Algèbre et géométrie 1

Bernard Le Stum

21 août 2023

– Nous voulons, autant que cela est possible, introduire dans toutes les sciences la finesse et la sévérité des mathématiques, sans nous imaginer que par là nous arriverons à connaître les choses, mais seulement pour déterminer nos relations humaines avec les choses (Friedrich Nietzsche, Le Gai Savoir).

Réalisé en LaTeX à partir du modèle Legrand Orange Book

Table des matières

Introduction

Ce cours d'algèbre et de géométrie commence par une introduction à la logique mathématique. Le but d'un mathématicien est de démontrer des théorèmes, ou en d'autres termes, d'énoncer et de valider des propositions. Le calcul propositionnel est un outil qui structure les raisonnements permettant d'obtenir un théorème à partir de résultats connus. Nous conclurons avec le si puissant raisonnement par récurrence.

L'étape suivante consiste à présenter le vocabulaire ensembliste qui a tant bouleversé les mathématiques contemporaines. De notre point de vue, il s'agira simplement de rassembler des éléments dans ce qu'on appelle un ensemble. On réalise alors que les opérations logiques ont une interprétation naturelle dans ce langage, ce qui permet de traiter avec une grande rigueur les problèmes mathématiques. Nous introduisons aussi la notion d'application, qui est au moins aussi importante que celle d'ensemble car elle permet de se transporter d'un ensemble dans un autre.

Nous allons ensuite appliquer nos méthodes à l'étude des nombres complexes. Afin de pouvoir utiliser la puissance du langage précédemment introduit, il est nécessaire de définir l'ensemble des nombres complexes de manière abstraite à partir de l'ensemble des nombres réels que l'on suppose donc connu. Il faut ensuite aussi définir différentes opérations (addition, multiplication, etc...) sur cet ensemble afin de pouvoir en manipuler les éléments. Nous présenterons systématiquement les propriétés de ces opérations de manière structurée afin de repérer facilement celles que nous retrouverons dans d'autres contextes.

Les plans vectoriel et affine seront eux aussi définis à partir des nombres réels. Sur le même schéma que précédemment, nous introduisons ensuite les opérations qui permettent de manipuler les vecteurs et les points. Puis nous étudions la notion de droite et finissons avec celle de barycentre qui permet de faire du calcul sur les points, ce qui peut sembler *a priori* bien optimiste.

Le plan euclidien n'est rien d'autre que le plan (vectoriel ou affine) muni d'une structure supplémentaire : un produit scalaire. Nous étudions cette structure d'abord

dans le cas vectoriel avant de nous intéresser au cas affine. Le produit scalaire nous permet de définir les notions de distance et d'angle et nous (re-) démontrerons de nombreux résultats classiques de la géométrie comme les théorèmes de Thales et de Pythagore à l'aide de nos nouveaux outils.

Enfin l'arithmétique. Il n'est pas raisonnable de vouloir définir les entiers à partir des nombres réels. Au contraire, c'est grâce aux entiers que l'on atteindra les réels. Nous allons donc partir de l'idée qu'un entier naturel n'est jamais que le successeur de celui qui le précède. On met alors a profit le principe du raisonnement par récurrence afin de définir les opérations classiques et d'établir leurs propriétés (addition, multiplication et ordre essentiellement). Fort de cette préparation, nous attaquons alors l'arithmétique proprement dite : division euclidienne, nombres premiers, etc. Une fois de plus, nous établissons avec une grande rigueur de nombreux résultats classiques.

La présentation ci-dessus peut inquiéter par son aspect théorique mais les six chapitres seront chacun illustrés par quelques exercices très abordables. Il n'est pas demandé aux étudiants de digérer tous les concepts introduits en cours. Celui qui saura faire ou même refaire parfaitement les exercices aura montré qu'il maîtrise suffisamment les techniques nécessaires. Mais avant de considérer qu'un exercice est effectivement terminé, il ne suffit pas d'en donner la réponse, même illustrée de calculs. Il faut rédiger une démonstration complète et rigoureuse, laquelle à partir des résultats déjà établis, permet de conclure. En cela, le cours peut et doit servir de modèle. La résolution d'un exercice se fait donc en deux parties qui peuvent cependant s'imbriquer : l'expérimentation scientifique consiste à retourner le problème dans tous les sens jusqu'à sa résolution, et la rédaction relève elle de la littérature scientifique. Il est alors essentiel de respecter toutes les règles littéraires. En particulier, l'utilisation d'abréviation devra être totalement maîtrisée sinon absente.

Comment travailler efficacement ? Commencer à faire les exercices avant de se présenter en travaux dirigés. Continuer sur place. Noter éventuellement certaines corrections si cela semble nécessaire. Refaire ensuite tous les exercices qui ont pu poser des problèmes et poursuivre. En parallèle, suivre attentivement le cours et le relire systématiquement dans la foulée. Certains pans de démonstration ne seront pas traités en cours. Il s'agit d'exercices supplémentaires généralement assez faciles mais plus abstraits que ce qui est fait en travaux dirigés. Il faut les faire aussi. Enfin, une bonne stratégie pour s'approprier le cours est d'en rédiger un résumé avec les principaux définitions et résultats.

Vous pouvez vous appuyer sur le cours en ligne mais aussi consulter tout ouvrage conçu pour les nouveaux venus à l'université [1]. Il y en a pléthore. Vous trouverez aussi de nombreux sites qui peuvent vous être utiles : forums sur lesquels les questions que vous pouvez vous poser ont déjà trouvé réponse, sites professionnels de mes collègues dans toute la France et même dans le monde, les encyclopédies comme Wikipedia...N'hésitez pas à converser avec vos camarades, à les aider ou à réclamer leur aide. N'hésitez pas non plus à vous tourner vers vos enseignants dont le rôle est de vous accompagner vers vos succès. Dans tous les cas, consacrez-y beaucoup de temps et d'énergie, et prenez-y du plaisir.

1. Les quatre premiers chapitres du cours http ://exo7.emath.fr/cours/livre-algebre-1.pdf sont assez proches de nos chapitres 1,2,3 et 6 respectivement.

1. Logique

Nous avons ici une approche extrêmement naïve de la logique mathématique qui vise seulement à inculquer les principes de base et présenter la mécanique sous-jacente au raisonnement. Pour une approche plus sérieuse, nous renvoyons par exemple vers [Kri07] ou [Bou70]. Nous utiliserons librement certaines notions et notations ensemblistes qui seront enseignées seulement ultérieurement.

1.1 Opérateurs logiques

Définition 1.1.1 Un *théorème* est un énoncé mathématique dont on sait qu'il est vrai [a]. Une *proposition* est un énoncé mathématique qui peut être vrai ou faux selon les valeurs des variables éventuelles [b].

a. C'est-à-dire démontré à partir des axiomes d'une théorie.

b. On devrait dire *prédicat* - en pratique, le mot « proposition » est souvent utilisé comme synonyme de « théorème ».

Exemple [1]

1. "$3 \geq 2$" est un théorème.
2. "$n \geq 2$" est une proposition qui dépend de l'entier naturel n (et ne peux donc pas être un théorème).
3. "$\forall n \in \mathbb{Z}_{\geq 0}, n \geq 2$ ou $n \leq 3$" est un théorème.
4. "$\exists n \in \mathbb{Z}_{\geq 0}, n \geq 2$" est aussi un théorème.
5. "$\forall n \in \mathbb{Z}_{\geq 0}, n \geq 2$" est une proposition (fausse) qui ne dépend pas de n (malgré les apparences).

Remarque

- Selon le contexte, au lieu de proposition, on dit aussi *affirmation*, *énoncé*, *assertion*, *formule*, *propriété*, *condition*, etc.

1. L'ensemble $\mathbb{Z}_{\geq 0}$ des entiers positifs est souvent plus simplement noté $\mathbb{N}$.

- Selon le contexte, au lieu de théorème, on dit aussi *axiome* (énoncé admis comme étant vrai), *tautologie* (théorème purement logique), *proposition valide*, *assertion satisfaite*, *formule juste*, etc.
- Un « énoncé mathématique » doit être « bien formulé », et pour être un théorème, il ne doit pas dépendre des variables.

Définition 1.1.2 Une *démonstration* consiste à décider [a] si une proposition (qui ne dépend pas des variables) est un théorème.

a. Par un raisonnement logique - nous ne discuterons pas la théorie de la démonstration.

Exemple Montrons que la fonction quadratique est continue. Il faut tout d'abord exprimer cette propriété sous une forme précise (faire un dessin) :

$$\forall a \in \mathbb{R}, \forall \varepsilon \in \mathbb{R}_{>0}, \exists \eta \in \mathbb{R}_{>0}, \forall x \in \mathbb{R}, |x-a| \leq \eta \Rightarrow |x^2 - a^2| \leq \varepsilon.$$

La formule va nous servir de squelette pour la démonstration. On remplace mécaniquement les $\forall$ par des "Soit", les $\exists$ par des "Posons" et les $\Rightarrow$ par des "Si ... alors". Ici, on va écrire :

« Soit a un réel. Soit ε un réel strictement positif. Posons $\eta = \boxed{\cdots}$: c'est bien un réel strictement positif. Soit x un réel. Si $|x-a| \leq \eta$, alors $|x^2-a^2| \boxed{\cdots} \leq \boxed{\cdots} \varepsilon$. ».

On n'a fait que réécrire en français le contenu de la proposition. L'étape suivante consiste à analyser la conclusion (dernières boîtes) afin de compléter les hypothèses (première boîte). L'idée est de se débarrasser de la variable auxiliaire x (en utilisant l'hypothèse $|x-a| \leq \eta$). On aura en effet (brouillon) :

$$|x^2 - a^2| = |x-a||x+a| = |x-a||2a + (x-a)| \leq \eta(2|a| + \eta) = 2|a|\eta + \eta^2.$$

Pour que $|x^2 - a^2| \leq \varepsilon$, il *suffit* donc que $2|a|\eta \leq \varepsilon/2$ et $\eta^2 \leq \varepsilon/2$. On peut alors conclure, c'est-à-dire faire la synthèse (on ne dessinera pas les boîtes, c'est moi qui souligne) :

Démonstration. Soit a un réel. Soit ϵ un réel strictement positif. Posons

$$\eta = \boxed{\begin{cases} \min\left\{\varepsilon/4|a|, \sqrt{\varepsilon/2}\right\} & \text{si } a \neq 0 \\ \sqrt{\varepsilon/2} & \text{si } a = 0 \end{cases}} :$$

c'est bien un réel strictement positif. Soit x un réel. Si

$$|x-a| \leq \eta,$$

alors

$$|x^2 - a^2| \boxed{= |x-a||2a + (x-a)| \leq \eta(2|a| + \eta)} \leq \boxed{\varepsilon/2 + \varepsilon/2 =} \varepsilon. \qquad \blacksquare$$

On remarquera qu'aucun symbole logique n'apparaît dans cette démonstration. Ceux-ci en sont bannis. Il s'agit de littérature scientifique. On exclura aussi toute abréviation dans un premier temps et on s'assurera d'en contrôler l'usage par la suite. On évitera aussi de polluer la démonstration par des éléments inutiles.

Définition 1.1.3 La *logique*[a] consiste à déterminer la vérité d'une proposition en fonction de la vérité des propositions qui la composent.

a. Plus précisément, il s'agit de la logique propositionnelle ou *calcul propositionnel*.

Voici les principaux *connecteurs logiques* qui permettent de construire de nouvelles propositions :

Définition 1.1.4

1. La *négation* d'une proposition $\mathcal{P}$ est la proposition "non $\mathcal{P}$" donnée par la table de vérité suivante :

$\mathcal{P}$	non $\mathcal{P}$
V	F
F	V

2. La *conjonction* des propositions $\mathcal{P}$ et $\mathcal{Q}$ est la proposition "$\mathcal{P}$ et $\mathcal{Q}$" donnée par la table de vérité suivante :

$\mathcal{P}$	Q	$\mathcal{P}$ et $\mathcal{Q}$
V	V	V
V	F	F
F	V	F
F	F	F

3. La *disjonction (inclusive)* des propositions $\mathcal{P}$ et $\mathcal{Q}$ est la proposition "$\mathcal{P}$ ou $\mathcal{Q}$" donnée par la table de vérité suivante :

$\mathcal{P}$	Q	$\mathcal{P}$ ou $\mathcal{Q}$
V	V	$V(*)$
V	F	V
F	V	V
F	F	F

4. L' *implication* des propositions $\mathcal{P}$ et $\mathcal{Q}$ est la proposition "$\mathcal{P} \Rightarrow \mathcal{Q}$" donnée par la table de vérité suivante :

$\mathcal{P}$	Q	$\mathcal{P} \Rightarrow \mathcal{Q}$
V	V	V
V	F	F
F	V	V
F	F	$V(*)$

5. L' *équivalence* des propositions $\mathcal{P}$ et $\mathcal{Q}$ est la proposition "$\mathcal{P} \Leftrightarrow \mathcal{Q}$" donnée

par la table de vérité suivante :

$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{P} \Leftrightarrow \mathcal{Q}$
V	V	V
V	F	F
F	V	F
F	F	V

Exemple La proposition "$2 > 3$" est fausse et la proposition "$1 < 4$" est vraie, donc
1. la proposition "$2 \leq 3$" est vraie (négation),
2. la proposition "$2 > 3$ et $1 < 4$" est fausse,
3. la proposition "$2 > 3$ ou $1 < 4$" est vraie,
4. la proposition "$2 > 3 \Rightarrow 1 < 4$" est vraie (étonnant non ?),
5. la proposition "$2 > 3 \Leftrightarrow 1 < 4$" est fausse.

Remarque
- $(*)$: Faire attention !
- En logique pure, on utilise plutôt les symboles $\neg$, $\wedge$, $\vee$, $\rightarrow$ et $\leftrightarrow$.
- Convention pour l'utilisation des parenthèses dans les formules :

$$\text{non} \quad > \quad \text{et}, \text{ou} \quad > \quad \Rightarrow, \Leftrightarrow \quad (> \quad \forall, \exists).$$

- Cette liste de connecteurs et redondante et peut tous les retrouver à partir de deux d'entre eux, par exemple « non » et « et ».
- Attention : quand on écrira « Proposition. On a : », il faudra lire « Les propositions qui suivent sont valides : ».

Proposition 1.1.5 Si $\mathcal{P}$, $\mathcal{Q}$ et $\mathcal{R}$ sont des propositions, on a
1. non non $\mathcal{P} \Leftrightarrow \mathcal{P}$,
2. $\mathcal{P}$ et $\mathcal{Q} \Leftrightarrow \mathcal{Q}$ et $\mathcal{P}$,
3. $\mathcal{P}$ ou $\mathcal{Q} \Leftrightarrow \mathcal{Q}$ ou $\mathcal{P}$,
4. ($\mathcal{P}$ et $\mathcal{Q}$) et $\mathcal{R} \Leftrightarrow \mathcal{P}$ et ($\mathcal{Q}$ et $\mathcal{R}$),
5. ($\mathcal{P}$ ou $\mathcal{Q}$) ou $\mathcal{R} \Leftrightarrow \mathcal{P}$ ou ($\mathcal{Q}$ ou $\mathcal{R}$),
6. non($\mathcal{P}$ ou $\mathcal{Q}$) $\Leftrightarrow$ non $\mathcal{P}$ et non $\mathcal{Q}$,
7. non($\mathcal{P}$ et $\mathcal{Q}$) $\Leftrightarrow$ non $\mathcal{P}$ ou non $\mathcal{Q}$,
8. $\mathcal{P}$ et ($\mathcal{Q}$ ou $\mathcal{R}$) $\Leftrightarrow$ ($\mathcal{P}$ et $\mathcal{Q}$) ou ($\mathcal{P}$ et $\mathcal{R}$),
9. $\mathcal{P}$ ou ($\mathcal{Q}$ et $\mathcal{R}$) $\Leftrightarrow$ ($\mathcal{P}$ ou $\mathcal{Q}$) et ($\mathcal{P}$ ou $\mathcal{R}$),
10. ($\mathcal{P} \Rightarrow \mathcal{Q}$) $\Leftrightarrow$ non $\mathcal{P}$ ou $\mathcal{Q}$,
11. non($\mathcal{P} \Rightarrow \mathcal{Q}$) $\Leftrightarrow$ $\mathcal{P}$ et non $\mathcal{Q}$ (*),
12. ($\mathcal{P} \Rightarrow \mathcal{Q}$) $\Leftrightarrow$ (non $\mathcal{Q} \Rightarrow$ non $\mathcal{P}$),
13. ($\mathcal{P} \Leftrightarrow \mathcal{Q}$) $\Leftrightarrow$ ($\mathcal{Q} \Leftrightarrow \mathcal{P}$),
14. ($\mathcal{P} \Leftrightarrow \mathcal{Q}$) $\Leftrightarrow$ (($\mathcal{P} \Rightarrow \mathcal{Q}$) et ($\mathcal{Q} \Rightarrow \mathcal{P}$)),
15. ($\mathcal{P} \Leftrightarrow \mathcal{Q}$) $\Leftrightarrow$ (non $\mathcal{P} \Leftrightarrow$ non $\mathcal{Q}$).

Démonstration. Il suffit d'élaborer les tables de vérité. Montrons par exemple la

tautologie numérotée 11) :

$\mathcal{P}$	Q	non $\mathcal{Q}$	$\mathcal{P} \Rightarrow \mathcal{Q}$	non$(\mathcal{P} \Rightarrow \mathcal{Q})$	$\mathcal{P}$ et non $\mathcal{Q}$	équivalence (11)
V	V	F	V	F	F	V
V	F	V	F	V	V	V
F	V	F	V	F	F	V
F	F	V	V	F	F	V

Les autres sont laissées en exercice. ■

Remarque
- La *règle du tiers exclus* est la tautologie "$\mathcal{P}$ ou non $\mathcal{P}$".
- La *règle d'inférence* est la tautologie "$\mathcal{P}$ et $(\mathcal{P} \Rightarrow \mathcal{Q}) \Rightarrow \mathcal{Q}$".
- Le *raisonnement par l'absurde* est la tautologie "non non $\mathcal{P} \Rightarrow \mathcal{P}$".
- La *disjonction des cas* est la tautologie "$(\mathcal{P} \Rightarrow \mathcal{Q})$ et (non $\mathcal{P} \Rightarrow \mathcal{Q}) \Rightarrow \mathcal{Q}$".

Exemple Disjonction des cas : on veut montrer que $n(n+1)$ est pair. Si n est pair, c'est gagné. Sinon, c'est $n+1$ qui est pair et on gagne aussi.

Remarque
- La *contraposée* de l'implication "$\mathcal{P} \Rightarrow \mathcal{Q}$" est l'implication "non $\mathcal{Q} \Rightarrow$ non $\mathcal{P}$" (qui lui est équivalente).
- La *réciproque* de l'implication "$\mathcal{P} \Rightarrow \mathcal{Q}$" est l'implication "$\mathcal{Q} \Rightarrow \mathcal{P}$".
- La *négation* de l'implication "$\mathcal{P} \Rightarrow \mathcal{Q}$" n'est *pas* une implication, c'est : "$\mathcal{P}$ et non $\mathcal{Q}$".
- Dans l'*implication* $\mathcal{P} \Rightarrow \mathcal{Q}$, on dit que $\mathcal{P}$ est l'*hypothèse* et que Q est la *conclusion*. Attention : lorsque l'hypothèse est fausse, l'implication est *vraie* même si la conclusion est fausse !
- Au lieu de dire "$\mathcal{P} \Rightarrow \mathcal{Q}$", on dit aussi que $\mathcal{P}$ est *suffisant* pour $\mathcal{Q}$ ou que $\mathcal{Q}$ est *nécessaire* pour $\mathcal{P}$ (ne pas confondre) ou encore : *si* $\mathcal{P}$ *alors* $\mathcal{Q}$.
- Au lieu de "$\mathcal{P} \Leftrightarrow \mathcal{Q}$", on dit aussi que $\mathcal{P}$ est *nécessaire et suffisant* pour $\mathcal{Q}$ ou encore : $\mathcal{P}$ *si et seulement si* $\mathcal{Q}$.

Exemple
1. La contraposée de l'implication "$n < 2 \Rightarrow n \leq 3$" est l'implication "$n > 3 \Rightarrow n \geq 2$" (qui est *aussi* vraie - attention, il faut un quantificateur pour dire ça).
2. La réciproque de l'implication "$n < 2 \Rightarrow n \leq 3$" est l'implication "$n \leq 3 \Rightarrow n < 2$" (qui elle est *fausse*).
3. La négation de l'implication "$n < 2 \Rightarrow n \leq 3$" est "$n < 2$ et $n > 3$" (qui est bien sûr fausse).
4. Il *suffit* que $n < 2$ pour que $n \leq 3$ et il est *nécessaire* que $n \leq 3$ pour que $n < 2$.
5. Pour que $n > 2$, il est nécessaire et suffisant que $n \geq 3$.

Dans la suite du cours, on utilisera librement toutes les tautologies (ce sont des théorèmes puisque n'importe qui peut faire une table de vérité pour les vérifier). On dira aussi souvent simplement « $\mathcal{P}$ » au lieu de « $\mathcal{P}$ est vraie » (par exemple, on dira que « $2 > 3$ » au lieu de « $2 > 3$ est vrai ».

1.2 Quantificateurs

Lorsque $\mathcal{P}$ est une proposition qui dépend (ou pas) d'une variable, on note $\mathcal{P}(a)$ la proposition obtenue en remplaçant la variable par a dans $\mathcal{P}$. On dit que a *satisfait la propriété* $\mathcal{P}$ si $\mathcal{P}(a)$ est vraie (c'est-à-dire un théorème).

Exemple Si $\mathcal{P} :=$ "$n \geq 2$", on peut considérer $\mathcal{P}(3) :=$ "$3 \geq 2$" ou $\mathcal{P}(1) :=$ "$1 \geq 2$". Mais on peut aussi considérer $\mathcal{P}(m) :=$ "$m \geq 2$", $\mathcal{P}(n+1) :=$ "$n+1 \geq 2$" ou même $\mathcal{P}(n) :=$ "$n \geq 2$" $= \mathcal{P}$.

Définition 1.2.1 Si $\mathcal{P}$ est une proposition qui dépend de $x \in E$, alors [a]
1. la proposition [b] "$\forall x \in E, \mathcal{P}(x)$" est vraie si la proposition $\mathcal{P}(x)$ est toujours vraie (quelle que soit la valeur de $x \in E$),
2. la proposition "$\exists x \in E, \mathcal{P}(x)$" est vraie si la proposition $\mathcal{P}(x)$ est parfois vraie (pour au moins une valeur de $x \in E$).

a. L'utilisation des virgules n'est pas nécessaire.
b. On devrait écrire "$\forall x\ x \in E \Rightarrow \mathcal{P}(x)$" - et de même pour $\exists$.

Remarque
- Pour que cette définition en soit effectivement une (c'est-à-dire qu'elle introduit du nouveau vocabulaire), il faut mentionner que $\forall$ est le *quantificateur universel* et que $\exists$ est le *quantificateur existentiel*.
- Ne pas confondre la proposition "$\forall x \in E, \mathcal{P}(x)$" qui ne dépend *pas* de x (et idem avec $\exists$) et la proposition $\mathcal{P}(x)$, qui elle dépend de x (on dira parfois *propriété* au lieu de proposition pour insister sur ce fait).
- On écrira parfois [2] $\forall x, y \in E$ au lieu de $\forall x \in E, \forall y \in E$ et idem avec $\exists$.
- Il est parfois pratique [3] d'écrire $\exists! x \in E, \mathcal{P}(x)$ pour exprimer qu'il existe un *unique* x dans E qui satisfait la propriété $\mathcal{P}$. Cela signifie donc que

$$\exists x \in E, \quad \mathcal{P}(x) \text{ et } (\forall y \in E, \mathcal{P}(y) \Rightarrow x = y).$$

Proposition 1.2.2 Si $\mathcal{P}$ est une proposition qui dépend de $x \in E$, alors
1. non $(\forall x \in E, \mathcal{P}(x)) \Leftrightarrow (\exists x \in E, \text{non } \mathcal{P}(x))$,
2. non $(\exists x \in E, \mathcal{P}(x)) \Leftrightarrow (\forall x \in E, \text{non } \mathcal{P}(x))$.

Démonstration. Dire que "non $(\forall x \in E, \mathcal{P}(x))$" est vraie signifie que "$\forall x \in E, \mathcal{P}(x)$" est fausse, c'est-à-dire que $\mathcal{P}(x)$ n'est pas toujours vraie ou encore que $\mathcal{P}(x)$ est parfois fausse, ce qui s'énonce aussi en disant que "non $\mathcal{P}(x)$" est parfois vraie, ou finalement que "$\exists x \in E, \text{non } \mathcal{P}(x)$" est vraie. La seconde assertion se montre de la même manière mais on peut aussi appliquer la première équivalence à "non $\mathcal{P}(x)$" : on a la suite d'équivalence

$$\begin{aligned}(\text{non } (\exists x \in E, \mathcal{P}(x)) &\Leftrightarrow (\text{non } (\exists x \in E, \text{non non} \mathcal{P}(x))) \\ &\Leftrightarrow (\text{non non } (\forall x \in E, \text{non } \mathcal{P}(x))) \\ &\Leftrightarrow (\forall x \in E, \text{non } \mathcal{P}(x)).\end{aligned}$$

■

2. On dispose aussi de la notation cartésienne $\forall (x, y) \in E^2$ qui est plus juste mais un peu lourde.
3. Attention, ce n'est pas un quantificateur.

Exemple La négation de

$$\forall x \in \mathbb{R}, \forall \varepsilon \in \mathbb{R}_{>0}, \exists \eta \in \mathbb{R}_{>0}, \forall y \in \mathbb{R}, |x-y| \leq \eta \Rightarrow |f(x)-f(y)| \leq \varepsilon$$

(f est continue sur $\mathbb{R}$) est

$$\exists x \in \mathbb{R}, \exists \varepsilon \in \mathbb{R}_{>0}, \forall \eta \in \mathbb{R}_{>0}, \exists y \in \mathbb{R}, |x-y| \leq \eta \text{ et } |f(x)-f(y)| > \varepsilon.$$

Pour montrer que la fonction

$$f(x) = \begin{cases} 0 & \text{si } x \neq 0 \\ 1 & \text{si } x = 0 \end{cases}$$

n'est pas continue, on fait (remplir les cases) : « Posons $x = \boxed{0}$. Posons $\epsilon = \boxed{1/2}$. Soit η un réel strictement positif. Posons $y = \boxed{\eta}$. On a $|x-y| \boxed{= |0-\eta| = \eta} \leq \eta$ et $|f(x)-f(y)| \boxed{= |0\text{-}1| = 1} > \boxed{1/2 =} \epsilon$ ».

On peut aussi considérer les fonctions

$$f(x) = \begin{cases} \sin \frac{1}{x} & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases} \quad \text{ou} \quad f(x) = \begin{cases} x \sin \frac{1}{x} & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases}$$

Il est alors difficile de dire si celles-ci sont continues ou pas.

On conclut avec le raisonnement par récurrence :

Théoreme 1.2.3 Si $\mathcal{P}$ est une proposition qui dépend de $n \in \mathbb{Z}_{\geq 0}$, alors

$$(\forall n \in \mathbb{Z}_{\geq 0}, \mathcal{P}(n)) \Leftrightarrow \mathcal{P}(0) \text{ et } \forall n \in \mathbb{Z}_{\geq 0}, \mathcal{P}(n) \Rightarrow \mathcal{P}(n+1).$$

Démonstration. Pour montrer l'équivalence, on montre l'implication ainsi que sa réciproque. Pour montrer l'implication, on suppose l'hypothèse satisfaite et on montre que les deux conclusions le sont aussi. Pour la première, il suffit de remarquer que $0 \in \mathbb{Z}_{\geq 0}$. Pour la seconde, il suffit de montrer que si $n \in \mathbb{Z}_{\geq 0}$ alors $\mathcal{P}(n+1)$ est vraie mais cela résulte du fait qu'alors $n+1 \in \mathbb{Z}_{\geq 0}$. Pour montrer l'implication réciproque, on considère en fait la contraposée (de la réciproque) :

$$(\exists n \in \mathbb{Z}_{\geq 0}, \text{non } \mathcal{P}(n)) \Rightarrow \text{non } \mathcal{P}(0) \text{ ou } \exists n \in \mathbb{Z}_{\geq 0}, \mathcal{P}(n) \text{ et non } \mathcal{P}(n+1).$$

On suppose donc qu'il existe n tel que $\mathcal{P}(n)$ soit fausse et on désigne alors par n_0 le plus petit de ces entiers naturels. Si $n_0 = 0$, on voit que $\mathcal{P}(0)$ est fausse et on a fini. Sinon, on pose $n = n_0 - 1$. On voit alors que $\mathcal{P}(n)$ est vraie puisque $n < n_0$ alors que $\mathcal{P}(n+1) = \mathcal{P}(n_0)$ est fausse. ■

Remarque

- Il s'agit du *principe de récurrence*. La condition $\mathcal{P}(0)$ est *l'initialisation* et la condition "$\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$" est *l'hérédité*.
- On peut aussi commencer la récurrence à n'importe quel $n = n_0 \in \mathbb{Z}$ au lieu de $n = 0$: il suffit de remplacer $\mathcal{P}$ par $\mathcal{P}(n - n_0)$.
- En pratique, on écrit :

« Montrons par récurrence sur $n \geq n_0$ que $\mathcal{P}(n)$ (est vrai).
Initialisation : Montrons que $\mathcal{P}(n_0)$ (est vrai). $\boxed{\cdots}$.
Hérédité : Soit $n \geq n_0$. Supposons que $\mathcal{P}(n)$ (est vrai). Montrons que $\mathcal{P}(n+1)$ (est alors aussi vrai). $\boxed{\cdots}$ ».

- On dispose aussi de la variante très utile suivante

$$(\forall n \in \mathbb{Z}_{\geq 0}, \mathcal{P}(n)) \Leftrightarrow (\forall n \in \mathbb{Z}_{\geq 0}, ((\forall m \in \mathbb{Z}_{\geq 0}, m < n \Rightarrow \mathcal{P}(m)) \Rightarrow \mathcal{P}(n)).$$

- On dispose enfin de la récurrence descendante qui sert à montrer une impossibilité

$$(\forall n \in \mathbb{Z}_{\geq 0}, \text{non } \mathcal{P}(n)) \Leftrightarrow (\forall n \in \mathbb{Z}_{\geq 0}, (\mathcal{P}(n) \Rightarrow (\exists m \in \mathbb{Z}_{\geq 0}, m < n \text{ et } \mathcal{P}(m)).$$

Exemple Comme application du raisonnement par récurrence, on veut montrer que $100! \geq 2^{100}$, c'est-à-dire [4] que

$$100 \times 99 \times \cdots \times 3 \times 2 \times 1 \geq \underbrace{2 \times \cdots \times 2}_{100 \text{ fois}}.$$

On va montrer en fait par récurrence sur l'entier naturel $n \geq 4$ que $n! \geq 2^n$. On a $4! = 24 \geq 16 = 2^4$ et si $n \geq 4$ est un entier naturel qui satisfait $n! \geq 2^n$, on aura bien

$$(n+1)! = (n+1)n! \geq 5n! \geq 5 \times 2^n \geq 2 \times 2^n = 2^{n+1}$$

(attention : l'hérédité fonctionne pour $n \geq 1$ mais l'initialisation ne peut commencer qu'à $n = 4$). On a donc montré que notre assertion est valide pour toute valeur de $n \geq 4$ et donc en particulier dans le cas $n = 100$.

