Faculté des Sciences
Département de Mathématique

Mathématiques élémentaires

(du point de vue universitaire)

Pierre Mathonet

Première année d'études de bachelier en Sciences Mathématiques
Année académique 2019-2020

Introduction

Le cours “mathématiques élémentaires” est introduit lors de l'année académique 2014-2015 au début de la filière d'études en mathématiques pour faciliter la transition secondaire-université et ainsi favoriser la réussite en première année.

Ses objectifs sont multiples : il s'agit d'abord de revoir certains points de l'enseignement mathématique qui ont été abordés ou utilisés dans votre cursus antérieur, mais sans toujours être approfondis. On adoptera un point de vue assez souvent différent de celui qui a été utilisé auparavant, l'accent étant mis sur la logique et les articulations entre les notions plutôt que sur les méthodes de calcul, qui ne seront pourtant pas oubliées.

Un second objectif important du cours est d'apprendre à rédiger, à comprendre et à étudier des textes mathématiques, en s'exerçant sur des notions qui ont déjà été rencontrées, plutôt que sur des contenus complètement nouveaux.

Quand on entreprend l'étude des mathématiques supérieures, on est assez vite confronté à des problèmes de définitions : en effet, les notions mathématiques introduites dans l'enseignement secondaire reposent souvent sur des idées intuitives, et il est difficile, voire impossible, qu'il en soit autrement. Cependant, quand on veut élever l'édifice mathématique, on doit être sûr de ses fondations, et les idées intuitives, si elles peuvent encore guider la démarche, doivent être remplacées par des définitions claires et cohérentes et par une démarche déductive logique. On part donc d'un nombre minimal de définitions et on tente de démontrer toutes les propriétés des objets que l'on étudie.

Cependant, certaines notions sont encore trop ardues pour être abordées dans ce cours de première année ou n'y trouvent pas naturellement leur place. C'est le cas de la théorie des ensembles dans sa forme actuelle. Nous n'aborderons que la théorie dite naïve des ensembles et ne donnerons pas une définition formelle des ensembles. C'est également le cas de la construction des nombres réels, qui fait souvent intervenir des notions de convergence, et a plus sa place dans un cours d'analyse. Nous conviendrons donc dans ce cours que les exemples que nous prenons sur les nombres réels sont basés sur la compréhension intuitive que vous en avez en sortant de l'enseignement secondaire. En particulier, nous utiliserons les nombres réels pour bâtir les nombres complexes et étudier leurs propriétés.

Dans le premier chapitre, nous rencontrerons tout d'abord la logique et quelques éléments de théorie naïve des ensembles et nous en déduirons quelques techniques de démonstration qui seront utiles dans tous les cours du cursus. Nous reverrons ensuite les nombres complexes, et nous en profiterons pour approfondir l'utilisation du symbole sommatoire.

Nous reverrons ensuite la construction des nombres naturels, entiers (relatifs) et rationnels. Nous élargirons les constructions pour découvrir des structures algébriques omniprésentes dans les mathématiques supérieures, que nous illustrerons par des éléments d'arithmétique modulaire.

Si le temps le permet, nous en profiterons pour revoir des notions importantes d'analyse et de géométrie, avec toujours le souci d'apprendre à rédiger, à comprendre et à étudier des écrits mathématiques, des plus simples aux plus complexes.

J'espère sincèrement que ce cours vous aidera à bien entamer votre cursus universitaire et je vous invite à commencer la lecture sans attendre.

Chapitre 1

Logique et ensembles

Ce chapitre présente une introduction à la logique et à la théorie des ensembles. Vous avez déjà rencontré la plupart des notions abordées ici, mais souvent sans les étudier pour elles-mêmes.

Comme dans tous les cours de mathématique, je commence par quelques définitions formelles. Ensuite, nous verrons quelques procédures systématiques qui permettent de n'oublier aucun cas de figure quand on est face à un problème logique, ou faisant appel à des ensembles ; c'est le cas des tables de vérité ou des diagrammes de Venn. Nous passerons ensuite en revue les techniques de démonstration classiques comme la contraposition ou le raisonnement par l'absurde, nous verrons comment démontrer une alternative et nous terminerons par les démonstrations par récurrence.

1.1 Logique

Nous commençons par donner une définition des assertions logiques, et des connecteurs qui permettent de former des assertions composées à l'aide d'assertions élémentaires.

Définition 1.1.1. On appelle *assertion* ou *proposition logique* toute phrase d'un langage donné dont on peut envisager sans ambiguïté le problème de sa vérité ou de sa fausseté.

Par exemple, on peut considérer les assertions suivantes.

1. "Aujourd'hui, je porte un pull rouge" ;
2. "3 est un nombre premier" ;
3. "3 n'est pas divisible par 2" ;
4. "tout nombre positif est pair" ;
5. "Il pleut" ;
6. "J'emporte un parapluie" ;
7. "Si Berlin est en Suisse, alors je viens de Mars" ;
8. "Si mon chat aboie, alors je gagne au lotto".

Les assertions sont construites de façon à être compréhensibles sans ambiguïté pour que l'on puisse décider si elles sont vraies ou fausses. Elles admettent donc des valeurs de vérité "vrai" et "faux" que l'on note aussi V et F ou 1 et 0.

Les phrases suivantes ne sont donc pas des propositions logiques.

1. "Quelle heure est-il ?"
2. "Paris est-elle la capitale de la France ?"
3. "Cette phrase est fausse."
4. "Je corniflute gauche bien."

En effet, les deux premières sont des questions. Les propositions logiques correspondantes pourraient être “Il est 15 heures”, “Paris n’est pas la capitale de la France”. La troisième est contradictoire, puisque si elle est vraie, elle doit alors être fausse et vice-versa. Enfin, la quatrième n’a pas de sens.

Les règles formatives (ou règles de syntaxe) permettent de construire de nouvelles propositions à partir d’anciennes. L’idée est qu’on déclare dans ces règles qui est une proposition. On commence par admettre qu’il existe des propositions élémentaires dites *propositions atomiques* ou *variables propositionnelles*, notées p, q, r, ..., puis on donne les règles stipulant qu’on peut en former de nouvelles, en utilisant les opérations logiques de négation, conjonction (et), disjonction (ou), implication ou bi-implication, encore appelées connecteurs logiques.

A ce point, on peut former des propositions logiques composées, mais on ne peut pas encore décider de la vérité de telles propositions, en fonction de la vérité ou la fausseté des propositions atomiques qui les composent. Cette étude s’appelle la *sémantique*.

On résout ce problème en associant à chaque connecteur une table de vérité qui précise la vérité de toute proposition logique composée à l’aide de ce connecteur. Une assertion composée a alors des valeurs de vérité qui dépendent des valeurs de vérité des assertions qui la composent.

Définition 1.1.2. Si P est une assertion, alors la négation de P est une assertion. On la note $\neg P$. Cette assertion est vraie si P est fausse et elle est fausse si P est vraie. La table de vérité de l’opérateur de négation $\neg$ est donc la suivante. [a]

P	$\neg P$
0	1
1	0

ou encore

P	$\neg P$
F	V
V	F

Remarque 1.1. Dans la suite, nous adopterons les valeurs 0 pour faux, et 1 pour vrai, mais vous pouvez conserver V et F si c’est plus concret pour vous.

Voici quelques exemples qui sont les négations des assertions introduites plus haut.

1. “Aujourd’hui, je ne porte pas un pull rouge” ;
2. “3 n’est pas un nombre premier” ;
3. “3 est divisible par 2” ;
4. “Il existe un nombre positif qui n’est pas pair” ; [b]
5. “Il ne pleut pas” ;
6. “Je n’emporte porte pas de parapluie” ;
7. “Mon chat aboie et je ne gagne pas au lotto”.

Comme dans le langage courant, nier deux fois revient à ne rien faire. On pourrait écrire $\neg(\neg P) = P$, quelle que soit l’assertion P. Arrêtons-nous un instant sur cette égalité. En effet, $\neg(\neg P)$ et P sont des assertions qui ne sont pas écrites de la même manière. On touche ici une définition importante.

Définition 1.1.3. Deux propositions logiques P et Q (composées à partir de propositions élémentaires) sont *logiquement équivalentes* [c] si elles ont les mêmes tables de vérité (i.e. les mêmes valeurs de vérité, dans tous les cas). On note alors $P \equiv Q$.

a. Voyez la construction de la table : la première colonne donne les deux valeurs possibles pour P, la deuxième donne les valeurs correspondantes de $\neg P$.

b. Il est important de remarquer que la négation de P :“tout nombre positif est pair” **n’est pas** “tout nombre positif est impair”, nous y reviendrons.

c. On dit aussi tautologiquement équivalentes.

Dans le cas de la double négation, on a bien

P	$\neg P$	$\neg(\neg P)$
0	1	0
1	0	1

et donc on peut noter $P \equiv \neg(\neg P)$, et dire que P et $\neg(\neg P)$ sont logiquement équivalentes. Il est important de noter que P et $\neg(\neg P)$ ont les mêmes valeurs de vérité, quel que soit le contexte et quel que soit P.

Dans une expression complexe, on peut toujours remplacer une assertion par une assertion logiquement équivalente sans changer la valeur de vérité globale. Dans le cas présent, on peut remplacer l'assertion $\neg(\neg P)$ par l'assertion P . Cela peut sembler fort théorique, mais vous pouvez utiliser ce fait dans le langage courant pour simplifier des phrases compliquées.

Exemple 1.1.1. La phrase
"Il n'est pas impossible que ce cours ne soit pas dépourvu de concepts nouveaux."
est logiquement équivalente à
"Il est possible que ce cours contienne des concepts nouveaux."

Voici maintenant deux connecteurs logiques bien connus dans la vie de tous les jours, le *et* et le *ou*. Il n'y a pas de grande surprise pour le "et". Pour le "ou", il faut juste noter qu'il n'est pas exclusif : en mathématiques, si on vous dit "tu peux avoir pour dessert une glace ou une coupe de fruit" vous pouvez répondre "d'accord, je mangerai les deux".

Définition 1.1.4. Si P et Q sont deux assertions, alors la conjonction de P et Q, notée $P \wedge Q$ ou "P et Q" est une assertion qui est vraie quand P est vraie et Q est vraie (simultanément) et fausse sinon. La table de vérité du connecteur "et" est donc [d]

P	Q	P et Q
0	0	0
0	1	0
1	0	0
1	1	1

On peut ainsi former les assertions

1. "Il pleut et je porte un pull rouge" ;
2. "J'emporte un parapluie et 3 est un nombre premier".

