z}$

(c) $x = -39 + 34k$ et $y = 249 - 217k$ où $k \in \mathbb{Z}$

(d) $x = -260 - 59k$ et $y = -150 - 34k$ où $k \in \mathbb{Z}$

Exercice 22 (B) (Examen 2010)
Soit $n \in \mathbb{N}^*$ et soit a et b deux diviseurs de n. Montrer que si a et b sont premiers entre eux, alors le produit ab divise aussi n.

Exercice 23 **(Examen 2011)**
Soient n, m et p des éléments de $\mathbb{N}^*$. On suppose que n et p sont premiers entre eux.

1. Soit d un diviseur de n. Montrer que d et p sont premiers entre eux.
2. Soit d un diviseur de n et mp. Montrer que d divise m.
3. Montrer que $\text{pgcd}(n, mp) = \text{pgcd}(n, m)$.

Exercice 24 (B) (Examen 2011)
Soit $a, b \in \mathbb{Z}$. Montrer que si a et b sont premier entre eux, alors $a + b$ et ab sont aussi premiers entre eux.

Nombres premiers

Exercice 25 Déterminer les couples (p_1, p_2) de nombres premiers tels que $p_1 - p_2 = 15$.

Exercice 26 Montrer que tout nombre *non premier* $n \in \mathbb{N}$ tel que $n \geq 6$ divise $(n-1)!$. On rappelle que $n! = n \cdot (n-1) \ldots 2 \cdot 1$.

Exercice 27 (B) Soit $p, q_1, \ldots, q_l$ des nombres premiers (non nécessairement distincts) tel que p divise le produit $q_1 \ldots q_l$. Montrer par récurrence qu'il existe $1 \leq i \leq l$ tel que $p = q_i$.

Exercice 28 (B) Soit n, m deux entiers ≥ 2 admettant les factorisations en nombres premiers

$$n = p_1^{n_1} \ldots p_k^{n_k} \quad \text{et} \quad m = p_1^{m_1} \ldots p_k^{m_k}$$

où les $p_1, \ldots, p_k$ sont des nombres premiers distincts. Alors montrer que

a) $\text{pgcd}(m, n) = p_1^{r_1} \ldots p_k^{r_k}$ où $r_i = \min(n_i, m_i)$.

b) $\text{ppcm}(m, n) = p_1^{r_1} \ldots p_k^{r_k}$ où $r_i = \max(n_i, m_i)$.

Exercice 29 Montrer que pour tout entier premier p, $\sqrt{p}$ n'est pas rationnel.

Exercice 30 (B) (a) Soit p un nombre premier. Montrer que : $\forall n \in \mathbb{N}^*$, $\text{pgcd}(p, n) = 1$ ou $\text{pgcd}(p, n) = p$.

(b) Soit p, q deux nombres premiers. Montrer que pour tout $n \in \mathbb{N}^*$, $p | q^n \Leftrightarrow p = q$.

Exercice 31 (B) (*Le crible d'Eratosthène*) Soit $n \in \mathbb{N}$, $n \geq 2$. On va donner une méthode pour trouver tous les nombres premiers entre 2 et n. On prend la liste de tous les entiers naturels compris

entre 2 et n et on raye les uns après les autres et de gauche à droite, certains éléments de la liste de la manière suivante : dès que l'on trouve un entier qui n'a pas encore été rayé, on le garde, et on raye tous les autres multiples de celui-ci. Puis on passe à l'entier non rayé suivant à sa droite. On s'arrête quand on ne trouve plus d'entier non rayé.

(a) Montrer que le crible s'arrête au nombre premier juste avant $\sqrt{n}$.

On note E_n l'ensemble de tous les entiers entre 2 et n non rayés.

(b) Montrer que p est un nombre premier entre 2 et n si et seulement si $p \in E_n$.

Exercice 32 (A) Déterminer pour quelles valeurs de $n \in \mathbb{N}$ les nombres suivants sont premiers :
(a) $2n^2 + 7n + 6$; (b) $3n^2 + 8n + 5$.

Réponses : (a) Aucune ; (b) $n = 0$.

Exercice 33 (B) (Démonstration du cours) (Corollaire 4.19) Soit n, m deux entiers ≥ 2 admettant les factorisations en nombres premiers $n = p_1^{n_1} \dots p_k^{n_k}$ et $m = p_1^{m_1} \dots p_k^{m_k}$ où $p_1, \dots, p_k$ sont des nombres premiers distincts. Montrer que $m|n$ si et seulement si : $\forall 1 \leq i \leq k,\ m_i \leq n_i$.

Calcul modulaire sur les entiers

Exercice 34 (A) Etant donné les choix pour $A \in \mathbb{Z}$ et $n \in \mathbb{N}^*$ ci-dessous, écrivez une expression de la forme $A \equiv r \pmod n$ avec $0 \leq r < n$:

(a) $A = 2^7$ et $n = 7$; (b) $A = 231$ et $n = 7$; (c) $A = 27x^5 - 9x^3 + 82$, $x \in \mathbb{Z}$ et $n = 9$.

(d) A est quelconque et n est un nombre premier qui apparaît dans la décomposition de A en nombres premiers.

Réponses : (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 35 (A) (Démonstration du cours) (Proposition 4.21) Soit $n \in \mathbb{N}^*$ et $x, y \in \mathbb{Z}$. Montrer que les énoncés suivants sont équivalents :

1. $x \equiv y \pmod n$;
2. $\overline{x} = \overline{y}$ dans $\mathbb{Z}/n\mathbb{Z}$;
3. $x \in y + n\mathbb{Z}$;
4. $y \in \overline{x}$;
5. $x + n\mathbb{Z} = y + n\mathbb{Z}$.

Exercice 36 Montrer que pour tout $x \in \mathbb{Z}$ on a : $\overline{7x^2 + 123x} = \overline{15x^4 + x^2}$ dans $\mathbb{Z}/3\mathbb{Z}$.

Exercice 37 (B) Soit $n \in \mathbb{N}^*$ et soit $a, b \in \mathbb{Z}$. Montrer que

(a) $\exists k \in \mathbb{Z},\ ka \equiv \text{pgcd}(a, b) \pmod b$; (b) $\exists l \in \mathbb{Z},\ lb \in \text{pgcd}(a, b) + a\mathbb{Z}$.

Exercice 38 (A) Soit $n \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$. Montrer que les propositions suivantes sont équivalentes :

1. $(a + n\mathbb{Z}) \cap (b + n\mathbb{Z}) \neq \emptyset$;
2. $\overline{a} = \overline{b}$ dans $\mathbb{Z}/n\mathbb{Z}$;
3. $a \equiv b \pmod{n}$.

Exercice 39 (B) Soit $n \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$ tel que $0 \leq a, b \leq n-1$. Montrer que $a = b$ si et seulement si $(a + n\mathbb{Z}) \cap (b + n\mathbb{Z}) \neq \emptyset$.