4. On rappelle que $n!$ est le produit de tous les entiers naturels non nuls inférieurs (ou égaux) à n.

1.3 Exercices (21 août 2023)

Exercice 1.1 Les propositions suivantes sont elles des tautologies ?

1. $\mathcal{P}$ ou non $\mathcal{Q}$,
2. $(\mathcal{P} \Rightarrow \mathcal{Q}) \Leftrightarrow$ non ($\mathcal{P}$ et non $\mathcal{Q}$),
3. $(\mathcal{P} \Rightarrow \mathcal{Q})$ et $(\mathcal{Q} \Rightarrow \mathcal{R}) \Rightarrow (\mathcal{P} \Rightarrow \mathcal{R})$,
4. (non $\mathcal{P} \Rightarrow$ non $\mathcal{Q}$) $\Leftrightarrow (\mathcal{P} \Rightarrow \mathcal{Q})$.

Exercice 1.2 Parmi les propositions suivantes, quelle est la négation de "$\mathcal{P} \Rightarrow \mathcal{Q}$" ?

1. $\mathcal{Q} \Rightarrow \mathcal{P}$,
2. non $\mathcal{P} \Rightarrow$ non $\mathcal{Q}$,
3. $\mathcal{P}$ ou non $\mathcal{Q}$,
4. $\mathcal{P}$ et non $\mathcal{Q}$.

Exercice 1.3

1. Donner une condition suffisante mais pas nécessaire pour qu'un entier naturel soit strictement plus grand que dix.
2. Donner une condition nécessaire mais pas suffisante pour qu'un entier naturel soit (exactement) divisible par six.

Exercice 1.4 Parmi les assertions suivantes relatives à une application $f : \mathbb{R} \to \mathbb{R}$, quelle est la contraposée de "f croissante $\Rightarrow f(3) \geq f(2)$" ?

1. $f(3) \geq f(2) \Rightarrow f$ croissante,
2. $f(3) < f(2) \Rightarrow f$ pas croissante,
3. f pas croissante $\Rightarrow f(3) < f(2)$.

Exercice 1.5 La proposition $\forall x \in \mathbb{R}, x > 1 \Rightarrow x^2 > 1$ est elle vraie ? Qu'en est-il des propositions

$$2 > 1 \Rightarrow 2^2 > 1, \quad 0 > 1 \Rightarrow 0^2 > 1 \quad \text{et} \quad (-2) > 1 \Rightarrow (-2)^2 > 1?$$

Exercice 1.6 Pour chacune des formules suivantes, écrire sa négation et décider (démonstration) si cela a un sens de leur validité respective :

1. $\exists n \in \mathbb{Z}_{\geq 0}, \forall m \in \mathbb{Z}_{\geq 0}, m \leq n$,
2. $\forall n \in \mathbb{Z}_{\geq 0}, \exists m \in \mathbb{Z}_{\geq 0}, m \leq n$,
3. $\exists x \in \mathbb{R}, x + y > 0$,
4. $\forall x \in \mathbb{R}, x + y > 0$,
5. $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x + y > 0$,
6. $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y > 0$,
7. $\exists x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y > 0$,
8. $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, x + y > 0$.

Exercice 1.7 Pour chacune des assertions suivantes relatives à une application $f : \mathbb{R} \to \mathbb{R}$, écrire la formule correspondante ainsi que sa négation et donner deux exemples qui satisfont l'assertion ainsi que deux autres qui ne la satisfont pas :

1. f est positive,
2. f est croissante,
3. f est croissante et positive,
4. f prend parfois des valeurs positives,
5. f est strictement positive,
6. f est paire.

Exercice 1.8 Montrer par contraposition les propriétés suivantes :

1. "Un entier naturel dont le carré est pair est automatiquement pair lui même",

2. “Un nombre réel dont le carré vaut deux est toujours strictement inférieur à deux”.

Exercice 1.9 Montrer par l'absurde les assertions suivantes :
1. “Zéro est le seul réel positif qui est inférieur à tout réel strictement positif”,
2. “La racine carrée de deux n'est pas un nombre entier”.

Exercice 1.10 On considère la propriété $\mathcal{P}$:=“$2^n > n^2$”.
1. Montrer que pour tout entier $n \geq 3$, on a $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$.
2. Pour quelles valeurs de l'entier naturel n a-t-on $\mathcal{P}(n)$?

Exercice 1.11
1. Montrer que si n est un entier naturel tel que $4^n + 5$ est un multiple entier de 3, alors il en va de même de $4^{n+1} + 5$.
2. Pour quelles valeurs de l'entier naturel n, le nombre $4^n + 5$ est-il un multiple entier de 3 ?
3. Montrer que si n est un entier naturel tel que $10^n + 7$ est un multiple entier de 9, alors il en va de même de $10^{n+1} + 7$.
4. Pour quelles valeurs de l'entier naturel n, le nombre $10^n + 7$ est-il un multiple entier de 9 ?

Exercice 1.12 Montrer par récurrence que pour tout réel positif x et pour tout entier naturel n, on a $(1+x)^n \geq 1 + nx$.

Exercice 1.13 Montrer par récurrence que les formules suivantes sont valides pour tout entier naturel n (non nul en ce qui concerne la dernière) :
1. $1 + 3 + 5 + \cdots + (2n+1) = (n+1)^2$,
2. $1 + 2 + 3 + \cdots + n = \dfrac{n(n+1)}{2}$,
3. $1 + 4 + 9 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$,
4. $-1 + 4 - 9 + \cdots + (-1)^n n^2 = (-1)^n \dfrac{n(n+1)}{2}$,
5. $\dfrac{1}{2} + \dfrac{1}{6} + \dfrac{1}{12} + \cdots + \dfrac{1}{n(n+1)} = \dfrac{n}{n+1} \quad (n \neq 0)$.

2. Ensembles

Nous choisissons une approche concrète de la notion d'ensemble et ne traitons pas du tout de la Théorie des ensembles proprement dite (voir [Kri07] ou [Bou70]) qui permet d'interpréter tous les objets mathématiques comme étant eux-même des ensembles.

2.1 Ensembles et sous-ensembles

Définition 2.1.1 Un *ensemble*[a] E est une « collection[b] d'objets » x appelés les *éléments* de E. On dit alors que x *appartient* à E et on écrit $x \in E$. Sinon, on écrit $x \notin E$.

a. Ce que nous définissons ici est en fait la relation d'appartenance.
b. On se place dans un *univers* fixé (et on ne considère que les petits ensembles) afin d'éviter les paradoxes.

Remarque
- Deux ensembles sont égaux si et seulement si ils ont les mêmes éléments.
- On peut décrire un ensemble :
  1. en *extension* : en donnant une liste de ses éléments,
  2. en *compréhension* : en donnant une propriété qui les caractérise.
- Passer d'une écriture en compréhension à une écriture en extension (trouver la solution à un problème) ou le contraire (modéliser un problème) forment les deux défis principaux à relever en mathématiques.
- On représente généralement les ensembles à l'aide de *diagrammes de Venn*, appelés aussi communément des *patates*.
- Attention : la collection de tous les ensembles n'est pas un ensemble (paradoxe de Russel).

Exemple 1. $\{1\}$, $\{2\}$ et $\{1, 2\}$ sont des ensembles distincts (*singletons* et *paire*).

2. $\{1,2\}$, $\{2,1\}$ et $\{1,2,2\}$ désignent le *même* ensemble (c'est une paire).
3. $\emptyset$ désigne l'ensemble vide (qui n'a aucun élément).
4. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ désignent respectivement l'ensemble des entiers relatifs, des nombres rationnels, des nombres réels et des nombres complexes.
5. Nous utiliserons des décorations explicites pour les autres ensembles de nombres et désignerons par exemple par $\mathbb{Z}_{\geq 0}$ l'ensemble des entiers naturels et par $\mathbb{R}_{>0}$ l'ensemble des réels strictement positifs.
6. $\{x \in \mathbb{R} \ / \ x^2 = 1\}$ (compréhension) désigne le *même* ensemble que $\{1,-1\}$ (extension).
7. $\{(x,y) \in \mathbb{R}^2 \ / \ x = y\}$ (compréhension) désigne le *même* ensemble que $\{(t,t) : t \in \mathbb{R}\}$ (extension).

Définition 2.1.2 Un ensemble E est *contenu* (ou *inclus*) dans un ensemble F si tout élément de E est aussi un élément de F. On écrit alors $E \subset F$ et on dit aussi que E est une *partie* ou un *sous-ensemble* de F. Sinon, on écrit $E \not\subset F$.

Remarque

- On a donc

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

- En pratique, on se donnera deux sous-ensembles disons A et B d'un ensemble donné E et on aura alors

$$A \subset B \Leftrightarrow \forall x \in E, x \in A \Rightarrow x \in B.$$

- On a toujours $\emptyset \subset E$.
- On écrit aussi $E \subsetneq F$ pour $E \subset F$ et $E \neq F$.

Exemple

1. $\emptyset \subsetneq \{1\} \subsetneq \{1,2\}$.
2. $\mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$: en effet $1/2 \notin \mathbb{Z}$, $\sqrt{2} \notin \mathbb{Q}$ et $i \notin \mathbb{R}$.

Proposition 2.1.3 Si E, F et G sont trois ensembles, alors

1. $E \subset E$,
2. $E \subset F$ et $F \subset G \Rightarrow E \subset G$,
3. $E \subset F$ et $F \subset E \Leftrightarrow E = F$.

Démonstration.

1. Clair.
2. On suppose que $E \subset F$ et $F \subset G$. Si $x \in E$, on aura nécessairement $x \in F$ et cette condition implique que $x \in G$. On voit ainsi que $E \subset G$.
3. Laissé en exercice. ■

Remarque Ces propriétés stipulent que l'inclusion est une *relation d'ordre* (réflexive, transitive et antisymétrique).

Exemple Pour montrer que les ensembles $E := \{x \in \mathbb{R} \ / \ x^2 = 1\}$ et $F := \{1,-1\}$ sont égaux, on montre

1. que $E \subset F$ (analyse) : si $x^2 = 1$, alors $(x-1)(x+1) = x^2 - 1 = 0$ si bien que $x - 1 = 0$ ou $x + 1 = 0$ et donc $x = 1$ ou $x = -1$,
2. puis que $F \subset E$ (synthèse) : on a $1^2 = 1$ et $(-1)^2 = 1$.

2.2 Opérations sur les ensembles

Définition 2.2.1 Soient E et F deux ensembles. Alors,
1. leur *intersection* est l'ensemble $E \cap F$ des éléments qui sont à la fois dans E et dans F,
2. leur *union* est l'ensemble $E \cup F$ des éléments qui sont soit dans E ou dans F (ou dans les deux).

Remarque
- On a donc

$$x \in E \cap F \Leftrightarrow x \in E \text{ et } x \in F$$

et

$$x \in E \cup F \Leftrightarrow x \in E \text{ ou } x \in F$$

- On a bien sûr

$$E \cap F \subset E \subset E \cup F \quad \text{et} \quad E \cap F \subset F \subset E \cup F.$$

Exemple
1. $\{1,2\} \cap \{1,3\} = \{1\}$ et $\{1,2\} \cup \{1,3\} = \{1,2,3\}$.
2. $[1,3] \cap [2,4] = [2,3]$ et $[1,3] \cup [2,4] = [1,4]$.

Proposition 2.2.2 Si E, F et G sont des ensembles, alors
1. $E \cap \emptyset = \emptyset$,
2. $E \cap E = E$,
3. $E \cap F = F \cap E$,
4. $(E \cap F) \cap G = E \cap (F \cap G)$,
5. $E \cup \emptyset = E$,
6. $E \cup E = E$,
7. $E \cup F = F \cup E$,
8. $(E \cup F) \cup G = E \cup (F \cup G)$,
9. $E \cap (F \cup G) = (E \cap F) \cup (E \cap G)$,
10. $E \cup (F \cap G) = (E \cup F) \cap (E \cup G)$.

Démonstration. Pour montrer l'assertion 9 par exemple, il suffit de désigner par $\mathcal{P}$, $\mathcal{Q}$ et $\mathcal{R}$ respectivement les conditions $x \in E$, $x \in F$ et $x \in G$ et d'utiliser la tautologie

$$\mathcal{P} \text{ et } (\mathcal{Q} \text{ ou } \mathcal{R}) \Leftrightarrow (\mathcal{P} \text{ et } \mathcal{Q}) \text{ ou } (\mathcal{P} \text{ et } \mathcal{R}).$$

Les autres résultats (laissés en exercice) s'obtiennent de la même manière (ou plus directement). ■

Remarque
- On écrira $E \cap F \cap G$ et $E \cup F \cup G$ sans les parenthèses puisqu'il n'y a pas d'ambiguïté.
- On dit que E et F sont *disjoints* si $E \cap F = \emptyset$.

- On définit aussi leur *différence* comme étant l'ensemble $E \setminus F$ des éléments qui sont dans E mais pas dans F (on réservera en pratique cette notation au cas $F \subset E$).
- On considère aussi parfois la *différence symétrique*

$$E \Delta F := (E \cup F) \setminus (E \cap F) = (E \setminus F) \cup (F \setminus E)$$

formée des éléments qui sont soit dans E, soit dans F, mais pas dans les deux.

Définition 2.2.3 Si A est une partie d'un ensemble E, son *complémentaire* dans E est l'ensemble

$$A^{\mathrm{c}} := \complement_E A := E \setminus A$$

des éléments qui sont dans E mais pas dans A.

Remarque
- On a donc

$$\forall x \in E, \quad x \in A^{\mathrm{c}} \Leftrightarrow x \notin A.$$

- Attention : n'utiliser la notation A^{c} (ou parfois aussi $\overline{A}$) que lorsque l'ensemble E est fixé.

Exemple
1. Si $E = \{1, 2\}$ et $A = \{1\}$, alors $A^{\mathrm{c}} = \{2\}$.
2. Si $E = [1, 3]$ et $A = [1, 2]$, alors $A^{\mathrm{c}} =]2, 3]$.
3. Si E est l'ensemble des entiers naturels et A est l'ensemble des nombres pairs, alors A^c est l'ensemble des nombres impairs.

Proposition 2.2.4
1. Si A est une partie d'un ensemble E, on a $(A^c)^c = A$,
2. Si A et B sont deux parties d'un ensemble E, on a

$$A \setminus B = A \cap B^c,$$

3. Si A et B sont deux parties d'un ensemble E, on a

$$(A \cap B)^{\mathrm{c}} = A^{\mathrm{c}} \cup B^{\mathrm{c}} \quad \text{et} \quad (A \cup B)^{\mathrm{c}} = A^{\mathrm{c}} \cap B^{\mathrm{c}}.$$

Démonstration.
1. Utiliser la tautologie non non $\mathcal{P} \Leftrightarrow \mathcal{P}$ avec $\mathcal{P}$:="$x \in A$",
2. Les deux ensembles sont définis par les mêmes conditions,
3. Conséquences immédiates de tautologies (exercice). ■

Définition 2.2.5 Le *produit (cartésien)* de deux ensembles E et F est l'ensemble $E \times F$ des *couples*[a] (x, y) avec $x \in E$ et $y \in F$.

a. Formellement, on a $(x, y) := \{x, \{x, y\}\}$.

Remarque
- On a donc $(x, y) \in E \times F \Leftrightarrow x \in E$ et $y \in F$.
- On a $(x, y) = (x', y') \Leftrightarrow x = x'$ et $y = y'$.

- Ne pas confondre paire et couple : on a $(1,2) \neq (2,1)$ et $(1,1)$ est bien un couple.
- On a $E \times F \neq F \times E$ sauf s'ils sont égaux ou si l'un des deux est vide : $E \times \emptyset = \emptyset \times F = \emptyset$.
- On peut aussi considérer l'ensemble $E \times F \times G$ des triplets si G est un autre ensemble (et au delà).

Exemple 1. $\{1,2\} \times \{3,4\} = \{(1,3),(1,4),(2,3),(2,4)\}$.
2. $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$.
3. On dispose de l'axe des abscisses

$$Ox := \{(x,0) : x \in \mathbb{R}\} = \{(x,y) \in \mathbb{R}^2 \ / \ y = 0\} \subset \mathbb{R}^2$$

et de l'axe des ordonnées

$$Oy := \{(0,y) : y \in \mathbb{R}\} = \{(x,y) \in \mathbb{R}^2 \ / \ x = 0\} \subset \mathbb{R}^2.$$

On a alors $\mathbb{R}_{\neq 0} \times \mathbb{R}_{\neq 0} = \mathbb{R}^2 \setminus (Ox \cup Oy)$.

2.3 Applications

Définition 2.3.1 Une *application*[a] $f : E \to F$ est une méthode qui permet d'associer à *tout* élément x de E *un* élément $f(x)$ de F. On dit que E est la *source* ou l'*ensemble de départ* de f et que F le *but* ou l'*ensemble d'arrivée*. On dit que $f(x)$ est l'*image* de x et que x est un *antécédent* de $f(x)$. Au lieu de $y = f(x)$, on écrira aussi $f : x \mapsto y$ (ne pas confondre avec $f : E \to F$).

a. Rigoureusement, c'est le triplet formé de la source, du but et du *graphe*.

Exemple 1. On peut définir une application

$$f : \{1,2\} \to \{3,4\}, \quad 1 \mapsto 3, \quad 2 \mapsto 3.$$

2. Les fonctions numériques classiques fournissent des applications (polynomiales, rationnelles, exponentielle, logarithme, trigonométriques, etc.) – attention : c'est le *domaine de définition* qui devient par défaut la source de l'application (par exemple $\ln : \mathbb{R}_{>0} \to \mathbb{R}$).
3. Si $E \subset F$, on peut considérer l'application d'inclusion $E \hookrightarrow F, x \mapsto x$. Dans le cas $E = F$, c'est l'*identité* Id_E de E.
4. On dispose d'une unique application $\emptyset \to E$ appelée application vide mais d'aucune application $E \to \emptyset$ (sauf si $E = \emptyset$).

Remarque • Deux applications f et g sont égales si et seulement si elles ont même source, disons E, même but, et que

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

- Le *graphe* d'une application f est l'ensemble $\{(x, f(x)) : x \in E\} \subset E \times F$. Une fois fixés E et F, il revient au même de se donner f ou son graphe.

- Ne pas confondre une application avec une *fonction* qui associe à *certains* éléments de E un élément de F (on rencontre aussi des fonctions *multivaluées* qui peuvent associer *plusieurs* éléments de F au même élément de E).
- Au lieu d'écrire $f(x)$, on devrait écrire $x.f$ comme font les informaticiens pour indiquer que la variable x subit la méthode f.

Définition 2.3.2 Une application $f : E \to F$ est
1. *injective* si $\forall x, x' \in E, f(x) = f(x') \Rightarrow x = x'$,
2. *surjective* si $\forall y \in F, \exists x \in E, f(x) = y$,
3. *bijective* si elle est à la fois injective et surjective.

Remarque
- L'injectivité dit que deux éléments distincts ne peuvent pas avoir la même image,
- la surjectivité dit que tout élément du but a au moins un antécédent,
- la bijectivité dit que tout élément du but a exactement un antécédent (voir ci-dessous).

Exemple
1. L'application $\exp : \mathbb{R} \to \mathbb{R}$ est injective mais pas surjective,
2. L'application $\mathbb{R} \to \mathbb{R}, x \mapsto x^3 - x$ est surjective mais pas injective,
3. L'application $\mathbb{R} \to \mathbb{R}, x \mapsto x^2$ n'est ni injective ni surjective,
4. L'application $\mathbb{R} \to \mathbb{R}, x \mapsto x^3$ est bijective.

Proposition 2.3.3 Une application $f : E \to F$ est bijective si et seulement si pour tout $y \in F$, il existe un unique $x \in E$ tel que $f(x) = y$.

Démonstration. Si f est bijective, alors elle est surjective. Donc, si $y \in F$, il existe au moins un $x \in E$ tel que $f(x) = y$. De plus, si on a aussi $f(x') = y$, alors nécessairement $f(x) = y = f(x')$ et donc $x = x'$ car f est injective. D'où l'unicité de l'antécédent. Inversement, si la condition est satisfaite, f est bien surjective et si $x, x' \in E$ satisfont $f(x) = f(x')$, on a nécessairement $x = x'$ par unicité. ■

Définition 2.3.4 On dit alors que l'application $f^{-1} : F \to E$ qui envoie y sur x est l'*application réciproque* de F.

Exemple
1. Si $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^3$, alors $f^{-1} : \mathbb{R} \to \mathbb{R}, x \mapsto \sqrt[3]{x}$.
2. Si $f : \mathbb{R}_{>0} \to \mathbb{R}, x \mapsto \ln(x)$, alors $f^{-1} : \mathbb{R} \to \mathbb{R}_{>0}, x \mapsto e^x$.

Remarque
- Si f est bijective, on a

$$\forall x \in E, \forall y \in F, \quad y = f(x) \Leftrightarrow f^{-1}(y) = x.$$

- Attention : si f n'est *pas* bijective, il n'existe *pas* d'application réciproque.

2.4 Composition

Définition 2.4.1 Si $f : E \to F$ et $g : F \to G$, sont deux applications, leur *composée* est l'application $g \circ f : E \to G$ définie par

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

Remarque
- Attention : la composition se fait « à l'envers ».
- Si on écrivait $x.f$ au lieu de $f(x)$, on écrirait aussi $f.g$ au lieu de $g \circ f$ et on aurait $x.(f.g) = (x.f).g$, ce qui serait plus léger et plus naturel.
- Si $A \subset E$, la *restriction* à A de $f : E \to F$ est la composée

  $$g := f_{|A} : A \hookrightarrow E \to F.$$

  On dit alors aussi que f est *un prolongement* de g à E (il y a en général plusieurs prolongements).

Exemple
1. Considérons

   $$f : \{1, 2, 3\} \to \{4, 5\}, \quad f(1) = f(2) = 4, f(3) = 5$$

   et

   $$g : \{4, 5\} \to \{6, 7\}, \quad g(4) = g(5) = 6.$$

   On aura alors

   $$g \circ f : \{1, 2, 3\} \to \{6, 7\}, \quad (g \circ f)(1) = (g \circ f)(2) = (g \circ f)(3) = 6.$$

2. Soient $f, g : \mathbb{R} \to \mathbb{R}$ données par $f(x) = x^2$ et $g(x) = x - 1$. On a alors $(g \circ f)(x) = x^2 - 1$ et $(f \circ g)(x) = (x - 1)^2$.
3. Soit

   $$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = 0 \text{ si } x \neq 0, f(0) = 1.$$

   La restriction de f à $\mathbb{R}_{>0}$ est l'application nulle $0 : \mathbb{R}_{>0} \to \mathbb{R}$. On peut la prolonger par continuité en 0 pour trouver l'application nulle $0 : \mathbb{R} \to \mathbb{R}$ qui est différente de f (ce sont deux prolongement *distincts* de la *même* application).

Proposition 2.4.2
1. Si $f : E \to F$ est une application, on a

   $$\mathrm{Id}_F \circ f = f \quad \text{et} \quad f \circ \mathrm{Id}_E = f,$$

2. si $f = E \to F$, $g : F \to G$ et $h : G \to H$ sont trois applications, on a

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

Démonstration. La première assertion est triviale et la seconde est immédiate : si $x \in E$, alors

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

Remarque On écrira simplement $h \circ g \circ f$ sans les parenthèses car il n'y a pas d'ambiguïté.

Proposition 2.4.3 La composée de deux applications injectives (resp. surjectives, resp. bijectives) l'est aussi.

Démonstration. On se donne deux applications $f = E \to F$ et $g : F \to G$.

1. (injectivité) Supposons que $x, x' \in E$ satisfont $(g \circ f)(x) = (g \circ f)(x')$. Si on pose $y = f(x)$ et $y' = f(x')$, on a donc $g(y) = g(f(x)) = (g \circ f)(x) = (g \circ f)(x') = g(f(x')) = g(y')$. Si g est injective, ça implique que $y = y'$, c'est-à-dire $f(x) = f(x')$, et si f aussi est injective, on aura donc $x = x'$.
2. (surjectivité) On se donne $z \in G$. Si g est surjective, il existe $y \in F$ tel que $g(y) = z$ et si f est surjective, il existe $x \in E$ tel que $f(x) = y$. On aura donc $(g \circ f)(x) = g(f(x)) = g(y) = z$.
3. (bijectivité) Résulte des deux autres cas. ■

Remarque On peut aussi montrer que si $g \circ f$ est injective (resp. surjective), alors f (resp. g) l'est aussi. Mais $g \circ f$ peut être bijective sans que ni f ni g ne le soient.

Exemple Les applications

$$f : \mathbb{R}_{\geq 0} \to \mathbb{R}, x \mapsto \sqrt{x} \quad \text{et} \quad g : \mathbb{R} \to \mathbb{R}_{\geq 0}, x \mapsto x^2$$

ne sont bijectives ni l'une ni l'autre mais leur composée $g \circ f$ est l'identité de $\mathbb{R}_{\geq 0}$ qui est bijective.

Proposition 2.4.4 Une application $f : E \to F$ est bijective si et seulement s'il existe une application $g : F \to E$ telle que $g \circ f = \mathrm{Id}_E$ et $f \circ g = \mathrm{Id}_F$. On a alors $g = f^{-1}$.

Démonstration. Montrons tout d'abord que l'on aura nécessairement $g = f^{-1}$ lorsque f est bijective. En effet, si $y \in F$, on a $f(g(y)) = (f \circ g)(y) = y$ et donc (par définition de f^{-1}), on aura $g(y) = f^{-1}(y)$. Montrons maintenant que f^{-1} satisfait bien la condition. En effet, si $x \in E$, on a $f(x) = f(x)$ et donc $f^{-1}(f(x) = x$ et si $y \in F$, on a $f^{-1}(y) = f^{-1}(y)$ et donc $f(f^{-1}(y)) = x$. Réciproquement, supposons l'existence de g. Si l'on prend $y \in F$, on aura $f(g(y)) = y$, ce qui montre que f est surjective. Et si $x, x' \in E$ satisfont $f(x) = f(x')$, on aura alors $x = g(f(x)) = g(f(x')) = x'$ et f est aussi injective. ■

Remarque Si on se donne deux applications $f : E \to F$ et $g : F \to E$, alors f est bijective et g est sa réciproque si et seulement si

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

Proposition 2.4.5
1. Si $f : E \to F$ est bijective, alors f^{-1} aussi et on a $(f^{-1})^{-1} = f$,
2. Si $f : E \to F$ et $g : F \to G$ sont bijectives, alors $(g \circ f$ aussi et on a$)$ $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Démonstration. 1. En effet, on aura bien $f \circ f^{-1} = \mathrm{Id}_F$ et $f^{-1} \circ f = \mathrm{Id}_E$.

2. En effet, on aura bien

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ \mathrm{Id}_F \circ f = f^{-1} \circ f = \mathrm{Id}_E$$

ainsi que

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ (f^{-1}) \circ g^{-1} = g \circ \mathrm{Id}_F \circ g^{-1} = g \circ g^{-1} = \mathrm{Id}_G. \blacksquare$$

2.5 Exercices (21 août 2023)

Exercice 2.1 Soient E, F, G trois ensembles.
1. Si $E \subset F \cup G$, a-t-on obligatoirement $E \subset F$ ou $E \subset G$?
2. Si $E \cap F \subset G$, a-t-on obligatoirement $E \subset G$ ou $F \subset G$?

Exercice 2.2 Soient A et B deux parties de $\mathbb{Z}_{\geq 0}$ qui se rencontrent (ne sont pas disjointes).
1. Le plus petit élément de $A \cap B$ est-il nécessairement le plus petit élément de A et de B ?
2. Le plus petit élément de $A \cup B$ est-il nécessairement le plus petit élément de A ou de B ?

Exercice 2.3 Soient A et B deux parties d'un ensemble E.
1. Déterminer une condition nécessaire et suffisante sur A et B pour qu'il existe une partie X de E telle que $A \cup X = B$? Déterminer alors toutes ces parties X.
2. Même question avec $A \cap X = B$.

Exercice 2.4 Soient A, B deux parties d'un ensemble E. Montrer que

1. $A \cup B \subset A \cap B \Rightarrow A = B$,
2. $A \cap B^{\mathrm{c}} \neq \emptyset \Rightarrow A \not\subset B$,
3. $A \smallsetminus B = A \Leftrightarrow B \smallsetminus A = B$.

Exercice 2.5 Soient A, B, C trois parties d'un ensemble E. Montrer que
1. $(A \cap B \subset A \cap C \text{ et } A \cup B \subset A \cup C) \Rightarrow B \subset C$,
2. $(A \cap B = A \cap C \text{ et } A \cup B = A \cup C) \Rightarrow B = C$.

Exercice 2.6 Soient E et F deux ensembles.
1. Un sous-ensemble X de $E \cup F$ est-il toujours de la forme $A \cup B$ avec $A \subset E$ et $B \subset F$?
2. Un sous-ensemble X de $E \times F$ est-il toujours de la forme $A \times B$ avec $A \subset E$ et $B \subset F$?

Exercice 2.7 Montrer que le disque unité dans $\mathbb{R}^2$ ne peut pas s'écrire comme produit de deux parties de $\mathbb{R}$.

Exercice 2.8 Les applications suivantes sont-elles injectives ? surjectives ? bijectives ?

1. $f : \mathbb{Z} \to \mathbb{Z}, n \mapsto 2n$,
2. $f : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{>0}, n \mapsto n + 1$,
3. $f : \mathbb{Z} \to \mathbb{Z}, n \mapsto -n$,
4. $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$,
5. $f : \mathbb{R} \to \mathbb{R}_{\geq 0}, x \mapsto x^2$,
6. $f : \mathbb{C} \to \mathbb{C}, z \mapsto z^2$.

Exercice 2.9 Soient $f : E \to F$ et $g : F \to G$ deux applications.
1. Si $g \circ f$ est surjective, f est elle automatiquement surjective ?
2. Si $g \circ f$ est surjective, g est elle automatiquement surjective ?
3. Si $g \circ f$ est injective, f est elle automatiquement injective ?
4. Si $g \circ f$ est injective, g est elle automatiquement injective ?

Exercice 2.10 1. Soient $f : E \to F$ et $g_1, g_2 : F \to G$ trois applications telles que $g_1 \circ f = g_2 \circ f$. A-t-on toujours $g_1 = g_2$? Et si f est injective ? Et si f est surjective ?
2. Soient $f_1, f_2 : E \to F$ et $g : F \to G$ trois applications telles que $g \circ f_1 = g \circ f_2$. A-t-on toujours $f_1 = f_2$? Et si g est injective ? Et si g est surjective ?

Exercice 2.11 On considère les applications $f, g : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ définies respectivement par

$$\forall n \in \mathbb{Z}_{\geq 0}, \quad f(n) = 2n \quad \text{et} \quad g(n) = \begin{cases} \frac{n}{2} & \text{si } n \text{ est pair} \\ \frac{n-1}{2} & \text{si } n \text{ est impair.} \end{cases}$$

Calculer $g \circ f$ et $f \circ g$ et dire pour chacune des applications f, g, $g \circ f$ et $f \circ g$ si elle est injective, surjective ou bijective.