Il est intéressant de remarquer que la valeur de vérité de $P \wedge Q$ est le minimum des valeurs de vérités de P et Q. Cela permet de faciliter les calculs, et cela justifie l'utilisation de 0 et 1, plutôt que F et V.
De la même manière on définit la disjonction de deux assertions.

Définition 1.1.5. Si P et Q sont deux assertions, alors la disjonction de P et Q, notée $P \vee Q$ ou "P ou Q" est une assertion qui est vraie quand au moins l'une des deux assertions P, Q est vraie et qui est fausse sinon. Sa table de vérité est donc la suivante [e].

P	Q	P ou Q
0	0	0
0	1	1
1	0	1
1	1	1

d. Ici, les deux premières colonnes permettent d'avoir les quatre valeurs possibles pour le couple (P, Q).
e. Notez la différence, dans la dernière ligne de la table, avec le "ou exclusif" souvent utilisé dans le langage courant.

Vous aurez sans doute remarqué que puisque P et Q peuvent prendre chacun deux valeurs de vérité, la table contient quatre lignes. Combien y aura-t-il de lignes pour des assertions composées de P, Q et R, ou encore de P, Q, R et S ? Voici quelques exemples simples.

1. "Il pleut ou je porte un pull rouge" ;
2. "J'emporte un parapluie ou 3 est un nombre premier".

Ici aussi, on peut remarquer que la valeur de vérité de $P \vee Q$ est le maximum des valeurs de vérités de P et Q.

Il est intéressant pour la suite de nos développements de déjà regarder quelques façons de construire des assertions logiques composées avec les trois connecteurs que nous avons vus jusqu'à présent.

Proposition 1.1.1. *On a les équivalences logiques suivantes*

1. $\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$;
2. $\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$;

Que veulent dire ces équivalences logiques sur des exemples ?

- La négation de "Il pleut ou je porte un pull rouge" est "il ne pleut pas et je ne porte pas de pull rouge".
- La négation de "Il pleut et nous sommes mardi" est "il ne pleut pas ou nous ne sommes pas mardi".
- Comment obtenir dans $\mathbb{R}$ une condition équivalente à $x^2 - 2x \neq 0$?
- Comment obtenir dans $\mathbb{R}^2$ une condition équivalente à $x^2(y-4) \geqslant 0$?

Passons maintenant aux implications et bi-implications, ces dernières étant encore appelées équivalences. La définition de l'implication est la première de ce chapitre qui soit un peu surprenante. L'implication est le "si...alors" du français. Pour bien comprendre la table de vérité ci-dessous, on peut se demander quand l'assertion "Si on est vendredi, alors je porte un pull rouge" est fausse. Si vous voulez faire une expérience scientifique pour mettre en défaut cette affirmation, vous ne viendrez certainement pas voir la couleur de mes vêtements un jeudi. Vous viendrez le vendredi. L'assertion est fausse uniquement dans le cas où on est vendredi et où je n'ai pas de pull rouge.

Définition 1.1.6. Si P et Q sont deux assertions, alors "P implique Q" est une assertion. On la note $P \Rightarrow Q$. Elle est toujours vraie sauf si P est vrai et Q faux. La table de vérité du connecteur $\Rightarrow$ est donc

P	Q	$P \Rightarrow Q$
0	0	1
0	1	1
1	0	0
1	1	1

On peut également dire "si P, alors Q" pour indiquer $P \Rightarrow Q$. Il est important de remarquer les deux premières lignes de la table de vérité. Quand P est faux, alors $P \Rightarrow Q$ est vrai. Voici quelques exemples :

1. "S'il pleut alors j'emporte un parapluie." [f]
2. "Si on est vendredi, je porte un pull rouge." [g]
3. "Si 3 est un nombre premier, alors je porte un pull rouge."

A titre d'exercice, on pourra démontrer l'équivalence logique entre $P \Rightarrow Q$ et $(\neg P) \vee Q$.

Finalement, on peut définir la bi-implication entre de deux assertions, encore appelée équivalence.

f. Cette implication ne donne aucune indication s'il ne pleut pas.
g. On peut aussi dire "Tous les vendredis, je porte un pull rouge."

Définition 1.1.7. Si P et Q sont deux assertions alors "P bi-implique Q", "P est équivalent à Q" est une assertion. On la note $P \Leftrightarrow Q$. Elle est vraie quand P implique Q et Q implique P sont vraies. La table de vérité du connecteur $\Leftrightarrow$ est donc

P	Q	$P \Leftrightarrow Q$
0	0	1
0	1	0
1	0	0
1	1	1

Vous remarquerez que $P \Leftrightarrow Q$ est vraie exactement quand P et Q ont la même valeur de vérité. Si P est équivalent à Q, on dira aussi que P est vrai si et seulement si Q est vrai. Voici quelques exemples

1. "J'emporte un parapluie si et seulement si il pleut" ;
2. "Je porte un pull rouge si et seulement si on est vendredi".

Remarquons que, par définition, nous avons $P \Leftrightarrow Q \equiv (P \Rightarrow Q)$ et $(Q \Rightarrow P)$.

Terminons cette liste d'opérations logiques en y ajoutant les deux *quantificateurs* : Le signe $\forall$ se lit "pour tout" et le signe $\exists$ se lit "il existe". Ainsi, si P et Q sont deux assertions, on peut écrire

$$\forall x : P, \exists y : Q$$

pour signifier "pour tout x tel que P , il existe un y tel que Q".

L'ordre des quantificateurs a de l'importance. En effet, dans l'assertion précédente, y peut varier en fonction de x, ce qui n'est pas le cas si on l'écrit dans l'autre sens. Par exemple, le lecteur conviendra que les assertions commençant par

"Pour tout garçon dans la salle, il existe une fille dans la salle telle que..."

et

"Il existe une fille dans la salle telle que pour tout garçon dans la salle..."

n'auront sans doute pas les mêmes significations. [h] Remarquez également que dans les expressions ci-dessus, les mots "pour tout" et "il existe" n'ont pas été remplacés par les symboles correspondants, qui ne devraient être utilisés que dans des expressions purement mathématiques (des "formules"). Voici un exemple qui vous sera utile dans le cours d'analyse. C'est la déinition de la convergence d'une suite vers 0.

Exemple 1.1.2. La convergence d'une suite numérique vers 0 :

$$\forall \varepsilon > 0, \exists N \in \mathbb{N} : n \geqslant N \Rightarrow |x_n| < \varepsilon.$$

Il est à noter qu'il y a un petit abus d'écriture dans cette notation, on devrait écrire

$$\forall \varepsilon > 0, \exists N \in \mathbb{N} : \forall n \in \mathbb{N}, (n \geqslant N \Rightarrow |x_n| < \varepsilon).$$

Mais en général, on écrira pas le quantificateur $\forall n \in \mathbb{N}$. On peut par exemple utiliser cette définition pour démontrer que la suite définie par $x_n = \frac{1}{n}$ pour tout $n \geqslant 1$ converge (tend) vers 0 quand n tend vers l'infini. On constatera que dans la démonstration, pour chaque ε, on peut trouver un N qui convient. Cela ne pourrait pas être le cas si on avait écrit une autre condition en inversant les quantificateurs, comme ceci :

$$\exists N \in \mathbb{N} : \forall \varepsilon > 0, \forall n \in \mathbb{N}, (n \geqslant N \Rightarrow |x_n| < \varepsilon).$$

Vous aurez le temps de vous familiariser avec ces expressions, mais j'insiste déjà sur le fait qu'il ne faut pas se contenter de les traduire mot à mot, mais bien essayer de se représenter ce qu'elles veulent dire.

h. Les personnes choquées par cette dernière assertion pourront échanger les mots "fille" et "garçon", et s'interroger sur ses implications morales.

On peut également se demander quelle est la négation de propositions contenant des quantificateurs. Sans entrer dans les détails, notons que la négation d'une proposition contenant $\forall$ s'exprime avec un $\exists$ et vice-versa.

Exemple 1.1.3.

1. La négation de "Tous les profs de math sont petits" est "Il existe un prof de math qui n'est pas petit".
2. La négation de "Il existe un cheval de course bon marché" est "Tous les chevaux de course coûtent cher".

Exercice 1.1.1. 1. Nier l'assertion $\forall x > 0, \exists y > 0 : y < x$.

2. Ecrivez l'assertion indiquant qu'une suite numérique ne converge pas vers 0.

En utilisant ces opérations logiques, on peut construire des assertions de plus en plus compliquées. Il faut être prudent et utiliser les parenthèses de la manière habituelle pour signifier l'ordre dans lequel il faut interpréter les connecteurs logiques. Par exemple, $P \wedge Q \vee R$ n'a pas de sens, car on pourrait l'interpréter de deux façons différentes : $(P \wedge Q) \vee R$ et $P \wedge (Q \vee R)$. Ces deux assertions ne sont pas logiquement équivalentes, comme le prouve le tableau de vérité suivant [i].

P	Q	R	$P \wedge Q$	$(P \wedge Q) \vee R$	$Q \vee R$	$P \wedge (Q \vee R)$
0	0	0	0	0	0	0
0	0	1	0	1	1	0
0	1	0	0	0	1	0
0	1	1	0	1	1	0
1	0	0	0	0	0	0
1	0	1	0	1	1	1
1	1	0	1	1	1	1
1	1	1	1	1	1	1

En effet, la cinquième et la dernière colonne ne sont pas égales. Le tableau donne aussi des cas précis où les assertions sont différentes. Par exemple, la deuxième ligne correspond à un cas où P et Q sont faux et R vrai, on voit que dans ce cas, $(P \wedge Q) \vee R$ est vraie et $P \wedge (Q \vee R)$ est fausse.

Par contre, les assertions $P \Rightarrow (Q \vee R)$ et $(P \Rightarrow Q) \vee R$ sont logiquement équivalentes, comme le prouve le tableau suivant.

P	Q	R	$Q \vee R$	$P \Rightarrow (Q \vee R)$	$P \Rightarrow Q$	$(P \Rightarrow Q) \vee R$
0	0	0	0	1	1	1
0	0	1	1	1	1	1
0	1	0	1	1	1	1
0	1	1	1	1	1	1
1	0	0	0	0	0	0
1	0	1	1	1	0	1
1	1	0	1	1	1	1
1	1	1	1	1	1	1

Exercice 1.1.2. Etudier la validité des équivalences logiques suivantes :

1. $(P \vee Q) \vee R \equiv P \vee (Q \vee R)$
2. $(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$
3. $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$
4. $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$

i. Les trois premières colonnes du tableau donnent toutes les valeurs de vérité possibles pour le triplet (P, Q, R). De plus on calcule facilement les autres colonnes, en considérant une colonne à la fois.