Exercice 40 Trouver $(\mathbb{Z}/n\mathbb{Z})^\times$ dans les cas suivants : $n = 5$; $n = 8$; $n = 12$ et $n = 15$.

Exercice 41 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 42 (A) Dans $\mathbb{Z}/11\mathbb{Z}$, montrer que les inversibles sont : $\overline{1}^{-1} = \overline{1}$, $\overline{2}^{-1} = \overline{6}$, $\overline{3}^{-1} = \overline{4}$, $\overline{5}^{-1} = \overline{9}$, $\overline{7}^{-1} = \overline{8}$ et $\overline{10}^{-1} = \overline{10}$.

Exercice 43 Trouver l'inverse de $342 + 997\mathbb{Z}$ dans $\mathbb{Z}/997\mathbb{Z}$.

Exercice 44 (A) **(Examen 2010)** (Suite de l'exercice 18)
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 45 (A) **(Examen 2011)** (Suite de l'exercice 20)
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 46 (B) Quel jour de la semaine serons-nous dans $10^{1000000000}$ jours si nous sommes aujourd'hui lundi ?

Réponse : Nous serons vendredi.

Exercice 47 (B) Soit $n \in \mathbb{N}$, $n \geq 2$. Montrer que les nombres $n! + 2, n! + 3, \ldots, n! + n$ ne sont pas premiers.

Exercice 48 (B) Soit $p \geq 5$ un nombre premier et soit

$$N = \sum_{k=1}^{p-1} \left[\frac{(p-1)!}{k} \right]^2 .$$

(a) Montrer que $N \in \mathbb{N}$ et que dans $\mathbb{Z}/p\mathbb{Z}$

$$\bar{N} = \sum_{k=1}^{p-1} \bar{k}^{-2} \left[\overline{(p-1)!} \right]^2 .$$

(b) Montrer que $N \equiv \sum_{k=1}^{p-1} k^2 \pmod{p}$.

(c) En déduire que p divise N.

Exercice 49 Soit a, b, n des entiers et $d = \text{pgcd}(a, n)$. Montrer que l'équation $ax \equiv b \pmod{n}$ a une solution dans $\mathbb{Z}$ si et seulement si $d|b$. Montrer que dans ce cas, il y a exactement d solutions dans $\mathbb{Z}/n\mathbb{Z}$.

Exercice 50 Déterminer si le système de congruence suivant admet une solution dans $\mathbb{Z}$. Si oui, la calculer. Cette solution est-elle unique ?

$$\begin{cases} 2x & \equiv & 3 \pmod{5} \\ 3x & \equiv & 1 \pmod{4} \end{cases}$$

Exercice 51 (B) Déterminer si les systèmes de congruence suivants admettent des solutions dans $\mathbb{Z}$. S'ils en admettent, les calculer. Ces solutions sont-elles uniques ?

(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) $\begin{cases} x & \equiv & 1 \pmod{2} \\ x & \equiv & 2 \pmod{3} \\ x & \equiv & 3 \pmod{4} \end{cases}$

Réponses : a) $x = 17 + 35\mathbb{Z}$; b) $x = 11 + 30\mathbb{Z}$; c) $x = 11 + 12\mathbb{Z}$;

Exercice 52 (B) (Démonstration du cours) Soit $a \in \mathbb{N}^*$ et p un nombre premier. Montrer par récurrence sur $n \in \mathbb{N}$ que p divise toujours $a^p - a$.
Indication : utiliser la formule du binôme de Newton

Annexe A

Le discours mathématique

Cette annexe est destinée à être discutée lors d'une séance d'exercices en classe. C'est l'annexe à laquelle le lecteur devrait se référer pour clarifier les bases du discours mathématique, et en comprendre la forme.

A.1 Structure du discours mathématique

Plus de 2500 ans d'histoire ont abouti à raffiner grandement le discours mathématique, pour le rendre clair, efficace, et précis. Dans cette annexe, nous allons passer en revue certaines des notions de base qui régissent ce discours, ainsi que celles qui guident le raisonnement mathématique. Nous allons illuster notre propos à l'aide de trois « énigmes » tirées du livre fascinant de R. Smullyan : *Le livre qui rend fou* [Smullyan 1997].

Énigme A.1. *Vous payez 20$ une bouteille de Shiraz. Le vin coûte 19$ de plus que le coût de la bouteille vide. Combien vaut cette bouteille vide ?*

Réponse : La bouteille vaut 50 cents.

Démonstration. (on dit aussi **preuve**) Le vin coûte 19$ de plus que le prix de la bouteille (c'est l'hypothèse de départ). Si on y ajoute le prix de la bouteille, on obtient le prix total 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 cents (dernière implication et conclusion). ■

Ainsi pour répondre correctement à une question (mathématique ou non d'ailleurs), on commence par énoncer clairement la question, puis sa réponse. On rédige ensuite clairement une preuve de ce

que l'on vient d'affirmer. C'est dans cette dernière partie que l'on utilise un **raisonnement logique** (qui dans l'exemple se composé « d'implications »). Plus spécifiquement, les phrases mathématiques sont des **propositions** ou **énoncés**, et le texte est une succession de propositions qui s'enchaînent logiquement pour constituer une **preuve**, ou **argument**.

On présente dans les pages qui suivent différents types d'énoncés mathématiques, ainsi que divers techniques de démonstration. Notre exposé restera assez informel. L'étude formelle du discours mathématique est l'objet du cours de logique.

A.1.1 Énoncé

Une phrase ayant pour but de définir des objets mathématiques, d'en affirmer les propriétés ou de les introduire est un **énoncé**. Il y a les trois types d'énoncés mathématiques typiques suivants.

- Un énoncé qui introduit dans le discours un nouvel objet est une **définition**. Une « bonne » définition est un outil de travail précieux. Elle permet de guider la réflexion.
  Par exemple, on a la définition de **valeur absolue** :
  « Pour x un nombre réel, le plus grand des nombres x et $-x$ est la valeur absolue de x. »
- Un énoncé qui désigne un objet par un symbole est une **notation**. Des notations claires facilitent grandement la compréhension du discours mathématique. Par oppositions, des notations maladroites le rendent facilement totalement incompréhensible.
  Par exemple :
  « On note $|x|$ la valeur absolue du réel x. »
  C'est probablement une mauvaise idée de désigner un nombre complexe par Ξ plutôt que par z. En effet, l'expression
  $$\frac{z}{\bar{z}} \qquad \text{deviendrait} \qquad \frac{\Xi}{\bar{\Xi}} \qquad (\text{hum}\,!).$$
- Un énoncé qui affirme qu'un objet mathématique a une certaine propriété est une **proposition**.

  Par exemple : la valeur absolue d'un nombre réel est toujours positive.

La règle que suit strictement [1] tout discours mathématique est qu'une proposition se doit d'être vraie ou fausse, mais certainement pas les deux à la fois ! Cela élimine d'office du discours mathématique toute assertion dont la vérité est sujette à interprétation, ou au point de vue.