Exercice 2.12 Si $f : E \to E$ est une application et $n \in \mathbb{Z}_{\geq 0}$, on définit f^n par récurrence en posant :

$$f^0 = \mathrm{Id}_E \quad \text{et} \quad \forall n \in \mathbb{Z}_{\geq 0}, f^{n+1} = f^n \circ f.$$

1. Montrer par récurrence que $\forall n \in \mathbb{Z}_{\geq 0}, f^{n+1} = f \circ f^n$.
2. Montrer par récurrence que si f est bijective, alors pour tout $n \in \mathbb{Z}_{\geq 0}$, f^n est aussi bijective et que $(f^n)^{-1} = (f^{-1})^n$.

Exercice 2.13 1. Déterminer une bijection entre $\mathbb{Z}_{\geq 1}$ et $\mathbb{Z}_{\geq 2}$,
2. en déduire une bijection entre $A_1 := \{\frac{1}{n} : n \in \mathbb{Z}_{\geq 1}\}$ et $A_2 := \{\frac{1}{n} : n \in \mathbb{Z}_{\geq 2}\}$,
3. montrer que $[0,1] \setminus A_1 = [0,1[\setminus A_2$,
4. en déduire une bijection entre $[0,1]$ et $[0,1[$.

Exercice 2.14 1. Établir une bijection entre $\mathbb{Z}_{\geq 0}$ et $\mathbb{Z}$ (on pourra compter alternativement les nombres positifs et les nombres négatifs).
2. Établir une bijection entre $\mathbb{Z}_{\geq 0}$ et $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ (on pourra compter les couples en oblique),
3. Établir une bijection entre $\mathbb{Z}_{\geq 0}$ et $\mathbb{Q}_{\geq 0}$ (on pourra sauter les fractions qu'on aura déjà comptées).

3. Nombres complexes

On peut imaginer que le monde visible n'est que la partie émergée d'un monde plus vaste. Par exemple, le monde en trois dimensions que l'on peut observer n'est peut-être qu'une partie d'un monde en six dimensions dont trois nous échappent. Ou bien le temps unidimensionnel peut être vu comme une droite dans un temps bidimensionnel qui peut donc lui être représenté par un plan. Il y aurait donc un temps imaginaire (en plus du temps réel). On se représente habituellement le temps par un nombre réel a qui est un multiple d'une unité fixée (l'année par exemple) à partir d'une origine fixée arbitrairement (la naissance de Jésus Christ par exemple). En bidimensionnel, il faut une unité imaginaire en plus, qu'on notera i et on peut alors se représenter notre temps « complexe » sous la forme « $a + ib$ » ou a et b sont deux nombres réels. De même que l'on peut effectuer des opérations sur les nombres réels, on peut aussi effectuer des opérations sur les nombres complexes. On décide que le nombre i vu comme un temps imaginaire permet de remonter le temps sans revenir sur nos pas par la formule magique $i^2 = -1$ (faire un dessin). Toutes les autres propriétés en résultent alors de manière presque mécanique.

Afin d'illustrer les notions introduites dans ce chapitre, nous nous permettrons d'anticiper un peu sur la partie du cours qui sera consacrée à la géométrie plane.

3.1 Définition

Définition 3.1.1 Un *(nombre) complexe*[a] est un nombre de la forme $z =$"$a + ib$" avec $a, b \in \mathbb{R}$. On dit que a est la *partie réelle* de z et on écrit $\mathrm{Re}(z)$. On dit que b est la *partie imaginaire* de z et on écrit $\mathrm{Im}(z)$.

a. D'un point de vue purement théorique, on peut voir un nombre complexe comme un couple de réels (a, b) et notre notation a une fonction essentiellement suggestive. Aussi, le mot *complexe* est à prendre dans le sens de *composé*, pas dans celui de *compliqué*.

On désigne par $\mathbb{C}$ l'ensemble des nombres complexes.

Remarque
- Notons que nous n'avons pas encore introduit d'opération sur les nombres complexes et que « $a + ib$ » n'est pour l'instant qu'une notation : c'est la *forme algébrique* de z.
- Si u est le vecteur de composantes (a, b) dans le plan (rapporté à une base), on dit que $z := a + ib$ est l'*affixe* du vecteur u (on obtient ainsi une bijection entre $\mathbb{C}$ et le plan vectoriel).
- Si M est le point de coordonnées (a, b) dans le plan (rapporté à un repère), on dit que $z := a + ib$ est l'*affixe* du point M (on obtient ainsi une bijection entre $\mathbb{C}$ et le plan affine).
- On dit que z est *réel* si $b = 0$ (et on écrit alors $z = a$) et que z est *imaginaire pur* si $a = 0$ (et on écrit alors $z = ib$). Géométriquement, cela correspond à l'axe des abscisses et à celui des ordonnées.
- On dit aussi parfois qu'un nombre complexe est *imaginaire* s'il n'est pas réel. Attention : la partie imaginaire d'un nombre complexe est un *réel* (c'est bien b et pas ib).

Exemple
1. Les nombres 0, 1, -1, $\sqrt{2}$ et π sont des nombres réels, et donc aussi des nombres complexes.
2. Les nombres i , $-i := i(-1)$ et $i2\pi$ sont des nombres imaginaires purs, et donc aussi complexes).
3. Les nombres $1 + i, -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ sont des nombres imaginaires, et donc aussi complexes, mais ce ne sont pas des imaginaires purs.
4. Le nombre 0 est l'unique nombre qui est à la fois réel et imaginaire pur (mais pas imaginaire !).

Proposition 3.1.2 Si $z, w \in \mathbb{C}$, on a

$$z = w \Leftrightarrow \begin{cases} \mathrm{Re}(z) = \mathrm{Re}(w) \\ \mathrm{Im}(z) = \mathrm{Im}(w) \end{cases}.$$

Démonstration. Par définition. ■

Définition 3.1.3 Si $z = a + ib$ avec $a, b \in \mathbb{R}$ et $w = c + id$ avec $c, d \in \mathbb{R}$, sont deux nombres complexes, leur *somme* est le nombre complexe

$$z + w := (a + c) + i(b + d).$$

Remarque
- L'opération qui consiste à *ajouter* des *termes* pour obtenir leur *somme* est l'*addition*.
- Le symbole $+$ sert à la fois dans l'écriture des nombres complexes, ainsi que pour représenter une somme de nombres réels ou de nombres complexes : heureusement, ces notations sont compatibles : $a + ib$ est bien la somme de a et de ib.

Proposition 3.1.4 Si $z, w \in \mathbb{C}$, on a

$$\mathrm{Re}(z+w) = \mathrm{Re}(z) + \mathrm{Re}(w) \quad \text{et} \quad \mathrm{Im}(z+w) = \mathrm{Im}(z) + \mathrm{Im}(w).$$

Démonstration. Résulte immédiatement des définitions (exercice). ■

Proposition 3.1.5 On a
1. $\forall z_1, z_2 \in \mathbb{C}, \quad z_1 + z_2 = z_2 + z_1$,
2. $\forall z_1, z_2, z_3 \in \mathbb{C}, \quad (z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$,
3. $\forall z \in \mathbb{C}, \quad z + 0 = z$,
4. $\forall z \in \mathbb{C}, \exists -z \in \mathbb{C}, \quad z + (-z) = 0$.

Démonstration. Résulte des propriétés analogues des réels (exercice). ■

Remarque
- La proposition exprime que $\mathbb{C}$ est un *groupe abélien* pour l'addition (respectivement commutatif, associatif, avec élément neutre et avec élément symétrique).
- On écrira tout simplement $z_1 + z_2 + z_3$ (sans mettre de parenthèses) car il n'y a pas d'ambiguïté.
- Si $z = a + ib$, on a donc $-z = (-a) + i(-b)$: c'est l'*opposé* de z.
- La *différence* entre deux nombre complexes z et w est

$$z - w := z + (-w)$$

(la *soustraction* est l'opération qui associe à deux *termes* leur *différence*).
- Si v_1 et v_2 sont deux vecteurs d'affixes z_1 et z_2, alors l'affixe de $v_1 \pm v_2$ est $z_1 \pm z_2$.
- Si M, N sont deux points d'affixes z, w, alors le vecteur $\overrightarrow{MN}$ a pour affixe $w - z$.

Exemple
1. $\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) + \left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right) = -1$
2. $(1+i) + (-1+i) + \cdots + ((-1)^n + i) = \frac{1 + (-1)^n}{2} + in$

Définition 3.1.6 Si $z = a + ib$ avec $a, b \in \mathbb{R}$ et $\lambda \in \mathbb{R}$, leur *produit (externe)* est $\lambda z := \lambda a + i\lambda b$.

Remarque
- On a alors toujours

$$\mathrm{Re}(\lambda z) = \lambda \mathrm{Re}(z) \quad \text{et} \quad \mathrm{Im}(\lambda z) = \lambda \mathrm{Im}(z).$$

- Si u est le vecteur d'affixe z, alors λu a pour affixe λz. Géométriquement, ça correspond à l'*homothétie* de rapport λ.
- On dispose des propriétés suivantes :
  1. $\forall z \in \mathbb{C}, \quad 1z = z$,
  2. $\forall z, w \in \mathbb{C}, \forall \lambda \in \mathbb{R}, \quad \lambda(z+w) = \lambda z + \lambda w$,
  3. $\forall z \in \mathbb{C}, \forall \lambda, \mu \in \mathbb{R}, \quad (\lambda+\mu)z = \lambda z + \mu z$,
  4. $\forall z \in \mathbb{C}, \forall \lambda, \mu \in \mathbb{R}, \quad (\lambda\mu)z = \lambda(\mu z)$.
- $\mathbb{C}$ est un *espace vectoriel réel* (groupe abélien ainsi que ces quatre propriétés).

Définition 3.1.7 Si $z = a + ib$ avec $a, b \in \mathbb{R}$, alors son *conjugué* est $\overline{z} := a - ib$.

Proposition 3.1.8 On a [a]
1. $\forall z \in \mathbb{C}, \quad \mathrm{Re}(\overline{z}) = \mathrm{Re}(z)$ et $\mathrm{Im}(\overline{z}) = -\mathrm{Im}(z)$,
2. $\forall z \in \mathbb{C}, \quad \mathrm{Re}(z) = \dfrac{z+\overline{z}}{2}$ et $\mathrm{Im}(z) = \dfrac{z-\overline{z}}{2i}$,
3. $\forall z, w \in \mathbb{C}, \quad \overline{z+w} = \overline{z} + \overline{w}$,
4. $\forall z \in \mathbb{C}, \quad \overline{\overline{z}} = z$.

a. Attention : la division par un imaginaire ne sera définie que plus tard.

Démonstration. Résulte immédiatement des définitions (exercice). ■

Remarque
- On a aussi $\overline{z-w} = \overline{z} - \overline{w}$ et $\overline{\lambda z} = \lambda \overline{z}$ si $\lambda \in \mathbb{R}$,
- La conjugaison complexe correspond à la *réflexion verticale* (c'est-à-dire symétrie par rapport à l'axe des abscisses).
- On a $z = \overline{z}$ si et seulement si z est réel et $z = -\overline{z}$ si et seulement si z est imaginaire pur.

3.2 Multiplication

Définition 3.2.1 Si $z = a + ib$ avec $a, b \in \mathbb{R}$ et $w = c + id$ avec $c, d \in \mathbb{R}$ sont deux nombres complexes, leur *produit* est le nombre complexe

$$z \times w := (ac - bd) + i(ad + bc).$$

Remarque
- La *multiplication* est l'opération qui associe à deux *facteurs* leur *produit*.
- En pratique, on écrira $zw := z \times w$ exactement comme pour les réels.
- On remarquera que $i^2 = i \times i = -1$. En fait, cette multiplication est l'unique multiplication (qui fait de $\mathbb{C}$ un corps) telle que $i^2 = -1$.
- Comme toujours, par convention, la multiplication sera prioritaire sur l'addition.

Proposition 3.2.2 On a
1. $\forall z_1, z_2 \in \mathbb{C}, \quad z_1 \times z_2 = z_2 \times z_1$,
2. $\forall z_1, z_2, z_3 \in \mathbb{C}, \quad (z_1 \times z_2) \times z_3 = z_1 \times (z_2 \times z_3)$,
3. $\forall z \in \mathbb{C}, \quad z \times 1 = z$,

4. $\forall z \in \mathbb{C}_{\neq 0}, \exists z^{-1} \in \mathbb{C}_{\neq 0}, \quad z \times z^{-1} = 1,$
5. $\forall z_1, z_2, z_3 \in \mathbb{C}, \quad z_1 \times (z_2 + z_3) = z_1 \times z_2 + z_1 \times z_3.$

Démonstration. Mis à part l'existence de l'inverse, il s'agit de vérifications élémentaires (laissées en exercice). Si $z = a + ib$ avec $a, b \in \mathbb{R}$, est non nul, on a $a \neq 0$ ou $b \neq 0$ si bien que $a^2 + b^2 \neq 0$. On vérifie alors que

$$(a+ib) \times \left(\frac{a}{a^2+b^2} + i\frac{-b}{a^2+b^2} \right)$$

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

Remarque

- On écrira tout simplement $z_1 \times z_2 \times z_3$ sans mettre de parenthèses car il n'y a pas d'ambiguïté.
- $\mathbb{C}$ est un *corps* (groupe abélien ainsi que ces cinq propriétés ($\mathbb{C}_{\neq 0}$ est un groupe abélien pour la multiplication + la distributivité)).
- On définit le *quotient*[1] de deux nombre complexes z et $w \neq 0$ par la formule

  $$\frac{z}{w} = z \times w^{-1}$$

  (l'opération correspondante est la *division*).
- Si $z \neq 0$, on dit que z^{-1} (ou de manière équivalente $1/z$) est l'*inverse* de z. On a toujours $(z^{-1})^{-1} = z$ et $(z \times w)^{-1} = z^{-1} \times w^{-1}$.
- Deux vecteurs u_1 et u_2 d'affixes z_1 et z_2 sont *colinéaires* (resp. *orthogonaux*) si et seulement si z_2/z_1 est réel (resp. imaginaire pur) ou si $z_1 = 0$.
- Si M_1, M_2, M_3 ont pour affixes z_1, z_2, z_3, alors le *triangle* $\{M_1, M_2, M_3\}$ est *plat* (resp. *rectangle* en M_1) si et seulement si $\dfrac{z_3 - z_1}{z_2 - z_1}$ est réel (resp. imaginaire pur) ou bien $z_1 = z_2$.

Exemple

1. $\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)\left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right) = \left(\frac{1}{4} + \frac{3}{4}\right) + i\left(\frac{\sqrt{3}}{4} - \frac{\sqrt{3}}{4}\right) = 1.$
2. $\dfrac{1-i}{1+i} = \dfrac{(1-i)(1-i)}{(1+i)(1-i)} = \dfrac{1-2i+(-1)}{1-(-1)} = \dfrac{-2i}{2} = -i.$

Proposition 3.2.3 On a $\forall z, w \in \mathbb{C}, \quad \overline{z \times w} = \overline{z} \times \overline{w}.$

Démonstration. Clair (exercice). $\blacksquare$

Remarque

- On en déduit que si $z \neq 0$, alors $\overline{z^{-1}} = \overline{z}^{-1}$ et donc aussi que

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

  lorsque $w \neq 0$.
- On vérifie aussi aisément que

  $$z \times \overline{z} = \mathrm{Re}(z)^2 + \mathrm{Im}(z)^2.$$

1. On ne parlera pas de *fraction* qui est une notion plus subtile.

Définition 3.2.4 Soit $z \in \mathbb{C}$ et $n \in \mathbb{Z}_{\geq 0}$. La *puissance* n-ème de z est définie par récurrence en posant $z^0 = 1$ et $z^{n+1} = z^n \times z$. Si $z \neq 0$, la puissance $(-n)$-ème de z est on pose $z^{-n} := (z^{-1})^n$.

Exemple 1. $i^4 = 1$.
2. $(1+i)^{-2} = -\dfrac{i}{2}$.

Proposition 3.2.5 1. $\forall z \in \mathbb{C}_{\neq 0}, \forall m, n \in \mathbb{Z}, \quad z^{m+n} = z^m \times z^n$,
2. $\forall z \in \mathbb{C}_{\neq 0}, \forall m, n \in \mathbb{Z}, \quad (z^m)^n = z^{mn}$,
3. $\forall z, w \in \mathbb{C}_{\neq 0}, \forall n \in \mathbb{Z}, \quad (z \times w)^n = z^n \times w^n$,

Démonstration. Montrons tout d'abord la seconde assertion dans le cas $m = -1$. Lorsque $n = 0$, c'est clair, lorsque $n > 0$, il suffit d'appliquer la définition à $-n$ et lorsque $n < 0$, il suffit d'appliquer la définition à z^{-1}.

Montrons maintenant la première assertion. On suppose d'abord que $m + n \geq 0$. Par symétrie, on peut alors supposer que $n \geq 0$ et procéder par récurrence sur n. On a bien sûr

$$z^{m+0} = z^m = z^m \times 1 = z^m \times z^0.$$

De plus, si on suppose que $z^{m+n} = z^m \times z^n$, on aura

$$z^{m+n+1} = z^{m+n} \times z = z^m \times z^n \times z = z^m \times z^{n+1}.$$

Si on suppose maintenant que $m + n < 0$, on aura

$$z^{m+n} = (z^{-1})^{-m-n} = (z^{-1})^{-m}(z^{-1})^{-n} = z^m z^n.$$

Les autres assertions se démontrent exactement de la même façon (exercice) ■

Remarque
- La démonstration de ces résultats utilise uniquement le fait que $\mathbb{C}_{\neq 0}$ est un groupe abélien pour la multiplication et pas une seule fois la définition des nombres complexe. La démonstration est donc identique en tout point à celle de la proposition analogue sur $\mathbb{R}$.
- On peut aussi montrer que

$$\forall z \in \mathbb{C}_{\neq 0}, \forall n \in \mathbb{Z}, \quad \overline{z^n} = \overline{z}^n.$$

- On peut inclure le cas $z = 0$ dans les différentes formules si on se limite aux entiers positifs :
  1. $\forall z \in \mathbb{C}, \forall m, n \in \mathbb{Z}_{\geq 0}, \quad z^{m+n} = z^m \times z^n$,
  2. $\forall z \in \mathbb{C}, \forall m, n \in \mathbb{Z}_{\geq 0}, \quad (z^m)^n = z^{mn}$,
  3. $\forall z, w \in \mathbb{C}, \forall n \in \mathbb{Z}_{\geq 0}, \quad (z \times w)^n = z^n \times w^n$.
  4. $\forall z \in \mathbb{C}, \forall n \in \mathbb{Z}_{\geq 0}, \quad \overline{z^n} = \overline{z}^n$.

Proposition 3.2.6 1. $\forall z, w \in \mathbb{C}, \forall n \in \mathbb{Z}_{\geq 0}, \quad (z+w)^n = \sum_{k=0}^{n} \binom{n}{k} z^k \times w^{n-k}$
$\left(= z^n + nz^{n-1}w + \frac{n(n-1)}{2} z^{n-2}w^2 + \ldots + nzw^{n-1} + w^n\right)$

2. $\forall z \in \mathbb{C}_{\neq 1}, \forall n \in \mathbb{Z}_{\geq 0}, \quad \dfrac{1-z^{n+1}}{1-z} = \sum_{k=0}^{n} z^k \quad (= 1 + z + z^2 + \cdots + z^n).$

Démonstration. La première est laissée en exercice (démonstration par récurrence). Pour la seconde, on calcule :

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

■

Remarque

- La démonstration de ces résultats utilise uniquement le fait que $\mathbb{C}$ est un corps et pas une seule fois la définition des nombres complexe. La démonstration est donc identique en tout point à celle de la proposition analogue sur $\mathbb{R}$.
- Dans la démonstration précédente, il faut utiliser la définition par récurrence des *coefficients binomiaux* (*triangle de Pascal*)

$$\binom{n}{0} := 1, \quad \binom{0}{k} := 0 \text{ si } k > 0 \quad \text{et} \quad \binom{n+1}{k+1} := \binom{n}{k} + \binom{n}{k+1}.$$

- Il faut aussi utiliser la définition par récurrence des *sommes partielles*

$$\sum_{k=0}^{0} z_k := z_0 \quad \text{et} \quad \sum_{k=0}^{n+1} z_k := \left(\sum_{k=0}^{n} z_k\right) + z_{n+1}.$$

- Pour la seconde, on peut aussi utiliser

$$(1 + z + z^2 + \ldots + z^n) - (z + z^2 + \ldots + z^n + z^{n+1}) = 1 - z^{n+1}.$$

Exemple 1. Si on pose $j := -\dfrac{1}{2} + i\dfrac{\sqrt{3}}{2}$, on a (formule du binôme)

$$j^3 = \left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)^3 = -\frac{1}{8} + 3 \times i\frac{\sqrt{3}}{8} + 3 \times \frac{3}{8} - i\frac{3\sqrt{3}}{8} = \frac{8}{8} = 1,$$

et donc (dernière formule)

$$0 = \frac{1-j^3}{1-j} = 1 + j + j^2,$$

si bien que

$$j^2 = -1 - j = -\frac{1}{2} - i\frac{\sqrt{3}}{2}.$$

2. On a $(2^3)^4 \neq 2^{(3^4)}$: le premier vaut 512 et le second est un nombre à 25 chiffres. On évitera donc d'écrire 2^{3^4} (sans parenthèses).

3.3 Exponentielle complexe

Définition 3.3.1 Si $z = a + ib$ avec $a, b \in \mathbb{R}$ est un nombre complexe, alors l'*exponentielle* de z est

$$e^z := e^a \cos(b) + ie^a \sin(b).$$

Exemple On a $e^{2i\pi} = e^0 = 1$, $e^{i\pi} = -1$, $e^{1+i\pi} = -e$ et $e^{i\frac{\pi}{2}} = i$.

Proposition 3.3.2
1. $e^0 = 1$,
2. $\forall z, w \in \mathbb{C}, \quad e^{z+w} = e^z \times e^w$,

Démonstration. La première assertion est immédiate et la seconde résulte des formules trigonométriques

$$\begin{cases} \cos(\theta_1 + \theta_2) &= \cos(\theta_1)\cos(\theta_2) - \sin(\theta_1)\sin(\theta_2) \\ \sin(\theta_1 + \theta_2) &= \cos(\theta_1)\sin(\theta_2) + \sin(\theta_1)\cos(\theta_2). \end{cases}$$

En effet, si $z = a + ib$ avec $a, b \in \mathbb{R}$ et $w = c + id$ avec $c, d \in \mathbb{R}$, on aura d'un coté

$$e^{z+w} = e^{a+c}(\cos(b+d) + i\sin(b+d))$$

et de l'autre

$$e^z \times e^w = e^a e^c(\cos(b)\cos(d) - \sin(b)\sin(d) + i(\cos(b)\sin(d) + \sin(b)\cos(d))).\blacksquare$$

Remarque
- La proposition dit que l'on a un *homomorphisme de groupes*

$$\mathbb{C} \to \mathbb{C}_{\neq 0}, \quad z \mapsto e^z$$

(avec l'addition sur la source et la multiplication sur le but). Le corollaire qui suit résulte *formellement* de ces propriétés.
- On peut aussi remarquer que pour tout $z \in \mathbb{C}$, on a $\overline{e^z} = e^{\overline{z}}$. Comme conséquence, on en déduit que si $x \in \mathbb{R}$, alors

$$\overline{e^{ix}} = e^{\overline{ix}} = e^{-ix} = \left(e^{ix}\right)^{-1}.$$

Corollaire 3.3.3
1. $\forall z \in \mathbb{C}, \quad e^z \neq 0$ et $e^{-z} = \dfrac{1}{e^z}$,
2. $\forall z, w \in \mathbb{C}, \quad e^{z-w} = \dfrac{e^z}{e^w}$,
3. $\forall z \in \mathbb{C}, \forall n \in \mathbb{Z}, \quad e^{nz} = (e^z)^n$.

Démonstration. 1. On a $e^z \times e^{-z} = e^{z-z} = e^0 = 1 \neq 0$ et donc $e^z \neq 0$.

2. Le même calcul nous montre que $e^{-z} = \dfrac{1}{e^z}$.
3. On a alors $e^{z-w} = e^z \times e^{-w} = \dfrac{e^z}{e^w}$.
4. Le cas $n \geq 0$ se traite par récurrence : on a $e^0 = 1 = (e^z)^0$ et si $e^{nz} = (e^z)^n$ alors

$$e^{(n+1)z} = e^{nz+z} = e^{nz} \times e^z = (e^z)^n \times e^z = (e^z)^{n+1}.$$

Lorsque $n < 0$ (si bien que $-n > 0$), on aura donc

$$e^{nz} = \frac{1}{e^{-nz}} = \frac{1}{(e^z)^{-n}} = (e^z)^n.$$

■

Remarque On dispose des *formules de Moivre*

$$e^{ix} = \cos(x) + i\sin(x) \quad \text{et} \quad e^{-ix} = \cos(x) - i\sin(x)$$

ainsi que des *formules d'Euler*

$$\cos(x) = \frac{e^{ix} + e^{-ix}}{2} \quad \text{et} \quad \sin(x) = \frac{e^{ix} - e^{-ix}}{2i}.$$

Exemple On peut retrouver des formules de trigonométrie :

1. Avec les formules de Moivre :

$$\begin{aligned}\cos(3x) + i\sin(3x) = e^{3ix} = (e^{ix})^3 = (\cos(x) + i\sin(x))^3 = \\ \cos^3(x) + 3i\cos^2(x)\sin(x) - 3\cos(x)\sin^2(x) - i\sin^3(x).\end{aligned}$$

On en déduit que

$$\left\{ \begin{array}{rcccl} \cos(3x) & = & \cos^3(x) - 3\cos(x)\sin^2(x) & = & 4\cos^3(x) - 3\cos(x) \\ \sin(3x) & = & 3\cos^2(x)\sin(x) - \sin^3(x) & = & 3\sin(x) - 4\sin^3(x). \end{array} \right.$$

2. Avec les formules d'Euler :

$$\begin{aligned}\cos^3(x) &= \left(\frac{e^{ix} + e^{-ix}}{2}\right)^3 \\ &= \frac{1}{8}(e^{3ix} + 3e^{ix} + 3e^{-ix} + e^{-3ix}) \\ &= \frac{1}{4}\left(\frac{e^{3ix} + e^{-3ix}}{2} + 3\frac{e^{ix} + e^{-ix}}{2}\right) \\ &= \frac{1}{4}(\cos(3x) + 3\cos(x)).\end{aligned}$$

On peut faire la même chose avec $\sin^3(x)$ et retrouver nos deux formules.

3.4 Module et argument

Proposition 3.4.1 Si $z \in \mathbb{C}_{\neq 0}$, il existe un unique $r \in \mathbb{R}_{>0}$ et un unique $\theta \in \mathbb{R}$ modulo 2π tels que $z = re^{i\theta}$.

Démonstration. En effet, si $z = a + ib$ avec $a, b \in \mathbb{R}$, on peut exprimer le couple (a, b) en coordonnées polaires de manière unique sous la forme $a = r\cos(\theta)$ et $b = r\sin(\theta)$ avec $r \in \mathbb{R}_{>0}$ et $\theta \in \mathbb{R}$ modulo 2π. ■

Remarque
- « modulo 2π » signifie « quitte à ajouter un multiple entier de 2π ». Au lieu de « égaux modulo 2π », on dit plutôt « congrus modulo 2π » et on écrit alors « $\theta_1 \equiv \theta_2 \mod 2\pi$ ».
- On peut fixer $\theta \in [0, 2\pi[$ ou $\theta \in]-\pi, \pi]$ par exemple mais ce choix est artificiel.
- On dit que $z = re^{i\theta}$ est la *forme exponentielle* de z car on peut l'écrire aussi $z = e^{\ln(r)+i\theta}$.
- De manière équivalente, la proposition nous dit que l'homomorphisme

$$\mathbb{C} \to \mathbb{C}_{\neq 0}, \quad z \mapsto e^z$$

est *surjectif* et que son *noyau* est $2i\pi\mathbb{Z} := \{2i\pi n : n \in \mathbb{Z}\}$.

Définition 3.4.2 On dit que r est le *module* de z, et on écrit $|z| = r$, et que $\theta \mod 2\pi$ est son *argument*, et on écrit $\arg(z) \equiv \theta \mod 2\pi$. On pose aussi $|0| = 0$ (mais l'argument de 0 est indéfini).

Exemple $|1| = 1$ et $\arg(1) \equiv 0$; $|-1| = 1$ et $\arg(-1) \equiv \pi$; $|i| = 1$ et $\arg(i) \equiv \pi/2$; $|1+i| = \sqrt{2}$ et $\arg(1+i) \equiv \pi/4$ (modulo 2π à chaque fois).

Remarque
- Si $z = a$ est un nombre réel, alors $|z| = |a|$, c'est-à-dire que le module étend aux complexes la valeur absolue réelle.
- Si $z, w \in \mathbb{C}_{\neq 0}$, on a

$$z = w \Leftrightarrow |z| = |w| \text{ et } \arg(z) \equiv \arg(w) \mod 2\pi.$$

- Les réels r et θ sont exactement les coordonnées *polaires* du vecteur d'affixe z.
- Pour représenter le produit de deux nombres complexes, on multiplie les rayons et on ajoute les angles (faire un dessin).
- L'image du vecteur d'affixe z par l'homothétie de rapport r (resp. la *rotation* d'angle θ) est le vecteur d'affixe rz (resp. $e^{i\theta}z$).
- La multiplication par un complexe correspond à la composée d'une homothétie (rapport = module) et d'une rotation (angle = argument).

Proposition 3.4.3
1. Si $z, w \in \mathbb{C}_{\neq 0}$, alors

$$|z \times w| = |z||w| \quad \text{et} \quad \arg(z \times w) \equiv \arg(z) + \arg(w) \mod 2\pi,$$

2. Si $z \in \mathbb{C}_{\neq 0}$, alors

$$|z^{-1}| = |z|^{-1} \quad \text{et} \quad \arg(z^{-1}) \equiv -\arg(z) \mod 2\pi,$$

3. Si $z, w \in \mathbb{C}_{\neq 0}$, alors

$$\left|\frac{z}{w}\right| = \frac{|z|}{|w|} \quad \text{et} \quad \arg\left(\frac{z}{w}\right) \equiv \arg(z) - \arg(w) \mod 2\pi,$$

4. Si $z \in \mathbb{C}_{\neq 0}$ et $n \in \mathbb{Z}$, alors

$$|z^n| = |z|^n \quad \text{et} \quad \arg(z^n) \equiv n \arg(z) \mod 2\pi,$$

5. Si $z \in \mathbb{C}_{\neq 0}$, alors

$$|\overline{z}| = |z| \quad \text{et} \quad \arg(\overline{z}) \equiv -\arg(z) \mod 2\pi.$$

Démonstration. Montrons la première assertion. On écrit $z = re^{i\theta}$ et $w = se^{i\varphi}$ avec $r, s \in \mathbb{R}_{>0}$ et $\theta, \varphi \in \mathbb{R}$. On a alors

$$z \times w = (re^{i\theta})(se^{i\varphi}) = (rs)(e^{i\theta}e^{i\varphi}) = (rs)e^{i\theta+i\varphi} = (rs)e^{i(\theta+\varphi)}$$

avec $rs \in \mathbb{R}_{>0}$ et $\theta + \varphi \in \mathbb{R}$. On en déduit que

$$|z \times w| = rs = |z||w|$$

et que

$$\arg(z \times w) \equiv \theta + \varphi \equiv \arg(z) + \arg(w) \mod 2\pi.$$

Les autres assertions se démontrent de la même façon et sont laissées en exercice. ■

Remarque
- Les résultats concernant les modules sont encore valides si z (ou w) est nul.
- On a $\arg(-z) \equiv \arg(z \times (-1)) \equiv \arg(z) + \arg(-1) \equiv \arg(z) + \pi \mod 2\pi$.
- Attention : si $\arg(z^n) \equiv \theta \mod 2\pi$, alors $\arg(z) \equiv \dfrac{\theta}{n} \mod \dfrac{2\pi}{n}$.
- Attention : on peut comparer les *modules* de deux nombres complexes z et z' et écrire par exemple $|z| \leq |z'|$ mais on ne compare jamais deux nombres complexes : on réserve la notation $x \leq y$ aux nombres *réels*.