On a également des relations entre les différentes constructions possibles. Ces relations sont données par des équivalences logiques entre certaines assertions. En voici un exemple classique.

Proposition 1.1.2. *Si P et Q sont deux assertions, l'assertion $P \Rightarrow Q$ est logiquement équivalente à l'assertion $\neg Q \Rightarrow \neg P$. En d'autres termes, on a,*

$$(P \Rightarrow Q) \equiv (\neg Q \Rightarrow \neg P).$$

En conséquence, démontrer l'assertion $\neg Q \Rightarrow \neg P$ est équivalent à démontrer $P \Rightarrow Q$. Cette technique de preuve s'appelle la *contraposition* et l'assertion $\neg Q \Rightarrow \neg P$ est la *contraposée* de l'assertion $P \Rightarrow Q$.

Démonstration. Démontrons cette proposition en utilisant des tables de vérité. On calcule successivement les valeurs de vérités des assertions en question en fonction de tous les cas possibles pour P et Q. On obtient le tableau suivant

P	Q	$\neg P$	$\neg Q$	$P \Rightarrow Q$	$\neg Q \Rightarrow \neg P$
0	0	1	1	1	1
0	1	1	0	1	1
1	0	0	1	0	0
1	1	0	0	1	1

On constate que les deux dernières colonnes sont égales. D'après notre définition de l'équivalence, cela veut dire que ces assertions sont logiquement équivalentes. □

On peut également se convaincre intuitivement que les assertions “Si on est vendredi, je porte un pull rouge” et “Si je ne porte pas de pull rouge, on n'est pas vendredi” veulent dire la même chose, c'est-à-dire, sont logiquement équivalentes.

Terminons cette introduction élémentaire à la logique par les *tautologies*. Voici un exemple. Si P et Q sont deux assertions, on peut calculer la table de vérité de l'assertion

$$((P \Rightarrow Q) \text{ et } P) \Rightarrow Q.$$

On a directement

P	Q	$P \Rightarrow Q$	$(P \Rightarrow Q)$ et P	$((P \Rightarrow Q)$ et $P) \Rightarrow Q$
0	0	1	0	1
0	1	1	0	1
1	0	0	0	1
1	1	1	1	1

L'assertion $((P \Rightarrow Q)$ et $P) \Rightarrow Q$ est donc toujours vraie, dans tous les cas de figure pour P et Q. C'est une tautologie.

Définition 1.1.8. Une assertion composée qui est vraie quelles que soient les valeurs de vérités des assertions qui la composent est une *tautologie*.

La notion de tautologie permet de formaliser d'un point de vue logique des techniques de démonstration. Voici premier exemple : dire que P et Q sont logiquement équivalentes, c'est dire que l'assertion $P \Leftrightarrow Q$ est une tautologie. Voici maintenant quelques raisonnements couramment utilisés.

Voici quelques exemples supplémentaires et techniques de démonstration basées sur des équivalences logiques.

1.1.1 La contraposition : quelques exemples

Je vous rappelle la contraposition (proposition 1.1.2).

Proposition 1.1.3. *Si P et Q sont deux assertions, l'assertion $P \Rightarrow Q$ est logiquement équivalente à l'assertion $\neg Q \Rightarrow \neg P$. En d'autres termes, on a,*

$$(P \Rightarrow Q) \equiv (\neg Q \Rightarrow \neg P).$$

D'après cette proposition, démontrer que P implique Q est équivalent à démontrer que $\neg Q$ implique $\neg P$.

Voici deux exemples.

Proposition 1.1.4. *Si $a, b \in \mathbb{R}$ sont tels que $a + b$ est irrationnel, alors a ou b est irrationnel.*

Démonstration. Si on note P l'assertion "$a + b$ est irrationnel" et Q l'assertion "a ou b est irrationnel", on cherche bien à démontrer que P implique Q. Il est plus facile de démontrer que $\neg Q$ implique $\neg P$. L'assertion $\neg Q$ est "a et b sont rationnels", tandis que l'assertion $\neg P$ est "$a + b$ est rationnel". Alors $\neg Q \Rightarrow \neg P$ est une assertion vraie par définition des rationnels. □

Bien sûr, j'ai rédigé la preuve pour faire apparaître le lien avec la proposition précédente. On rédigera plutôt comme ceci.

Démonstration. Procédons par contraposition et supposons que a et b soient rationnels. Alors $a + b$ est rationnel, par définition des rationnels. □

Proposition 1.1.5. *Si n est un nombre entier tel que n^2 est pair, alors n est pair.*

Démonstration. On démontre la proposition contraposée. Supposons que n soit impair. Alors, il existe $k \in \mathbb{Z}$ tel que $n = 2k + 1$. On calcule alors $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$ et on constate que n^2 est impair. □

Avec l'habitude, on n'indique même plus qu'il s'agit d'une démonstration par contraposée, et cela n'inquiète pas le lecteur expérimenté.

1.1.2 La démonstration par l'absurde

Cette méthode de démonstration est très utilisée. Elle consiste à supposer que ce que l'on veut démontrer est faux et à arriver à une absurdité (encore appelée une contradiction), c'est à dire la conjonction d'une assertion et de sa négation. Ce type de démonstration est également basé sur une équivalence logique.

Proposition 1.1.6. *Pour toutes assertions P et Q, l'assertion P est logiquement équivalente à $(\neg P) \Rightarrow (Q \wedge (\neg Q))$.*

Démonstration. La preuve est immédiate, à l'aide de tables de vérités. □

Voici un exemple classique, qui peut être énoncé facilement quand on connaît les nombres réels : "Le nombre $\sqrt{2}$ est irrationnel". J'énonce ce résultat en ne présupposant pas que $\sqrt{2}$ existe, puisque nous ne l'avons pas défini.

Proposition 1.1.7. *Il n'existe pas de nombre rationnel z tel que $z^2 = 2$.*

Démonstration. Nous allons supposer que l'assertion à démontrer est fausse, et montrer que cela conduit à une contradiction. On suppose donc qu'il existe un nombre rationnel z satisfaisant $z^2 = 2$. Par définition des rationnels[j], il existe des nombres entiers p et q (q

j. Prenez la définition de l'enseignement secondaire, si vous voulez, elle est équivalente à celle que je vous donnerai.

non nul), tels que $z = \frac{p}{q}$. On peut supposer que q est le nombre positif et minimal[k] tel que $z = \frac{p}{q}$. On a alors $2 = \frac{p^2}{q^2}$, ou encore $p^2 = 2q^2$.

Alors p^2 est pair, et par la proposition 1.1.5, p est pair. Il existe alors $r \in \mathbb{Z}$ tel que $p = 2r$. On a alors $4r^2 = p^2 = 2q^2$, qui donne $q^2 = 2r^2$. Alors q est pair : il existe $s \in \mathbb{N}$, tel que $q = 2s$. Puisque q n'est pas nul, on a $s < q$, et visiblement $z = \frac{p}{q} = \frac{2r}{2s} = \frac{r}{s}$. Donc q n'est pas minimal, cela donne la contradiction. □

Il n'existe des dizaines de preuves de la proposition précédente. On peut également trouver d'autres contradictions ou d'autres façons d'obtenir la contradiction utilisée ici.

1.1.3 Contre-exemple et démonstration d'une alternative

La proposition suivante, que l'on démontre sans difficulté, permet de justifier l'emploi du contre-exemple.

Proposition 1.1.8. *On a l'équivalence logique* $\neg(P \Rightarrow Q) \equiv P \wedge (\neg Q)$.

Il arrive souvent que l'on doive démontrer une assertion qui s'exprime comme une disjonction (un "ou"). On a une technique simple qui permet d'avoir une hypothèse en plus à sa disposition. Cette technique est basée sur le résultat suivant.

Proposition 1.1.9. *On a les équivalences logiques suivantes :*

$$P \Rightarrow (Q \vee R) \equiv (P \wedge (\neg Q)) \Rightarrow R \quad et \quad P \Rightarrow (Q \vee R) \equiv (P \wedge (\neg R)) \Rightarrow Q.$$

Démonstration. Démontrons la première équivalence. La deuxième se démontre de manière analogue. On a

$$P \Rightarrow (Q \vee R) \equiv (\neg P) \vee (Q \vee R) \equiv ((\neg P) \vee Q) \vee R \equiv \neg(P \wedge (\neg Q)) \vee R,$$

et la dernière assertion est logiquement équivalente à $(P \wedge (\neg Q)) \Rightarrow R$. □

Voici un exemple simple, non mathématique : pour prouver l'assertion "si je vis sur mars, alors je suis bleu ou j'ai quatre bras", on peut prouver "si je vis sur mars et si je ne suis pas bleu alors j'ai quatre bras".

1.1.4 La disjonction des cas

Il s'agit encore ici de prouver une implication où l'une des deux assertions contient une alternative (une disjonction "ou"). Il ne faut pas confondre avec la section précédente : l'alternative est ici avant l'implication.

Proposition 1.1.10. *On a l'équivalence* $(P$ *ou* $Q) \Rightarrow R \equiv (P \Rightarrow R)$ *et* $(Q \Rightarrow R)$.

La démonstration peut être faite à l'aide de tables de vérités. Je la laisse comme exercice. Cette proposition montre que pour démontrer $(P$ ou $Q) \Rightarrow R$, il faut traiter tous les cas. Voici un exemple simple.

Proposition 1.1.11. *Si* n *est entier naturel, alors* $n(n+1)$ *est pair.*

Démonstration. Si est est un nombre naturel, alors il est pair ou impair. Nous pouvons donc démontrer que si n est pair ou impair, alors $n(n+1)$ est pair. Si n est pair, alors il existe $k \in \mathbb{N}$ tel que $n = 2k$. On a alors $n(n+1) = 2k(2k+1)$ et ce nombre est pair. Si n est impair, alors il existe $k \in \mathbb{N}$ tel que $n = 2k+1$. On a alors $n(n+1) = (2k+1)(2k+2) = 2(2k+1)(k+1)$ et ce nombre est pair également. □

k. Ce sera intéressant de le montrer à l'aide de la définition de $\mathbb{Q}$ que je vous donnerai, et de la propriété du bon ordre de $\mathbb{N}$, que nous verrons sous peu également.