1. Les mathématiciens constructivistes acceptent que la véracité d'un énoncé ne soit pas obligatoirement déterminée « à priori ». Autrement dit, ils acceptent qu'il y ait des énoncés pour lesquels on peut dire : « on ne sait pas encore ». Cela élimine la possibilité d'élaborer des preuves reposant sur le principe du « tiers exclu », et donc des preuves par l'absurde. Cela n'a vraiment d'impact que pour des situations qui font intervenir des ensembles infinis.

A.1.2 Opérations sur les propositions

L'idée exploitée ici est de construire des propositions plus complexes, à partir de propositions plus simples. L'approche est similaire à cele qui consiste à construire des formules complexes à partir de formules simples, en utilisant des opérations comme la somme, le produit, etc.

On a les « opérations » suivantes sur les propositions, qui permettent de construire de nouvelles propositions à partir de propositions données comme P, Q, où R. C'est proposition peuvent être mathématiques ou, pour développer l'intuition, et des énoncés en langage usuel, du genre : « tous les hommes sont mortels ». Les opérations sont les suivantes :

La **négation** d'une proposition P est notée non(P). Cette nouvelle proposition est vraie si et seulement si P est faux. Si, par exemple, P désigne la proposition « tous les hommes sont mortels », alors non(P) désigne la proposition « il existe au moins un homme qui est immortel ». Il est clair que non(non(P)) = P.

Attention : la négation, ou contraire, de « ce tableau est noir » est « ce tableau n'est pas noir ». Ce n'est pas « ce tableau est blanc ».

La **disjonction** de deux propositions, notée « P ou Q », affirme qu'au moins l'une des deux propositions est vraie. Autrement dit, les propositions P et Q ne peuvent pas être toutes les deux fausses.

La **conjonction** de deux propositions, notée « P et Q » affirme que les deux propositions sont vraies en même temps.

L'**'implication**, notée « si P, alors Q », ou encore $P \Rightarrow Q$, affirme que si P est vraie alors Q doit l'être aussi.

Exemple. Soit x un nombre réel. Alors $x > 0 \Rightarrow x \geq 0$. **Attention**, le contraire n'est pas vrai (car x peut prendre la valeur 0).

L'**équivalence**, notée « P si et seulement si Q », ou encore $P \Leftrightarrow Q$, affirme que P est vraie si et seulement si Q est vraie. Une stratégie typique pour montrer $P \Leftrightarrow Q$, est de montrer que $P \Rightarrow Q$ et que $Q \Rightarrow P$.

Exemple. Une proposition P est vraie si et seulement si sa négation non(P) est fausse.

Réécriture de la preuve de l'énigme A.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 cents.

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

Par hypothèse on a :

$$\begin{aligned} 20 &= b+v \quad \text{et} \quad v = 19+b \\ \Rightarrow 20 &= 19+2b \\ \Rightarrow\ b &= 0,5 \end{aligned}$$

D'où la bouteille vaut 50 cents. ■

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.

Attention : 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.

A.1.3 Raisonnement, ou comment démontre-t-on une implication $P \Rightarrow Q$?

Le raisonnement direct

La plupart du temps, on fait comme suit : on suppose comme hypothèse de départ que P est vrai ; 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 Q est vrai.

Le raisonnement indirect

On peut aussi démontrer sa contraposée : la contraposée de $P \Rightarrow Q$ est non$(Q) \Rightarrow$ non(P). En effet, une implication et sa contraposée sont toujours équivalentes ; démontrer l'une revient à démontrer l'autre, et vice-versa. Un exemple : on considère P la proposition « x est pair » et Q la proposition « x n'est pas le carré d'un entier impair ». Pour montrer $P \Rightarrow Q$, c'est-à-dire x pair $\Rightarrow$ x n'est pas le carré d'un entier impair, on montrera *non*(Q)$\Rightarrow$ non(P), c'est-à-dire : $x = n^2$ et n impair $\Rightarrow$ x impair.

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 non(P) est vraie, et montrer par une suite d'implications logiques que cette hypothèse est absurde. Donc comme non(P) est fausse, alors P est vraie.

On note tout d'abord que *non*$(P \Rightarrow Q)$ équivaut à P *et non*(Q). Ainsi, pour montrer que $P \Rightarrow Q$, on suppose par **l'absurde** que P et non(Q) sont vraies, et on montre que forcément non(P) est aussi

vraie. Ceci est absurde en vertu de notre règle qui dit que soit P est vraie, soit non(P) est vraie. Donc Q est vraie et : $P \Rightarrow Q$.

Voici un exemple de ce raisonnement.

Énigme A.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 1 homme politique honnête. En vertu de P_1, la proposition non(Q) est : il y a au moins deux hommes politiques honnêtes.

Procédons par contradiction. Supposons que Q est fausse, c'est-à-dire que non(Q) est vraie.

Alors, il existe au moins une paire d'hommes politiques honnêtes. Donc non(P_2) est vraie, ce qui est une contradiction de l'hypothèse de départ (P_2 est vraie).

D'où non(Q) est fausse, autrement dit, Q est vraie. ■

On voit dans cette preuve que l'on a aussi utilisé des implications. En fait il est courant que les différents types de raisonnements s'entremêlent dans une preuve.

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 ».

Énigme A.3 (Le premier asile)**.** « *Dans le premier asile, Craig n'interrogea que deux personnes.*

– *Dîtes-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 4 cas possibles pour la condition de Durand : il est un médecin fou, ou un médecin sain d'esprit, ou encore un patient fou ou finalement un patient sain d'esprit. Si Durand est un médecin fou ou un patient sain d'esprit, on a automatiquement notre réponse. Il ne reste donc que deux cas.

1er cas : Durand est un médecin sain d'esprit. Donc il dit la vérité. D'où Dupont est un médecin. Mais comme Dupont dit que Durand est un patient, l'affirmation de Dupont est fausse, et donc Dupont est fou. On a bien dans ce cas un médecin fou ou un patient sain d'esprit !

2e cas : Durand est un patient fou. Son affirmation est donc fausse, d'où Dupont est 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. ■

A.2 Le langage de la théorie 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.

A.2.1 Ensembles

La théorie des ensembles a été introduite par Georg Cantor. On peut en donner une axiomatique rigoureuse qui n'est pas discutée ici (voir cependant l'appendice A.5). Un **ensemble** est une collection d'objets. La théorie suppose que les ensembles contiennent des **éléments**, et on écrit $a \in A$ pour dire que ≪ a est un élément de A ≫ ou que ≪ a appartient à A ≫. Si a n'est pas un élément de A, on écrit $a \notin A$ et on lit ≪ a n'appartient pas à A ≫ ou ≪ a n'est pas dans A ≫. L'appartenance (ou pas) à un ensemble doit être claire. Autrement dit, cette appartenance ne doit pas être question de point de vue,

on d'interprétation. Comme pour tout concept mathématique, il est important de bien comprendre quand deux ensembles sont égaux. La règle est toute simple (mais on l'oublie parfois) :

« Deux ensembles sont égaux si et seulement si ils ont les mêmes éléments. »

Autrement dit, pour « connaître » un ensemble il faut savoir dire quels en sont les éléments.