Corollaire 3.4.4 $\forall \zeta \in \mathbb{C}, \forall n \in \mathbb{Z}_{\geq 0}, \quad \zeta^n = 1 \Leftrightarrow \exists k \in \mathbb{Z}, \zeta = e^{\frac{2ik\pi}{n}}$.

Démonstration. On aura

$$\begin{aligned}
\zeta^n = 1 &\Leftrightarrow |\zeta^n| = 1 \text{ et } \arg(\zeta^n) \equiv 0 \mod 2\pi \\
&\Leftrightarrow |\zeta|^n = 1 \text{ et } n\arg(\zeta) \equiv 0 \mod 2\pi \\
&\Leftrightarrow |\zeta| = 1 \text{ et } \arg(\zeta) \equiv 0 \mod \frac{2\pi}{n} \\
&\Leftrightarrow \zeta = e^{\frac{2ik\pi}{n}} \text{ avec } k \in \mathbb{Z}.
\end{aligned}$$

■

Remarque
- On dit alors que ζ est une *racine n-ème de l'unité*.

- En faisant varier k entre 0 et $n-1$, cela correspond géométriquement aux sommets du polygone régulier à n cotés.
- Si $\zeta^n = 1$ et $\zeta \neq 1$, alors $1 + \zeta + \zeta^2 + \cdots + \zeta^{n-1} = 0$.

Exemple
1. On a $e^{\frac{2i\pi}{2}} = -1$ et $1 + (-1) = 0$,
2. On a $e^{\frac{2i\pi}{3}} = j$ et $1 + j + j^2 = 0$ (triangle équilatéral),
3. On a $e^{\frac{2i\pi}{4}} = i$ et $1 + i + i^2 + i^3 = 0$ (carré).

Proposition 3.4.5 On a pour tout $z \in \mathbb{C}$,

$$|z|^2 = z \times \overline{z} \quad (= \mathrm{Re}(z)^2 + \mathrm{Im}(z)^2).$$

Démonstration. La seconde égalité est là pour mémoire et pour la première, il suffit de remarquer que

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

et, si $z \neq 0$,

$$\arg(z \times \overline{z}) \equiv \arg(z) + \arg(\overline{z}) \equiv \arg(z) - \arg(z) \equiv 0.$$ ■

Remarque
- On a $|\mathrm{Re}(z)| \leq |z|$ avec égalité si et seulement si z est réel.
- On a $|\mathrm{Im}(z)| \leq |z|$ avec égalité si et seulement si z est imaginaire pur.

Proposition 3.4.6 On a
1. $\forall z \in \mathbb{C}, \quad z = 0 \Leftrightarrow |z| = 0$,
2. $\forall z, w \in \mathbb{C}, \quad |z + w| \leq |z| + |w|$,
3. $\forall z, w \in \mathbb{C}, \quad |z \times w| = |z||w|$.

Démonstration. Seule la seconde assertion (*inégalité triangulaire*) mérite vraiment une démonstration : on a

$$\begin{aligned} |z+w|^2 &= (z+w)(\overline{z+w}) \\ &= z\overline{z} + w\overline{z} + z\overline{w} + w\overline{w} \\ &= |z|^2 + 2\mathrm{re}(z\overline{w}) + |w|^2 \\ &\leq |z|^2 + 2|z\overline{w}| + |w|^2 \\ &= |z|^2 + 2|z||w| + |w|^2 \\ &= (|z| + |w|)^2. \end{aligned}$$ ■

Remarque
- On a utilisé le fait que deux nombres *positifs* sont dans le même ordre que leurs carrés.
- On a *égalité* triangulaire $|z + w| = |z| + |w|$ si et seulement si $\arg(z) \equiv \arg(w) \mod 2\pi$.
- On aura aussi toujours $||z| - |w|| \leq |z - w|$.
- L'application $z \mapsto |z|$ est ce qu'on appelle une *valeur absolue* (les trois propriétés de la proposition).

Remarque
- Si on désigne par u le vecteur d'affixe z, on a $\|u\| = |z|$ (norme).
- Si on désigne par M et M' les points d'affixes respectifs z et z', alors $MM' = |z' - z|$ (distance).
- Le *cercle* (resp. *disque*) de centre M_0 d'affixe z_0 et de rayon $r \geq 0$ a pour équation $|z - z_0| = r$ (resp. $|z - z_0| \leq r$).
- La *médiatrice* des points M_1 et M_2 d'affixes respectifs z_1 et z_2 a pour équation $|z - z_1| = |z - z_2|$.
- Si on désigne par u_1 et u_2 les vecteurs d'affixes respectifs z_1 et z_2, alors

$$\widehat{(u_1, u_2)} \equiv \arg\left(\frac{z_2}{z_1}\right).$$

- Si on désigne par M_1, M_2 et M_3 les points d'affixes respectifs z_1, z_2 et z_3, alors

$$\widehat{M_2M_1M_3} \equiv \arg\left(\frac{z_3 - z_1}{z_2 - z_1}\right).$$

3.5 Equations algébriques

Lemme 3.5.1 Tout $\alpha \in \mathbb{C}_{\neq 0}$ possède exactement deux racines carrées (opposées) dans $\mathbb{C}_{\neq 0}$.

Démonstration. Il s'agit de résoudre $z^2 = \alpha$, ou de manière équivalente, puisque $\alpha \neq 0$,

$$|z|^2 = |\alpha| \quad \text{et} \quad \arg(z^2) \equiv \arg(\alpha) \mod 2\pi,$$

ce qui nous donne

$$|z| = \sqrt{|\alpha|} \quad \text{et} \quad \arg(z) \equiv \frac{\arg(\alpha)}{2} \mod \pi,$$

et finalement

$$|z| = \sqrt{|\alpha|} \quad \text{et} \quad \arg(z) \equiv \left| \begin{array}{l} \frac{\arg(\alpha)}{2} \\ \frac{\arg(\alpha)}{2} + \pi \end{array} \right. \mod 2\pi. \qquad \blacksquare$$

Remarque
- La *racine carrée* d'un réel *positif* x est l'*unique* réel *positif* dont le carré vaut x. On le note $\sqrt{x}$. On utilise *jamais* cette notation si $x \notin \mathbb{R}_{\geq 0}$.
- La même démonstration montre que α possède exactement n racines n-èmes.

Exemple Trouver les racines carrées de $-8i$ dans $\mathbb{C}$.

1. Méthode multiplicative : on cherche r, θ tels que $(re^{i\theta})^2 = -8i$, c'est-à-dire

$$r^2 = |-8i| = 8 \quad \text{et} \quad 2\theta = \arg(-8i) \equiv -\pi/2 \mod 2\pi.$$

On voit donc que $r = 2\sqrt{2}$ et $\theta \equiv -\pi/4 \mod \pi$, c'est-à-dire $\theta \equiv -\pi/4 \mod 2\pi$ ou $\theta \equiv 3\pi/4 \mod 2\pi$. On trouve donc

$$2\sqrt{2}(\cos(-\pi/4) + i\sin(-\pi/4)) = 2\sqrt{2}\left(\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right) = 2 - 2i$$

et

$$2\sqrt{2}(\cos(3\pi/4) + i\sin(3\pi/4)) = 2\sqrt{2}\left(-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) = -2 + 2i.$$

2. Méthode additive : on cherche $a, b \in \mathbb{R}$ tels que $(a+ib)^2 = -8i$, c'est-à-dire $a^2 - b^2 + 2iab = -8i$. En remarquant que, nécessairement, on aura aussi

$$a^2 + b^2 = |(a+ib)^2| = |-8i| = 8,$$

on est ramenés à résoudre

$$\begin{cases} a^2 + b^2 &= 8 \\ a^2 - b^2 &= 0 \\ 2ab &= -8. \end{cases}$$

On en déduit immédiatement que $a = \pm 2$ et donc que $b = \mp 2$ si bien que les racines sont $2 - 2i$ et $-2 + 2i$.

Proposition 3.5.2 Soient $\alpha, \beta, \gamma \in \mathbb{C}$ avec $\alpha \neq 0$ et $\Delta := \beta^2 - 4\alpha\gamma$. Si $\Delta \neq 0$, alors l'équation $\alpha z^2 + \beta z + \gamma = 0$ a exactement deux solutions

$$\frac{-\beta + \delta_1}{2\alpha} \quad \text{et} \quad \frac{-\beta + \delta_2}{2\alpha},$$

où δ_1 et δ_2 sont *les* deux racines de Δ. Si $\Delta = 0$, alors $\dfrac{-\beta}{2\alpha}$ est l'unique solution.

Démonstration. Classique : on écrit

$$\alpha z^2 + \beta z + \gamma = \alpha\left(\left(z + \frac{\beta}{2\alpha}\right)^2 - \frac{\Delta}{4\alpha^2}\right).$$

Les racines carrées de $z + \dfrac{\beta}{2\alpha}$ sont exactement $\dfrac{\delta_1}{2\alpha}$ et $\dfrac{\delta_2}{2\alpha}$ et on en déduit z. ■

Exemple Pour résoudre $z^2 - 2iz - 1 + 2i = 0$, on calcule

$$\Delta = (-2i)^2 - 4(-1 + 2i) = -8i$$

et on se souvient que ses racines sont $2 - 2i$ et $-2 + 2i$. On en déduit que les racines sont

$$z_1 = \frac{2i + 2 - 2i}{2} = 1 \quad \text{et} \quad z_2 = \frac{2i - 2 + 2i}{2} = -1 + 2i.$$

On aurait aussi pu remarquer que 1 était racine évidente et factoriser

$$z^2 - 2iz - 1 + 2i = (z-1)(z + 1 - 2i). \quad ☺$$

Remarque Si z_1 et z_2 sont les solutions (avec éventuellement $z_1 = z_2$ lorsque $\Delta = 0$) de $\alpha z^2 + \beta z + \gamma = 0$, alors

$$\alpha z^2 + \beta z + \gamma = \alpha(z - z_1)(z - z_2).$$

En particulier, on a

$$z_1 + z_2 = -\frac{\beta}{\alpha} \quad \text{et} \quad z_1 z_2 = \frac{\gamma}{\alpha}.$$

3.6 Exercices (21 août 2023)

Exercice 3.1 Représenter les points M_k d'affixes z_k pour $k = 1, \dots, 5$ avec

$$z_1 = -2, \quad z_2 = 2i, \quad z_3 = 2 + 2i, \quad z_4 = 2 - 2i, \quad z_5 := -2 - 2i.$$

Exercice 3.2 Déterminer la partie réelle et la partie imaginaire de :

1. $z = \dfrac{1}{1+i}$,
2. $z = \dfrac{1+i}{1-i}$,
3. $z = (1+i)^4$,
4. $z = \left(\dfrac{1}{2} - i\dfrac{\sqrt{3}}{2}\right)^3$.

Exercice 3.3 On considère le nombre complexe

$$z = \frac{1}{2} + i\frac{\sqrt{3}}{2}.$$

1. Calculer z^2 et z^3.
2. En déduire z^n pour tout $1 \leq n \leq 6$.
3. En déduire l'inverse z^{-1} de z.
4. En déduire aussi la valeur de $(1 + i\sqrt{3})^5$.
5. En déduire finalement les valeurs de

$$(1 + i\sqrt{3})^5 + (1 - i\sqrt{3})^5 \quad \text{et} \quad (1 + i\sqrt{3})^5 - (1 - i\sqrt{3})^5.$$

Exercice 3.4 On pose $z = 2e^{i\pi/4}$.

1. Déterminer les formes exponentielles de $\overline{z}$, z^{-1}, $-z$ et iz.
2. Représenter tous ces nombres dans le plan complexe.

Exercice 3.5 Donner la forme exponentielle des nombres complexes suivants :

1. $z = 1$,
2. $z = -1$,
3. $z = i$,
4. $z = -i$,
5. $z = 1 + i$,
6. $z = 1 - i$,
7. $z = -1 + i\sqrt{3}$,
8. $z = 1 + i\sqrt{3}$.

Exercice 3.6 Utiliser les formules d'Euler pour linéariser les expressions suivantes :

1. $\cos^5(x)$,
2. $\sin^5(x)$,
3. $\cos^2(3x)\sin^2(5x)$,
4. $\cos^2(x)\sin^4(x)$.

Exercice 3.7 Montrer que $e^{i\frac{\pi}{12}} = \dfrac{e^{i\frac{\pi}{3}}}{e^{i\frac{\pi}{4}}}$. En déduire les valeurs de $\cos(\pi/12)$ et $\sin(\pi/12)$.

Exercice 3.8 Déterminer la forme exponentielle des nombres suivants :

1. $z = (1+i)^9$,
2. $z = (1-i)^7$,
3. $z = \dfrac{(1+i)^9}{(1-i)^7}$.

Exercice 3.9 Montrer que si $a, b \in \mathbb{R}$ satisfont $|a-b| < \pi$, alors le module et l'argument de $z := e^{ia} + e^{ib}$ sont respectivement $r = 2\cos\frac{a-b}{2}$ et $\theta = \frac{a+b}{2}$. Où a-t-on utilisé l'hypothèse ?

Exercice 3.10 Représenter dans le plan complexe l'ensemble des points M dont l'affixe z vérifie la condition suivante :

1. $|z-1| = |z-3-2i|$,
2. $|z-3| = |z-1-i|$,
3. $|z-2+i| = \sqrt{5}$,
4. $|(1+i)z-2-i| = 2$,
5. $|z+3-i| \leq 2$,
6. $|z+3-i| \geq |z|$,
7. $|z| < |z+3-i| < 2$.

Exercice 3.11 Déterminer les racines carrées des nombres complexes suivants :

1. $z = 5+12i$,
2. $z = 1+4\sqrt{5}i$,
3. $z = 1+i\sqrt{3}$.

Exercice 3.12 Résoudre dans $\mathbb{C}$ les équations suivantes

1. $2z^2-6z+5=0$,
2. $5z^2+(9-7i)z+2-6i=0$,
3. $z^2+(2+i)z-1+7i=0$.

Exercice 3.13 Montrer que si $s, p, z_1, z_2 \in \mathbb{C}$, alors z_1 et z_2 sont les solutions de l'équation $z^2 - sz + p = 0$ si et seulement si $z_1+z_2 = s$ et $z_1 z_2 = p$.

Exercice 3.14 Déterminer les racines n-èmes de z dans les cas suivants :

1. $n=3$ et $z = 1+i$,
2. $n=4$ et $z = 4i$,
3. $n=6$ et $z = \dfrac{1-i\sqrt{3}}{1+i}$.

Exercice 3.15 On désigne par $\mathbb{Z}[i]$ l'ensemble des *entiers de Gauss*, c'est-à-dire les nombres qui s'écrivent $m+in$ avec $m, n \in \mathbb{Z}$.

1. Montrer que si $\alpha, \beta \in \mathbb{Z}[i]$, alors $\alpha+\beta \in \mathbb{Z}[i]$ et $\alpha\beta \in \mathbb{Z}[i]$.
2. Montrer que si $\alpha \in \mathbb{Z}[i]$, alors $|\alpha| = 0$ ou $|\alpha| \geq 1$.
3. Déterminer tous les couples d'entiers (m, n) tels que $m^2+n^2 = 1$.
4. Déterminer tous les éléments *inversibles* de $\mathbb{Z}[i]$, c'est-à-dire les nombres complexes non nuls α tels que $\alpha, \alpha^{-1} \in \mathbb{Z}[i]$.

Exercice 3.16

1. Montrer que si $u, v \in \mathbb{C}$ et $x = u+v$, alors $x^3 = 51x+104$ si et seulement si $u^3+v^3+3uv(u+v) = 51(u+v)+104$.
2. En déduire que si $uv = 17$, alors $x^3 = 51x+104$ si et seulement si u^3 et v^3 sont les solutions de $X^2 - 104X + 4913 = 0$.
3. Résoudre cette équation du second degré et montrer que ses solutions sont des cubes d'entiers de Gauss.
4. En déduire que l'équation originale $x^3 = 51x+104$ a une solution entière que l'on déterminera.

4. Géométrie affine

Nous n'aborderons que la géométrie plane, mais sous une forme qui permet une généralisation immédiate des énoncés *et* des démonstrations. En fait, une fois les premières propriétés établies, les énoncés comme les démonstrations ignorent complètement le fait que nous sommes dans le plan cartésien, et pas dans un espace quelconque.

4.1 Vecteurs et points

Définition 4.1.1 Le *plan affine* (resp. *vectoriel*) cartésien [a] est l'ensemble $\mathcal{P}$ (resp. $\overrightarrow{\mathcal{P}}$) des *points* P de *coordonnées* $a, b \in \mathbb{R}$ (resp. des *vecteurs* u de *composantes* $x, y \in \mathbb{R}$).

a. Il s'agit dans un cas comme dans l'autre, de se représenter les points ou les vecteurs par des couples de réels une fois fixé une base ou un repère.

Remarque

- On écrira alors $P\binom{a}{b}$ (resp. $u\binom{x}{y}$).
- Alternativement, on désignera par a_P et b_P les coordonnées de P (resp. par x_u et y_u les composantes de u).
- On mettra parfois une flèche sur les vecteurs $u \in \overrightarrow{\mathcal{P}}$ afin d'aider à la compréhension et on écrira donc $\overrightarrow{u}$ au lieu de u (c'est purement décoratif).
- Cette définition fait jouer un rôle particulier aux vecteurs $\overrightarrow{i}\binom{1}{0}$ et $\overrightarrow{j}\binom{0}{1}$, ainsi qu'au point $O\binom{0}{0}$. Pour insister sur ce fait, on dira que $\overrightarrow{\mathcal{P}}$ (resp. $\mathcal{P}$) est le plan affine rapporté à (ou muni de) la *base* $(\overrightarrow{i}, \overrightarrow{j})$ (resp. au (ou muni du) *repère* $(O, \overrightarrow{i}, \overrightarrow{j})$. On fera un dessin.
- Toutes les définitions qui suivent s'étendent sans difficulté à l'espace (de dimension trois ou plus) et presque tous les énoncés restent alors valables (on peut aussi remplacer $\mathbb{R}$ par n'importe quel corps !).

Définition 4.1.2 Si $u\binom{x}{y}$ et $v\binom{y}{t}$ sont deux vecteurs du plan, leur *somme* est le vecteur $(u+v)\binom{x+z}{y+t}$. Si $u\binom{x}{y}$ est un vecteur du plan et λ un réel, leur *produit* est $(\lambda u)\binom{\lambda x}{\lambda y}$.

Proposition 4.1.3
1. $\forall u, v \in \overrightarrow{\mathcal{P}}, u+v = v+u$,
2. $\forall u, v, w \in \overrightarrow{\mathcal{P}}, (u+v)+w = u+(v+w)$,
3. $\exists \overrightarrow{0} \in \overrightarrow{\mathcal{P}}, \forall u \in \overrightarrow{\mathcal{P}}, u + \overrightarrow{0} = u$,
4. $\forall u \in \overrightarrow{\mathcal{P}}, \exists -u \in \overrightarrow{\mathcal{P}}, u + (-u) = \overrightarrow{0}$,
5. $\forall u \in \overrightarrow{\mathcal{P}}, \forall \lambda, \mu \in \mathbb{R}, (\lambda\mu)u = \lambda(\mu u)$,
6. $\forall u \in \overrightarrow{\mathcal{P}}, 1u = u$,
7. $\forall u, v \in \overrightarrow{\mathcal{P}}, \forall \lambda \in \mathbb{R}, \lambda(u+v) = \lambda u + \lambda v$,
8. $\forall u \in \overrightarrow{\mathcal{P}}, \forall \lambda, \mu \in \mathbb{R}, (\lambda+\mu)u = \lambda u + \mu u$.

Démonstration. Tout cela se vérifie composante par composante. Par exemple, pour montrer l'égalité 7, on doit s'assurer que

$$\begin{cases} \lambda(x_u + x_v) &= \lambda x_u + \lambda x_v \\ \lambda(y_u + y_v) &= \lambda y_u + \lambda y_v. \end{cases}$$

Les autres vérifications sont laissées en exercice. ■

Remarque
- On écrira tout simplement $u+v+w$ car il n'y a pas d'ambiguïté.
- Le vecteur nul $\overrightarrow{0}$ est unique et l'opposé $-u$ de u ne dépend que de u.
- Les vecteurs du plan forment un *espace vectoriel* sur $\mathbb{R}$ (les huit propriétés de l'énoncé).
- La *différence* entre deux vecteurs u et v est $u - v = u + (-v)$.
- On peut toujours simplifier les additions : $u + v = u + w \Rightarrow v = w$.
- De même, $\lambda u = \lambda v \Leftrightarrow \lambda = 0$ ou $u = v$ (et $\lambda u = \mu u \Leftrightarrow u = \overrightarrow{0}$ ou $\lambda = \mu$).
- On dit que $\mathcal{B} := (u, v)$ est une *base* de $\overrightarrow{\mathcal{P}}$ si tout vecteur w s'écrit de manière unique sous la forme $w = \lambda u + \mu v$ avec $\lambda, \mu \in \mathbb{R}$. On dit alors que λ et μ sont les *composantes* du vecteur w *dans la base* $\mathcal{B}$.
- $(\overrightarrow{i}, \overrightarrow{j})$ est une base et les composantes de $u\binom{x}{y}$ dans cette base sont alors justement les *composantes* x et y définies plus haut.

Lemme 4.1.4 Si u, v et w sont trois vecteurs du *plan*, il existe $\lambda, \mu, \nu \in \mathbb{R}$ non tous nuls tels que $\lambda u + \mu v + \nu w = \overrightarrow{0}$.

Démonstration. On doit résoudre le système

$$\begin{cases} \lambda x_u + \mu x_v + \nu x_w = 0 \\ \lambda y_u + \mu y_v + \nu y_w = 0. \end{cases}$$

C'est un système linéaire homogène de deux équations à trois inconnues qui a nécessairement au moins une solution non nulle. Vérifions cela directement. En général, on peut prendre

$$\lambda := x_v y_w - x_w y_v, \quad \mu := x_w y_u - x_u y_w \quad \text{et} \quad \nu := x_u y_v - x_v y_u$$

(la vérification est laissée en exercice). Mais il faut aussi traiter le cas ou ces trois quantités sont nulles. On peut alors toujours supposer par symétrie que $x_u \neq 0$ (sinon $u = v = w = \overrightarrow{0}$ et on peut prendre $\lambda = \mu = \nu = 1$). La dernière condition $x_u y_v - x_v y_u = 0$ implique alors que $x_v u - x_u v + 0w = 0$. ■

Exemple Si $u\binom{1}{-1}$, $v\binom{1}{4}$ et $w\binom{3}{2}$, on a $2u + v - w = 0$.

Remarque
- On dit que u, v, w sont *liés* ou *linéairement dépendants*.
- Attention : dans l'espace, il faut quatre vecteurs, etc.

Définition 4.1.5 Le *translaté* du point $P\binom{a}{b} \in \mathcal{P}$ par le vecteur $u\binom{x}{y} \in \overrightarrow{\mathcal{P}}$ est le point $(P+u)\binom{a+x}{b+y} \in \mathcal{P}$.

Proposition 4.1.6
1. $\forall P \in \mathcal{P}, \quad P + \overrightarrow{0} = P$,
2. $\forall P \in \mathcal{P}, \forall u, v \in \overrightarrow{\mathcal{P}}, \quad (P+u)+v = P+(u+v)$,
3. $\forall P, Q \in \mathcal{P}, \exists! \overrightarrow{PQ} \in \overrightarrow{\mathcal{P}}, \quad Q = P + \overrightarrow{PQ}$.

Démonstration. C'est toujours la même chanson. Par exemple, pour l'assertion 3, on doit résoudre

$$\begin{cases} a_Q = a_P + x \\ b_Q = b_P + y \end{cases}$$

qui a pour unique solution

$$\begin{cases} x = a_Q - a_P \\ y = b_Q - b_P. \end{cases} \tag{4.1}$$

Le reste est laissé en exercice. ■

Remarque
- Les composantes de $\overrightarrow{PQ}$ sont données par les formules (4.1).
- On peut réécrire la proprité (3) sous la forme

$$\forall P, Q \in \mathcal{P}, \forall u \in \overrightarrow{\mathcal{P}}, \quad u = \overrightarrow{PQ} \Leftrightarrow Q = P + u.$$

- On peut alors réécrire la propriété (2) sous la forme

$$\forall P, Q, R \in \mathcal{P}, \quad \overrightarrow{PR} = \overrightarrow{PQ} + \overrightarrow{QR}.$$

  C'est la *relation de Chasles*.
- La propriété (1) s'écrit alors

$$\forall P, Q \in \mathcal{P}, \quad \overrightarrow{PQ} = \overrightarrow{0} \Leftrightarrow P = Q.$$

- On en déduit que

$$\forall P, Q \in \mathcal{P}, \quad \overrightarrow{QP} = -\overrightarrow{PQ}.$$

Remarque
- On dit que $\overrightarrow{\mathcal{P}}$ *agit* ou *opère* sur $\mathcal{P}$ (les deux premières conditions de la proposition) de manière *simplement transitive* (la dernière).
- Si $\mathcal{B} := (u, v)$ est une base de $\overrightarrow{\mathcal{P}}$ et $P \in \mathcal{P}$, on dit que $\mathcal{R} := (P, u, v)$ est un *repère* du plan affine. Les composantes du vecteur $\overrightarrow{PQ}$ dans la base $\mathcal{B}$ s'appellent alors les *coordonnées* du point Q dans le repère $\mathcal{R}$.
- $(O, \overrightarrow{i}, \overrightarrow{j})$ est un repère et les coordonnées de $P\binom{a}{b}$ dans ce repère sont justement ses *coordonnées* a et b définies plus haut.

Exemple Si $P\binom{1}{-2}$, $Q\binom{-3}{4}$ et $R\binom{5}{6}$, alors $\overrightarrow{PQ}\binom{-4}{6}$, $\overrightarrow{QR}\binom{8}{2}$ et $\overrightarrow{PR}\binom{4}{8}$, et on a bien $\overrightarrow{PQ} + \overrightarrow{QR} = \overrightarrow{PR}$.

4.2 Droites

Définition 4.2.1 Un sous-ensemble $\Delta \subset \overrightarrow{\mathcal{P}}$ est une *droite vectorielle* s'il existe $u \in \overrightarrow{\mathcal{P}}$ non nul tel que

$$\Delta = \{\lambda u : \lambda \in \mathbb{R}\}.$$

On dit alors que u est un *vecteur directeur* de Δ.

Proposition 4.2.2 Soit Δ une droite vectorielle. Alors,
1. $\overrightarrow{0} \in \Delta$,
2. $\forall v, w \in \Delta, v + w \in \Delta$,
3. $\forall \mu \in \mathbb{R}, \forall v \in \Delta, \mu v \in \Delta$.

Démonstration. Soit u un vecteur directeur de Δ.
1. On a $\overrightarrow{0} = 0u$,
2. si on écrit $v = \lambda_1 u$ et $w = \mu u$, on a $v + w = (\lambda + \mu)u$,
3. si on écrit $v = \lambda u$, on a $\mu v = (\mu\lambda)u$. ■

Remarque
- On dit que Δ est un *sous-espace vectoriel* de $\mathcal{P}$ (ces trois propriétés).
- Tout élément v de Δ s'écrit de manière unique sous la forme $v = \lambda u$: $\{u\}$ est une *base* de Δ et λ est la *composante* de v dans *cette* base.
- La droite dirigée par $u\binom{\alpha}{\beta}$ a pour *paramétrisation*

$$\begin{cases} x = \lambda\alpha \\ y = \lambda\beta. \end{cases}$$

Cela signifie que

$$v \in \Delta \Leftrightarrow \exists \lambda \in \mathbb{R}, x_v = \lambda\alpha \text{ et } y_v = \lambda\beta \quad \text{(extension)}.$$

- La droite dirigée par $u\binom{\alpha}{\beta}$ a pour *équation* $\beta x - \alpha y = 0$. Cela signifie que

$$v \in \Delta \Leftrightarrow \beta x_v - \alpha y_v = 0 \text{ (compréhension)}.$$

Proposition 4.2.3 Si Δ et Δ' sont deux droites vectorielles, on a soit $\Delta = \Delta'$, ou alors $\Delta \cap \Delta' = \{\overrightarrow{0}\}$.

Démonstration. On désigne par u et u' des vecteurs directeurs de Δ et Δ'. Supposons qu'il existe $v \in \Delta \cap \Delta'$ non nul. On écrit alors $v = \alpha u$ et $v = \alpha' u'$ et on a $\alpha, \alpha' \neq 0$. On en déduit que $u = \frac{\alpha'}{\alpha} u' \in \Delta'$ et donc que $\Delta \subset \Delta'$ (par la troisième propriété ci-dessus). L'autre inclusion par symétrie. ■

Remarque
- Si Δ est une droite vectorielle et $v \in \Delta$ est non nul, alors v est automatiquement un vecteur directeur de Δ.
- Des vecteurs sont dit *colinéaires* s'ils appartiennent à une même droite.
- Deux vecteurs u et v sont colinéaires si et seulement si il existe $\lambda, \mu \in \mathbb{R}$ non tous les deux nuls tels que $\lambda u + \mu v = 0$. On dit aussi qu'ils sont *liés* ou *linéairement dépendants*.
- Deux vecteurs non colinéaires forment toujours une base du plan, et réciproquement.
- On peut aussi définir *un plan* dans l'espace comme étant une partie de la forme

  $$\{\lambda u + \mu v : \lambda \in \mathbb{R}\}.$$

  avec u, v non colinéaires. On dispose alors de la notion de vecteurs *coplanaires*.

Définition 4.2.4 Un sous-ensemble $D \subset \mathcal{P}$ est une *droite (affine)* si l'ensemble

$$\overrightarrow{D} = \{\overrightarrow{PQ} : P, Q \in D\}$$

est une droite vectorielle, appelée *direction* de D. Un vecteur directeur de $\overrightarrow{D}$ sera aussi appelé *vecteur directeur* de D.