1.2 Théorie des ensembles

Passons maintenant à la description des ensembles, avec une première définition.

Définition 1.2.1. Un *ensemble* est une collection d'objets possédant une ou plusieurs propriétés communes [a]. Ces objets sont les *éléments* ou *points* de l'ensemble.

On notera généralement un ensemble par une lettre majuscule.
Les *éléments* peuvent par exemple être donnés

1. de manière explicite, par des symboles tels que $1, 2, 3, a, b \ldots$;
2. par un symbole générique affecté par un ou plusieurs indices, x_i où i est un élément quelconque d'un autre ensemble.

Un ensemble peut être donné

1. de manière explicite, en donnant tous ses éléments, (définition en *extension*) comme par exemple $A = \{1, 2, 3, 4\}$ ou $B = \{a, b, c, d, e\}$;
2. de manière explicite, mais sans donner tous les éléments, que l'on peut remplacer par des points de suspension, comme $C = \{1, 2, \ldots, 100\}$, ou encore $D = \{a, b, c, \ldots, z\}$.
3. en décrivant la propriété caractérisant ses éléments, (définition en *compréhension*) comme dans
$$\{n : n \text{ est entier, pair et compris entre 1 et 99}\}.$$

En général, si P est une assertion, on désigne par $\{x : P\}$ ou par $\{x|P\}$ l'ensemble des objets x pour lesquels la propriété P est vérifiée.

Passons maintenant aux propriétés et aux relations entre éléments et ensembles.

1. ***Ensemble vide*** : il existe un ensemble qui ne contient pas d'éléments, l'ensemble vide, noté $\varnothing$.
2. ***Appartenance*** : on écrit $x \in A$ (x appartient à A) pour signifier que x est un élément de l'ensemble A.
3. ***Inclusion*** : on écrit $B \subset A$ (B est inclus dans A, ou B est un sous-ensemble de A) quand tout élément de B est aussi un élément de A. Dans ce cas, on dit que B est un sous-ensemble de A. L'ensemble vide est un sous-ensemble de tout ensemble donné.

   Par exemple, si $B = \{2, 4, 6, 8\}$, $A = \{n : n \text{ est un nombre entier pair}\}$, on a $B \subset A$.
4. ***Egalité*** : on écrit $A = B$ (A et B sont égaux) quand les ensembles A et B ont les mêmes éléments. Cela se traduit aussi par le fait que $A \subset B$ et $B \subset A$.

Les inclusions et l'égalité s'expriment également en termes d'implications : on a $A \subset B$ si l'implication $x \in A \Rightarrow x \in B$ est vraie, quel que soit l'objet x considéré. De même, on a $A = B$ si l'équivalence $x \in A \Leftrightarrow x \in B$ est vraie, quel que soit l'objet x considéré.

Enfin, on peut nier ces implications et écrire par exemple $x \notin A$, $B \not\subset A$ ou $A \neq B$, et par un léger abus de langage, on pourra écrire et lire ces symboles dans l'autre sens : $A \ni a$, $A \supset B$ ou $A \not\ni a$.

Soient A et B deux ensembles donnés, on peut construire les ensembles suivants :

1. ***Union*** : l'ensemble $A \cup B$ est formé par les éléments qui appartiennent à A ou à B. On a donc, d'un point de vue logique
$$(x \in A \cup B) \equiv ((x \in A) \,\text{ou}\, (x \in B)).$$
2. ***Intersection*** : l'ensemble $A \cap B$ est formé par les éléments qui appartiennent à A et B. On a donc, d'un point de vue logique
$$(x \in A \cap B) \equiv ((x \in A) \,\text{et}\, (x \in B)).$$

a. Ce n'est pas une définition extrêmement rigoureuse puisque le terme "collection" n'a pas été défini.

3. ***Différence*** : l'ensemble $A \setminus B$ (lisez A moins B) est formé par les éléments qui appartiennent à A et pas à B. On a donc, d'un point de vue logique

$$(x \in A \setminus B) \equiv ((x \in A) \,\text{et}\, \neg(x \in B)).$$

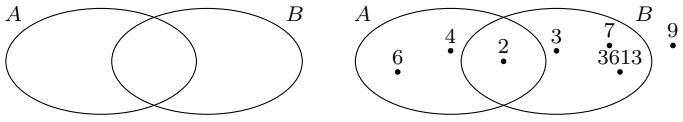
On peut représenter des ensembles à l'aide de diagrammes. Les plus utilisés sont sans doute les diagrammes de Venn [b]. Ils permettent de visualiser les opérations qui ont été définies plus haut de manière très simple. Voici comment on les construit.

— On représente l'ensemble par une courbe fermée, généralement un cercle ou une ellipse (appelée parfois patate).
— Si on veut marquer qu'un objet est un élément de l'ensemble, on le place dans la région déterminée par la courbe [c]. On n'est pas obligé de représenter tous les éléments de l'ensemble en question, et c'est souvent impossible.
— On représente plusieurs ensembles (généralement 2, 3 ou 4) par plusieurs courbes fermées.

Exemple 1.2.1. On note A l'ensemble des nombres entiers pairs et strictement positifs. On le représente par le diagramme à gauche dans la figure suivante. Si on veut marquer que 2 et 4 sont des éléments de cet ensemble, on les y indique avec un point, comme dans le diagramme à droite dans la figure suivante. Notez que la position n'a pas d'importance, à l'intérieur de la région en forme de patate.

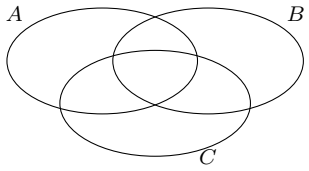
Prenons maintenant un exemple avec deux ensembles, donc avec un diagramme comportant deux patates.

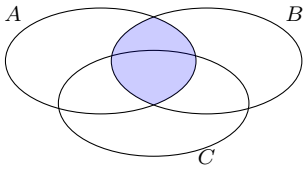
Exemple 1.2.2. Soit A l'ensemble des nombres pairs strictement positifs et B l'ensemble des nombres premiers. [d] Voici à gauche la représentation générale des deux ensembles, et à droite quelques éléments des deux ensembles. On peut ajouter également des points "en dehors" des deux ensembles.

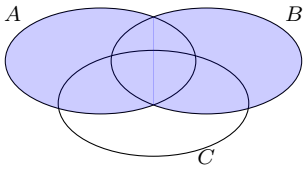


Cette représentation permet de visualiser aisément les unions et les intersections de deux ou plusieurs ensembles et d'avoir une intuition sur des égalités entre ensembles (sans toutefois constituer une démonstration rigoureuse). On peut en effet colorier ou hachurer les zones représentant les ensembles que l'on considère. Voici un exemple à trois ensembles [e]. A gauche, on a représenté la situation générale, au milieu, on a colorié la zone représentant $A \cap B$, à droite la zone représentant $A \cup B$.

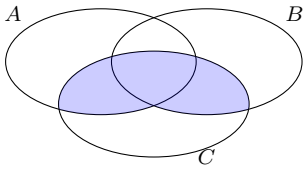
b. John Venn (1834-1923) les formalisa en 1880.
c. La plus petite des deux, évidemment.
d. Un nombre premier est un nombre entier naturel qui admet exactement deux diviseurs distincts.
e. Vous pouvez toujours adopter cette représentation pour trois ensembles







On peut aller encore plus loin et colorier par exemple la zone représentant $(A \cup B) \cap C$:



On peut alors constater sur cette représentation la relation

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

La proposition suivante présente un certain nombre de relations que nous avons déjà rencontrées en logique. Elles peuvent être démontrées en utilisant des tables de vérité, et j'en donne un exemple, ou en se ramenant à une propriété logique équivalente.

Proposition 1.2.1. *Si X est un ensemble et si A, B, C sont trois sous-ensembles de X, alors*

1. $X \cup X = X$, $X \cap X = X$;
2. $X \setminus X = \varnothing$, $X \setminus \varnothing = X$, $\varnothing \cup X = X$, $\varnothing \cap X = \varnothing$;
3. $A \cup B = B \cup A$, $A \cap B = B \cap A$;
4. $(A \cup B) \cup C = A \cup (B \cup C)$, $(A \cap B) \cap C = A \cap (B \cap C)$;
5. $A \cup (X \setminus A) = X$, $A \cap (X \setminus A) = \varnothing$;
6. *si* $A \subset B$, *alors* $A \cap C \subset B \cap C$;
7. *si* $A \subset B$, *alors* $A \cup C \subset B \cup C$;
8. $A \cap B \subset A \subset A \cup B$;
9. *si* $C \subset A$ *et* $C \subset B$, *alors* $C \subset A \cap B$;
10. *si* $A \subset C$ *et* $B \subset C$, *alors* $A \cup B \subset C$;
11. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
12. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
13. $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$;
14. $(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C)$;
15. $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$;
16. $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$.

Preuve de l'assertion 12. Etant donné un objet x, on a les 3 assertions $x \in A$, $x \in B$ et $x \in C$, qui peuvent toutes prendre les valeurs Vrai (1) ou faux (0). On calcule alors la table de vérité suivante.

$x \in A$	$x \in B$	$x \in C$	$x \in (B \cup C)$	$x \in (A \cap B)$	$x \in (A \cap C)$	$x \in A \cap (B \cup C)$	$x \in (A \cap B) \cup (A \cap C)$
0	0	0	0	0	0	0	0
0	0	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	1	1	1	0	0	0	0
1	0	0	0	0	0	0	0
1	0	1	1	0	1	1	1
1	1	0	1	1	0	1	1
1	1	1	1	1	1	1	1

On constate que les assertions $x \in A \cap (B \cup C)$ et $x \in (A \cap B) \cup (A \cap C)$ sont logiquement équivalentes. □

C'est un bon exercice de voir toutes ces assertions à l'aide de diagrammes de Venn. Il est également important d'essayer de les retenir. Les assertions 11 et 12 sont des règles de distributivité. Les assertions 15 et 16 correspondent à la négation logique et sont appelées lois de De Morgan.

Puisque les opérations d'union et d'intersection sur les ensembles sont associatives on peut définir l'union et l'intersection de plusieurs ensembles. On donnera facilement un sens aux expressions du type $A_1 \cup \cdots \cup A_n$ ou $B_1 \cap \cdots \cap B_p$, où n et p sont des nombres naturels. Il arrivera aussi que l'on note ces ensembles

$$\cup_{k=1}^{n} A_k \quad \cap_{k=1}^{p} B_k.$$

Il s'agit d'un raccourci d'écritures fort utile, et que nous emploierons chaque fois que c'est possible, avec une opération associative et commutative. Vous les reverrez d'ici peu en algèbre avec les sommes. Il est important de noter que dans ces expressions, la lettre k est dite muette et peut être remplacée par n'importe quel autre symbole. C'est exactement le même principe que la lettre x dans $\int_0^3 \sin(x)\mathrm{d}x$.