Décrire un ensemble. Deux façons typiques (déjà utilisées) de décrire un ensemble consistent à : soit, donner la liste de tous ses éléments (quand il n'en contient pas trop), soit via la description d'une propriété qui caractérise ses éléments. L'écriture $E = \{x_1, x_2, ..., x_m\}$ signifie donc que E est composé des éléments $x_1, x_2, \ldots, x_m$; il peut y avoir des répétitions d'éléments : par exemple, $\{a, b, a\}$ représente le même ensemble que $\{a, b\}$. On a donc les présentations équivalentes

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

d'un même ensemble qui contient les trois éléments : a, b et c. L'ordre dans lequel on écrit les éléments n'importe pas : par exemple, $\{b, a\}$ représente le même ensemble que $\{a, b\}$. Fréquemment, on se donne une propriété P pour définir un ensemble. On écrit par exemple : on écrit $A = \{x \in E \,|\, x \text{ possède } P\}$ pour dire que A est l'ensemble des éléments de E qui possèdent la propriété P. Autrement dit, on affirme que pour tout élément x de E : $x \in A$ si et seulement si x possède la propriété P. Pour montrer qu'un élément x de E est en fait dans A, il suffira donc de montrer que x a la propriété P. Et réciproquement, si $x \in E$ a la propriété P, il est forcément dans A.

Typiquement, sans les définir trop rigoureusement ici, on commence par considérer des ensembles « simples » de base comme

- L'ensemble des **entiers naturels**,
$$\mathbb{N} := \{0, 1, 2, 3, \ \ldots\};$$
- L'ensemble des **entiers**,
$$\mathbb{Z} := \{\ \ldots\ , -3, -2, -1, 0, 1, 2, 3, \ \ldots\};$$
- L'ensemble des **nombres rationnels**,
$$\mathbb{Q} := \{a/b \mid a \in \mathbb{Z}, \quad b \in \mathbb{N}, \text{ et } b \neq 0\};$$

l'ensemble $\mathbb{R}$ des **nombres réels**, qui inclut les nombres rationnels et tous les nombres qu'on peut construire [2] à partir de ceux-ci par « passage à la limite », (par exemple, π, $\sqrt{2}$) ; l'ensemble $\mathbb{C}$ des **nombres complexes** ; l'ensemble de lettres (minuscules) de l'alphabet

$$\mathcal{A} := \{a, b, c, d, \ \ldots\ , z\};$$

ou encore des ensembles d'objets divers comme

$$\{\bullet, \bullet, \bullet\}, \qquad \text{ou} \qquad \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}.$$

2. À voir dans un cours d'analyse.

L'ensemble qui ne contient aucun élément est, par définition, l'ensemble **vide** et on le représente par le symbole $\emptyset$.

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 Bertrand Russell (1872-1970) dans tout bon livre de logique). Pour éviter cela, nous ne travaillerons qu'avec un petit nombre d'ensembles bien étudiés et stables. Tous les ensembles considérés s'obtiennent à partir de l'ensemble vide et d'axiomes de construction d'ensembles (voir section A.5).

Ensemble fini et infini

Définition. Un ensemble E est **fini** si on peut écrire $E = \{x_1, \ldots, x_n\}$, avec $n \in \mathbb{N}$ fixé. Si les éléments x_i sont tous distincts, alors on dit que l'entier n est le **cardinal** 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.

A.2.2 Sous-ensembles

Définitions et notations

Soit A et E deux ensembles.

1. Si tous les éléments de A appartiennent à E, on dit que A est **contenu** dans E et on écrit $A \subseteq E$. Dans ce cas on dit que A est un **sous-ensemble** de E.
2. $\emptyset$ et E sont des sous-ensembles particuliers de E ; un sous-ensemble autre que ceux-ci est un **sous-ensemble propre** de E.
3. Le symbole $\subseteq$ est appelé **l'inclusion**.
4. Si A n'est pas un sous-ensemble de E, on écrit $A \nsubseteq E$.

Exemple. $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$. Ce qui signifie que $\mathbb{N} \subseteq \mathbb{Z}$, $\mathbb{Z} \subseteq \mathbb{Q}$, etc., mais aussi que $\mathbb{N} \subseteq \mathbb{Q}$. On dit que l'inclusion est **transitive**.

Vocabulaire

On trouvera dans la littérature d'autres manières classiques de se référer à un sous-ensemble. Soit E un ensemble et A un sous-ensemble de E. On peut aussi écrire et dire que A est *inclus* dans E, ou encore que A est **une partie** de E. On trouvera, et on utilisera aussi, la notation suivante : $E \supseteq A$ (E contient A).

Attention, la notation $A \subset E$ peut signifier deux choses : **soit que** $A \subseteq E$, **soit que** $A \subseteq E$ et $A \neq E$. Dans ce cours, nous préciserons toujours si $A \neq E$.

Remarque. Tout sous-ensemble d'un ensemble fini est fini.

L'ensemble des sous-ensembles

On note $\mathcal{P}(E)$ l'ensemble des sous-ensembles de l'ensemble E :

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

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

Remarque. Si $|E| = n$, alors $|\mathcal{P}(E)| = 2^n$. La démonstration est difficile et nécessite plus d'outils que ceux présentés dans ce cours.

Démonstration de l'inclusion

Dans la pratique, quand on veut montrer qu'un ensemble A est inclus dans un ensemble E, on doit montrer qu'un élément quelconque de A est forcément aussi un élément de E. Autrement dit que : $x \in A \Rightarrow x \in E$.

De plus, pour montrer que $A = E$, on doit montrer que $A \subseteq E$ et $E \subseteq A$. Autrement dit que : $x \in A \;\Leftrightarrow\; x \in E$.

Complémentaire et différence

Si $A \subseteq E$, le *complémentaire* de A par rapport à l'ensemble E est l'ensemble formé des éléments de E qui n'appartiennent pas à A. On le note A^c, et on lit A **complément** lorsqu'il n'y a pas d'ambiguïté sur E. On a donc pour x élément de E : $x \in A^c \;\Leftrightarrow\; x \notin A$. En d'autres termes

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

La différence de deux ensembles A et B, notée $A \setminus B$ (lire A **moins** B), est le nouvel ensemble défini par

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

En particulier, si $A \subseteq E$ alors $A^c = E \setminus A$.

Exemple. Dans le cas d'un ensemble E qui contient 0, comme $\mathbb{N}, \mathbb{R}$, on écrit $E^* = E \setminus \{0\}$.