Remarque
- Attention : il y a plusieurs façons d'écrire $u = \overrightarrow{PQ}$ avec $P, Q \in D$ lorsque $u \in \overrightarrow{D}$. Par contre, si on *fixe* $P \in D$ et $u \in \overrightarrow{D}$, il existe un *unique* $Q \in D$ tel que $u = \overrightarrow{PQ}$ (c'est $P + u$).
- Si $P \in D$, on a

  $$\overrightarrow{D} = \{\overrightarrow{PQ} : Q \in D\} \quad \text{et} \quad D = \{P + u : u \in \overrightarrow{D}\}.$$

- Soient $P \in D$ et $u \in \overrightarrow{D}$ non nul. Si $Q \in D$, il existe un *unique* $\lambda \in \mathbb{R}$ tel que $\overrightarrow{PQ} = \lambda u$: (P, u) est un *repère* de Δ et λ est la *coordonnée* de Q dans *ce* repère.
- La droite dirigée par $u\binom{\alpha}{\beta}$ et passant par et passant par $P\binom{a}{b}$ a pour *paramétrisation*

  $$\begin{cases} x = \lambda\alpha + a \\ y = \lambda\beta + b. \end{cases}$$

- La droite dirigée par $u\binom{\alpha}{\beta}$ et passant par $P\binom{a}{b}$ a pour équation

  $$\beta x - \alpha y - (\beta a - \alpha b) = 0.$$

- On dit que des points sont *alignés* s'ils appartiennent à une même droite affine.
- Trois points P, Q, R sont alignés si et seulement si les vecteurs $\overrightarrow{PQ}$ et $\overrightarrow{PR}$ sont colinéaires.
- Par deux points distincts P et Q, il passe une droite et une seule que l'on note (PQ). De plus, $\overrightarrow{PQ}$ est alors un vecteur directeur de (PQ).

Exemple Pour tracer une droite affine, il suffit de trouver deux points P et Q sur la droite. Si celle-ci est donnée par une équation, on peut généralement les prendre sur les axes : avec l'équation $2x - 3y + 6 = 0$, on peut choisir $P\binom{-3}{0}$ et $Q\binom{0}{2}$.

Proposition 4.2.5 — Théorème d'incidence. Si D et D' sont deux droites affines, seuls ces différents cas de figure peuvent se présenter :
1. $\exists P \in \mathcal{P}, D \cap D' = \{P\}$,
2. $D \cap D' = \emptyset$,
3. $D = D'$.

Démonstration. Supposons que $D \cap D' \neq \emptyset$ et donc qu'il existe $P \in D \cap D'$. Si $\overrightarrow{D} = \overrightarrow{D'}$, alors

$$D = D' = \{P + u : u \in \overrightarrow{D} \ (= \overrightarrow{D'})\}.$$

Sinon, on sait que $\overrightarrow{D} \cap \overrightarrow{D'} = \{\overrightarrow{0}\}$. Supposons que $Q \in D \cap D'$. On aura alors $\overrightarrow{PQ} \in \overrightarrow{D} \cap \overrightarrow{D'} = \{\overrightarrow{0}\}$ si bien que $P = Q$. ■

Remarque
- Les droites sont alors dites respectivement *sécantes* en P, *disjointes* ou *confondues*.
- On dit plus généralement que des droites affines (trois droites par exemple) sont *concourantes en* P si P est leur unique point commun.

Définition 4.2.6 Deux droites affines D et D' sont *parallèles*, et on écrit alors $D /\!/ D'$, si $\overrightarrow{D} = \overrightarrow{D'}$.

Proposition 4.2.7
1. Si D est une droite affine, alors $D /\!/ D$,
2. Si D, D' et D'' sont trois droites affines, alors $D /\!/ D'$ et $D' /\!/ D'' \Rightarrow D /\!/ D''$,
3. Si D et D' sont deux droites affines, alors $D /\!/ D' \Leftrightarrow D' /\!/ D$.

Démonstration. Immédiat. ■

Remarque
- Par un point donné, il passe une droite et une seule parallèle à une droite donnée.
- Le parallélisme est une *relation d'équivalence* (réflexive, transitive et symétrique).

Proposition 4.2.8 Dans le *plan* affine, deux droites sont soit sécantes, soit parallèles (c'est *faux* dans l'espace).

Démonstration. On se donne deux droites, l'une dirigée par u et passant par P et l'autre dirigée par u' et passant par P'. Puisqu'on est dans le plan, il existe α, α', λ non tous nuls tels que $\alpha u + \alpha' u' + \lambda \overrightarrow{PP'} = \overrightarrow{0}$. Si $\lambda = 0$, alors u et u' sont colinéaires et $D /\!\!/ D'$. Sinon, on peut écrire $\overrightarrow{PP'} = v - v'$ avec $v = -\frac{\alpha}{\lambda} u \in \overrightarrow{D}$ et $v' = \frac{\alpha'}{\lambda} u' \in \overrightarrow{D}'$. Si on pose $Q = P + v \in D$, on a $v = \overrightarrow{PQ}$. On en déduit que $\overrightarrow{P'Q} = \overrightarrow{P'P} + \overrightarrow{PQ} = v' \in \overrightarrow{D}'$ si bien que $Q \in D'$ et $D \cap D' \neq \emptyset$. ■

Définition 4.2.9 Un quadruplet de points (P, Q, R, S) est un *parallélogramme* si $\overrightarrow{PQ} = \overrightarrow{SR}$.

Remarque
- On dit que P, Q, R et S sont les *sommets* du parallélogramme, que $\{P, Q\}$, $\{Q, R\}$, $\{R, S\}$, et $\{P, S\}$ sont les *cotés* et que $\{P, R\}$ et $\{Q, S\}$ sont les *diagonales*.
- Si P, Q, R sont trois points du plan, on dit que $\{P, Q, R\}$ est un *triangle*, que P, Q et R sont les *sommets* et que $\{P, Q\}$, $\{P, R\}$, $\{Q, R\}$ sont les *cotés* (*opposés* à R, Q et P). Le triangle est dit *aplati* si les points P, Q et R sont alignés.

Proposition 4.2.10 Un quadruplet de points *(distincts) non alignés* (P, Q, R, S) est un parallélogramme si et seulement si $(PQ) /\!\!/ (SR)$ et $(PS) /\!\!/ (QR)$.

Démonstration. La condition signifie que les vecteurs $\overrightarrow{PQ}$ et $\overrightarrow{SR}$ d'une part, et $\overrightarrow{PS}$ et $\overrightarrow{QR}$ d'autre part, sont colinéaires. En d'autres termes, on peut écrire

$$\overrightarrow{SR} = \lambda \overrightarrow{PQ} \quad \text{et} \quad \overrightarrow{PS} = \mu \overrightarrow{QR}$$

avec $\lambda, \mu \in \mathbb{R}$. La condition est donc clairement nécessaire puisqu'on peut poser alors $\lambda = 1$ et $\mu = 1$:

$$\overrightarrow{SR} = \overrightarrow{PQ} \quad \text{et} \quad \overrightarrow{PS} = \overrightarrow{PQ} + \overrightarrow{QR} + \overrightarrow{RS} = \overrightarrow{QR}.$$

Réciproquement, on aura

$$\overrightarrow{QR} = \overrightarrow{QP} + \overrightarrow{PS} + \overrightarrow{SR} = -\overrightarrow{PQ} + \mu \overrightarrow{QR} + \lambda \overrightarrow{PQ}$$

si bien que $(1-\mu)\overrightarrow{QR} + (1-\lambda)\overrightarrow{PQ} = 0$. Si $\lambda \neq 1$, alors les vecteurs sont colinéaires et les points P, Q, R sont alignés (et S aussi du coup puisque les droites sont parallèles). ■

4.3 Barycentres

Lemme 4.3.1 Soient $P, Q \in \mathcal{P}$ et $a, b \in \mathbb{R}$ tels que $a + b \neq 0$. Alors il existe un unique $G \in \mathcal{P}$ tel que

$$a\overrightarrow{GP} + b\overrightarrow{GQ} = \overrightarrow{0}.$$

Démonstration. On a

$$a\overrightarrow{GP} + b\overrightarrow{GQ} = a\overrightarrow{GP} + b(\overrightarrow{GP} + \overrightarrow{PQ}) = (a+b)\overrightarrow{GP} + b\overrightarrow{PQ}.$$

Puisque $\overrightarrow{GP} = -\overrightarrow{PG}$, a condition s'écrit donc

$$\overrightarrow{PG} = \frac{b}{a+b}\overrightarrow{PQ} \quad \text{ou encore} \quad G = P + \frac{b}{a+b}\overrightarrow{PQ}. \qquad \blacksquare$$

D'où l'existence et l'unicité.

Définition 4.3.2 On dit que G est le *barycentre* des points P et Q affectés des *poids* a et b. Lorsque $a = b$, on dit que G est le *milieu* de $\{P, Q\}$.

Exemple Le barycentre de $P\binom{0}{0}$ et $Q\binom{1}{0}$ avec les poids

1. 1 et 0 est $G\binom{0}{0} = P$,
2. 0 et 1 est $G\binom{1}{0} = Q$,
3. 1 et 1 est leur milieu $G = \binom{1/2}{0} =: I$,
4. 1 et 2 est $G\binom{2/3}{0}$,
5. 1 et -2 est $G\binom{2}{0}$.

Remarque

- On dit aussi que (P, a) et (Q, b) sont des *points pondérés* et on écrit parfois

$$G = \mathrm{Bar}((P, a), (Q, b)).$$

- On a $x_G = \dfrac{ax_P + bx_Q}{a+b}$ et $y_G = \dfrac{ay_P + by_Q}{a+b}$.
- Si P et Q sont alignés horizontalement et que a et b sont positifs, on peut vraiment penser à une balance lestée de poids a et b en P et Q respectivement et reposant en G.
- On peut multiplier (ou diviser) a et b par la même constante non nulle sans changer le barycentre. On peut donc se ramener au cas $a + b = 1$.
- Les points P, Q et G sont toujours alignés.
- Si $P \neq Q$, alors la droite (PQ) est l'ensemble de tous les barycentres de P et de Q :

$$M \in (PQ) \Leftrightarrow (\exists a, b \in \mathbb{R}, a + b \neq 0 \text{ et } a\overrightarrow{MP} + b\overrightarrow{MQ} = \overrightarrow{0}).$$

- Par définition, I est le *milieu* de (P, Q) si $\overrightarrow{IP} + \overrightarrow{IQ} = \overrightarrow{0}$, c'est-à-dire $\overrightarrow{PI} = \frac{1}{2}\overrightarrow{PQ}$. On dit aussi que P et Q sont *symétriques* par rapport à I.
- Les diagonales d'un parallélogramme se coupent en leur milieu.
- La droite joignant un sommet d'un triangle non aplati au milieu du coté opposé s'appelle la *médiane*.

Proposition 4.3.3 Si G est le barycentre de P et Q avec les poids a et b, et $M \in \mathcal{P}$, on a

$$a\overrightarrow{MP} + b\overrightarrow{MQ} = (a+b)\overrightarrow{MG}.$$

Démonstration. On a

$$\begin{aligned} a\overrightarrow{MP} + b\overrightarrow{MQ} &= a(\overrightarrow{MG} + \overrightarrow{GP}) + b(\overrightarrow{MG} + \overrightarrow{GQ}) \\ &= (a+b)\overrightarrow{MG} + a\overrightarrow{GP} + b\overrightarrow{GQ} \\ &= (a+b)\overrightarrow{MG}. \end{aligned}$$

■

Proposition 4.3.4 Soient P, Q, R trois points du plan et $a, b, c \in \mathbb{R}$ tels que $a+b+c \neq 0$. Alors il existe un unique $G \in \mathcal{P}$ tel que

$$a\overrightarrow{GP} + b\overrightarrow{GQ} + c\overrightarrow{GR} = \overrightarrow{0}.$$

Si $a+b \neq 0$ et H est le barycentre de P et Q affectés des poids a et b alors G est le barycentre de H et R affectés des poids $a+b$ et c .

Démonstration. Pour l'existence, on peut supposer par symétrie que $a+b \neq 0$. Si H désigne le barycentre de P et Q affectés des poids a et b et G celui de H et R affectés des poids $a+b$ et c, on aura

$$a\overrightarrow{GP} + b\overrightarrow{GQ} + c\overrightarrow{GR} = (a+b)\overrightarrow{GH} + c\overrightarrow{GR} = \overrightarrow{0}.$$

Pour l'unicité, on suppose que M est un autre candidat si bien que

$$a\overrightarrow{MP} + b\overrightarrow{MQ} + c\overrightarrow{MR} = \overrightarrow{0}.$$

En retranchant terme à terme dans les deux égalités, on trouve $(a+b+c)\overrightarrow{GM} = 0$ et comme $a+b+c \neq 0$, on aura $\overrightarrow{GM} = 0$ et donc $M = G$. ■

Remarque

- On dit que G est le *barycentre* des points P, Q, R affectés des poids a, b, c.
- La propriété est appelée *associativité des barycentres*. Elle est donc donnée par la formule

$$\mathrm{Bar}((P,a),(Q,b),(R,c)) = \mathrm{Bar}((\mathrm{Bar}((P,a),(Q,b)), a+b),(R,c)).$$

- On dit *centre de gravité* du triangle lorsque $a = b = c$.
- Si G est le barycentre de P, Q, R avec les poids a, b, c, et $M \in \mathcal{P}$, on a

$$a\overrightarrow{MP} + b\overrightarrow{MQ} + c\overrightarrow{MR} = (a+b+c)\overrightarrow{MG}.$$

- On peut définir et construire de la même manière le barycentre (et en particulier le centre de gravité) de quatre, cinq points, etc.
- Le centre de gravité du triangle est aux 2/3 de la médiane en partant d'un sommet. En particulier, les médianes sont concourantes (en ce point).
- Comme toujours, tout cela est aussi valide dans l'espace.

Définition 4.3.5 Si P et Q sont deux points, le *segment* $[P, Q]$ est l'ensemble des barycentres de P et Q à poids positifs (ou plus généralement de même signe).

Remarque

- En d'autres termes,

$$M \in [P, Q] \Leftrightarrow (\exists a, b \in \mathbb{R}_{\geq 0}, a + b \neq 0 \text{ et } a\overrightarrow{MP} + b\overrightarrow{MQ} = \overrightarrow{0}).$$

- Alternativement, $M \in [P, Q] \Leftrightarrow (\exists \lambda \in [0, 1], \overrightarrow{PM} = \lambda\overrightarrow{PQ})$.
- On applique systématiquement le vocabulaire des paires de points aux segments en disant par exemple qu'un segment est un coté d'un triangle ou en parlant du milieu d'un segment.
- Nous utiliserons plutôt le vocabulaire des paires de points laissant au lecteur le soin de traduire.
- Jusqu'à l'introduction de la notion de segment, tout le contenu de ce chapitre fait sens sur un corps quelconque comme $\mathbb{C}$ par exemple (même si l'intuition géométrique est alors perdue) ou le corps $\mathbb{F}_2$ à deux éléments (« pair » et « impair »).

4.4 Exercices (21 août 2023)

Les plans affine et vectoriel sont tacitement munis respectivement d'une base et d'un repère. On illustrera *systématiquement* les exercices par des figures.

Exercice 4.1 On considère les vecteurs $u\binom{1}{-2}$, $v\binom{-3}{2}$ et $w\binom{2}{2}$. Déterminer $a, b, c \in \mathbb{R}$ non tous nuls tels que $au + bv + cw = 0$. Quelles sont les composantes du vecteur w dans la base (u, v) ?

Exercice 4.2 On considère les points $P\binom{3}{2}$, $Q\binom{2}{1}$, $R\binom{4}{-1}$ et $S\binom{-2}{-3}$. Calculez $\overrightarrow{PQ}$, $\overrightarrow{QR}$, $\overrightarrow{RS}$ et $\overrightarrow{SP}$ et vérifiez que $\overrightarrow{PQ} + \overrightarrow{QR} + \overrightarrow{RS} + \overrightarrow{SP} = \overrightarrow{0}$.

Exercice 4.3

1. Déterminer une paramétrisation ainsi qu'une équation pour la droite passant par $P\binom{1}{-2}$ et dirigée par $u\binom{1}{2}$.
2. Déterminer une équation pour la droite paramétrée par

$$\begin{cases} x = 3\lambda + 1 \\ y = \lambda - 1, \end{cases} \qquad \lambda \in \mathbb{R}.$$

3. Trouver une paramétrisation pour la droite d'équation $2x + 3y + 1 = 0$.

Exercice 4.4 On considère les points $P\binom{-1}{3}$, $Q\binom{7}{-1}$, $R\binom{4}{2}$ et $S\binom{0}{4}$. Les droites (PQ) et (RS) sont elles parallèles ? Est-ce que (P, Q, R, S) est un parallélogramme ?

Exercice 4.5 Soient P et Q deux points du plan. Construire si possible le barycentre des points pondérés

1. $(P, 1)$ et $(Q, 3)$,
2. $(P, 2)$ et $(Q, 2)$,
3. $(P, -1)$ et $(Q, 2)$,
4. $(P, -2)$ et $(Q, -6)$,
5. $(P, -2)$ et $(Q, 2)$.

Exercice 4.6 On désigne par $O\binom{0}{0}$ l'origine du plan et on considère les points $P\binom{1}{1}$ et $Q\binom{5}{3}$.

1. Calculer les coordonnées du barycentre (s'il existe)
   (a) G_1 de $(P, 2)$ et $(Q, 1)$,
   (b) G_2 de $(P, -1)$, $(Q, 2)$ et $(O, 3)$.
2. Déterminer (s'ils existent) des réels a et b tels que $H\binom{-1}{0}$ soit le barycentre de (P, a) et (Q, b).
3. Déterminer (s'ils existent) des réels a et b tels que O soit le barycentre de (P, a) et (Q, b).
4. Déterminer (s'il existe) le point R tel que O soit le centre de gravité du triangle $\{P, Q, R\}$.

Exercice 4.7 Soient P, Q, R, S quatre points distincts du plan, K le barycentre de $(P, 3)$ et $(Q, 1)$, J le milieu de $\{R, S\}$, G le centre de gravité du triangle $\{Q, R, S\}$ et I le milieu de $\{P, G\}$. Les points I, J, K sont ils alignés ?

Exercice 4.8 Soient P, Q, R trois points distincts, I le barycentre de $(P, 2)$ et $(Q, 1)$ et J le barycentre de $(Q, 1)$ et $(R, -2)$.

1. Soit G le barycentre de $(P, 2)$, $(Q, 1)$ et $(R, -2)$. Pourquoi les points P, J, G d'une part et les points R, I, G d'autre part sont ils alignés ?
2. Montrer que les droites (QG) et (PR) sont parallèles.

Exercice 4.9 Soient P, Q, R trois points du plan, K le symétrique de P par rapport à R, J le point défini par $\overrightarrow{RJ} = \frac{1}{3}\overrightarrow{RQ}$ et I le milieu de $\{P, Q\}$. Montrer que I, J, K sont alignés.

Exercice 4.10 Soient P, Q, R trois points non alignés et $a, b, c \in \mathbb{R}$ avec $b \neq 0$ ou $c \neq 0$ tels que $a + b + c \neq 0$. Soit M le barycentre des points (P, a), (Q, b) et (R, c). Montrer que

1. si $b + c = 0$, alors (PM) et (QR) sont parallèles,
2. si (PM) et (QR) sont sécantes en G, alors G est le barycentre de (Q, b) et (R, c).

Exercice 4.11 Soient P, Q, R trois points non alignés, P' le milieu de $\{Q, R\}$, S le milieu de $\{P, P'\}$ et T le point d'intersection de (PQ) et (RS).

1. Montrer que S est le barycentre de $(P, 2)$, $(Q, 1)$ et $(R, 1)$.
2. En déduire que T est le barycentre de $(P, 2)$ et $(Q, 1)$.

Exercice 4.12 Soit (P, Q, R, S) un parallélogramme non aplati, K le milieu de $\{P, S\}$, I le milieu de $\{Q, R\}$ et J le points défini par $\overrightarrow{PJ} = \frac{2}{3}\overrightarrow{PQ}$.

1. Exprimez K comme barycentre de P et S ainsi que J comme barycentre de P et Q.
2. Montrer que les droites (SJ) et (QK) sont sécantes en un point G que l'on exprimera comme barycentre de P, Q et S.
3. Montrer que les droites (SJ), (QK) et (PI) sont concourantes.

Exercice 4.13 Soient $\{P, Q, R\}$ un triangle et $a, b \in \mathbb{R}$ avec $a + b \neq 0$. Soient P' le barycentre de (Q, a) et (R, b), Q' le barycentre de (R, a) et (P, b) et R' le barycentre de (P, a) et (Q, b). Montrer que les triangles $\{P, Q, R\}$ et $\{P', Q', R'\}$ ont même centre de gravité.

Exercice 4.14 Démontrer le théorème de Varignon : si P, Q, R, S sont quatre points quelconques et I, J, K, L les milieux respectifs de $\{P, Q\}$, $\{Q, R\}$, $\{R, S\}$ et $\{S, P\}$, alors (I, J, K, L) est un parallélogramme.

Exercice 4.15 Soit $\{P, Q, R\}$ un triangle. Déterminer l'ensemble des points M du plan tel que le vecteur $\overrightarrow{MP} + \overrightarrow{MQ} + \overrightarrow{MR}$ soit colinéaire au vecteur $\overrightarrow{PQ}$.

Exercice 4.16 Soit $\{P, Q, R\}$ un triangle.

1. Déterminer l'ensemble A des valeurs de $m \in \mathbb{R}$ pour lesquelles le barycentre G_m de $(P, 1)$, (Q, m) et $(R, -1)$ est bien défini. Déterminer ensuite l'ensemble des points G_m lorsque m décrit A.
2. Même question avec $(P, 1)$, (Q, m) et $(R, 1)$.

5. Géométrie euclidienne

Nous allons nous concentrer sur le plan euclidien cartésien (obtenu en fixant une base ou un repère orthonormé). Notre présentation permet cependant de généraliser immédiatement toutes les notions introduites sans aucune difficulté.

5.1 Produit scalaire

On rappelle que le plan vectoriel est rapporté à une base (orthonormée) $(\overrightarrow{i}, \overrightarrow{j})$.

Définition 5.1.1 Le *produit scalaire (cartésien*[a]*)* de deux vecteurs $u\binom{x}{y}$ et $v\binom{z}{t}$ du plan est le réel $u \cdot v = xz + yt$.

a. On dit aussi *usuel*.

Exemple $\binom{1}{0} \cdot \binom{0}{1} = 0$, $\binom{1}{0} \cdot \binom{1}{0} = 1$ et $\binom{1}{2} \cdot \binom{3}{4} = 11$.

Proposition 5.1.2
1. $\forall u \in \overrightarrow{\mathcal{P}}, \quad u \neq \overrightarrow{0} \Leftrightarrow u \cdot u > 0$,
2. $\forall u, v \in \overrightarrow{\mathcal{P}}, \quad u \cdot v = v \cdot u$,
3. $\forall u, v, w \in \overrightarrow{\mathcal{P}}, \quad u \cdot (v + w) = u \cdot v + u \cdot w$,
4. $\forall u, v \in \overrightarrow{\mathcal{P}}, \forall \lambda \in \mathbb{R}, \quad (\lambda u) \cdot v = \lambda(u \cdot v)$.

Démonstration. Tout cela se vérifie aisément. Par exemple, pour l'assertion 3), il faut s'assurer que

$$x_u(x_v + x_w) + y_u(y_v + y_w) = (x_u x_v + y_u y_v) + (x_u x_w + y_u y_w).$$

Le reste est laissé en exercice. ■

Remarque • On a $\overrightarrow{0} \cdot u = 0$.

- On a toujours $u \cdot (v - w) = u \cdot v - u \cdot w$.
- On définit plus généralement *un* produit scalaire comme étant une application ayant ces quatre propriétés.
- On peut montrer que, quitte à changer de base, tout produit scalaire est de la forme ci-dessus.
- On parle de *plan euclidien* lorsque le plan est muni du (ou d'un) produit scalaire.
- De nouveau, tout ceci se généralise immédiatement au cas d'un espace de dimension supérieure.

Définition 5.1.3 La *norme (euclidienne)* d'un vecteur u est $\|u\| = \sqrt{u \cdot u}$.

Remarque Pour $u\binom{x}{y}$, on a donc $\|u\| = \sqrt{x^2 + y^2}$.

Exemple $\left\|\binom{1}{0}\right\| = 1$, $\left\|\binom{3}{4}\right\| = 5$ et $\left\|\binom{5}{12}\right\| = 13$.

Lemme 5.1.4 $\forall u, v \in \overrightarrow{\mathcal{P}}, \quad \|u + v\|^2 = \|u\|^2 + 2u \cdot v + \|v\|^2$.

Démonstration. On a

$$\begin{aligned}\|u + v\|^2 &= (u + v) \cdot (u + v) \\ &= u \cdot u + u \cdot v + v \cdot u + v \cdot v \\ &= \|u\|^2 + 2u \cdot v + \|v\|^2.\end{aligned}$$

■

Remarque

- On dispose aussi des autres *identités remarquables*

$$\|u - v\|^2 = \|u\|^2 - 2u \cdot v + \|v\|^2 \quad \text{et} \quad (u + v) \cdot (u - v) = \|u\|^2 - \|v\|^2.$$

- On peut retrouver le produit scalaire à partir de la norme euclidienne :

$$u \cdot v = \frac{\|u + v\|^2 - \|u\|^2 - \|v\|^2}{2} = \frac{\|u + v\|^2 - \|u - v\|^2}{4}$$

- On peut montrer que c'est effectivement un produit scalaire en utilisant la règle (du parallélogramme) :

$$\|u + v\|^2 + \|u - v\|^2 = 2\|u\|^2 + 2\|v\|^2.$$

Théoreme 5.1.5 — Cauchy-Schwarz. On a

$$\forall u, v \in \overrightarrow{\mathcal{P}}, \quad |u \cdot v| \leq \|u\|\|v\|$$

avec égalité si et seulement si u et v sont colinéaires.

Démonstration. Si $u = 0$, c'est clair. On suppose donc $u \neq 0$. Si $\lambda \in \mathbb{R}$, on a

$$0 \leq \|\lambda u - v\|^2 = \|u\|^2\lambda^2 - 2(u \cdot v)\lambda + \|v\|^2.$$

Or un polynôme du second degré (puisque $u \neq 0$) qui est toujours positif a un discriminant négatif :

$$\Delta = (2(u \cdot v))^2 - 4\|u\|^2\|v\|^2 \leq 0.$$

On en déduit l'inégalité de Cauchy-Schwarz. On a égalité si et seulement si $\Delta = 0$, ce qui signifie que le polynôme peut s'annuler et donc qu'il existe $\lambda \in \mathbb{R}$ tel que $\|\lambda u - v\| = 0$, ce qui signifie que $\lambda u - v = 0$, ce qui veut bien dire que u et v sont colinéaires (puisque $u \neq 0$). ■

Remarque
- Lorsque $u \neq 0$, on a égalité quand $v = \lambda u$ avec $\lambda \in \mathbb{R}$. Le cas $u \cdot v = \|u\|\|v\|$ correspond au cas $\lambda \geq 0$ (et $u \cdot v = -\|u\|\|v\|$ si $\lambda < 0$).
- On peut démontrer le théorème de Cauchy-Schwarz en utilisant les composantes des vecteurs mais la démonstration ci-dessus est un grand classique qui s'adapte à bien d'autres contextes.

Exemple Si $u\binom{3}{4}$ et $v\binom{5}{12}$, on a $\|u\| = 5$ et $\|v\| = 13$ si bien que $u \cdot v = 63 \leq 65 = \|u\|\|v\|$.

Proposition 5.1.6
1. $\forall u \in \overrightarrow{\mathcal{P}}, \quad u = \overrightarrow{0} \Leftrightarrow \|u\| = 0$,
2. $\forall u, v \in \overrightarrow{\mathcal{P}}, \quad \|u + v\| \leq \|u\| + \|v\|$,
3. $\forall u \in \overrightarrow{\mathcal{P}}, \forall \lambda \in \mathbb{R}, \quad \|\lambda u\| = |\lambda|\|u\|$.

Démonstration.
1. Résulte de la positivité.
2. on a grâce au théorème de Cauchy-Schwartz,
$$\|u + v\|^2 = \|u\|^2 + 2u \cdot v + \|v\|^2 \leq \|u\|^2 + 2\|u\|\|v\| + \|v\|^2 = (\|u\| + \|v\|)^2,$$
3. on a $\|\lambda u\|^2 = (\lambda u) \cdot (\lambda u) = \lambda^2\|u\|^2$. ■

Remarque
- On définit plus généralement *une* norme comme étant une application ayant ces trois propriétés (c'est une notion indépendante de celle de produit scalaire).
- On en déduit que $|\|u\| - \|v\|| \leq \|u - v\|$ et aussi que $\| - u\| = \|u\|$.

Définition 5.1.7 Deux vecteurs u et v sont *orthogonaux* si $u \cdot v = 0$, et on écrit alors $u \perp v$. Deux droites vectorielles Δ et Δ' sont *orthogonales* si

$$\forall u \in \Delta, \forall u' \in \Delta', \quad u \perp u',$$

et on écrit alors $\Delta \perp \Delta'$.

Remarque
- Si u et v sont deux vecteurs orthogonaux de norme 1 dans le plan, on dit que $\mathcal{B} := (u, v)$ est une *base orthonormée*.

- $\mathcal{B} := (\overrightarrow{i}, \overrightarrow{j})$ est une base orthonormée.
- Deux droites vectorielles sont orthogonales si et seulement si leurs vecteurs directeurs sont orthogonaux.
- Si Δ est une droite dirigée par u, un vecteur *normal* à Δ est un vecteur non nul n orthogonal à u.
- La droite d'équation $ax + by = 0$ a pour vecteur normal $n\binom{a}{b}$ (et vecteur directeur $u\binom{-b}{a}$).
- Réciproquement, si n est un vecteur non nul, alors les vecteurs orthogonaux à n forment une droite Δ.

Lemme 5.1.8 Dans le plan vectoriel euclidien, si $\Delta \perp \Delta'$ et $\Delta' \perp \Delta''$, alors $\Delta = \Delta''$ (c'est *faux* dans l'espace).

Démonstration. Si on choisit des vecteurs directeurs u, u', u'', dans le plan on peut écrire $\alpha u + \alpha' u' + \alpha'' u'' = \overrightarrow{0}$ avec $\alpha, \alpha', \alpha''$ non tous nuls. Mais on a alors

$$0 = u' \cdot \overrightarrow{0} = u' \cdot (\alpha u + \alpha' u' + \alpha'' u'') = \alpha u' \cdot u + \alpha' u' \cdot u' + \alpha'' u' \cdot u'' = \alpha' \|u'\|^2.$$

Et il suit que $\alpha' = 0$ et donc $\alpha u + \alpha'' u'' = \overrightarrow{0}$ avec α, α'' non tous nuls. Les vecteurs sont donc colinéaires. ■

5.2 Géométrie classique

On rappelle que le plan affine est rapporté à un repère (orthonormé) $(O, \overrightarrow{i}, \overrightarrow{j})$.

Définition 5.2.1 La *distance* entre deux points P et Q est $PQ = \|\overrightarrow{PQ}\|$.

Proposition 5.2.2
1. $\forall P, Q \in \mathcal{P}, \quad PQ = QP$,
2. $\forall P, Q \in \mathcal{P}, \quad PQ = 0 \Leftrightarrow P = Q$,
3. $\forall P, Q, R \in \mathcal{P}, \quad PR \leq PQ + QR$.