1.2.1 Un mot sur le paradoxe de Russell

J'ai présenté ci-dessus les rudiments de la théorie naïve des ensembles, et nous avons constaté que la définition même d'un ensemble n'en était pas une. Cela ne semble pas poser de problème puisque nous avons l'habitude dans la vie courante de travailler avec des collections d'objets et de pouvoir considérer intuitivement des unions, des intersections, des complémentaires...

Comme vous commencez à le percevoir, tout ce qui n'est pas parfaitement défini à partir d'axiomes ou de leurs conséquences peut comporter des risques en mathématiques. C'est également le cas de la théorie naïve des ensembles : elle est contradictoire. En effet, on peut, en utilisant les ensembles ainsi définis, trouver une proposition qui n'est ni vraie ni fausse. Cette proposition est un paradoxe, et montre que la théorie naïve des ensembles est incomplète. Rassurez-vous, on a depuis complété la théorie (en fait de plusieurs façons), et vous n'aurez pas à vous soucier du fait que la théorie des ensembles soit incomplète avant longtemps dans vos études.

Je vous livre cependant cette propriété paradoxale, publiée par B. Russell en 1903.

Considérons les ensembles suivants : $A = \{1, 2, 3, a, b, 2\}$ et $B = \{1, 2, 3, 4, B, a, u, v\}$. On voit une différence entre les deux ensembles. En effet, on a $B \in B$. Puisque les ensembles sont des collections quelconques. Cela ne pose pas de problème.

Appelons donc ensembles extraordinaires ceux qui, comme B, se contiennent eux-mêmes. Appelons également ordinaires les ensembles qui ne se contiennent pas eux-mêmes, c'est à dire ceux qu'on a l'habitude de voir.

Considérons l'ensemble R des ensembles ordinaires. Cet ensemble conduit au paradoxe : on se demande si R est ordinaire ou extraordinaire.

S'il est ordinaire, alors il ne se contient pas comme élément, donc $R \notin R$, donc R est extraordinaire.

S'il est extraordinaire, alors $R \in R$, donc R est ordinaire.

1.3 Relations, applications, injections, surjections

Le but de cette section est de reconstruire la notion d'application. Elle généralise ce que vous avez appelé "fonction" dans l'enseignement secondaire. La plupart d'entre vous a eu une définition qui s'exprime comme ceci
"Une fonction est une loi qui à tout x associe un y, on note alors $y = f(x)$."
On entend même dire (et aussi écrire) "la fonction $f(x)$", ou "la fonction $y = f(x)$", "x et y sont des variables liées par f"...

Il y a plusieurs problèmes dans cette "définition" et dans les conceptions qui en découlent. Le problème le plus évident est qu'on n'a pas dit ce que pouvait être x. On peut donc préciser la définition comme ceci :
"Une fonction d'un ensemble A dans un ensemble B est une loi qui à tout $x \in A$ associe un $y \in B$, on note alors $y = f(x)$."
Cela a l'air plus scientifique, plus précis, mais il y a encore un problème : qu'est-ce qu'une "loi" ?

Dans la première partie de cette section, nous allons donner un sens à cette définition, en explicitant ce que l'on veut dire par "loi" dans cette définition un peu bancale. Cela se fait à l'aide du concept de relation, qui est à la fois plus simple et plus général que celui de fonction. Nous ne définirons pas ce que pourraient être les variables, car on ne parle pas de variables en mathématique. La notion d'ensemble remplit en effet le rôle que jouent les variables en sciences : quand un scientifique parle de la "variable température", le mathématicien envisage l'ensemble de toutes les températures possibles, et c'est vriapour toutes les "variables" scientifiques.

Pour définir ce qu'est une relation, nous aurons besoin de la notion de produit cartésien d'ensembles. Pour deux ensembles, cette notion est assez simple à définir.

Définition 1.3.1. Si A et B sont deux ensembles, alors le produit cartésien de A et B est l'ensemble

$$A \times B = \{(a, b) : a \in A \text{ et } b \in B\}.$$

On peut bien entendu étendre cette définition de produit à plusieurs ensembles. L'opération "produit" n'est pas tout à fait associative, et on devrait en toute précision mettre des parenthèses, mais cela ne posera pas de problème de faire un léger abus et de les oublier.

Définition 1.3.2. Si $A_1, \ldots, A_n$ sont des ensembles ($n \in \mathbb{N}$), alors le produit cartésien $A_1 \times \cdots A_n$ est l'ensemble

$$A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) : a_1 \in A_1, \ldots, a_n \in A_n\}.$$

Donnons directement la définition d'une relation d'un ensemble A vers un ensemble B.

Définition 1.3.3. Une relation $\mathcal{R}$ de A dans B est une partie de $A \times B$. On appelle A l'ensemble de départ et B l'ensemble d'arrivée de $\mathcal{R}$.

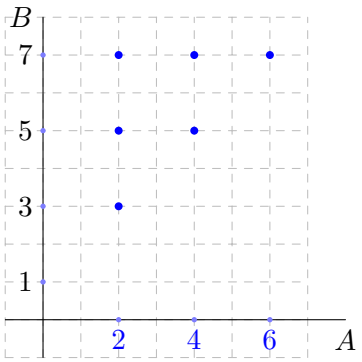
Si le couple (a, b) appartient $\mathcal{R}$, on note $a\mathcal{R}b$ et on dit que a est en relation avec b. Le lien entre les deux notations est donc

$$\mathcal{R} = \{(a, b) \in A \times B | a\mathcal{R}b\}.$$

Exemple 1.3.1. Posons $A = \{2, 4, 6\}$ et $B = \{1, 3, 5, 7\}$. La relation "est plus petit que", de A dans B est

$$\mathcal{R} = \{(2, 3), (2, 5), (2, 7), (4, 5), (4, 7), (6, 7)\}.$$

On peut bien sûr représenter le produit cartésien comme d'habitude par un graphique plan et on représente alors facilement la relation :



On peut définir une relation de A dans B par une assertion définissant l'appartenance à cette relation : par exemple, définissons $\mathcal{R}'$ par $x\mathcal{R}'y$ si et seulement si $y = x + 3$. On a alors $\mathcal{R}' = \{(2, 5), (4, 7)\}$. Je vous laisse faire la représentation graphique.

Voici encore trois exemples.

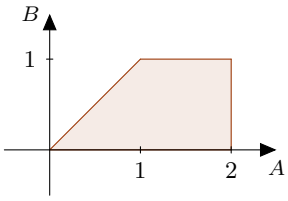
1. Considérons la relation $\geqslant$ de $A = [0, 2]$ dans $B = [0, 1]$ donnée par

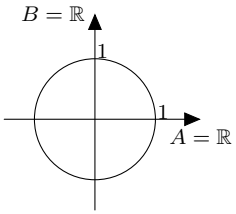
$$\mathcal{R}_1 = \{(x, y) \in [0, 2] \times [0, 1] : x \geqslant y\}.$$

2. Soit $\mathcal{R}_2$ la relation de $\mathbb{R}$ dans $\mathbb{R}$ définie par

$$x\mathcal{R}_2 y \quad \text{si, et seulement si} \quad x^2 + y^2 = 1.$$

Elle se représentent visiblement par

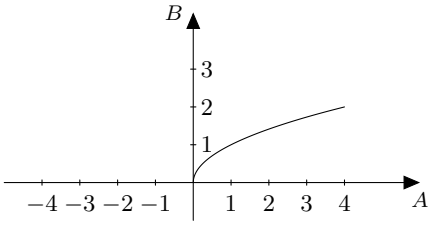




3. Terminons par la relation $\mathcal{R}_3$ définie de $A = [-4, 4]$ dans $B = [0, 3]$ par

$$x\mathcal{R}_3 y \quad \text{si, et seulement si} \quad y^2 - x = 0.$$

Elle est représentée par



Remarquez que par convention, quand on peut représenter une relation par un graphique plan, on indique l'ensemble de départ sur un axe horizontal. Cette convention n'a rien de mathématique, puisque l'horizontalité n'est pas définie.

Définition 1.3.4. Soit $\mathcal{R}$ une relation de A dans B. On appelle *domaine* de $\mathcal{R}$ l'ensemble des points a de A qui sont en relation avec au moins un élément b de B. On le note $\mathrm{dom}_{\mathcal{R}}$ ou $\mathrm{dom}(\mathcal{R})$ ou encore $D_{\mathcal{R}}$. On a

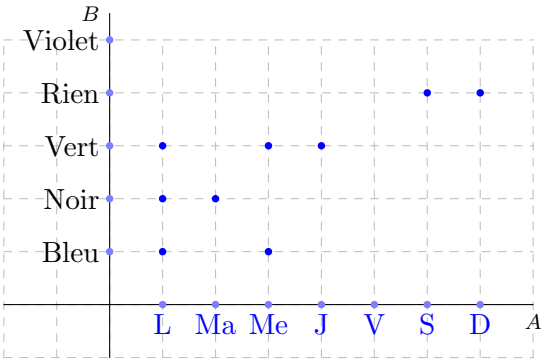
$$\mathrm{dom}_{\mathcal{R}} = \mathrm{dom}(\mathcal{R}) = D_{\mathcal{R}} = \{a \in A : \exists b \in B : a\mathcal{R}b\}.$$

On appelle *codomaine* ou *image* de $\mathcal{R}$ l'ensemble $\mathrm{Im}(\mathcal{R})$ (ou $\mathrm{Im}_{\mathcal{R}}$) des points b de B tels qu'il existe au moins un élément a de A qui soit en relation avec b. On a

$$\mathrm{Im}_{\mathcal{R}} = \mathrm{Im}(\mathcal{R}) = \{b \in B : \exists a \in A : a\mathcal{R}b\}.$$

Voici quelques exemples :

1. si A est l'ensemble des jours de la semaine et B un ensemble de couleurs de chaussettes que je peux porter, on peut considérer la relation suivante, de l'ensemble $A = \{\mathrm{L}, \mathrm{Ma}, \mathrm{Me}, \mathrm{J}, \mathrm{V}, \mathrm{S}, \mathrm{D}\}$ dans l'ensemble $B = \{\text{bleu}, \text{noir}, \text{vert}, \text{blanc}, \text{violet}\}$.