A.2.3 Produit cartésien

1. Un **couple** (a, b) est la donnée de a comme première coordonnée et b comme seconde coordonnée.

2. Si A et B sont des ensembles, le **produit cartésien** de A et B est l'ensemble
$$A \times B = \{(a,b) \,|\, a \in A, b \in B\}$$
et se lit « A croix B ».
Exemples. (a) Le plan $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$.
(b) Si $A = \{A, R, D, V, 10, 9, 8, 7, 6, 5, 4, 3, 2\}$ et $B = \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$, alors le produit cartésien de ces deux ensembles est l'ensemble à 52 éléments suivants :
$$\{(A,\spadesuit), (R,\spadesuit), \ldots, (2,\spadesuit), (A,\heartsuit), \ldots, (2,\heartsuit), (A,\diamondsuit), \ldots, (2,\diamondsuit), (A,\clubsuit), \ldots, (2,\clubsuit)\}.$$

3. Si $n \in \mathbb{N}^*$ et E est un ensemble, le produit cartésien n fois de E est l'ensemble défini par récurrence
$$E^n = E \times E^{n-1} \quad (= \underbrace{E \times E \times E \times \ldots \times E}_{n \text{ fois}})$$
dont les éléments sont appelés **n-uplets**.
Exemples. (a) L'espace $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$. (b) L'espace $\mathbb{R}^n$. (c) Le plan $\mathbb{R}^2$.

Remarque. (a) $\emptyset \times E = E \times \emptyset = \emptyset$; en effet, il n'existe pas de couple (a,b) tel que $a \in E$ et $b \in \emptyset$!

(b) En général $A \times B \neq B \times A$; par exemple, si $A = \{0,1\}$ et $B = \{1\}$, alors
$$\{(0,1),(1,1)\} = \{0,1\} \times \{1\} \neq \{1\} \times \{0,1\} = \{(1,0),(1,1)\}$$

(c) Il faut distinguer le **couple** (a,b), où l'ordre de a et b est important, de la **paire** $\{a,b\}$ qui est un ensemble, où l'ordre de a et b n'est pas important. En général, les couples sont différents : $(a,b) \neq (b,a)$; mais pas les paires : $\{a,b\} = \{b,a\}$

A.2.4 Union et intersection

On appelle **réunion** ou **union** de deux ensembles A et B l'ensemble formé de tous les éléments qui appartiennent à A **ou** à B ou aux deux ; on le note $A \cup B$ et on lit « A union B ». Donc
$$A \cup B = \{x \,|\, x \in A \text{ ou } x \in B\}.$$
Exemple. $\{1,3,-2,\pi\} \cup \{\pi, \sqrt{2}, 10, 11\} = \{1,3,-2,\pi,\sqrt{2},10,11\}$.

On appelle **intersection** de deux ensembles A et B l'ensemble formé des éléments communs à A **et** B ; on le note $A \cap B$ et on lit « A inter B ». Donc
$$A \cap B = \{x \,|\, x \in A \text{ et } x \in B\}.$$
Exemples. $\{1,3,5\} \cap \{1,2,3\} = \{1,3\}$.

Remarque. (a) $A \subseteq A \cup B$; (b) $A \cap B$ est un sous-ensemble de A, de B et de $A \cup B$; (c) $A \cap B = A \Leftrightarrow A \subseteq B$ (exercice).

Définition. Si $A \cap B = \emptyset$, on dit que A et B sont **disjoints**, sinon on dit que A et B se **coupent**.

Exemple. Nombres pairs et impairs

L'ensemble des nombres pairs est noté $2\mathbb{Z}$, et celui des nombres impairs est

$$\mathcal{I} = \{2k+1 \,|\, k \in \mathbb{Z}\}.$$

Alors on a $2\mathbb{Z} \cap \mathcal{I} = \emptyset$ et $2\mathbb{Z} \cup \mathcal{I} = \mathbb{Z}$. En français cela veut dire qu'un nombre entier est soit pair, soit impair, mais pas les deux à la fois ! On dit en mathématique que l'ensemble des nombres pairs et l'ensemble des nombres impairs forment une **partition** de $\mathbb{Z}$.

Compatibilités entre union, intersection et complément

On va donner ici les propriétés algébriques fondamentales des ensembles, propriétés qui vont nous permettre de ≪ calculer ≫ avec les ensembles.

Proposition A.1. *Soit A, B, C trois ensembles, alors*

1. *$A \cap A = A$ et $A \cup A = A$ (idempotence) ;*
2. *$A \cup B = B \cup A$ et $A \cap B = B \cap A$ (commutativité) ;*
3. *$A \cup \emptyset = A$ et $A \cap \emptyset = \emptyset$; et si $A \subseteq B$ alors $A \cup B = B$ et $A \cap B = A$ (existence d'éléments neutres).*

Démonstration. Exercice. ■

A.3 Les fonctions

Quand on introduit une notion mathématique, comme celle d'ensemble, il est toujours bien (essentiel !) d'expliquer comment interagissent les objets ainsi définis. Pour les ensembles, la description de ces interactions fait apparaître la notion de **fonction**. En fait, bien que ce soit l'une des notions les plus importantes des mathématiques, la définition rigoureuse moderne de la notion de fonction n'apparaît qu'au XIX^{e}(en 1837). Elle est due à Johann Dirichlet (1805-1859). Dans le langage de la théorie des ensembles, elle prend la forme suivante.

Définition. Soit A et B deux ensembles. Une fonction f de A vers B, on écrit $f : A \to B$, est une règle qui associe à chaque élément de a un unique élément de B. Plus techniquement, f est un sous-ensemble de $A \times B$, et on écrit $f(a) = b$ si et seulement si le couple (a, b) appartient à ce sous-ensemble. On demande (et c'est tout) que f soit tel que

1. pour tout $a \in A$, il existe un b tel que $f(a) = b$,
2. si $f(a) = b$ et $f(a) = c$, alors $b = c$.

Dans une première introduction à la théorie des ensembles, la correspondance établie par une bijection $f : A \to B$, entre les éléments de A et ceux de B, est souvent introduite par une représentation naïve comme celle de la Figure A.1. De façon plus précise, on a la définition suivante. Une fonction f de A vers B, est une **bijection**, si on a une fonction **inverse** $f^{-1} : B \to A$, pour la composition, c.-à-d. :

$$f^{-1} \circ f = \mathrm{Id}_A, \text{ et } f \circ f^{-1} = \mathrm{Id}_B. \tag{A.1}$$

Il est très facile de vérifier qu'il ne peut y avoir qu'un inverse pour la composition, c.-à-d. :

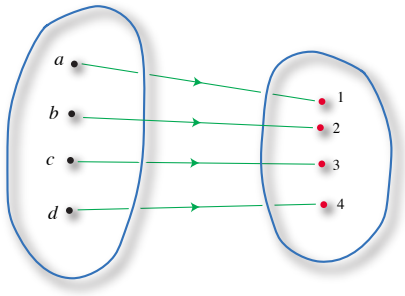


FIGURE A.1 – Représentation naïve d'une bijection.