Démonstration.
1. On a $\|\overrightarrow{PQ}\| = \| - \overrightarrow{PQ}\| = \|\overrightarrow{QP}\|$,
2. on a $\|\overrightarrow{PQ}\| = 0 \Leftrightarrow \overrightarrow{PQ} = \overrightarrow{0}$,
3. on a $\|\overrightarrow{PR}\| = \|\overrightarrow{PQ} + \overrightarrow{QR}\| \leq \|\overrightarrow{PQ}\| + \|\overrightarrow{QR}\|$. ■

Exemple Si $P\binom{1}{2}$ et $Q\binom{5}{5}$, alors $PQ = \sqrt{(5-1)^2 + (5-2)^2} = 5$.

Remarque
- On a égalité dans l'inéquation si et seulement si $Q \in [P, R]$.
- On définit plus généralement *une* distance comme étant une application ayant ces propriétés (toute norme définit une distance).
- On peut maintenant définir le *cercle* de centre Ω et de *rayon* $r \in \mathbb{R}_{\geq 0}$:

$$\mathcal{C} = \{P \in \mathcal{P} \ / \ \Omega P = r\}.$$

- Un *diamètre* du cercle $\mathcal{C}$ est une paire de points distincts P et Q de $\mathcal{C}$ tels que $\Omega \in (PQ)$ (Ω est alors nécessairement le milieu de $\{P, Q\}$).

- On définit aussi la *médiatrice* de $\{P, Q\}$:

$$\mathcal{D} = \{M \in \mathcal{P} \ / \ PM = QM\}.$$

- Si P et Q sont deux points distincts, la médiatrice de $\{P, Q\}$ est la droite orthogonale à (PQ) passant par le milieu I de $\{P, Q\}$
- Pour démontrer la propriété précédente, on montrera d'abord que

$$\overrightarrow{MI} \cdot \overrightarrow{PQ} = \frac{1}{2}(MQ^2 - MP^2).$$

- Les médiatrices d'un triangle non aplati sont concourantes au centre du *cercle circonscrit* (c'est-à-dire l'unique cercle passant par les sommets).

Théoreme 5.2.3 — de Thales. Soient P, Q, R, S, T cinq points distincts. Si (PQ) et (RS) sont sécantes en T et $(PR) /\!/ (QS)$, alors

$$\frac{TQ}{TP} = \frac{TS}{TR} = \frac{QS}{PR}.$$

Démonstration. D'une part, on peut écrire $\overrightarrow{TQ} = \lambda \overrightarrow{TP}$ et $\overrightarrow{TS} = \mu \overrightarrow{TR}$, si bien que

$$\overrightarrow{PR} = \overrightarrow{TR} - \overrightarrow{TP} \quad \text{et} \quad \overrightarrow{QS} = \overrightarrow{TS} - \overrightarrow{TQ} = \mu \overrightarrow{TR} - \lambda \overrightarrow{TP}.$$

D'autre part, comme $(PR) /\!/ (QS)$, on peut écrire $\overrightarrow{QS} = \nu \overrightarrow{PR}$, c'est-à-dire

$$\mu \overrightarrow{TR} - \lambda \overrightarrow{TP} = \nu(\overrightarrow{TR} - \overrightarrow{TP})$$

ou encore $(\nu - \mu)\overrightarrow{TR} - (\nu - \lambda)\overrightarrow{TP} = 0$. Puisque les vecteurs ne sont pas colinéaires, on a $\nu - \mu = \nu - \lambda = 0$, c'est-à-dire $\lambda = \mu = \nu$ et donc $|\lambda| = |\mu| = |\nu|$. ■

Remarque
- Les conclusions restent vraies sous les hypothèses plus faibles P, R, T distincts (on peut avoir $Q = S$, $P = Q$ ou $R = S$ par exemple). On peut faire encore mieux en reformulant la conclusion.
- Attention : la réciproque du théorème de Thales nécessite de contrôler l'ordre des points sur les droites.

Définition 5.2.4 Deux droites affines D et D' sont *orthogonales* si $\overrightarrow{D} \perp \overrightarrow{D}'$ et on écrit alors $D \perp D'$.

Remarque
- Si (u, v) est une base orthonormée du plan, on dit que $\mathcal{R} := (P, u, v)$ est un *repère orthonormé*.
- $(O, \overrightarrow{i}, \overrightarrow{j})$ est un repère orthonormé.
- On dit que deux droites sont *perpendiculaires* si elle sont orthogonales et sécantes (automatique dans le plan).
- Si $D /\!/ D'$ et $D \perp D''$, alors $D' \perp D''$.

Lemme 5.2.5 Dans le plan affine euclidien, si $D \perp D'$ et $D' \perp D''$, alors $D /\!\!/ D''$ (c'est *faux* dans l'espace).

Démonstration. En effet, on a $\overrightarrow{D} \perp \overrightarrow{D}'$ et $\overrightarrow{D}' \perp \overrightarrow{D}''$, et donc $\overrightarrow{D} = \overrightarrow{D}''$. ■

Théoreme 5.2.6 — de Pythagore. Soient P, Q, R trois points distincts du plan. Alors,

$$(PQ) \perp (PR) \Leftrightarrow QR^2 = PQ^2 + PR^2.$$

Démonstration. On utilise la formule $\|u+v\|^2 = \|u\|^2 + 2u \cdot v + \|v\|^2$ avec $u = \overrightarrow{QP}$ et $v = \overrightarrow{PR}$. ■

Remarque
- On dit alors que le triangle est *rectangle* en P.
- Lorsque le triangle n'est pas rectangle, on dispose du théorème d'Al Kashi : $QR^2 = PQ^2 + PR^2 - 2\overrightarrow{PQ} \cdot \overrightarrow{PR}$.
- On définit une *hauteur* d'un triangle non aplati comme étant une droite passant par un sommet et perpendiculaire au coté opposé.
- Les hauteurs d'un triangle sont concourantes en un point appelé *orthocentre*.
- Le centre de gravité, le centre du cercle circonscrit et l'orthocentre sont alignés sur ce qu'on appelle la *droite d'Euler*.

Proposition 5.2.7 — Règle du parallélogramme. Si (P, Q, R, S) est un parallélogramme, on a

$$PR^2 + QS^2 = PQ^2 + QR^2 + RS^2 + ST^2 \quad (= 2PQ^2 + 2QR^2).$$

Démonstration. On utilise la formule $\|u+v\|^2 + \|u-v\|^2 = 2\|u\|^2 + 2\|v\|^2$ avec $u = \overrightarrow{PQ}$ et $v = \overrightarrow{PS}$. ■

Remarque
- Cela signifie que « la somme des carrés des diagonales est égale à la somme des carrés des cotés ».
- On démontre de la même façon la *règle de la médiane* : si I est le milieu de $\{P, Q\}$ et $M \in \mathcal{P}$, on a

$$MP^2 + MQ^2 = 2MI^2 + \frac{1}{2}PQ^2.$$

- Pour démontrer la règle de la médiane, on peut aussi appliquer la règle du parallélogramme à (M, P, N, Q) ou N est le symétrique de M par rapport à I.

Proposition 5.2.8 Soient P, Q, M trois trois points distincts du plan. Alors, $(MP) \perp (MQ)$ si et seulement si M est situé sur le cercle de diamètre $\{P, Q\}$.

Démonstration. Si I désigne le milieu de $\{P, Q\}$, on a

$$\begin{aligned}\overrightarrow{MP} \cdot \overrightarrow{MQ} &= (\overrightarrow{MI} + \overrightarrow{IP}) \cdot (\overrightarrow{MI} + \overrightarrow{IQ}) \\ &= (\overrightarrow{MI} + \overrightarrow{IP}) \cdot (\overrightarrow{MI} - \overrightarrow{IP}) \\ &= MI^2 - IP^2.\end{aligned}$$

On voit donc que $\overrightarrow{MP} \cdot \overrightarrow{MQ} = 0$ si et seulement si $IM = IP$. ■

Remarque
- Alternativement, cela signifie que le centre du cercle circonscrit à un triangle rectangle est le milieu de l'*hypoténuse* (le plus grand coté).
- Ce résultat est aussi une conséquence de la règle de la médiane avec la condition $MI = \frac{1}{2}PQ$.

5.3 Angle

Définition 5.3.1 Si u et v sont des vecteurs non nuls du plan, leur *angle (non orienté)* [a] est l'unique réel $\widehat{(u, v)} \in [0, \pi]$ tel que

$$u \cdot v = \|u\|\|v\| \cos \widehat{(u, v)}.$$

a. On devrait dire *la mesure de l'angle*.

Remarque
- Grâce au théorème de Cauchy-Schwarz, le nombre

$$-1 \leq \frac{u \cdot v}{\|u\|\|v\|} \leq 1$$

est en effet le cosinus d'un unique angle compris entre 0 et π. En d'autres termes, on a

$$\widehat{(u, v)} := \arccos\left(\frac{u \cdot v}{\|u\|\|v\|}\right).$$

- On dit aussi angle *géométrique* au lieu d'angle non orienté.
- Nous ne considérerons *pas* ici les *angles orientés* dont la valeur est un réel modulo 2π (qui dépend aussi du déterminant des vecteurs).
- Lorsque $\|u\| = \|v\| = 1$, on a $u \cdot v = \cos \widehat{(u, v)}$.
- On a

$$\sin \widehat{(u, v)} = \sqrt{1 - \cos^2 \widehat{(u, v)}} \quad (\geq 0)$$

puisque $\widehat{(u, v)} \in [0, \pi]$.
- On a $\widehat{(v, u)} = \widehat{(u, v)}$ et $\widehat{(u, \lambda v)} = \widehat{(u, v)}$ si $\lambda > 0$.

Proposition 5.3.2 Soient u et v deux vecteurs non nuls. Alors, on a
1. $\widehat{(u, v)} = 0$ si et seulement si $v = \lambda u$ avec $\lambda > 0$,
2. $\widehat{(u, v)} = \pi$ si et seulement si $v = \lambda u$ avec $\lambda < 0$,

3. $\widehat{(u,v)} = \frac{\pi}{2}$ si et seulement si $u \perp v$,
4. $\widehat{(u,v)} + \widehat{(u,-v)} = \pi$.

Démonstration. Les deux premières assertions reposent sur le cas d'égalité dans le théorème de Cauchy-Schwartz :

1. $\widehat{(u,v)} = 0 \Leftrightarrow \cos\widehat{(u,v)} = 1 \Leftrightarrow u \cdot v = \|u\|\|v\|$,
2. $\widehat{(u,v)} = \pi \Leftrightarrow \cos\widehat{(u,v)} = -1 \Leftrightarrow u \cdot v = -\|u\|\|v\|$,
3. $\widehat{(u,v)} = \frac{\pi}{2} \Leftrightarrow \cos\widehat{(u,v)} = 0 \Leftrightarrow u \cdot v = 0$,
4. $\cos\left(\pi - \widehat{(u,v)}\right) = -\cos\widehat{(u,v)} = \cos\widehat{(u,-v)}$ et $0 \leq \pi - \widehat{(u,v)} \leq \pi$. ■

Remarque On parle respectivement d'*angle nul*, d'*angle plat*, d'*angle droit* et d'*angles supplémentaires*.

Théoreme 5.3.3 Soient u, v, w trois vecteurs non nuls tels que $w = \lambda u + \mu v$ avec $\lambda, \mu \geq 0$. On a alors

$$\widehat{(u,v)} = \widehat{(u,w)} + \widehat{(w,v)}.$$

Démonstration. De manière équivalente, il faut montrer que

$$\cos\left(\widehat{(u,w)} + \widehat{(w,v)}\right) = \cos\widehat{(u,v)} \quad \text{et} \quad \sin\left(\widehat{(u,w)} + \widehat{(w,v)}\right) \geq 0.$$

On peut bien sûr supposer que $\|u\| = \|v\| = \|w\| = 1$ si bien que

$$1 = \|w\|^2 = \|\lambda u + \mu v\|^2 = \lambda^2 + 2\lambda\mu u \cdot v + \mu^2.$$

D'autre part, on aura aussi

$$\cos\left(\widehat{(u,w)}\right) = u \cdot w = u \cdot (\lambda u + \mu v) = \lambda\|u\|^2 + \mu u \cdot v = \lambda + \mu u \cdot v$$

On en déduit que

$$\begin{aligned}
\sin\left(\widehat{(u,w)}\right) &= \sqrt{1 - (\lambda + \mu u \cdot v)^2} \\
&= \sqrt{1 - \lambda^2 - \mu^2(u \cdot v)^2 - 2\lambda\mu u \cdot v} \\
&= \sqrt{\mu^2 - \mu^2(u \cdot v)^2} \\
&= \mu\sqrt{1 - (u \cdot v)^2}.
\end{aligned}$$

De même, on a

$$\cos\left(\widehat{(v,w)}\right) = \lambda u \cdot v + \mu \quad \text{et} \quad \sin\left(\widehat{(v,w)}\right) = \lambda\sqrt{1 - (u \cdot v)^2}.$$

En appliquant la formule $\cos(x+y) = \cos(x)\cos(y) - \sin(x)\sin(y)$, on obtient

$$\begin{aligned}
\cos\left(\widehat{(u,w)} + \widehat{(w,v)}\right) &= (\lambda + \mu u \cdot v)(\lambda u \cdot v + \mu) - \lambda\mu(1 - (u \cdot v)^2) \\
&= (\lambda^2 + \mu^2)u \cdot v + \lambda\mu(1 + (u \cdot v)^2) - \lambda\mu(1 - (u \cdot v)^2) \\
&= (\lambda^2 + \mu^2 + 2\lambda\mu u \cdot v)u \cdot v \\
&= u \cdot v \\
&= \cos\widehat{(u,v)}.
\end{aligned}$$

Enfin, on applique la formule $\sin(x+y) = \cos(x)\sin(y) + \cos(y)\sin(x)$ qui donne

$$\begin{aligned}\sin\left(\widehat{(u,w)} + \widehat{(w,v)}\right) &= (\lambda + \mu u\cdot v)\lambda\sqrt{1-(u\cdot v)^2} + (\lambda u\cdot v + \mu)\mu\sqrt{1-(u\cdot v)^2}\\ &= (\lambda^2+\mu^2+2\lambda\mu u\cdot v)\sqrt{1-(u\cdot v)^2}\\ &= \sqrt{1-(u\cdot v)^2}\\ &\geq 0.\end{aligned}$$

■

Définition 5.3.4 Si P, Q, R sont trois points avec $Q \neq P$ et $R \neq P$, l'angle en P du triangle $\{P, Q, R\}$ est $\widehat{QPR} := (\widehat{\overrightarrow{PQ}, \overrightarrow{PR}})$.

Proposition 5.3.5 1. Si $\{P, Q, R\}$ est un triangle rectangle en P, alors

$$\cos(\widehat{PQR}) = \sin(\widehat{PRQ}) = \frac{PQ}{QR}.$$

2. Si P, Q, R sont trois points distincts, alors

$$\frac{\sin(\widehat{PQR})}{PR} = \frac{\sin(\widehat{QPR})}{QR} = \frac{\sin(\widehat{PRQ})}{PQ}.$$

Démonstration. 1. On calcule

$$QP\times QR\cos(\widehat{PQR}) = \overrightarrow{QP}\cdot\overrightarrow{QR} = \overrightarrow{QP}\cdot(\overrightarrow{QP}+\overrightarrow{PR}) = QP^2+\overrightarrow{QP}\cdot\overrightarrow{PR} = QP^2$$

et

$$\sin^2(\widehat{PRQ}) = 1-\cos^2(\widehat{PRQ}) = 1-\frac{PR^2}{QR^2} = \frac{QR^2-PR^2}{QR^2} = \frac{PQ^2}{QR^2}.$$

2. Si on désigne par H l'intersection de la hauteur issue de P et de la droite (QR), on a

$$\frac{\sin(\widehat{PQR})}{PR} = \frac{\sin(\widehat{PQH})}{PR} = \frac{PH}{PQ\times PR}$$

qui est symétrique en Q et R. ■

Remarque • Le second résultat se nomme parfois *la règle des sinus*.
• On dispose aussi du *théorème de Pythagore généralisé* ou *théorème d'Al Kashi*

$$QR^2 = PQ^2 + PR^2 - 2\times PQ\times PR\times\cos\left(\widehat{QPR}\right).$$

Proposition 5.3.6 Si $\{P, Q, R\}$ est un triangle non aplati, on a

$$\widehat{PQR} = \widehat{PRQ} \Leftrightarrow PR = PQ.$$

Démonstration. On calcule

$$\cos(\widehat{PQR}) = \frac{\overrightarrow{QP}\cdot\overrightarrow{QR}}{QP\times QR} = \frac{\overrightarrow{QP}\cdot(\overrightarrow{QP}+\overrightarrow{PR})}{QP\times QR} = \frac{QP^2+\overrightarrow{QP}\cdot\overrightarrow{PR}}{QP\times QR} = \frac{PQ-PR\cos(\widehat{QPR})}{QR}$$

et on a donc de même

$$\cos(\widehat{PRQ}) = \frac{PR-PQ\cos(\widehat{QPR})}{QR}.$$

On a donc égalité si et seulement si

$$PQ-PR\cos(\widehat{QPR}) = PR-PQ\cos(\widehat{QPR}).$$

Or cette égalité peut se réécrire

$$(1+\cos(\widehat{QPR})(PQ-PR) = 0.$$

Comme les points ne sont pas alignés, on a $\widehat{QPR}\neq\pi$. ■

Remarque
- Cela signifie qu'un triangle non aplati a deux cotés de même longueur si et seulement si il a deux angles égaux (triangle *isocèle*).
- On en déduit qu'un triangle non aplati a tous ses cotés de même longueur si et seulement si il a tous ses angles égaux (triangle *équilatéral*).

Théoreme 5.3.7 Si P,Q,R sont trois points distincts du plan, alors

$$\widehat{QPR}+\widehat{PQR}+\widehat{PRQ} = \pi.$$

Démonstration. En effet, on a $u+v=w$ avec $u=\overrightarrow{PQ}, v=\overrightarrow{QR}, w=\overrightarrow{PR}$, et donc

$$\begin{aligned}\widehat{QPR}+\widehat{PQR}+\widehat{PRQ} &= \widehat{(u,w)}+\widehat{(-u,v)}+\widehat{(w,v)}\\ &= \widehat{(u,v)}+\widehat{(-u,v)}\\ &= \pi.\end{aligned}$$

■

Remarque Le relâchement de cette égalité (dans un sens ou dans l'autre) donne naissance aux géométries non euclidiennes (hyperbolique ou elliptique) : si on trace un (grand) triangle sur le sol terrestre, la somme des (mesures des) angles est strictement supérieure à π.

5.4 Exercices (21 août 2023)

On fera toujours un dessin lorsque cela est possible.

Exercice 5.1 Soit $\{P, Q, R\}$ un triangle avec $PQ = 7$, $PR = 5$ et $QR = 6$.

1. Calculer $\overrightarrow{QP} \cdot \overrightarrow{PR}$ et en déduire $\overrightarrow{PQ} \cdot \overrightarrow{PR}$
2. Soit $H \in (PQ)$ l'unique point tel que $(RH) \perp (PQ)$. Calculer RH.

Exercice 5.2 On considère le triangle $\left\{P\binom{1}{3}, Q\binom{2}{0}, R\binom{-3}{1}\right\}$.

1. Déterminer une équation de la hauteur issue de P.
2. Déterminer une équation de la hauteur issue de Q.
3. En déduire les coordonnées de l'orthocentre.

Exercice 5.3 Soit (P, Q, R, S) un parallélogramme à sommets (tous) distincts.

1. Montrer, en utilisant une identité remarquable, que $PR^2 - QS^2 = 4\overrightarrow{PQ} \cdot \overrightarrow{PS}$.
2. En déduire que (PQ) et (PS) sont perpendiculaires si et seulement si $PR = QS$ (rectangle).
3. Montrer, en utilisant une identité remarquable, que $PQ^2 - QR^2 = \overrightarrow{PR} \cdot \overrightarrow{SQ}$.
4. En déduire que (PR) et (QS) sont perpendiculaires si et seulement si $PQ = QR$ (losange).

Exercice 5.4

1. Montrer, en utilisant une identité remarquable, que si P, Q, R, S sont des points quelconques, alors
$$PR^2 = PQ^2 + QR^2 + 2\overrightarrow{PQ} \cdot \overrightarrow{QR} \text{ et } QS^2 = QR^2 + RS^2 + 2\overrightarrow{QR} \cdot \overrightarrow{RS}.$$
2. En déduire que « dans un parallélogramme la somme des carrés des diagonales est égale à la somme des carrés des cotés ».

Exercice 5.5 Soient $\{P, Q, R\}$ un triangle non aplati et O le centre du cercle circonscrit.

1. On désigne par H le point du plan tel que $\overrightarrow{OH} = \overrightarrow{OP} + \overrightarrow{OQ} + \overrightarrow{OR}$.
   (a) Montrer que $\overrightarrow{PH} \cdot \overrightarrow{QR} = 0$.
   (b) En déduire que H est l'orthocentre du triangle.
2. Montrer que, si G désigne le centre de gravité du triangle, alors O, G et H sont alignés et plus précisément que $\overrightarrow{OH} = 3\overrightarrow{OG}$.

Exercice 5.6 Soient P et Q deux points quelconques et I le milieu de $\{P, Q\}$.

1. Montrer que si M est un point quelconque, on a
$$\overrightarrow{MP} \cdot \overrightarrow{MQ} = MI^2 - \frac{1}{4}PQ^2.$$
2. En déduire que l'ensemble des points M du plan tels que
$$\overrightarrow{MP} \cdot \overrightarrow{MQ} = \frac{3}{4}PQ^2$$
est un cercle dont on déterminera le centre et le rayon.

Exercice 5.7 Soient P et Q deux points quelconques, I le barycentre de $(P,3)$ et $(Q,1)$ et J le barycentre de $(P,3)$ et $(Q,-1)$.

1. Montrer que pour tout point M, on a
$$\overrightarrow{MI}\cdot\overrightarrow{MJ} = \frac{9}{8}MP^2 - \frac{1}{8}MQ^2.$$
2. En déduire que l'ensemble des points M du plan tels que $MP = \frac{1}{3}MQ$ est un cercle dont on déterminera le centre et le rayon.

Exercice 5.8 Soient P et Q deux points quelconques et I le milieu de $\{P,Q\}$.

1. Montrer que si M est un point quelconque, on a
$$MP^2 + MQ^2 = 2MI^2 + \frac{1}{2}PQ^2.$$
2. En déduire que l'application $M \mapsto MP^2 + MQ^2$ admet un minimum que l'on déterminera.

Exercice 5.9 Soient P,Q,R trois points quelconques et G le barycentre de $(P,2)$, $(Q,1)$ et $(R,-1)$.

1. Montrer que si M est un point quelconque, alors
$$2MP^2 + MQ^2 - MR^2 = 2GP^2 + GQ^2 - GR^2 + 2MG^2.$$
2. En déduire que l'application $M \mapsto 2MP^2+MQ^2-MR^2$ possède un minimum que l'on déterminera.

Exercice 5.10 Soient P,Q,R trois points quelconques. Déterminer (on fera un dessin !) les points M du plan tels que

1. $\|\overrightarrow{MP} - 3\overrightarrow{MQ}\| \leq 2$,
2. $\|2\overrightarrow{MP} + \overrightarrow{MQ} - \overrightarrow{MR}\| = \|2\overrightarrow{MP} - \overrightarrow{MQ} - \overrightarrow{MR}\|$,
3. $\|\overrightarrow{MP} + 2\overrightarrow{MQ}\| = \|2\overrightarrow{MP} + \overrightarrow{MR}\|$.

Exercice 5.11 On considère les points suivants
$$P\begin{pmatrix}-\frac{1}{2}\\ \frac{\sqrt{3}}{2}\end{pmatrix}, \quad Q\begin{pmatrix}0\\ -1\end{pmatrix} \quad \text{et} \quad R\begin{pmatrix}\frac{\sqrt{3}}{2}\\ \frac{1}{2}\end{pmatrix}.$$
On s'intéresse à la transformation qui envoie un point M du cercle Γ circonscrit au triangle $\{P,Q,R\}$ sur le barycentre M' des points $(P,1),(Q,1),(R,1),(M,3)$.

1. Montrer que Γ est le cercle de centre O et de rayon 1
2. Soit G le centre du gravité du triangle. Exprimer M' comme barycentre de G et de M.
3. Soit H le milieu de $\{G,O\}$. Montrer que M' est situé sur un cercle Γ' de centre H dont on déterminera le rayon.
4. On désigne par P',Q',R' les images des points P,Q,R respectivement par notre transformation. Montrer que Γ' est le cercle circonscrit au triangle $\{P',Q',R'\}$.

6. Arithmétique

Avant de développer l'arithmétique proprement dite, nous montrons les propriétés élémentaires des opérations sur les entiers à partir de leur définition intuitive.

6.1 Entiers relatifs

Définition 6.1.1 L'ensemble des *entiers naturels*[a] (resp. *relatifs*) est

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\} \quad (\text{resp. } \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}).$$

a. Pour plus de rigueur, il faudrait présenter les 5 axiomes de Peano.

Remarque

- Tout entier naturel s'obtient de manière unique en un nombre fini d'étapes à partir de 0 en associant à un entier naturel p son *successeur* que l'on notera « $p + 1$ » (c'est une notation, nous n'avons pas encore introduit l'addition des nombres entiers).
- Tout entier relatif est soit un entier naturel $n = p$, soit l'*opposé* $n = -p$ d'un entier naturel non nul (ou alternativement $n = -(p + 1)$ ou p est un entier naturel quelconque).
- On pose $-0 := 0$ et si p est un entier naturel non nul, on pose $-(-p) := p$ et on dit que c'est l'*opposé* de $-p$.
- On a toujours $-(-n) = n$: lorsque $n = p \in \mathbb{N}$, c'est la définition et si $n = -p$ avec $p \in \mathbb{N}$, alors $-n = -(-p) = p$ et donc $-(-n) = -p = n$.
- On a aussi

$$n \in \mathbb{N} \text{ et } -n \in \mathbb{N} \Leftrightarrow n = 0.$$

- Si p est un entier naturel, on pose $|-p| := |p| := p$. On aura ainsi toujours $|-n| = |n|$

- Si p est un entier naturel, on définit le *successeur* de $n := -(p+1)$ comme étant $n+1 := -p$.

Définition 6.1.2 L'*addition* des entiers est l'opération qui associe à $m, n \in \mathbb{Z}$ leur *somme* $m+n$ définie

1. par récurrence si $n = p \in \mathbb{N}$ par
$$m+0 := m \quad \text{et} \quad m+(p+1) := (m+p)+1,$$
2. par la formule $m+(-p) := -(-m+p)$ si $n = -p$ avec $p \in \mathbb{N}_{\neq 0}$.

La *soustraction* de deux nombres entiers leur associe leur *différence*
$$m-n := m+(-n).$$

Proposition 6.1.3
1. $\forall m, n \in \mathbb{Z}, \quad m+n = n+m.$
2. $\forall n_1, n_2, n_3 \in \mathbb{Z}, \quad (n_1+n_2)+n_3 = n_1+(n_2+n_3),$
3. $\forall n \in \mathbb{Z}, \quad n+0 = n,$
4. $\forall n \in \mathbb{Z}, \quad -n+n = 0.$

Démonstration. La démonstration de ces propriétés est extrêmement laborieuse. L'assertion 3) résulte de la définition et on procède ensuite par étapes successives.

- On montre que $-(m+n) = -m-n$: si $n = p \in \mathbb{N}$, ça résulte des définitions :
$$-m-p = -m+(-p) = -(m+p),$$
et sinon, on écrit $n = -p$ avec $p \neq 0$ et on a $m+n = m-p = -(-m+p)$ si bien que $-(m+n) = -m+p = -m-n$.
- On montre que $-(n+1)+1 = -n$: si $n = p \in \mathbb{N}$, c'est la définition et si $n = -(p+1)$, on a bien
$$\begin{aligned} -(n+1)+1 &= -(-(p+1)+1)+1 \\ &= -(-p)+1 \\ &= p+1 \\ &= -n \end{aligned}$$
- On montre que $m+(n+1) = (m+n)+1$: lorsque $n = p \in \mathbb{N}$, c'est la définition et sinon, on peut écrire $n = -(p+1)$ avec $p \in \mathbb{N}$ et on calcule alors $m+(-(p+1)+1) = m-p$ ainsi que
$$\begin{aligned} (m-(p+1))+1 &= -(-m+(p+1))+1 \\ &= -((-m+p)+1)+1 \\ &= -(-(m-p)+1)+1 \\ &= -(-(m-p)) \\ &= m-p. \end{aligned}$$
- On montre par récurrence que $(m+n)+p = m+(n+p)$ lorsque $p \in \mathbb{N}$: on a $(m+n)+0 = m+n = m+(n+0)$, et si on suppose que $(m+n)+p = m+(n+p)$,

on aura

$$\begin{aligned}(m+n)+(p+1) &= ((m+n)+p)+1\\ &= (m+(n+p))+1\\ &= m+((n+p)+1)\\ &= m+(n+(p+1)).\end{aligned}$$

- On montre que $(m+n)-p = m+(n-p)$ lorsque $p \in \mathbb{N}$: on a

$$\begin{aligned}(m+n)-p &= -(-(m+n)+p)\\ &= -((-m-n)+p)\\ &= -(-m+(-n+p))\\ &= m-(-n+p)\\ &= m+(n-p).\end{aligned}$$

  L'assertion 2) est ainsi enfin démontrée et on peut dorénavant omettre les parenthèses dans une somme.
- On montre que $0+n = n\ (= n+0)$: si $p \in \mathbb{N}$, on a $0+0=0$ et si on suppose que $0+p=p$, on aura $0+p+1 = p+1$; on en déduit qu'on a aussi $0-p = -(0+p) = -p$.
- On a $-1+1 = 0 = 1-1$: D'un coté, c'est la définition et de l'autre $1-1 = -(-1+1) = -0 = 0$.
- On montre par récurrence sur $p \in \mathbb{N}$ que $1+p = p+1$: on a bien sûr $1+0 = 1 = 0+1$ et si $1+p = p+1$, alors $1+p+1 = p+1+1$.
- On montre par récurrence sur $p \in \mathbb{N}$ que $1-p = -p+1$: on a bien sûr $1-0 = 1 = -0+1$ et si $1-p = -p+1$, alors $1-(p+1) = 1-p-1 = -p+1-1 = -p+0 = -p$ et $-(p+1)+1 = -p-1+1 = -p+0 = -p$.
  On voit que l'assertion 1) est satisfaite dans le cas ou $n=1$.
- On montre par récurrence sur $p \in \mathbb{N}$ que $p+m = m+p$: on sait déjà que $0+m = m = m+0$ et si on suppose que $p+m = m+p$, on aura $p+1+m = p+m+1 = m+p+1$.
- On montre que si $p \in \mathbb{N}$, alors $-p+m = m-p$: en effet, on aura $-(-p+m) = p-m = -m+p = -(m-p)$.
  Cela démontre l'assertion 1) et on peut dorénavant intervertir l'ordre des éléments dans une somme.
- On montre par récurrence sur $p \in \mathbb{N}$ que $-p+p = 0$: On a bien sûr $-0+0 = 0+0 = 0$ et si $-p+p = 0$, alors $-(p+1)+p+1 = -p-1+p+1 = -p+p-1+1 = 0+0 = 0$.
  Par symétrie, on voit que l'assertion 4) est toujours satisfaite. ■

Remarque
- Comme nous l'avons déjà fait au cours de la démonstration, on écrira $n_1+n_2+n_3$ sans les parenthèses puisqu'il n'y a pas d'ambiguïté.
- $\mathbb{Z}$ est un groupe abélien pour l'addition (ces quatre propriétés).
- Si $p, q \in \mathbb{N}$, alors $p+q \in \mathbb{N}$ (les trois premières propriétés sont toujours satisfaites mais leur démonstration est dans ce cas bien plus élémentaire).