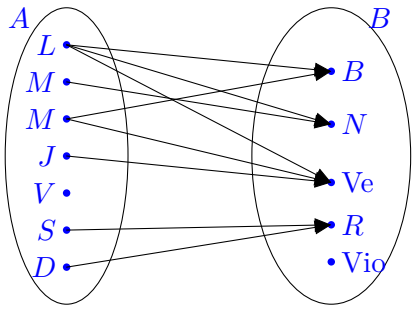
On constate qu'il n'y a pas de point de B qui soit en relation avec vendredi (V), donc $\mathrm{dom}_{\mathcal{R}} = A \setminus \{V\}$. De même, aucun point de A n'est en relation avec violet, et on calcule donc que $\mathrm{Im}_{\mathcal{R}} = B \setminus \{\text{Violet}\}$.

2. Soit la relation $\mathcal{R}_2$ de $\mathbb{N}$ dans $\mathbb{N}$ définie par $x\mathcal{R}_2 y$ si, et seulement si $x + y = 3$. On constate que le domaine de $\mathcal{R}_2$ est $\{0, 1, 2, 3\}$, tandis que son image est également $\{0, 1, 2, 3\}$.
3. Soit la relation $\mathcal{R}_3$ de $\mathbb{R}$ dans $\mathbb{R}$ définie par $x\mathcal{R}_2 y$ si, et seulement si $|x| + |y| = 3$. Le domaine de $\mathcal{R}_3$ est égal à $[-3, 3]$, et son image aussi. Il est intéressant de représenter cette relation dans le plan, identifié à $\mathbb{R}^2$ au moyen d'un repère orthonormé : on obtient un carré. Vous verrez en analyse qu'il s'agit de la boule de centre $(0, 0)$ et de rayon 3, pour la distance de Manhattan.

En ce qui concerne les représentations graphiques que l'on peut faire d'une relation, nous connaissons déjà une façon de représenter un produit, même de manière schématique, dans le plan. Nous avons utilisé cette représentation dans le premier exemple ci-dessus. Il existe une autre représentation graphique, en termes de diagramme de Venn. C'est la représentation *sagittale*.

Définition 1.3.5. La représentation sagittale d'une relation $\mathcal{R}$ de A dans B est obtenue en représentant les ensembles par des diagrammes de Venn et en indiquant une flèche [a] de $a \in A$ vers $b \in B$ quand $a\mathcal{R}b$.

Dans notre exemple de chaussettes, cela donne ceci.



On constate facilement sur cette représentation que V n'est pas dans le domaine de $\mathbb{R}$ car aucune flèche ne part de V. De même "Violet" n'est pas dans l'image car aucune flèche n'arrive à "Violet". Cette représentation sagittale a d'autres avantages : elle permet de visualiser facilement la définition de la composée de deux relations, ainsi que de la relation réciproque.

Définition 1.3.6. Si $\mathcal{R} : A \to B$ et $\mathcal{R}' : B \to C$ sont des relations, alors la relation composée $\mathcal{R}' \circ \mathcal{R} : A \to C$ est définie par [b]

$$\mathcal{R}' \circ \mathcal{R} = \{(a, c) \in A \times C : \exists b \in B : a\mathcal{R}b \quad \text{et} \quad b\mathcal{R}'c\}.$$

a. En latin, sagitta veut dire flèche, cela a également donné le mot sagittaire.
b. Attention à l'ordre dans lequel on écrit les relation $\circ$ se lit "après".

En termes de représentation sagittale, a est donc en relation avec c pour $\mathcal{R}' \circ \mathcal{R}$ si on peut connecter a à c par deux flèches successives (la première de $\mathcal{R}$ et la seconde de $\mathcal{R}'$), aboutissant et partant d'un point intermédiaire $b \in B$.

Cette définition nous permettra d'ici peu de composer des applications et d'obtenir par exemple la relation

$$\mathcal{R} = \{(x, y) \in \mathbb{R}^2 : y = \sin^2(x^3)\}$$

comme la composée des relations $\mathcal{R}_1 = \{(x, y) \in \mathbb{R}^2 : y = x^3\}$, $\mathcal{R}_2 = \{(y, z) \in \mathbb{R}^2 : z = \sin(y)\}$ et $\mathcal{R}_3 = \{(z, a) \in \mathbb{R}^2 : a = z^2\}$. On a alors $\mathcal{R} = \mathcal{R}_3 \circ (\mathcal{R}_2 \circ \mathcal{R}_1)$.

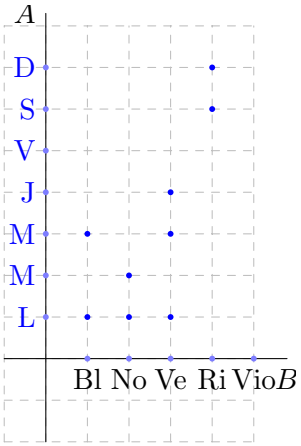
Exercice 1.3.1. Montrer que la composition des relations est associative : on a $\mathcal{R}_3 \circ (\mathcal{R}_2 \circ \mathcal{R}_1) = (\mathcal{R}_3 \circ \mathcal{R}_2) \circ \mathcal{R}_1$, quelles que soient les relations $\mathcal{R}_1$, $\mathcal{R}_2$, $\mathcal{R}_3$.

En ce qui concerne la relation réciproque, elle est obtenue sur le diagramme simplement en inversant le sens des flèches. Il s'agit donc d'une relation de B vers A, si $\mathcal{R}$ est une relation de A dans B. Plus formellement, on a la définition suivante.

Définition 1.3.7. Si $\mathcal{R} : A \to B$ est une relation, alors la relation inverse (ou réciproque) de $\mathcal{R}$ est la relation $\mathcal{R}^{-1} : B \to A$ définie par

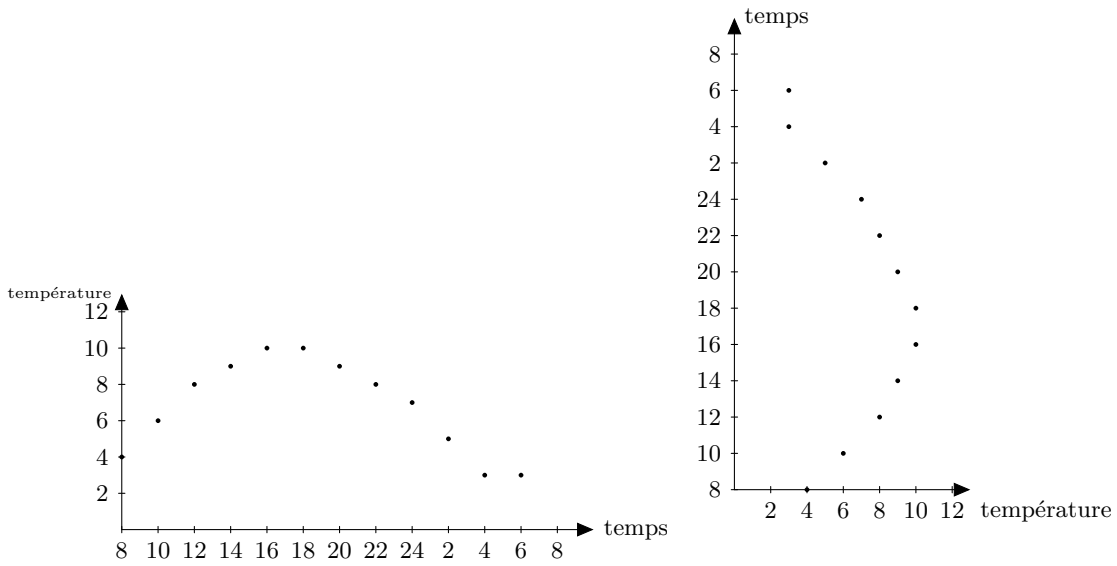
$$\mathcal{R}^{-1} = \{(b, a) \in B \times A : a\mathcal{R}b\}.$$

Nous avons déjà la représentation sagittale de $\mathcal{R}^{-1}$. Si on se concentre sur la représentation en produit cartésien, il suffit de lire le graphique dans l'autre sens : de B vers A. Cependant, comme on prend souvent la convention de représenter l'ensemble de départ horizontalement [c], on place B sur l'axe horizontal et A sur l'axe vertical, et on considère les mêmes point qu'avant. Cela revient géométriquement à effectuer une symétrie orthogonale qui échange les axes. Pour l'exemple des chaussettes, on a la représentation suivante de $\mathcal{R}^{-1}$:



Voici encore un exemple d'une relation liant l'heure et la température observée, et de sa relation réciproque :

c. Comme je l'ai dit plus haut, cela n'a rien de mathématique, mais c'est très courant en sciences.



Il est également intéressant de calculer la composée d'une relation et de sa réciproque.

Exercice 1.3.2. Démontrer que $\mathrm{dom}_{\mathcal{R}^{-1}} = \mathrm{Im}_{\mathcal{R}}$ et $\mathrm{Im}_{\mathcal{R}^{-1}} = \mathrm{dom}_{\mathcal{R}}$.

Ayant une relation à sa disposition, on peut en créer d'autres en restreignant l'ensemble de départ ou l'ensemble d'arrivée. C'est l'objet de la définition suivante.

Proposition 1.3.1. *Si $\mathcal{R} : A \to B$ est une relation, et si A' est un sous-ensemble de A, alors la restriction de $\mathcal{R}$ à A' est la relation $\mathcal{R}|_{A'} : A' \to B$ définie par*

$$\mathcal{R}|_{A'} = \{(a, b) \in A' \times B : a\mathcal{R}b\}.$$

On restreint donc l'ensemble de départ. Cela a bien sûr une influence sur l'image de la relation en général. Par exemple, si $\mathcal{R} = \{(x, y) \in \mathbb{R}^2 : y = x^2\}$, alors $\mathcal{R}|_{[0,+\infty[} = \{(x, y) \in [0, +\infty[\times\mathbb{R} : y = x^2\}$ a la même image que $\mathcal{R}$, tandis que $\mathcal{R}|_{[0,2]}$ admet $[0, 4]$ pour image.

On peut aussi restreindre l'ensemble d'arrivée et définir la restriction de $\mathcal{R}$ à $B' \subset B$ comme étant $\{(a, b) \in A \times B' : a\mathcal{R}b\}$. Je n'utiliserai pas directement cette restriction et je n'introduis donc pas de notation particulière.