Proposition A.2. *Pour toute fonction $f : A \to B$, si $g : B \to A$ est telle que*

$$g \circ f = \mathrm{Id}_A, \text{ et } f \circ g = \mathrm{Id}_B, \tag{A.2}$$

alors $g = f^{-1}$.

Pour montrer que $f : A \to B$ est une bijection, il faut donc montrer qu'on peut construire une fonction qui satisfait (A.2).

Parmi les propriétés particulières des fonctions, l'injectivité et la surjectivité sont très certainement des notions importantes. Une fonction $f : A \to B$ est dite **injective** si et seulement si

« *Pour chaque élément y de B, il existe au plus un élément x de A tel que $f(x) = y$.* »

Autrement dit, la fonction f et un processus qui

« *choisit des éléments $f(x)$ de B, un pour chaque x dans A, tous distincts,* »

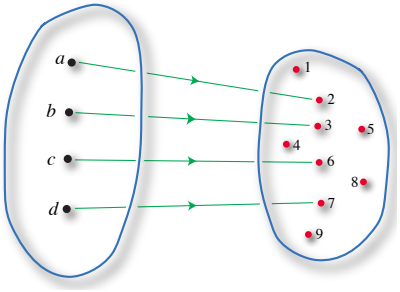


FIGURE A.2 – Représentation naïve d'une injection.

c'est-à-dire qu'un élément ne peut-être choisi qu'une seule fois. Une formulation un peu plus technique (mais plus facile à manipuler) de cette définition prend la forme suivante. Une fonction $f : A \to B$ est injective si et seulement si, pour tout a et tout b dans A

$$a \neq b \qquad \Longrightarrow \qquad fa) \neq f(b), \tag{A.3}$$

ce qui équivaut (c'est la contraposée) à dire aussi que

$$f(a) = f(b) \quad \text{entraine forcément} \quad b = b. \tag{A.4}$$

Une fonction $f : A \Rightarrow B$ est dite **surjective** si et seulement si

« *Pour chaque élément y de B, il existe au moins un élément x de A tel que $f(x) = y$.* »

Autrement dit, f est un processus qui

« *choisit chaque élément y de B au moins une fois.* »

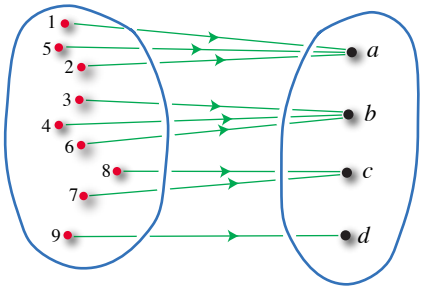


FIGURE A.3 – Représentation naïve d'une surjection.

La proposition suivante donne une autre stratégie pour démontrer qu'un fonction est bijective.

Proposition A.3. *Une fonction qui est à la fois surjective et injective est une fonction bijective.*

Cantar à souligné que deux ensembles ont même cardinal si et seulement si il existe une bijection entre les deux ensembles. Entre ensembles finis, cela correspond à la définition qu'on s'est déjà donné. Cependant, cela devient une définition nouvelle pour des ensembles infinis. Cela a mené à une des constatations les plus surprenantes de l'histoire des mathématiques, à savoir qu'il y a plusieurs infinis, de plus en plus grands.

A.4 Exercices de l'annexe A

Raisonnement

Exercice 1 (A) 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 2 Parmi les énoncés suivants, lequel est la négation de « les éléphants ne sont pas tous roses » :
(a) il y a un éléphant rose ; (b) il existe un éléphant gris ; (c) tous les éléphants sont roses ; (d) il y a un éléphant qui n'est pas rose.

Lequel lui est équivalent ? Pourquoi ?

Exercice 3 (A) écrire la négation des propositions suivantes, où $x, y \in \mathbb{R}$.

(a) $x > y$; (b) $x \geq y$; (c) $x > y$ ou $x < y$; (d) $x \neq y$.

Réponses : (a) $x \leq y$; (b) $x < y$; (c) $x = y$; (d) $x = y$.

Exercice 4 écrire la contraposée des implications suivantes :

(a) $P \Rightarrow Q$;

(b) $P \Rightarrow \text{non}(Q)$;

(c) $\text{non}(P) \Rightarrow Q$;

(d) tous les chats sont gris ;

(e) chaque sport est bon pour la santé ;

(f) aucune hirondelle ne fait le printemps.

Exercice 5 (A) Ce soir aura lieu la 6e 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 3 parties à 2 en faveur des Canadiens. On considère les propositions suivantes :

A : Les Canadiens remportent la 6e partie.

B : Les Canadiens remportent la Coupe Stanley.

Que peut-on dire des 4 propositions suivantes :

(a) $B \Rightarrow A$; (b) $A \Rightarrow B$; (c) $\text{non}(B) \Rightarrow \text{non}(A)$;

(d) $\text{non}(A) \Rightarrow \text{non}(B)$.

On rappelle que le vainqueur de la Coupe est celui qui remporte le premier 4 parties de la série finale, et qu'il n'y a pas de parties nulles.

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

Les ensembles

Exercice 6 (A) Répondre par vrai ou faux aux questions suivantes. Justifier votre 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) $\{\{4,5\},\{1,2\}\} \subseteq \{1,2,4,5\}$; (d) $\emptyset \in \{a,b\}$; (e) $\emptyset \subseteq \{a,b,f,g\}$; (f) $\emptyset \in \{\emptyset,\{\emptyset\}\}$;

(g) $\emptyset \subseteq \emptyset$; (h) $\{\emptyset\} \in \{\emptyset,\{\emptyset\}\}$; (i) $\{\emptyset\} \subseteq \{\emptyset,\{\emptyset\}\}$; (j) $\{\emptyset,\{1\},\{2,3\}\} \subseteq \{\{1\},\{2,3\}\}$;

(k) $\{\{4\}\} \in \{3,\{4\}\}$; (l) $\{\{\emptyset\}\} \in \{\emptyset,\{\emptyset\}\}$; (m) $\{\{1,2\}\} \subseteq \{\emptyset,\{1,2\}\}$; (n) $\{\{\emptyset\}\} \subseteq \{\emptyset,\{\emptyset\}\}$.

Réponses : (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 7 Soit $A = \{1, 2, 3\}$, $B = \{4, 5\}$ et $C = \{2, 3, 4, 5\}$. Écrire les ensembles suivants :

(a) $\mathcal{P}(A)$; (b) $\mathcal{P}(\mathcal{P}(B))$; (c) $A \setminus B$; (d) $B \setminus A$; (e) B^c dans C ; (f) $C \setminus A$;

(g) $C \setminus B$; (h) $A \setminus C$; (i) $B \setminus C$.