Définition 6.1.4 La *multiplication* des entiers est l'opération qui associe à $m, n \in \mathbb{Z}$ leur *produit* mn défini

1. par récurrence si $m = p \in \mathbb{N}$ par
$$0n := 0 \quad \text{et} \quad (p+1)n := pn + n,$$
2. par la formule $(-p)n := -(pn)$ si $m = -p$ avec $p \in \mathbb{N}_{\neq 0}$.

Proposition 6.1.5
1. $\forall m, n \in \mathbb{Z}, \quad mn = nm,$
2. $\forall n_1, n_2, n_3 \in \mathbb{Z}, \quad (n_1 n_2) n_3 = n_1 (n_2 n_3),$
3. $\forall n \in \mathbb{Z}, \quad 1n = n,$
4. $\forall n_1, n_2, n_3 \in \mathbb{Z}, \quad n_1(n_2 + n_3) = n_1 n_2 + n_1 n_3.$

Démonstration. Analogue à la démonstration précédente (exercice). ■

Remarque
- On écrira $n_1 n_2 n_3$ sans les parenthèses puisqu'il n'y a pas d'ambiguïté.
- $\mathbb{Z}$ est un *anneau commutatif* (groupe abélien pour l'addition plus ces quatre propriétés).
- $\mathbb{Z}$ est un anneau *intègre* :
$$\forall m, n \in \mathbb{Z}, \quad mn = 0 \Leftrightarrow m = 0 \text{ ou } n = 0.$$
- Si $p, q \in \mathbb{N}$, alors $pq \in \mathbb{N}$ (et les propriétés se démontrent bien plus facilement).

Définition 6.1.6 L'opération *puissance* associe à $m \in \mathbb{Z}$ et $p \in \mathbb{N}$ la *puissance p-ème de m* définie par récurrence sur p par
$$m^0 := 1 \quad \text{et} \quad m^{p+1} = m^p m.$$

Proposition 6.1.7
1. $\forall m \in \mathbb{Z}, p, q \in \mathbb{N}, \quad m^{p+q} = m^p m^q,$
2. $\forall m \in \mathbb{Z}, p, q \in \mathbb{N}, \quad m^{pq} = (m^p)^q,$
3. $\forall m, n \in \mathbb{Z}, p \in \mathbb{N}, \quad (mn)^p = m^p n^p.$

Démonstration. Exercice de récurrence. ■

Remarque On dispose aussi de l'importante formule du binôme
$$\forall m, n \in \mathbb{Z}, \forall p \in \mathbb{N}, \quad (m+n)^p = \sum_{k=0}^{p} \binom{p}{k} m^k n^{p-k}.$$

Définition 6.1.8 L'*ordre* dans $\mathbb{Z}$ est la relation définie par
$$m \leq n \Leftrightarrow n - m \in \mathbb{N}.$$

Remarque
- On dit alors que m est *inférieur (ou égal)* à n.
- On dira que m est *strictement inférieur* à n et on écrira $m < n$ si, de plus, $m \neq n$.

- On utilise aussi le vocabulaire et les notations symétriques ($\geq, >$: supérieur et supérieur strict).
- On a $\mathbb{N} = \mathbb{Z}_{\geq 0}$ et nous utiliserons désormais cette notation.

Proposition 6.1.9 1. $\forall n \in \mathbb{Z}, \quad n \leq n$,
2. $\forall n_1, n_2, n_3 \in \mathbb{Z}, \quad n_1 \leq n_2$ et $n_2 \leq n_3 \Rightarrow n_1 \leq n_3$,
3. $\forall n, m \in \mathbb{Z}, \quad n \leq m$ et $m \leq n \Rightarrow m = n$.

Démonstration. 1. $n - n = 0 \in \mathbb{Z}_{\geq 0}$,
2. $n_3 - n_1 = (n_3 - n_2) + (n_2 - n_1) \in \mathbb{Z}_{\geq 0}$,
3. $n - m \in \mathbb{Z}_{\geq 0}$ et $-(n - m) \in \mathbb{Z}_{\geq 0}$, donc $n - m = 0$. ■

Remarque
- Ces propriétés définissent une *relation d'ordre* sur $\mathbb{Z}$ (réflexive, transitive, antisymétrique).
- Il est important aussi de noter que l'ordre est *total* :

$$\forall m, n \in \mathbb{Z}, \quad m \leq n \text{ ou } n \leq m.$$

Proposition 6.1.10 1. $\forall n_1, n_2, n_3 \in \mathbb{Z}, \quad n_1 + n_3 \leq n_2 + n_3 \Leftrightarrow n_1 \leq n_2$,
2. $\forall m, n \in \mathbb{Z}, \forall p \in \mathbb{Z}_{>0}, \quad mp \leq np \Leftrightarrow m \leq n$.

Démonstration. Laissé en exercice. ■

Remarque
- On a

$$\forall m, n \in \mathbb{Z}, \quad -m \leq -n \Leftrightarrow n \leq m.$$

- On peut montrer aussi que

$$\forall m, n \in \mathbb{Z}_{\geq 0}, p \in \mathbb{Z}_{>0} \quad m^p \leq n^p \Leftrightarrow m \leq n.$$

- Vérifions que l'ensemble des inversibles de $\mathbb{Z}$ est $\mathbb{Z}^\times = \{-1, 1\}$. On rappelle que $m \in \mathbb{Z}$ est *inversible* s'il existe $n \in \mathbb{Z}$ tel que $mn = 1$. Clairement, on a $1 \times 1 = 1$ et $(-1) \times (-1) = 1$. Réciproquement, si $mn = 1$, alors quitte à remplacer m et n par leurs opposés, on peut supposer $m, n \geq 0$. On a alors nécessairement $m, n > 0$ si bien que $mn = 1 \leq n$ et donc $m \leq 1$ si bien que $m = 1$.

Définition 6.1.11 Soit $E \subset \mathbb{Z}$.
1. Un *majorant* (resp. *minorant*) de E est un $n \in \mathbb{Z}$ tel que

$$\forall k \in E, \quad k \leq n \quad (\text{resp. } \forall k \in E, \quad n \leq k).$$

2. Si $k_0 \in E$ et k_0 est un majorant (resp. minorant) de E, on dit que k_0 est *le plus grand élément* (resp. *le plus petit élément*) de E.

Exemple 1. 4 est un majorant de $E := \{1, 2, 3\}$ mais 3 et 5 sont aussi des majorants. En fait, 3 est le plus grand élément.

2. L'ensemble E des entiers naturels pairs n'a pas majorant.

Remarque
- Il n'existe pas toujours de majorant (resp. minorant) mais si c'est le cas, il y en a toujours une infinité.
- Si E possède un majorant (resp. minorant), on dit que E est *majorée* (resp. *minorée*). Si les deux conditions sont remplies, on dit *bornée*.
- Le plus grand (resp. plus petit) élément n'existe pas toujours mais s'il existe, il est *unique*. On l'appelle aussi le *maximum* (resp. *minimum*) de E et on le note $\max(E)$ (resp. $\min(E)$).
- Si n est un entier quelconque, on a $|n| = \max\{n, -n\}$.
- n est un majorant de E si et seulement si $-n$ est un minorant de $-E := \{-k : k \in E\}$ (et k_0 est le plus grand élément de E si et seulement si $-k_0$ est le plus petit élément de $-E$). Et réciproquement.

Théoreme 6.1.12 Toute partie majorée (resp. minorée) non vide de $\mathbb{Z}$ possède un plus grand (resp. plus petit) élément.

Démonstration. Il suffit de traiter le cas d'une partie E majorée par un entier n. On montre en fait par récurrence sur $p \in \mathbb{Z}_{\geq 0}$ l'implication suivante

$$(\exists k_0 \in E, n \leq k_0 + p) \Rightarrow (\exists k_0 \in E, \forall k \in E, k \leq k_0).$$

Il suffira pour conclure d'exhiber un seul $p \in \mathbb{Z}_{\geq 0}$ qui satisfait l'hypothèse. Pour notre récurrence, le cas $p = 0$ est immédiat car alors $n = k_0$ est un majorant qui est dans E. On suppose maintenant que la propriété est satisfaite pour un certain $p \in \mathbb{Z}_{\geq 0}$ et qu'il existe $k_0 \in E$ tel que $n \leq k_0 + p + 1$. S'il existe $k \in E$ tel que $n \leq k + p$, on peut conclure par récurrence. Sinon, pour tout $k \in E$, on a $k + p < n \leq k_0 + p + 1$ si bien que $k \leq k_0$ qui est donc le plus grand élément de E. Pour conclure, puisque $E \neq \emptyset$, on peut trouver $k_0 \in E$ et l'hypothèse est donc satisfaite avec $p = n - k_0 \in \mathbb{Z}_{\geq 0}$. ■

Remarque
- Comme corollaire, on voit que les entiers naturels sont *bien ordonnés* : toute partie non-vide possède un un plus petit élément.
- Ironie du sort, cette propriété fut cruciale pour démontrer la validité du raisonnement par récurrence. Or ce principe est incontournable dans cette section (y compris dans notre dernière démonstration). Ceci mérite une réflexion que nous préférons remettre à plus tard.
- L'assertion est bien sûr fausse dans $\mathbb{R}$ où $[0, 1[$ est borné mais n'a pas de plus grand élément : il faut alors faire intervenir la notion plus subtile de *borne supérieure* (plus petit des majorants) ou *inférieure* qui se note sup (resp. inf) - à ne pas confondre avec max (resp. min).

6.2 Division et congruence

Théoreme 6.2.1 Si $a \in \mathbb{Z}$ et $b \in \mathbb{Z}_{\neq 0}$, alors il existe $q, r \in \mathbb{Z}$ uniques tels que $a = bq + r$ et $0 \leq r < |b|$.

Démonstration.
- Existence : lorsque $a = 0$, on peut prendre $q = r = 0$ et on suppose dorénavant que $a \neq 0$. Si $b > 0$, on considère l'ensemble

$$E := \{c \in \mathbb{Z} \ / \ a < b(c+1)\}.$$

C'est un ensemble minoré (par $-|a|$ par exemple) et non-vide (car contenant $|a|$ par exemple). Il possède donc un plus petit élément q si bien que

$$bq \leq a < b(q+1)$$

et il suffit alors de poser $r = a - bq$. Lorsque $b < 0$, on écrit $a = |b|q' + r$ et on pose $q = -q'$.
- Unicité : supposons que $bq_1 + r_1 = bq_2 + r_2$ avec $0 \leq r_1, r_2 < |b|$. On a alors $|b||q_2 - q_1| = |r_2 - r_1|$ si bien que $0 \leq |b||q_2 - q_1| < |b|$. Puisque $b \neq 0$, cela signifie que $0 \leq |q_2 - q_1| < 1$ et donc $q_2 = q_1$. On a alors aussi $r_2 = r_1$. ■

Remarque Dans la démonstration, nous avons affirmé que E est minoré par $-|a|$. En effet, si $c + 1 \geq 0$, alors $-|a| \leq -1 \leq c$ (puisque $a \neq 0$). Et si $c + 1 < 0$, alors $-|a| \leq a < b(c+1) < c + 1$ (puisque $b > 0$). Nous avons aussi affirmé que $|a| \in E$. En effet, $a \leq |a| < |a| + 1 \leq b(|a| + 1)$ (puisque $b > 0$ encore).

Définition 6.2.2 On dit alors que q est le *quotient* et que r est le *reste* de la *division euclidienne* de a par b.

Exemple Effectuons la division euclidienne de 733 par 13 :

$$\begin{array}{r|l} 733 & 13 \\ 83 & 56 \\ 5 & \end{array} .$$

Le quotient vaut 56 et le reste vaut 5 : en effet, on a

$$733 = 13 \times 56 + 5 \quad \text{et} \quad 0 \leq 5 < 13.$$

Définition 6.2.3 La *division* dans $\mathbb{Z}$ est la relation définie par

$$b \mid a \quad \Leftrightarrow \quad (\exists q \in \mathbb{Z}, a = qb).$$

On dit alors que b est un *diviseur* de a ou que a est un *multiple* de b.

Remarque
- Si $b \neq 0$, alors $b \mid a$ si et seulement si le reste dans la division euclidienne de a par b est 0.
- Attention : tout entier divise 0 mais 0 est l'unique multiple de 0.
- On a $b \mid a \Leftrightarrow |b| \mid |a|$.

- Si $b \mid a$ et $a \neq 0$, alors $|b| \leq |a|$.
- Lorsque $b \neq 0$, on a $a/b \in \mathbb{Q}$ et $b \mid a \Leftrightarrow a/b \in \mathbb{Z}$. On évitera en fait ce genre de considération.

Exemple $13 \mid 1001, -1 \mid 2, 1 \mid 0, 0 \nmid 1, 6 \nmid 10$.

Proposition 6.2.4 1. $\forall a \in \mathbb{Z}, \quad a \mid a$,
2. $\forall a, b, c \in \mathbb{Z}, \quad a \mid b$ et $b \mid c \Rightarrow a \mid c$,
3. $\forall a, b \in \mathbb{Z}, \quad a \mid b$ et $b \mid a \Leftrightarrow |a| = |b|$.

Démonstration. 1. $a = a1$,
2. Si $b = pa$ et $c = qb$, alors $c = (pq)a$,
3. Si $b = pa$ et $a = qb$, alors $a = (pq)a$ si bien que, soit $a = 0$ et alors $b = 0$ aussi, ou bien $pq = 1$ et alors $|p| = |q| = 1$.

■

Remarque On obtient donc une relation de *préordre* (les deux premières propriétés) sur $\mathbb{Z}$ et d'*ordre* (les trois) sur $\mathbb{Z}_{\geq 0}$. Attention cependant que cet ordre n'est pas *total* : on a $2 \nmid 3$ et $3 \nmid 2$.

Proposition 6.2.5 Si $\forall a, b, c \in \mathbb{Z}$, on a
1. $a \mid b$ et $a \mid c \Rightarrow a \mid (b + c)$,
2. $a \mid b \Rightarrow a \mid bc$,
3. $ac \mid bc \Leftrightarrow (a \mid b$ ou $c = 0)$.

Démonstration. 1. Si $b = pa$ et $c = qa$, alors $b + c = (p + q)a$,
2. Si $b = pa$, alors $bc = (pc)a$,
3. on a $bc = pac \Leftrightarrow (b = pa$ ou $c = 0)$.

■

Remarque Comme conséquence, on voit que :
- si $a \mid b$ et $a \mid c$, alors $a \mid b - c$,
- si $a \mid b$, alors $a \mid c \Leftrightarrow a \mid (b + c)$,
- Si $a \mid b$, alors $a^k \mid b^k$ (on verra la réciproque plus tard).

Définition 6.2.6 Deux entiers a et b sont *congrus* modulo un entier n si n divise $b - a$. On écrit alors $a \equiv b \mod n$.

Exemple On a $9 \equiv 5 \mod 2$ mais aussi $9 \equiv 1 \mod 2$ et $9 \equiv 5 \mod 4$. On a $25 \equiv -1 \mod 13$.

Remarque
- Plus prosaïquement, « congrus modulo n » signifie comme toujours : « égaux quitte à ajouter un multiple entier de n ».
- On a $a \equiv b \mod n$ si et seulement si a et b ont même reste dans la division euclidienne par n (si $a, b \neq 0$).
- Le reste dans la division de a par b est le plus petit entier naturel r tel que $a \equiv r \mod b$ (si $b \neq 0$).
- On a $b \mid a \Leftrightarrow a \equiv 0 \mod b$.

Proposition 6.2.7 1. $\forall a \in \mathbb{Z}, a \equiv a \mod n$,
2. $\forall a, b \in \mathbb{Z}, a \equiv b \mod n$ et $b \equiv c \mod n \Leftrightarrow a \equiv c \mod n$,
3. $\forall a, b \in \mathbb{Z}, a \equiv b \mod n \Leftrightarrow b \equiv a \mod n$.

Démonstration. 1. On a $n \mid 0 = a - a$,
2. si $n \mid (b-a)$ et $n \mid (c-b)$, alors $n \mid ((b-a)+(c-b) = (c-a)$,
3. si $n \mid (b-a)$ alors $n \mid (a-b) = -(b-a)$.

■

Remarque Cela signifie que la relation de congruence est une relation d'équivalence.

Proposition 6.2.8 Si $a \equiv a' \mod n$ et $b \equiv b' \mod n$, alors $a+b \equiv a'+b' \mod n$ et $ab \equiv a'b' \mod n$

Démonstration. Si n divise $a'-a$ et $b'-b$, alors n divise leur somme $(a'-a)+(b'-b) = (a'+b')-(a+b)$. De même, n divise $a'(b'-b)$ ainsi que $(a'-a)b$ et donc leur somme $a'(b'-b)+(a'-a)b = a'b'-ab$. ■

Remarque
- On aura aussi $a - b \equiv a' - b' \mod n$ lorsque $a \equiv a' \mod n$ et $b \equiv b' \mod n$.
- Si $a \equiv b \mod n$ et $k \in \mathbb{Z}$, alors $ka \equiv kb \mod n$.
- Si $a \equiv b \mod n$ et $k \in \mathbb{Z}_{\geq 0}$, alors $a^k \equiv b^k \mod n$.
- Si $k \in \mathbb{Z}_{\neq 0}$, alors $a \equiv b \mod n \Leftrightarrow ka \equiv kb \mod kn$ (attention au module).

Exemple Quel est le reste dans la division de 100^{1000} par 13 ? On a déjà

$$100 = 13 \times 7 + 9 \equiv 9 \mod 13.$$

On en déduit que $100^{1000} \equiv 9^{1000} \mod 13$. On calcule ensuite

$$9^2 = 81 = 13 \times 6 + 3 \equiv 3 \mod 13 \text{ (pas bon)},$$

puis

$$9^3 = 9 \times 9^2 \equiv 9 \times 3 = 27 = 13 \times 2 + 1 \equiv 1 \mod 13 \text{ (bon)}.$$

On a $1000 = 3 \times 333 + 1$ et on en déduit que

$$100^{1000} \equiv 9^{1000} = 9^{3\times 333+1} = (9^3)^{333} \times 9 \equiv 1^{333} \times 9 = 1 \times 9 = 9$$

si bien que le reste est 9.

6.3 pgcd et ppcm

Lemme 6.3.1 Si $a, b \in \mathbb{Z}$, alors il existe
1. un plus grand diviseur commun (pgcd) à a et b si on suppose que $a \neq 0$ ou $b \neq 0$, on le note $a \wedge b$,
2. un plus petit multiple commun strictement positif (ppcm) à a et b si on suppose que $a \neq 0$ et $b \neq 0$, on le note $a \vee b$.

Démonstration. 1. L'ensemble des diviseurs communs est majoré (par $|a|$ par exemple si c'est a qui est non nul) et non-vide (puisqu'il contient toujours 1). Il possède donc un plus grand élément.
2. Les multiples communs strictement positifs forment un ensemble minoré (par 0) et non-vide (puisqu'il contient $|ab|$). Celui-ci possède donc un plus petit élément. ■

Par *convention*, $0 \wedge 0 = 0$ et $a \vee 0 = 0 \vee b = 0$.

Proposition 6.3.2 1. $\forall a, b \in \mathbb{Z}, \quad a \wedge b = b \wedge a \quad$ et $\quad a \vee b = b \vee a$,
2. $\forall a, b \in \mathbb{Z}, \quad (a \wedge b) \wedge c = a \wedge (b \wedge c) \quad$ et $\quad (a \vee b) \vee c = a \vee (b \vee c)$,
3. $\forall a \in \mathbb{Z}, \quad a \wedge 0 = |a| \quad$ et $\quad a \vee 0 = 0$,
4. $\forall a \in \mathbb{Z}, \quad a \wedge 1 = 1 \quad$ et $\quad a \vee 1 = |a|$.

Démonstration. Exercice. ■

Remarque
- On a $a \wedge b = 0 \Leftrightarrow a = b = 0$ et $a \vee b = 0 \Leftrightarrow a = 0$ ou $b = 0$.
- On a toujours $a \wedge b := |a| \wedge |b|$ et $a \vee b := |a| \vee |b|$.
- On a $a \mid b \Leftrightarrow a \wedge b = |a| \Leftrightarrow a \vee b = |b|$.
- On écrira $a \wedge b \wedge c$ et $a \vee b \vee c$ puisqu'il n'y a pas d'ambiguïté. Notons que c'est en fait le plus plus grand diviseur commun (resp. plus petit multiple commun strictement positif) à a, b et c (ou 0).

Exemple $6 \wedge 10 \wedge 15 = (6 \wedge 10) \wedge 15 = 2 \wedge 15 = 1$ et $6 \vee 10 \vee 15 = (6 \vee 10) \vee 15 = 30 \vee 15 = 30$.

Lemme 6.3.3 Soient $a, p, b, q \in \mathbb{Z}$ tels que $a = bq + r$. Alors, $a \wedge b = b \wedge r$.

Démonstration. Si on suppose que $c \mid b$, on aura $c \mid bq$ et donc $c \mid a \Leftrightarrow d \mid r$ si bien que $c \mid a \wedge b \Leftrightarrow c \mid b \wedge r$. ■

Remarque On en déduit l'*algorithme d'Euclide* pour déterminer le pgcd de deux entiers a et b : on pose $d_0 := a, d_1 := b$ puis on définit d_{n+2} par la récurrence

$$d_n = q_n d_{n+1} + d_{n+2} \quad \text{avec } 0 \leq d_{n+2} < d_{n+1}$$

jusqu'à ce que $d_{n+1} = 0$; on aura alors

$$a \wedge b = d_0 \wedge d_1 = d_1 \wedge d_2 = \cdots = d_n \wedge d_{n+1} = d_n \wedge 0 = d_n.$$

Exemple On a $598 \wedge 414 = 46$:

$$598 = 414 \times 1 + 184,$$
$$414 = 184 \times 2 + 46,$$
$$184 = 46 \times 4 + 0.$$

Théoreme 6.3.4 — de Bézout. Si $a, b, d \in \mathbb{Z}$, alors

$$|d| = a \wedge b \Leftrightarrow (d \mid a, d \mid b \text{ et } \exists u, v \in \mathbb{Z}, au + bv = d).$$

Démonstration. Dans le cas ou $d = 0$, l'assertion est trivialement vraie et on peut donc supposer dorénavant que $d \neq 0$. La condition est alors clairement suffisante : si $c \mid a$ et $c \mid b$, alors $c \mid d = au + bv$ et donc $c \leq |d|$. Pour montrer qu'elle est nécessaire, on raffine l'algorithme d'Euclide (ci-dessus) en définissant deux suites finies $u_n, v_n \in \mathbb{Z}$ telles que $d_n = au_n + bv_n$. On pose tout d'abord

$$u_0 := 1, \quad v_0 := 0, \quad u_1 := 0, \quad v_1 := 1$$

On a donc bien $d_0 = a$ et $d_1 = b$. Si $d_{n+1} = 0$, on a $d_n = d$ et il suffit donc de poser $u := u_n$ et $v := v_n$. Sinon, on a $d_n = q_n d_{n+1} + d_{n+2}$ avec $0 \leq d_{n+2} < d_{n+1}$. On pose alors

$$u_{n+2} := u_n - q_n u_{n+1} \quad \text{et} \quad v_{n+2} = v_n - q_n v_{n+1}.$$

On a aura bien

$$\begin{aligned} au_{n+2} + bv_{n+2} &= a(u_n - q_n u_{n+1}) + b(v_n - q_n v_{n+1}) \\ &= au_n + bv_n - q_n(au_{n+1} + bv_{n+1}) \\ &= d_n - q_n d_{n+1} \\ &= d_{n+2}. \end{aligned}$$

■

Exemple

1. On a $1 \times 3 - 1 \times 2 = 1$, $1 \times 4 - 1 \times 2 = 2$, $1 \times 4 - 1 \times 3 = 1$, $1 \times 5 - 2 \times 2 = 1$, etc.
2. On a $-2 \times 598 + 3 \times 414 = 46$:

$$\begin{aligned} 598 &= 1 \times 598 + 0 \times 414 \\ 414 &= 0 \times 598 + 1 \times 414 \quad (-1 \times -) \\ 184 &= 1 \times 598 - 1 \times 414 \quad (-2 \times -) \\ 46 &= -2 \times 598 + 3 \times 414. \end{aligned}$$

3. Méthode alternative (voir ci-dessous) : la division euclidienne usuelle nous fournit

$$\begin{aligned} 598 &= 1 \times 414 + 184, \\ 414 &= 2 \times 184 + 46. \end{aligned}$$

On en déduit

$$\begin{aligned} 46 &= 414 - 2 \times 184 \\ &= 414 - 2 \times (598 - 1 \times 414) \\ &= -2 \times 598 + 3 \times 414. \end{aligned}$$

4. On a

$$10 \wedge 6 = 2 = -1 \times 10 + 2 \times 6 \quad \text{et} \quad 15 \wedge 2 = 1 = 1 \times 15 - 7 \times 2.$$

On en déduit

$$15 \wedge 10 \wedge 6 = 1 = 1 \times 15 - 7 \times (-1 \times 10 + 2 \times 6) = 1 \times 15 + 7 \times 10 - 14 \times 6.$$

Remarque

- Comme conséquence du théorème de Bézout, on voit que

$$c \mid a \text{ et } c \mid b \Leftrightarrow c \mid a \wedge b.$$

- Alternative à l'algorithme d'Euclide étendu (voir ci-dessus) : on détermine la suite d_n comme d'habitude en posant $d_0 := a, d_1 := b$ puis par récurrence

$$d_n = q_n d_{n+1} + d_{n+2} \quad \text{avec } d_{n+2} < d_{n+1}$$

jusqu'à ce que $d_n = a \wedge b$. On remonte ensuite par récurrence en posant $u_1 = 0$ et $u_2 = 1$, puis $u_{k+2} = u_k - q_{n-k-1} u_{k+1}$, de telle sorte que $d_n = u_k d_{n-k} + u_{k-1} d_{n-k+1}$ et il suffit de prendre $k = n$.
- En utilisant le théorème de Bézout et la formule du binôme, on peut montrer que pour tout $n > 0$, on a

$$a^n \wedge b^n = (a \wedge b)^n.$$

On se ramène au cas où $a \wedge b = 1$ et on écrit $1 = au + bv$ puis

$$1 = (au + bv)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i} (au)^i (bv)^{2n-i}$$

$$= \left(\sum_{i=n}^{2n} \binom{2n}{i} (au)^{i-n} (bv)^{2n-i} \right) a^n + \left(\sum_{i=0}^{n-1} \binom{2n}{i} (au)^i (bv)^{n-i} \right) b^n.$$

6.4 Entiers premiers entre eux

Définition 6.4.1 Deux entiers a et b sont *premiers entre eux* si $a \wedge b = 1$.

Exemple On a $2 \wedge 3 = 1$, $1000 \wedge 1001 = 1$, $10000 \wedge 59 = 1$.

Corollaire 6.4.2 Deux entiers a et b sont premiers entre eux si et seulement si il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. ■

Remarque Attention : ce résultat n'est pas valable dans des situations plus générales : par exemple les polynômes X et Y sont premiers entre eux (ils n'ont pas de diviseur commun non constant) mais on ne peut pas écrire $XU(X,Y) + YV(X,Y) = 1$ avec deux polynômes U et V.

Théoreme 6.4.3 Soient $a, b \in \mathbb{Z}$ premiers entre eux et $c \in \mathbb{Z}$. Alors,
1. (lemme de Gauss) $a \mid bc \Leftrightarrow a \mid c$,
2. $(a \mid c \text{ et } b \mid c) \Leftrightarrow ab \mid c$.

Démonstration. Dans chaque cas, la condition est clairement suffisante et il reste à montrer qu'elle est nécessaire. On écrit $au + bv = 1$ et on a donc $acu + bcv = c$ si bien que,
1. si $a \mid bc$, alors $a \mid bcv$ et comme $a \mid acu$, on voit que $a \mid c$,
2. si $a \mid c$ alors $ab \mid bcv$, et si $b \mid c$ alors $ab \mid acu$, et on a donc $ab \mid c$. ■

Corollaire 6.4.4 — Théorème chinois. Soient m et n deux entiers premiers entre eux. Alors,

$$\forall a, b \in \mathbb{Z}, \quad a \equiv b \mod n \text{ et } a \equiv b \mod m \Leftrightarrow a \equiv b \mod mn$$

Démonstration. En effet, on a $n \mid b-a$ et $m \mid b-a$ si et seulement si $mn \mid b-a$. ■

Proposition 6.4.5 Si $a, b \in \mathbb{Z}$, on a
1. $(a \wedge b)(a \vee b) = |ab|$,
2. $\forall c \in \mathbb{Z}, \quad c \mid (a \wedge b) \Leftrightarrow (c \mid a \text{ et } c \mid b)$,
3. $\forall c \in \mathbb{Z}, \quad (a \vee b) \mid c \Leftrightarrow (a \mid c \text{ et } b \mid c)$.

Démonstration. La seconde assertion résulte du théorème de Bézout. Pour la troisième, on voit immédiatement que la condition est nécessaire et il reste à montrer qu'elle est suffisante. On pose $d := a \wedge b$. Si $d = 0$, on a aussi $a = b = 0$ et tout est clair. Sinon, on écrit $a = da'$, $b = db'$ si bien que $a' \wedge b' = 1$. Supposons que $a \mid c$ et $b \mid c$. On a alors en particulier $d \mid c$ si bien que $c = dc'$. On en déduit que $a' \mid c'$ et $b' \mid c'$ et le lemme de Gauss implique que $a'b' \mid c'$ si bien que $da'b' \mid dc' = c$. Cela montre que $a \vee b = d|a'b'|$ et que $a \vee b \mid c$. Et on a alors aussi $(a \wedge b)(a \vee b) = d^2|a'b'| = |ab|$. ■

Corollaire 6.4.6 $\forall a, b, c \in \mathbb{Z}, \quad ca \wedge cb = |c|(a \wedge b)$ et $ca \vee cb = |c|(a \vee b)$

Démonstration. Si $c = 0$, c'est clair. Et de même, si $a = 0$ ou $b = 0$. Sinon, d est un diviseur (resp. multiple) commun à a et b si et seulement si $|c|d$ est un diviseur (resp. multiple) commun à ca et cb. ■

6.5 Nombres premiers

Définition 6.5.1 Un entier p est *premier* s'il possède un unique diviseur strictement plus grand que 1.

Remarque
- L'unique diviseur strictement plus grand que 1 est nécessairement $|p|$.
- Attention : traditionnellement, un *nombre premier* est un entier *naturel* qui est premier.
- Un entier p est premier si et seulement si $|p|$ est premier.