1.4 Applications

Passons maintenant au premier type particulier de relation. Il s'agit des relations de type application. Je les définis en deux temps, car elles sont caractérisées par deux propriétés distinctes. La première de ces propriétés est le fait de pouvoir associer à tout élément de A *au plus* un élément de B. L'élément de B est alors déterminé *en fonction* de l'élément de A que l'on considère. Dans le cas de la relation $\mathcal{R}$: temps $\to$ température, la température est exprimée en fonction de l'heure : à chaque heure, il correspond au plus une température. Si on regarde la relation réciproque, pour certaines températures, il y a plusieurs heures associées, donc l'heure ne s'exprime pas en fonction de la température. Passons maintenant à la définition formelle.

Définition 1.4.1. Une relation $\mathcal{R}$ de A dans B est de type fonctionnel si tout point a de $\mathrm{dom}_{\mathcal{R}}$ est en relation avec exactement un élément de B.

On a comme d'habitude une formulation équivalente, puisqu'on analyse en fait l'unicité de l'élément de B qui est associé à chaque point de A. Une relation est donc de type fonctionnel si l'implication suivante est vraie

$$(a \in A, b_1, b_2 \in B, a\mathcal{R}b_1, a\mathcal{R}b_2) \Rightarrow b_1 = b_2.$$

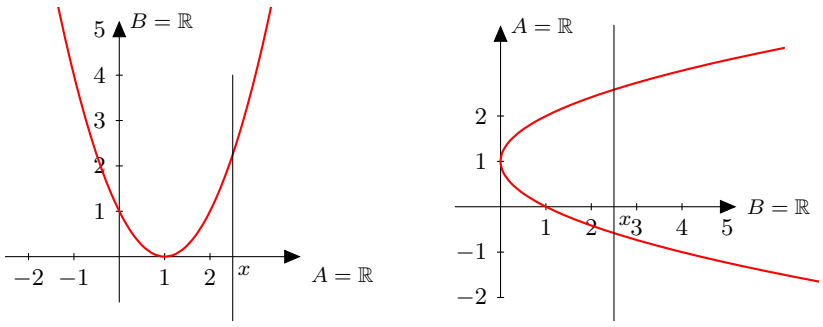


FIGURE 1.1 – Deux relations

Cela donne lieu sur la représentation graphique (quand elle est possible), à un test élémentaire.

La relation à gauche de $A = \mathbb{R}$ dans $B = \mathbb{R}$ est de type fonctionnel : à chaque point de A correspond au plus un point de B, comme on le voit en représentant l'ensemble des couples $\{(x, b) : b \in B\}$ pour chaque $x \in A$ [a]. Pour information, cette relation s'écrit $\{(x, (x-1)^2) : x \in \mathbb{R}\}$. A droite, il s'agit de la relation réciproque, de $B = \mathbb{R}$ dans $A = \mathbb{R}$. On constate qu'elle n'est pas de type fonctionnel, puisqu'il existe au moins un point [b] de l'ensemble de départ (ici B) qui est en relation plus d'un point de l'ensemble d'arrivée (A).

Dans une relation de type fonctionnel $\mathcal{R} : A \to B$, le point $b \in B$ associé à un point a de A est unique (quand il existe). Cela lui vaut un nom.

Définition 1.4.2. Si $\mathcal{R} : A \to B$ est de type fonctionnel, alors si $(a, b) \in \mathcal{R}$, on dit que b est l'image de a par $\mathcal{R}$.

Parmi les relations de type fonctionnel, il en est qui sont particulières : celles pour lesquelles tout point de a admet une image. De manière équivalente, ce sont les relations $\mathcal{R} : A \to B$ dont le domaine est A.

Définition 1.4.3. Une relation $\mathcal{R} : A \to B$ est de type application si les deux conditions suivantes sont satisfaites :

1. La relation $\mathcal{R}$ est de type fonctionnel ;
2. Le domaine de $\mathcal{R}$ est égal à A.

On peut bien sûr résumer ces deux conditions : la première stipule que tout point a de A est en relation avec au plus un point b de B. La deuxième s'écrit également "tout point a de A est en relation avec au moins un point b de B". La conjonction des deux conditions s'écrit donc de manière équivalente :

"Tout point a de A est en relation avec exactement un point de b de B."

Bien entendu, si on dispose d'une relation de type fonctionnel $\mathcal{R}$ de A dans B, on peut toujours en faire une relation de type application en restreignant son ensemble de départ à son domaine. Ce fait, bien qu'évident, vaut bien une proposition.

Proposition 1.4.1. *Si $\mathcal{R} : A \to B$ est de type fonctionnel, alors $\mathcal{R}|_{\mathrm{dom}(\mathcal{R})}$ est de type application.*

Remarque 1.2. Il est important de remarquer que les définitions que nous venons de poser ne disent rien sur les points de B : il peut exister des points de B qui ne sont images d'aucun point de A, et aussi des points de B qui sont images de plusieurs points de A.

Voici quelques exemples.

a. C'est la droite verticale représentée sur le graphique.
b. Ici encore, on le voit en traçant des droites verticales sur les représentations graphiques.

Exemple 1.4.1. Les relations suivantes sont de type application :

1. $\mathcal{R}_1 : \mathbb{R} \to \mathbb{R}$ définie par $\mathcal{R}_1 = \{(x, x^2) : x \in \mathbb{R}\}$;
2. $\mathcal{R}_2 : \mathbb{R} \to [0, +\infty[$ définie par $\mathcal{R}_2 = \{(x, x^2) : x \in \mathbb{R}\}$;
3. $\mathcal{R}_3 : [0, +\infty[\to [0, +\infty[$ définie par $\mathcal{R}_3 = \{(x, x^2) : x \in \mathbb{R}\}$.

Par contre la relation $\mathcal{R}_4 : \mathbb{R} \to \mathbb{R}$ définie par $\mathcal{R}_4 = \{(x, \mathrm{tg}(x)) : x \in \mathbb{R}\}$ n'est pas une relation car $\mathrm{tg}(x)$ n'est pas défini pour tout $x \in \mathbb{R}$.

Il est important de remarquer que l'ensemble d'arrivée peut dans une certaine mesure être modifié sans changer le caractère "application" d'une relation. Ainsi, la relation $\mathcal{R}_2$ est de type application. En élargissant l'ensemble d'arrivée pour obtenir la relation $\mathcal{R}_1$, on conserve une relation de type application.

Je ne peux terminer cette section sur les applications sans faire le lien avec la notion que vous avez vue en secondaire, et qui est bien souvent la seule utilisée en sciences.

Elle n'est pas bien difficile à faire : une relation de type application $\mathcal{R} : A \to B$ est la donnée, pour chaque point a de A, d'un unique point $b \in B$, qui est l'image de a. On peut donc voir une relation comme une "transformation" qui transforme chaque point de A en son image. On note alors l'application par une lettre (souvent f [c], et on précise la transformation en question : on a alors la notation complète suivante :

$$f : A \to B : a \mapsto f(a).$$

Elle indique que f est une application de A dans B qui à chaque point a de A associe son image $f(a)$. On obtient ainsi la notion d'application qui a été introduite dans l'enseignement secondaire.

Définition 1.4.4 (Intuitive mais incomplète)**.** Une application f de A dans B est une "loi de transformation" qui associe à tout point x de A, associe un point $f(x)$ de B [d].

Bien entendu, partant de cette vision "loi de transformation" d'une application de A dans B, il n'est pas difficile de récupérer la relation de type application correspondante : si on considère la "loi de transformation" qui transforme tout x dans $\mathbb{R}$ en $\sin(x)$, alors la relation de type application correspondante (au sens de notre définition officielle) est

$$\mathcal{R} = \{(x, \sin(x)) : x \in \mathbb{R}\}.$$

Cette relation s'écrit encore $\{(x, y) \in \mathbb{R}^2 : y = \sin(x)\}$. Nous avons donc fait le lien également avec une formulation utilisée dans l'enseignement secondaire où l'on parle parfois de la "fonction $y = \sin(x)$". L'avantage évident de notre approche est qu'il n'y a pas à se poser de question sur le statut de x et y (on parle dans l'enseignement secondaire de variables ou d'indéterminées). Ici, nous considérons la relation $\{(x, y) \in \mathbb{R}^2 : y = \sin(x)\}$, et x et y sont toujours des nombres réels.

L'avantage fondamental de notre approche de la notion d'application par rapport à celle qui a été généralement suivie dans l'enseignement secondaire est qu'elle ne fait appel à aucun concept non défini : elle est basée sur les notions de sous-ensemble et de produit cartésien et des notions d'existence et d'unicité. Si j'avais défini "Une application est une loi de transformation...", il aurait été naturel que vous me demandiez de définir ce qu'est une loi de transformation. Je n'aurais pas eu de réponse à donner, à part une association particulière entre des points de deux ensembles... et on se serait ramené à la définition qui a été donnée plus haut.

Le point de vue intuitif "loi de transformation" que vous avez connu jusqu'à présent est maintenant intégré à une définition précise. Vous pouvez donc continuer à penser les applications comme des lois de transformation, mais si on vous demande de définir cette

c. On utilise souvent f parce que, lorsque $B = \mathbb{R}$ ou $B = \mathbb{C}$, les applications sont appelées fonctions, mais tout autre symbole convient.

d. Donc f transforme x en $f(x)$.

notion avec toute la rigueur nécessaire (c'est-à-dire à partir des objets mathématiques définis en amont), vous savez maintenant que ces lois de transformations sont associées à des relations de type application. Résumons ces diverses constatations dans une proposition [e].

Proposition 1.4.2. *Si $\mathcal{R}$ est une relation de type application de A dans B, alors elle définit une "loi de transformation" de A dans B : $a \in A$ est transformé en $b \in B$ si, et seulement si $(a, b) \in \mathcal{R}$. Réciproquement, si $f : A \to B : a \mapsto f(a)$ est une "loi de transformation", elle définit une relation de type application, appelée le* graphe de f *et notée G_f :*

$$G_f = \{(a, f(a)) : a \in A\} = \{(a, b) \in A \times B : b = f(a)\}.$$

Dans la suite, nous utiliserons la notation $f : A \to B : a \mapsto f(a)$, et nous pourrons penser f comme une loi de transformation, tout en sachant que si nous devons utiliser la définition dans une preuve, il s'agit bien d'une relation.