Exercice 8 Soit A et B deux ensembles. Montrer que :

1. Si $A \subseteq B$ et $A^c = B \setminus A$, alors (i) $A \cup A^c = B$; (ii) $A^c \cap A = \emptyset$; (iii) $\emptyset^c = B$; (iv) $B^c = \emptyset$.

2. $A \subseteq B$ si et seulement si $A \cap B = A$.

Exercice 9 (B) (Lois de Morgan) Soit $A \subseteq E$ et $B \subseteq E$ des ensembles. Montrer que :

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

Exercice 10 (B) (Démonstration du cours) Soit A et B deux ensembles. Montrer que $A \cap B = A \Leftrightarrow A \subseteq B$.

Exercice 11 (B) (Démonstration du cours) Démontrer le théorème A.1 : Soit A, B, C trois ensembles, alors

1. $A \cap A = A$ et $A \cup A = A$ (idempotence) ;
2. $A \cup B = B \cup A$ et $A \cap B = B \cap A$ (commutativité) ;
3. $A \cup \emptyset = A$ et $A \cap \emptyset = \emptyset$; et si $A \subseteq B$ alors $A \cup B = B$ et $A \cap B = A$ (existence d'éléments neutres).

A.5 Axiomatique de la théorie des ensembles (*)

La présentation ci-dessous ne vise qu'à donner une idée de ce à quoi peut ressembler une théorie axiomatique des ensembles. Le but est simplement de montrer qu'il existe une (des) axiomatique rigoureuse pour la notion d'ensemble. Dans un premier temps, le lecteur est encouragé à simplement survoler la description qui suit. Pour en savoir plus, il faudra suivre un cours sur le sujet, ou consulter un livre plus spécialisé, comme

J.-L.Krivine, *Théorie axiomatique des ensembles*, Presses Universitaires de France, 1969.

Il existe plusieurs systèmes axiomatiques formels pour la théorie des ensembles. L'un des plus connus est le système **ZFC** de Zermelo-Fraenkel (avec l'axiome du choix). L'axiomatique ZFC se décrie dans le contexte du calcul des prédicats avec relation d'égalité. Toute la théorie étant formulée en terme d'ensembles, on doit se rappeler que les éléments d'ensembles sont aussi des ensembles. Tout est, en quelque sorte, construit à partir de l'ensemble vide. Par exemple, on a les ensembles tous distincts

$$\emptyset, \qquad \{\emptyset\}, \qquad \{\{\emptyset\}\}, \qquad \{\emptyset, \{\emptyset\}\}, \qquad \{\{\emptyset, \{\emptyset\}\}\}$$

La relation d'appartenance $x \in A$ et la notion d'ensemble ne sont définies que par le fait qu'elles satisfont les axiomes suivants. La relation d'inclusion $A \subseteq B$ est définie par

$$(A \subseteq B) \qquad \text{ssi} \qquad \forall x \ (x \in A \Rightarrow x \in B).$$

1) Axiome d'extensionalité. Deux ensembles sont égaux, si et seulement si ils ont les mêmes éléments. En formule,

$$\forall A \ \forall B \ [\forall x \ (x \in A \Leftrightarrow x \in B) \Rightarrow (A = B)]. \tag{A.5}$$

2) Axiome de la paire. Pour tous ensembles A et B, on peut construire un ensemble C dont les seuls éléments sont A et B. Autrement dit, on permet ici de construire

$$C := \{A, B\}.$$

En formule,

$$\forall A \ \forall B \ \exists C[\forall x \ (x \in C) \Leftrightarrow (x = A \ \text{ ou } x = B)]. \tag{A.6}$$

3) Axiome de la réunion. Pour tout ensemble A, on peut construire un ensemble B dont les seuls éléments sont tous ceux qui sont éléments des éléments de A. Autrement dit, on permet ici la construction de l'ensemble

$$B := \bigcup_{x \in A} x.$$

En formule,

$$\forall A \ \forall B \ \exists C[\forall x \ (x \in C) \Leftrightarrow (x = A \ \text{ ou } x = B)]. \tag{A.7}$$

4) Axiome de l'ensemble des parties. Pour tout ensemble A, on peut construire l'ensemble B des sous-ensembles de A. Autrement dit, on permet ici la construction de l'ensemble

$$B := \{x \mid x \subseteq A\}.$$

En formule,

$$\forall A\ \exists B\ \forall x (x \in B) \Leftrightarrow (x \subseteq A). \tag{A.8}$$

5) Axiome de l'infini. Cet axiome permet de construire (au moins un) ensemble infini. C'est l'ensemble

$$\begin{aligned} A := \{\quad & \emptyset, \\ & \{\emptyset\}, \\ & \{\emptyset, \{\emptyset\}\}, \\ & \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \\ & \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}, \ \ldots\}. \end{aligned}$$

Cet axiome permet aussi (avec les précédents) de construire l'ensemble $\mathbb{N}$ des entiers positifs. En formule,

$$\exists A\ (\emptyset \in A) \quad \text{et} \quad (x \cup \{x\} \in A). \tag{A.9}$$

6) Schéma d'axiomes de compréhension. Pour tout ensemble A, on peut construire le sous-ensemble B des éléments de A qui satisfont une propriété P (exprimée dans le langage de la théorie des ensembles). Autrement dit, on permet ici la construction de

$$B := \{x \in A \mid P(x)\}.$$

En formule,

$$\forall y_1\ \cdots\ \forall y_n\ \forall A\ \exists B\ \forall x[(x \in B) \Leftrightarrow (x \in A \text{ et } P(x, y_1, \ldots, y_n)). \tag{A.10}$$

Les y_i sont ici simplement des paramètres auxiliaires dont on pourrait avoir besoin pour formuler plus facilement la propriété P. On dit qu'on a un « schéma » d'axiomes, parce qu'il y a un axiome pour chaque choix de P.

7) Schéma d'axiomes de remplacement. Pour tout ensemble A et toute relation fonctionnelle F, on a un ensemble

$$B := \{y \mid x \in A \text{ et } F(x, y)\}.$$

Pour exprimer ceci en formule (simplifiée[3]), rappelons d'abord que F est une relation fonctionnelle, on écrit $\mathsf{Fonct}(F)$, si et seulement si

$$\mathsf{Fonct}(F) \qquad \text{ssi} \qquad \forall x\ \forall y_1\ \forall y_2\ [(F(x, y_1) \text{ et } F(x, y_2)) \Rightarrow (y_1 = y_2)].$$

3. La formulation plus juste fait apparaître des paramètres dans F comme dans l'axiome précédent.

Alors l'axiome se présente comme

$$\mathsf{Fonct}(F) \Rightarrow \forall A\ \exists B\ \forall y\ [y \in B \Leftrightarrow \exists x\ (x \in A \text{ et } F(x,y))].$$

8) Axiomes de fondation. Pour tout ensemble A non vide, il existe un ensemble B, appartenant à A, qui n'a aucun élément en commun avec A, c'est-à-dire que

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

En formule,

$$\forall A[(A \neq \emptyset) \text{ et } \exists B\ (B \in A \text{ et } A \cap B = \emptyset)]. \tag{A.11}$$

9) Axiomes du choix. Pour tout ensemble A, d'ensembles non vides, le produit cartésien des éléments de A est non vide. En formule,

$$[\forall x \in A\ (x \neq \emptyset)] \Rightarrow \prod_{x \in A} x \neq \emptyset. \tag{A.12}$$

Annexe B

Relations d'équivalence

Nous allons nous intéresser ici aux relations qui servent à regrouper les éléments d'un ensemble par « familles », ce sont les relation d'équivalence.