- Les nombres 0 et 1 ne sont pas premiers (tous les entiers divisent 0 et seulement 1 et -1 divisent 1).
- La définition correcte d'*entier premier* est en fait la condition (équivalente) du lemme d'Euclide que nous verrons plus bas. La définition ci-dessus est plutôt celle d'un entier *irréductible* (qui est en fait équivalente).

Exemple
1. $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, \ldots$
2. $3, 5, 17, 257, 65537$ (nombres de Fermat).
3. $3, 7, 127, 8191$ (nombres de Mersenne).

Lemme 6.5.2 Si $n > 1$ n'est pas premier, alors il existe un nombre premier p tel que $p \mid n$ et $p^2 \leq n$.

Démonstration. Puisque $n > 1$, il existe un diviseur p de n avec $p > 1$. On peut supposer que p est le plus petit. Comme première conséquence, on voit que p est premier (car tout diviseur de p est aussi un diviseur de n). On écrit ensuite $n = pa$. Puisque n n'est pas premier, on a nécessairement $a > 1$. Comme a est un diviseur de n et que $a > 1$, on doit avoir $p \leq a$ si bien que $p^2 \leq pa = n$. ■

Remarque
- Le *crible d'Ératosthène* est un algorithme qui permet de trouver tous les nombres premiers (inférieurs à $n > 1$ fixé). On fait la liste croissante de tous les entiers entre 2 et n. On pose $p = 2$ et on commence la boucle. On raye tous les autres multiples de p. Soit q le prochain entier qui n'est pas rayé. Si $q^2 > n$, on arrête. Sinon, on pose $p := q$ et on reprend la boucle.
- Le lemme nous montre aussi que deux entiers a et b ne sont pas premier entre eux si et seulement si ils ont un facteur premier en commun (leur pgcd est plus grand que un - ou nul).

Lemme 6.5.3 Un entier p est premier si et seulement si

$$\forall a \in \mathbb{Z}, \quad p \wedge a = 1 \Leftrightarrow p \nmid a$$

(a est premier avec p si et seulement si a n'est pas un multiple de p).

Démonstration. Supposons que p est premier et soit a un entier quelconque. Si $p \mid a$, alors $p \wedge a = |p| > 1$ puisque p est premier. Réciproquement, si $p \wedge a = d > 1$, alors $d \mid p$ et donc $|p| = d$ puisque p est premier si bien que $p \mid a$. La réciproque est laissée en exercice. ■

Lemme 6.5.4 — d'Euclide. Un entier $p \neq 0, 1, -1$ est premier si et seulement si

$$\forall a, b \in \mathbb{Z}, \quad p \mid ab \Leftrightarrow p \mid a \text{ ou } p \mid b$$

(p divise un produit si et seulement si il divise un des facteurs).

Démonstration. On a bien sûr toujours :

$$p \mid a \text{ ou } p \mid b \Rightarrow p \mid ab.$$

On vient de voir que si $p \nmid a$, alors $p \wedge a = 1$. Il résulte alors du lemme de Gauss que si $p \mid ab$, alors nécessairement $p \mid b$. La réciproque est laissée en exercice. ■

Remarque On voit donc par récurrence sur $n \geq 1$ que $p \mid a^n \Leftrightarrow p \mid a$.

Corollaire 6.5.5 $\forall a, b \in \mathbb{Z}, \forall n \in \mathbb{Z}_{>0}, \quad a^n \wedge b^n = (a \wedge b)^n.$

Démonstration. On suppose pour commencer que a et b sont premiers entre eux et on montre que $a^n \wedge b^n$ n'a aucun diviseur premier (c'est-à-dire est égal à 1). En effet, grâce au lemme d'Euclide, un tel diviseur premier diviserait nécessairement $a \wedge b$ (par conjonction des cas). En général, on écrit $a = da'$ et $b = db'$ avec $a' \wedge b' = 1$. ■

Théoreme 6.5.6 Tout entier $n > 1$ s'écrit de manière unique sous la forme

$$n = p_1^{v_1} \dots p_r^{v_r}$$

avec $1 < p_1 < \cdots < p_r$ premiers et $v_1, \dots, v_r \geq 1$.

Démonstration. Si n est premier, c'est clair. On désigne maintenant par p le plus grand diviseur premier de n. Si on se donne une décomposition de n comme dans le théorème, on a, grâce au lemme d'Euclide, $p \mid p_i$ pour un certain $i \in \{1, \cdots, r\}$. Et comme p_i est premier, $p = p_i$. On aura donc nécessairement $p_r = p$. On procède ensuite par récurrence sur n. On sait déjà que 2 est premier et on peut aussi supposer que n n'est pas premier. On peut donc écrire a $n = mp$ avec $1 < m < n$, et par récurrence, $m = p_1^{v_1} \cdots p_r^{v_r}$ de manière unique avec $1 < p_1 < \cdots < p_r$ premiers et $v_1, \dots, v_r \geq 1$. On a nécessairement $p_r \leq p$. Si $p_r = p$, on a pas le choix : on remplace v_r par $v_r + 1$. Sinon, on a pas le choix non plus : on rajoute $p_{r+1} := p$. ■

Remarque On en déduit que le nombre de diviseurs positifs de n est $(v_1 + 1)(v_2 + 1) \cdots (v_r + 1)$. Par exemple, les diviseurs de 12 sont $1, 2, 3, 4, 6, 12$, on a $12 = 2^2 \times 3^1$ et $(2 + 1)(1 + 1) = 6$.

Exemple
1. $2 = 2^1$, $3 = 3^1$, $4 = 2^2$, $5 = 5^1$, $6 = 2^1 \times 3^1$, $7 = 7^1$, $8 = 2^3$, $9 = 3^2$, $10 = 2^1 \times 5^1$, $11 = 11^1$, $12 = 2^2 \times 3$, etc.
2. $1000 = 2^3 \times 5^3$, $1001 = 7 \times 11 \times 13$, $1002 = 2 \times 3 \times 167$

Remarque
- On dit que $\mathbb{Z}$ est un anneau *factoriel*.
- Si p est un nombre premier, on pose $v_p(n) = v_i$ si $p = p_i$ et $v_p(n) = 0$ sinon. On peut alors réécrire la formule du théorème sous la forme

$$n = \prod_{p \text{ premier}} p^{v_p(n)}$$

(puisque $v_p(n)$ est presque toujours nul donc $p^{v_p(n)}$ vaut presque toujours 1).

- On prolonge v_p à $\mathbb{Z}$ tout entier en posant $v_p(1) = 0$, $v_p(0) = +\infty$ et $v_p(-n) = v_p(n)$.
- À p fixé, l'application v_p est une *valuation* :
  1. $v_p(1) = 0$, $v_p(0) = +\infty$,
  2. $\forall m, n \in \mathbb{Z}, v_p(m+n) \geq \min(v_p(m), v_p(n))$,
  3. $\forall m, n \in \mathbb{Z}, v_p(mn) = v_p(m) + v_p(n)$.
- Comme conséquence, on voit que si $n \in \mathbb{Z}$ et $k \in \mathbb{Z}_{\geq 0}$, alors $v_p(n^k) = kv_p(n)$.
- On a $m \mid n \Leftrightarrow \forall p$ premier, $v_p(m) \leq v_p(n)$.
- On peut en déduire que si $k > 0$, alors $m \mid n \Leftrightarrow m^k \mid n^k$.

Corollaire 6.5.7 Si $n = p_1^{v_1} \dots p_r^{v_r}$ et $m = p_1^{w_1} \dots p_r^{w_r}$ avec $p_1, \dots, p_r$ premiers distincts, alors

$$n \wedge m = p_1^{\min(v_1,w_1)} \dots p_r^{\min(v_r,w_r)} \quad \text{et} \quad n \vee m = p_1^{\max(v_1,w_1)} \dots p_r^{\max(v_r,w_r)}. \qquad \blacksquare$$

Exemple On a $n := 231868 = 2^2 \times 7^3 \times 13^2$ et $m := 8190 = 2 \times 3^2 \times 5 \times 7 \times 13$ donc $n \wedge m = 2 \times 7 \times 13 = 182$.

Lemme 6.5.8 Si p est un nombre premier et $0 < k < p$, alors $\binom{p}{k}$ est un multiple de p.

Démonstration. On a montre par récurrence la formule

$$k\binom{p}{k} = p\binom{p-1}{k-1}$$

et on conclut avec le lemme d'Euclide. $\blacksquare$

Remarque C'est faux si p n'est pas premier comme le montre le cas de $\binom{4}{2} = 6$ qui n'est pas un multiple de 4.

Théoreme 6.5.9 — de Fermat (petit). Si l'entier n n'est pas un multiple du nombre premier p, alors $n^{p-1} - 1$ est un multiple de p.

Démonstration. Grâce au lemme d'Euclide, il suffit de montrer que $n^p \equiv n \mod p$ pour tout $n \in \mathbb{Z}$. On procède par récurrence pour $n \geq 0$, le cas $n = 0$ étant trivial. On aura

$$(n+1)^p = \sum_{k=0}^{p} \binom{p}{k} n^k = n^p + 1 \equiv n + 1 \mod p.$$

Lorsque $n < 0$, il suffit de remarquer que on a $n^p - n = -(|n|^p - |n|)$. $\blacksquare$

Remarque

- En termes de congruences, le théorème dit que

$$n \not\equiv 0 \mod p \quad \Rightarrow \quad n^{p-1} \equiv 1 \mod p.$$

- Le petit théorème de Fermat est un corollaire du théorème de Lagrange qui dit que l'ordre d'un élément divise l'ordre d'un groupe : en effet, il existe exactement $p-1$ entiers non nuls modulo p (ordre) et un produit d'entiers non-nuls modulo p est toujours non nul modulo p (groupe).
- Le test de primalité de Fermat permet de dire si un nombre p est *probablement premier* en regardant si 2^{p-1}, 3^{p-1}, etc. sont congrus à 1 modulo p. Par exemple, $2^8 = 256 \equiv 4 \mod 9$ donc 9 n'est pas premier.

6.6 Exercices (21 août 2023)

La calculette pourra être utilisée comme outil d'aide à la décision mais en aucun cas comme argument scientifique.

Exercice 6.1 Effectuer les divisions euclidiennes suivantes :

1. 100001 par 101, 2. 656665 par 11, 3. 66227 par 13.

Exercice 6.2 Sachant que $12079233 = 75968 \times 159 + 321$, déterminer le reste de la division euclidienne de 12079233 par 75968 puis par 159.

Exercice 6.3 Soit n un entier naturel. Quelles valeurs peut prendre le reste de la division euclidienne de 3^n par 7 ? Même question avec 38^n.

Exercice 6.4

1. Pour quelles valeurs de l'entier naturel n le nombre $4^n + 2^n + 1$ est il divisible par 7 ?
2. Même question avec $9^n + 3^n + 1$ et 13.
3. Même question avec $25^n + 5^n + 1$ et 31.

Exercice 6.5 Déterminer en fonction de la parité de l'entier naturel n le reste dans la division de $7^n + 1$ par 8.

Exercice 6.6 Quel est le reste de la division euclidienne de 247^{349} par 7 ?

Exercice 6.7

1. Montrer que $\forall n \in \mathbb{Z}_{>0}, 6^n \equiv 6 \mod 10$.
2. En déduire le chiffre des unités du nombre 123456^{789}.
3. Montrer que $56^6 \equiv 56 \mod 100$.
4. Quel est le chiffre des dizaines de 123456^{789}.

Exercice 6.8

1. Déterminer les trois derniers chiffres de 49^2 et de 401^5 en utilisant la formule du binôme.
2. En déduire les trois derniers chiffres de 7^{20} puis de 7^{1001} ?

Exercice 6.9

1. Calculer le pgcd de 231868 et 8190. En déduire leur ppcm.
2. Même question avec 23145 et 17.
3. Même question avec 12345 et 678.

Exercice 6.10 Déterminer deux entiers u et v tels que

1. $23u + 35v = 1$, 2. $27u + 25v = 1$.

Exercice 6.11

1. Déterminer le pgcd d de $a := 2873$ et $b := 1001$ ainsi que deux entiers relatifs u et v tels que $au + bv = d$.
2. Peut-on trouver deux entiers u et v tels que $au + bv = 15$?

Exercice 6.12

1. Montrer que tout entier pair a vérifie $a^2 \equiv 0 \mod 4$.
2. Montrer que tout entier impair a vérifie $a^2 \equiv 1 \mod 8$.
3. Soient a, b, c trois entiers *impairs*.
   (a) Quel est le reste de la division de $a^2 + b^2 + c^2$ par 8 ? En déduire que ce n'est pas un carré d'un entier.

(b) En développant $(a+b+c)^2$, montrer que $ab+bc+ac \equiv 3 \mod 4$. En déduire que ce n'est pas non plus le carré d'un entier.

Exercice 6.13
1. Montrer que si a et b sont premiers entre eux alors a et $a+b$ sont aussi premiers entre eux.
2. Montrer que si a est premier avec b et c, alors a est premier avec bc
3. Montrer que si a et b sont premiers entre eux, alors pour tous entiers naturels k et l, a^k et b^l sont aussi premiers entre eux.

Exercice 6.14 Peux-t-on mettre les nombres 1 à 30 dans les cases d'un tableau de 5 lignes et 6 colonnes de sorte qu'en additionnant les nombres de chaque colonne on trouve toujours la même somme ?

Exercice 6.15
1. Montrer que si n est un entier quelconque, alors $8n+7$ et $6n+5$ sont toujours premiers entre eux.
2. Même question avec $2n+3$ et n^2+3n+2.
3. Même question avec $5^{n+1}+6^{n+1}$ et 5^n+6^n.

Exercice 6.16
1. Résoudre dans $\mathbb{Z}$ l'équation $6a+11b=1$.
2. Résoudre dans $\mathbb{Z}$ l'équation $6a+11b=6$.
3. Résoudre dans $\mathbb{Z}$ l'équation $6a+12b=5$.

Exercice 6.17 Résoudre

$$a,b \in \mathbb{Z}_{\geq 0}, \quad a \wedge b = 18 \text{ et } a \vee b = 360?$$

Exercice 6.18 On veut résoudre

$$a,b \in \mathbb{Z}_{>0}, \quad \begin{cases} a+b=51 \\ a \vee b = 216. \end{cases} \tag{6.1}$$

1. Décomposer 51, 72 et 216 en produits de facteurs premiers.
2. Quel est le pgcd de 51 et 216 ?
3. Déterminer toutes les décompositions de 72 et 216 en produits d'entiers naturels premiers entre eux.
4. Montrer que si a et b sont solutions du système (6.1), alors leur pgcd divise celui de 51 et 216.
5. Conclure.

Exercice 6.19 Les nombres 111, 1111, 11111 (persévérer), 111111 sont ils premiers ?

Exercice 6.20 Décomposer en facteur premiers les entiers 46848, 2379, 1001 et 2873.

Exercice 6.21
1. Montrer que si p premier divise à la fois $a+b$ et ab, alors p divise nécessairement a et b.
2. En déduire que si a et b sont premiers entre eux, alors $a+b$ et ab sont aussi premiers entre eux.

7. Ensembles (optionnel)

7.1 Parties d'un ensemble

Définition 7.1.1 L'*ensemble des parties* d'un ensemble E est l'ensemble $\mathcal{P}(E)$ dont les éléments sont les sous-ensembles de E.

Exemple On a $\mathcal{P}(\emptyset) = \{\emptyset\} \neq \emptyset$, $\mathcal{P}(\{1\}) = \{\emptyset, \{1\}\}$ et

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

Remarque
- Attention : $\mathcal{P}(E)$ est un ensemble dont les éléments sont eux mêmes des ensembles.
- On a $A \in \mathcal{P}(E) \Leftrightarrow A \subset E$.
- Si $E \subset F$, alors $\mathcal{P}(E) \subset \mathcal{P}(F)$.

Définition 7.1.2 Une *partition* d'un ensemble E est un sous-ensemble $\mathcal{E} \subset \mathcal{P}(E)$ tel que
1. $\forall A \in \mathcal{E}, A \neq \emptyset$,
2. $\forall A, B \in \mathcal{E}, A \cap B \neq \emptyset \Rightarrow A = B$,
3. $\forall x \in E, \exists A \in \mathcal{E}, x \in A$.

Exemple
1. Attention : une partition est un ensemble dont les éléments sont eux mêmes des ensembles.
2. Les partitions de $\{1,2,3\}$ sont
$$\{\{1\},\{2\},\{3\}\}, \{\{1,2\},\{3\}\}, \{\{1,3\},\{2\}\}, \{\{2,3\},\{1\}\} \text{ et } \{\{1,2,3\}\}.$$
3. $\{\mathbb{R}_{\geq 0}, \mathbb{R}_{<0}\}$ est une partition de $\mathbb{R}$.
4. Si on désigne par I l'ensemble des imaginaires purs, $\{\mathbb{R}, I\}$ n'est pas une partition de $\mathbb{C}$.

Définition 7.1.3 Soit $f : E \to F$ une application.

1. Si $A \subset E$, alors l'*image directe* de A par f est
$$f(A) := \{f(x), x \in A\}.$$
2. Si $B \subset F$, alors l'*image réciproque* de B par f est
$$f^{-1}(B) := \{x \in E, f(x) \in B\}.$$

Exemple
1. Avec $f : \{1, 2\} \to \{3, 4\}$ défini par $f(1) = f(2) = 3$, on aura
   - $f(\emptyset) = \emptyset$, $f(\{1\}) = \{3\}$, $f(\{2\}) = \{3\}$ et $f(\{1, 2\}) = \{3\}$.
   - $f^{-1}(\emptyset) = \emptyset$, $f^{-1}(\{3\}) = \{1, 2\}$, $f^{-1}(\{4\}) = \emptyset$ et $f^{-1}(\{3, 4\}) = \{1, 2\}$,
2. avec $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$, on a $f([-1, 1]) = [0, 1]$ et $f^{-1}([-1, 1] = [-1, 1]$,

Remarque
- Attention : l'image ainsi que l'image réciproque d'un ensemble sont des ensembles.
- On dit que $\mathrm{Im}(f) := f(E)$ est l'*image de* f. Ne pas confondre avec le *but* (ou *ensemble d'arrivée*) de f qui est F.
- On a
$$\forall y \in F, y \in f(A) \Leftrightarrow \exists x \in A, f(x) = y \quad \text{et} \quad \forall x \in E, x \in f^{-1}(B) \Leftrightarrow f(x) \in B.$$
- L'image directe définit une application $f : \mathcal{P}(E) \to \mathcal{P}(F)$ et l'image réciproque définit une application $f^{-1} : \mathcal{P}(F) \to \mathcal{P}(E)$.
- Si $x \in E$, on a $f(\{x\}) = \{f(x)\}$
- Si f est *bijective*, alors $f^{-1}(\{y\}) = \{f^{-1}(y)\}$.

Proposition 7.1.4 Soit $f : E \to F$ une application. Alors,

1. Soient $A, A' \subset E$, on a
   (a) Si $A \subset A'$, alors $f(A) \subset f(A')$,
   (b) $f(A \cap A') \subset f(A) \cap f(A')$ (*),
   (c) $f(A \cup A') = f(A) \cup f(A')$,
2. soient $B, B' \subset F$, on a
   (a) Si $B \subset B'$, alors $f^{-1}(B) \subset f^{-1}(B')$,
   (b) $f^{-1}(B \cap B') = f^{-1}(B) \cap f^{-1}(B')$,
   (c) $f^{-1}(B \cup B') = f^{-1}(B) \cup f^{-1}(B')$,
3. (a) Si $A \subset E$, alors $A \subset f^{-1}(f(A))$,
   (b) Si $B \subset F$, alors $f(f^{-1}(B)) \subset B$.

(*) : Attention !

Démonstration.
1. (a) Si $y \in f(A)$, il existe $x \in A$ tel que $y = f(x)$. Si $A \subset A'$, on aura aussi $x \in A'$ et donc $y = f(x) \in f(A')$.
   (b) Formel.
   (c)
   - Inclusion : si $x \in A \cup A'$, on a $x \in A$ ou $x \in A'$ et donc, $f(x) \in f(A)$ ou $f(x) \in f(A')$.
   - Réciproque : formel.
2. (a) Si $x \in f^{-1}(B)$, alors $f(x) \in B$ et si $B \subset B'$, on aura $f(x) \in b'$ si bien que $x \in f^{-1}(B')$.

(b) Dire que $x \in f^{-1}(B \cap B')$ signifie que $f(x) \in B \cap B'$ et dire que $x \in f^{-1}(B) \cap f^{-1}(B')$ signifie que $f(x) \in B$ et $f(x) \in B'$.
(c) Même chose.

3. (a) Si $x \in A$, alors $f(x) \in f(A)$ et donc $x \in f^{-1}(f(A))$,
(b) Si $y \in f(f^{-1}(B))$, on peut écrire $y = f(x)$ avec $x \in f^{-1}(B)$ et on a donc $y = f(x) \in B$. ■

Exemple On peut construire des « contre-exemples » avec la fonction $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$:

1. Si $A = \mathbb{R}_{\geq 0}$ et $A' = \mathbb{R}_{\leq 0}$, on a $f(A \cap A') = \{0\} \subsetneq \mathbb{R}_{\geq 0} = f(A) \cap f(A')$,
2. Si $A = \mathbb{R}_{\geq 0}$, alors $A \subsetneq \mathbb{R}_{\geq 0} = \mathbb{R} = f^{-1}(f(A))$,
3. Si $B = \mathbb{R}$, alors $f(f^{-1}(B)) = \mathbb{R}_{\geq 0} \subsetneq \mathbb{R} = B$.

7.2 Relations

Définition 7.2.1 Une *relation* $\mathcal{R}$ dans un ensemble E est une façon d'apparier [a] les éléments de E. On écrira $x\mathcal{R}y$ si x et y sont appariés par la relation $\mathcal{R}$.

a. Rigoureusement parlant, c'est une partie de $E \times E$.

Exemple

1. On dispose toujours de la relation d'*égalité* dans n'importe quel ensemble E : chaque $x \in E$ est en relation avec lui même mais avec personne d'autre.
2. On dispose aussi de la relation *vide* : aucun élément n'est en relation avec un autre.
3. À l'autre extrême, on dispose de la relation *totale* ou tout le monde est en relation avec tout le monde.
4. On dispose de l'*ordre usuel* sur $\mathbb{Z}$ ou $\mathbb{R}$.
5. On dispose aussi de la *divisibilité* sur $\mathbb{Z}_{\geq 0}$ ou sur $\mathbb{Z}$.
6. On dispose de la relation de *congruence* modulo 2π sur $\mathbb{R}$ ou modulo n sur $\mathbb{Z}$.
7. On dispose du parallélisme sur les droites du plan.

Remarque On peut aussi définir une relation entre deux ensembles distincts E et F en appariant un élément de E avec un élément de F. Une application devient alors un cas particulier de relation.

Définition 7.2.2 Une relation $\mathcal{R}$ sur un ensemble E est

1. *réflexive* si $\forall x \in E, x\mathcal{R}x$,
2. *transitive* si $\forall x, y, z \in E, x\mathcal{R}y$ et $y\mathcal{R}z \Leftrightarrow x\mathcal{R}z$,
3. *symétrique* si $\forall x, y \in E, x\mathcal{R}y \Leftrightarrow y\mathcal{R}x$,
4. *antisymétrique* si $\forall x, y \in E, x\mathcal{R}y$ et $y\mathcal{R}x \Leftrightarrow x = y$.

Exemple

1. Dans tous les exemples ci-dessus, seule la relation vide n'est pas réflexive.
2. Toutes sont transitives.
3. Les relations d'égalité, vide, totale de congruence et de parallélisme sont symétriques
4. Les relations d'égalité, d'ordre usuel et de division dans $\mathbb{Z}_{\geq 0}$ sont antisymétriques.

Définition 7.2.3 Une *relation d'équivalence* (resp. *relation d'ordre*) est une relation qui est
1. réflexive,
2. symétrique (resp. antisymétrique),
3. transitive.

Exemple
1. Les relations d'égalité, totale, de congruence et de parallélisme sont des relations d'équivalence.
2. Les relations d'égalité, d'ordre usuel et de division dans $\mathbb{Z}_{\geq 0}$ sont des relations d'ordre.

Remarque
- Une relation qui est réflexive et transitive est parfois appelée relation de *préordre* (divisibilité dans $\mathbb{Z}$ par exemple).
- Une relation d'ordre est dite *totale* si

$$\forall x, y \in E, \quad x \leq y \text{ ou } y \leq x$$

(relation d'ordre usuelle par exemple).

Définition 7.2.4 Si $\mathcal{R}$ est une relation d'équivalence sur E, alors la *classe* de $x \in E$ pour la relation $\mathcal{R}$ est le sous-ensemble

$$\overline{x} := \{y \in E, \quad x\mathcal{R}y\}.$$

Exemple
1. La classe de x pour la relation d'égalité est $\{x\}$;
2. La classe de x pour la relation totale est E.
3. La classe de $\theta \in \mathbb{R}$ pour la congruence modulo 2π est $\{\theta + k2\pi, k \in \mathbb{Z}\}$.
4. La classe de $m \in \mathbb{Z}$ pour la congruence modulo n est $\{m + kn, k \in \mathbb{Z}\}$.
5. La classe de la droite D pour le parallélisme est $\{t_u(D), u \in \overrightarrow{\mathcal{P}}\}$.

Théoreme 7.2.5 Si $\mathcal{R}$ est une relation d'équivalence sur E, alors l'ensemble

$$E/\mathcal{R} := \{\overline{x}, x \in E\}$$

des classes d'éléments de E est une partition de E.

Démonstration. Si $x \in E$, alors $x\mathcal{R}x$ (réflexivité) et donc $x \in \overline{x}$ qui est bien non-vide. Supposons maintenant que $x, y \in E$ satisfont $\overline{x} \cap \overline{y} \neq \emptyset$. Il existe alors $z \in E$ tel que $z \in \overline{x}$ et $z \in \overline{y}$, c'est-à-dire $x\mathcal{R}z$ et $y\mathcal{R}z$. Maintenant, si $x' \in \overline{x}$, alors $x\mathcal{R}x'$ et donc (symétrie et transitivité) $y\mathcal{R}x'$ si bien que $x' \in \overline{y}$. On aura donc $\overline{x}' \subset \overline{x}$ et, par « symétrie », $\overline{x} = \overline{y}$. Finalement, si $x \in E$, on a $x \in \overline{x}$ (par réflexivité encore). ■

Remarque
- On dit que $E/\mathcal{R}$ est l'*ensemble quotient* de E par la relation $\mathcal{R}$ et que l'application $\pi : E \to E/\mathcal{R}, x \mapsto \overline{x}$ est l'*application quotient*. On dit aussi que x est un *représentant* de $\overline{x}$.
- Réciproquement, si $\mathcal{E}$ est une partition de E, alors la relation définie par

$$x\mathcal{R}y \Leftrightarrow \exists A \in \mathcal{E}, x \in A \text{ et } y \in A$$

est une relation d'équivalence sur E.

Exemple 1. Si $\mathcal{R}$ est la relation d'égalité sur E, alors $E/\mathcal{R} = \{\{x\}, x \in E\}$ peut s'identifier à E.
2. Si $\mathcal{R}$ est la relation totale sur E, alors $E/\mathcal{R} = \{E\}$ a un seul élément.
3. Si $\mathcal{R}$ est la relation de congruence modulo 2π, alors $\mathbb{R}/\mathcal{R}$ peut s'identifier à $[0, 2\pi[$.
4. Si $\mathcal{R}$ est la relation de congruence modulo n, alors $\mathbb{Z}/\mathcal{R}$ peut s'identifier à $\{0, 1, \ldots, n-1\}$.
5. Si $\mathcal{R}$ est la relation de parallélisme, alors $\mathcal{P}/\mathcal{R}$ peut s'identifier à $\overrightarrow{\mathcal{P}}$.

7.3 Cardinal

Définition 7.3.1 Le *cardinal* d'un ensemble E est le « nombre d'éléments [a] » de cet ensemble. On le note $\mathrm{card}(E)$ ou plus simplement $|E|$ en pratique.

a. Formellement, c'est sa classe d'équivalence pour les bijections.

En pratique, on écrit $|E| = |F|$ lorsqu'il existe une bijection $E \simeq F$ (et $|E| \neq |F|$ sinon) et $|E| \leq |F|$ s'il existe seulement une injection $E \hookrightarrow F$ (et $|E| < |F|$ si, en plus, on a $|E| \neq |F|$).

Exemple 1. On a $0 = |\emptyset|$, $1 = |\{0\}|$ et plus généralement $n = |\{0, \ldots, n-1\}|$.
2. On a $|\mathbb{N} \setminus \{0\}| = |\mathbb{N}|$ car le décalage $n \mapsto n-1$ est une bijection.
3. On a $|\mathbb{N}| < |\mathbb{R}|$ car il n'existe pas de suite contenant tous les réels.
4. En fait, on a $|\mathbb{N}| = |\mathbb{Q}| < |\mathbb{R}| = |\mathbb{C}|$.

Définition 7.3.2 Un ensemble E est *fini* s'il existe $n \in \mathbb{N}$ tel que $|E| = n$. Sinon, E est *infini*. Enfin, E est *dénombrable* si $|E| = |\mathbb{N}|$.

Remarque
- On a $|E| \leq |F|$ si et seulement si $E = \emptyset$ ou bien il existe une surjection $F \twoheadrightarrow E$.
- On a toujours $|E| < |\mathcal{P}(E)|$ et il existe donc une infinité de cardinaux infinis.
- On dispose aussi du *théorème de Cantor-Bernstein* (difficile) :

$$|E| = |F| \Leftrightarrow (|E| \leq |F| \text{ et } |F| \leq |E|).$$

- La relation $|E| = |F|$ est une relation d'équivalence sur les ensembles et la relation $|E| \leq |F|$ est une relation d'ordre sur les cardinaux.

Bibliographie

[BS09] Stéphane Balac et François Sturm. *Algèbre et analyse : cours de mathématiques de première année avec exercices corrigés*. Presses polytechniques et universitaires romandes, 2009.

[Bou70] Nicolas Bourbaki. *Éléments de mathématique. Théorie des ensembles*. Hermann, Paris, 1970, 349 pp. (not consecutively paged) (cf. pages 7, 17).

[Esc16] Jean-Pierre Escofier. *Toute l'algèbre pour la licence*. Dunod, 2016.

[Hal67] Paul Halmos. *Introduction à la théorie des ensembles*. Eyrolles, 1967.

[Kri07] Jean-Louis Krivine. *Théorie des ensembles*. 2e édition. Numéro 5. Paris : Cassini, 2007 (cf. pages 7, 17).

[LM03a] François Liret et Dominique Martinais. *Algèbre - 1re année*. Dunod, 2003.

[LM03b] François Liret et Dominique Martinais. *Algèbre et géométrie - 2e année*. Dunod, 2003.

[RW13] Jean-Pierre Ramis et André Warusfel. *Mathématiques Tout en un pour la Licence 1 - 2e édition*. Dunod, 2013.

[ST77] Ian Stewart et David Tall. *The foundations of mathematics*. Oxford University Press, 1977.

[Was08] Pierre Wassef. *Arithmétique*. Vuibert, 2008.