Définition. Soit E un ensemble. On dit que « $\equiv$ » est une **relation d'équivalence** si « $\equiv$ » est telle que :

Réflexive : $\forall x \in E$, on a $x \equiv x$.

Symétrique : $\forall x, y \in E$, $x \equiv y \Longrightarrow y \equiv x$.

Transitive : $\forall x, y, z \in E$, $x \equiv y$ et $y \equiv z$ implique $x \equiv z$.

Exemple. (a) Si $E = \{\text{habitants du Québec}\}$, on peut définir la relation suivante : deux habitants du Québec x et y sont en relation $x \equiv y$ si et seulement si x et y ont le même nom de famille. C'est une relation d'équivalence.

(b) Soit E un ensemble quelconque. Considérons la relation « $\equiv$ » sur E définie par : $x \equiv y$ si $x = y$ (autrement dit, $\equiv$ est l'égalité sur E). Alors « $\equiv$ » est bienune relation d'équivalence ($x = x$, $x = y \Leftrightarrow y = x$ et si $x = y$, $y = z$ alors $x = z$).

B.1 Classes d'équivalence et ensemble quotient

Très souvent on construit un nouvel ensemble en considérant comme équivalents certains éléments d'un plus grand ensemble. Il est important de se familiariser avec les aspects techniques de ce type de construction.

Définition. Soit E un ensemble et $\equiv$ une relation d'équivalence sur E.

1. Par définition, la **classe d'équivalence** de $a \in E$ est le sous-ensemble de E

$$[a] = \{x \in E \,|\, x \equiv a\}.$$

2. Une *classe d'équivalence* de $\equiv$ 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 $(E/\equiv)$, et on dit due c'est **l'ensemble quotient** de E par la relation d'équivalence $\ll \equiv \gg$.

Remarque. L'ensemble quotient $(E/\equiv)$ est un objet de première importance en mathématiques. Il est très important de bien en comprendre la nature : les éléments de $(E/\equiv)$ sont les classes d'équivalence de $\equiv$, en d'autres termes, des sous-ensembles de E. Donc $(E/\equiv) \subseteq \mathcal{P}(E)$. Une classe d'équivalence n'est jamais vide : $a \in [a]$ car $a \equiv a$.

Exemple. On reprend dans l'ordre les exemples précédents.

(a) $(E/\equiv)$ est en bijection avec l'ensemble des noms représentés au Québec.

(b) Dans ce cas, les classes d'équivalence sont les singletons de E, c'est-à-dire les sous-ensembles à un élément de E. Donc $(E/\equiv)$ est $\ll$ en bijection $\gg$ avec E.

Proposition B.1. *Soit $\equiv$ une relation d'équivalence sur E et $x, y \in E$, alors*

1. $x \in [y] \;\Leftrightarrow\; [x] = [y]$;
2. $[x] \cap [y] \neq \emptyset \;\Leftrightarrow\; [x] = [y]$. *Autrement dit, deux classes d'équivalence $\lambda, \lambda' \in (E/\equiv)$ sont disjointes si et seulement si $\lambda \neq \lambda'$.*

Démonstration.

(1) Il faut montrer une double inclusion. Soit $z \in [x]$, alors $z \equiv x$ et $x \equiv y$ et donc par transitivité de la relation $\equiv$, on obtient $z \equiv y$. Ainsi $z \in [y]$ et donc $[x] \subseteq [y]$. Soit maintenant $z \in [y]$, alors $z \equiv y$ et $y \equiv x$. Comme auparavant, on peut conclure par transitivité de la relation $\equiv$ que $z \in [x]$ et donc que $[y] \subseteq [x]$. La réciproque est triviale.

(2) Si $[x] \cap [y] \neq \emptyset$ alors il existe $z \in [x] \cap [y]$. Donc $x \equiv z$ et $z \equiv y$. D'où $x \equiv y$. Donc $x \in [y]$ et $y \in [x]$. Par (1) on conclut à l'égalité. 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 représentant.

Définition. Soit $\equiv$ une relation d'équivalence sur E. Un sous-ensemble I de E est un **système de représentants** des classes d'équivalence de $\equiv$ si pour toute classe d'équivalence $A \in (E/\equiv)$, 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 à nouveau la relation d'équivalence sur E : $x \equiv y$ si $f(x) = f(y)$. Alors $I = \mathbb{R}^+$ est un système de représentants des classes d'équivalence de R. En effet, dans chaque classe $A = \{-a, a\} \in (E/\equiv)$ il n'y a qu'un unique élément positif $x \in I$ et on a bien $[x] = A$.

Proposition B.2. *Soit E un ensemble fini et $\equiv$ une relation d'équivalence sur E. Soit I un système de représentants de $(E/\equiv)$, alors $|(E/\equiv)| = |I|$.*

Démonstration. Notons $k = |I|$, alors par définition de I on peut écrire $I = \{x_1, \dots x_k\}$ avec les x_i distincts. Il s'en suit que $(E/\equiv) = \{[x_1], \dots, [x_k]\}$ et donc que $|(E/\equiv)| = k = |I|$. ■

B.3 Exercices

Exercice 1 (B) Soit $\equiv$ la relation sur $\mathbb{R}$ définie par : $x \equiv y$ si $|x| = |y|$.

(a) Montrer que c'est une relation d'équivalence et déterminer son ensemble quotient $\mathbb{R}/\equiv$.

(b) Montrer que $\mathbb{R}^+$ est un système de représentants des classes d'équivalence de $\equiv$.

Exercice 2 (B) Sur l'ensemble $E = \{1, 2, 3, \dots, 30\}$ définissons la relation $\equiv$ par : $i \equiv j$ si tout nombre premier p qui divise i divise aussi j. Vérifier que $\equiv$ est bien une relation d'équivalence, écrire l'ensemble quotient et trouver un système de représentants.

Exercice 3 (B) Soit $\equiv_a$, $\equiv_b$ deux relations d'équivalence sur E. Montrer que la relation $\equiv$ sur E définie par : $x \equiv y$ si ($x \equiv_a y$ et $x \equiv_b y$) est une relation d'équivalence. Décrire les classes d'équivalence de $\equiv$ en fonction de celles de $\equiv_1$ et de $\equiv_2$.

Bibliographie

[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).

[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`.

Index