Terminons cette section par la notion de composée d'applications. Nous avons déjà défini la composée de relations en général, il suffit donc de vérifier que cette définition s'applique aux relations de type application.

Proposition 1.4.3. *La composée de relations de type application est de type application. Plus précisément, si on a $\mathcal{R} : A \to B$, $\mathcal{R}' : B \to C$, $\mathcal{R} = G_f$ et $\mathcal{R}' = G_g$, alors $\mathcal{R}' \circ \mathcal{R} : A \to C$ s'écrit $G_{g \circ f}$ où $(g \circ f)(a) = g(f(a))$, pour tout $a \in A$.*

Démonstration. Il suffit de vérifier que $\mathcal{R}' \circ \mathcal{R}$ satisfait les deux conditions pour être de type application. Par définition, pour $a \in A$ et $c \in C$, on a $(a, c) \in \mathcal{R}' \circ \mathcal{R}$ si, et seulement si, il existe $b \in B$ tel que $a\mathcal{R}b$ et $b\mathcal{R}'c$. Mais puisque $\mathcal{R}$ est de type application, pour tout $a \in A$, il existe un unique b tel que $a\mathcal{R}b$, c'est l'image de a, notée $f(a)$. De même, pour tout $b \in B$ (et en particulier $f(a)$), il existe un unique c tel que $b\mathcal{R}'c$, c'est $g(b)$. En conclusion, pour tout $a \in A$, il existe un unique $c \in C$ tel que $a\mathcal{R}' \circ \mathcal{R}c$, c'est $g(f(a))$. □

1.5 Applications réciproques

Nous avons défini les relations réciproques en toute généralité, et la réciproque d'une relation existe toujours. Nous avons ensuite défini des relations particulières : les applications. Il est naturel de se demander si la réciproque d'une application est encore une application. Un bref coup d'oeil à la figure 1.1 montre que ce n'est pas toujours vrai. La question naturelle qui se pose est de déterminer des conditions sur $\mathcal{R}$ pour que $\mathcal{R}^{-1}$ soit de type application. La réponse à ce question est simple. La voici.

Proposition 1.5.1. *Soit $\mathcal{R} : A \to B$ une relation de type application. Alors $\mathcal{R}^{-1}$ est de type application si, et seulement si, pour tout $b \in B$ il existe un unique $a \in A$ tel que $a\mathcal{R}b$.*

Démonstration. Il suffit de traduire le fait que $\mathcal{R}^{-1}$ soit de type application : c'est le cas si, et seulement si, pour tout $b \in B$ il existe un unique $a \in A$ tel que $(b, a) \in \mathcal{R}^{-1}$. Mais la condition $(b, a) \in \mathcal{R}^{-1}$ est par définition équivalente à $(a, b) \in \mathcal{R}$, ou encore à $a\mathcal{R}b$. □

Cette proposition mène à a définition suivante.

Définition 1.5.1. Une application $f : A \to B$ telle que pour tout $b \in B$ il existe un unique $a \in A$ tel que $f(a) = b$ est une bijection.

Bien entendu, la condition pour que f soit une bijection est une conjonction : existence et unicité. Comme dans la définition des applications, il est utile de séparer ces deux conditions. Cela donne lieu à deux propriétés des applications, l'injectivité et la surjectivité.

Considérons les deux relations de la figure 1.1. La première est une application, et

e. Cette proposition est nécessairement bancale, puisqu'elle donne un lien entre un concept bien défini, celui de relation et un concept mal défini, celui de loi de transformation.

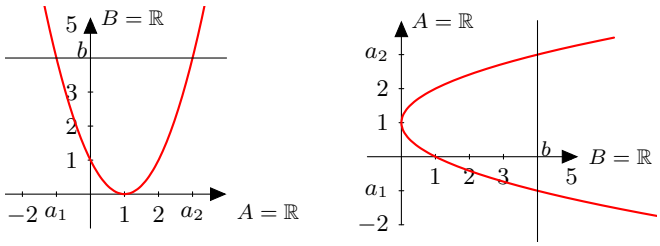


FIGURE 1.2 – Une application non injective et sa réciproque

sa réciproque ne l'est pas. Elle n'est en effet pas de type fonctionnel : il existe un point $b \in B$ qui est en relation avec deux points a_1 et a_2 de A. Cela peut se voir directement sur l'application f et nous amène à la définition.

Définition 1.5.2. Une application $f : A \to B$ est injective [a] si il n'existe pas $a_1, a_2 \in A$ tels que $a_1 \neq a_2$ et $f(a_1) = f(a_2)$.

Bien sûr cette définition n'est pas facile à mettre en oeuvre, puisqu'elle est basée sur l'inégalité $a_1 \neq a_2$. On passe donc naturellement à la contraposée qui fournit une définition équivalente pour l'injectivité.

Proposition 1.5.2. *Une application $f : A \to B$ est injective si, et seulement si, pour tous $a_1, a_2 \in A$, si $f(a_1) = f(a_2)$, alors $a_1 = a_2$.*

Démonstration. Il suffit de contraposer la condition de la définition. □

Remarque 1.3. Il y a une erreur fréquemment commise avec cette définition, elle consiste à renverser le sens de l'implication et à écrire "si $a_1 = a_2$ alors $f(a_1) = f(a_2)$." Cette condition n'apporte évidemment aucune information supplémentaire au fait que f soit une application.

Voici quelques exemples et contre-exemples.

Exemple 1.5.1.

1. L'application $f_1 : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$ n'est pas injective. En effet, on constate que $f_1(-2) = f_1(2) = 4$.
2. L'application $f_2 : [0, +\infty[\to \mathbb{R} : x \mapsto x^2$ est injective. En effet, soient $x, y \in [0, +\infty[$ tels que $f(x) = f(y)$. On a alors $x^2 = y^2$, ou encore $(x - y)(x + y) = 0$. Si on fixe $y \geqslant 0$ et que l'on cherche tous les x satisfaisant cette équation, on trouve $x = y$ ou $x = -y$. La deuxième solution n'est possible pour $x \geqslant 0$ que si $x = y = 0$. On a donc bien montré que $f(x) = f(y)$ implique $x = y$, pour tous $x, y \in [0, +\infty[$.
3. L'application $f_3 :]-\infty, 0] \to \mathbb{R} : x \mapsto x^2$ est injective, pour la même raison.
4. Il en va de même pour l'application $f_4 : A \to \mathbb{R} : x \mapsto x^2$, pour tout sous-ensemble A de $\mathbb{R}$ dont l'intersection avec la paire $\{-x, x\}$ contient au plus un élément, pour tout $x \in \mathbb{R}$.
5. L'application $f_5 : \mathbb{R} \to \mathbb{R} : x \mapsto \sin(x)$, appelée application sinus [b] n'est pas injective. En effet, on a $\sin(\frac{\pi}{3}) = \sin(\frac{2\pi}{3})$.
6. L'application $\sin :]-\frac{\pi}{2}, \frac{\pi}{2}[\to \mathbb{R}$ est injective. Cela peut se voir à partir du cercle trigonométrique, ou en résolvant l'équation $\sin(x) = \sin(y)$ à partir des propriétés du sinus, pour tout nombre y fixé dans $]-\frac{\pi}{2}, \frac{\pi}{2}[$.

Passons maintenant à quelques résultats sur les applications injectives. Le premier n'est pas surprenant puisque c'est pour l'obtenir que l'on a posé la définition.

a. On dit aussi que $f : A \to B$ est une injection.

b. Cette application sera redéfinie au cours d'analyse à partir de l'exponentielle des nombres complexes. Je me base ici sur la définition que vous en avez à partir du cercle trigonométrique.

Proposition 1.5.3. *Si $f : A \to B$ est une application injective, alors G_f^{-1} est une relation de type fonctionnel.*

Démonstration. Par définition, puisque G_f^{-1} est une relation de B dans A, on doit montrer que si $b \in B$, $a_1, a_2 \in A$ sont tels que $bG_f^{-1}a_1$ et $bG_f^{-1}a_2$, alors on a $a_1 = a_2$. Mais les deux conditions s'écrivent aussi $a_1 G_f b$ et $a_2 G_f b$, ou encore $b = f(a_1)$ et $b = f(a_2)$. Vu l'injectivité de f, on obtient $a_1 = a_2$. □

Remarque 1.4. La réciproque de cette proposition est vraie et est laissée comme exercice.

Nous pouvons également traduire l'injectivité en termes d'équations.

Proposition 1.5.4. *Une application $f : A \to B$ est injective si, et seulement si, pour tout $b \in B$, l'équation*

$$f(x) = b, \ (x \in A) \tag{1.1}$$

admet au plus une solution.

Démonstration. Ici encore, on utilise une simple traduction de la définition.

Supposons que f est une application injective et montrons que (1.1) admet au plus une solution. Si tel n'est pas le cas, il existe $x_1, x_2 \in A$ tels que $x_1 \neq x_2$ et $f(x_1) = b$ et $f(x_2) = b$. Mais alors l'injectivité de f implique $x_1 = x_2$, une absurdité.

Réciproquement, si l'équation (1.1) admet au plus une solution, alors l'application f est injective. Soient en effet $a_1, a_2 \in A$ tels que $f(a_1) = f(a_2)$. On pose alors $b = f(a_1)$ et on constate que a_1 et a_2 sont deux solutions de l'équation (1.1). On doit donc avoir $a_1 = a_2$. □

Passons maintenant à la surjectivité, qui correspondra à la deuxième condition pour que la réciproque d'une application soit une application. Considérons encore la figure 1.1. Une deuxième raison pour laquelle la réciproque n'est pas une application est que son domaine n'est pas égal à son ensemble de départ, à savoir B : On constate que le point

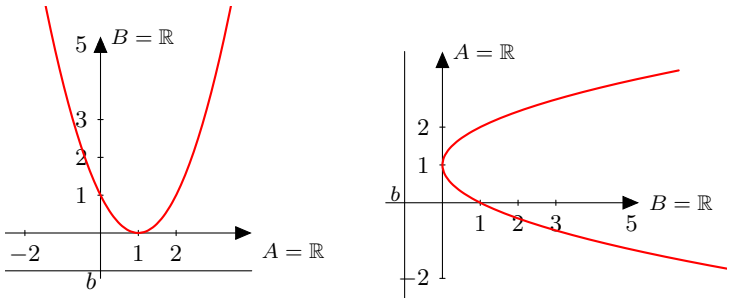


FIGURE 1.3 – Une application non surjective et sa réciproque

$b \in B$ n'est pas dans le domaine de la relation représentée à droite. Cela se voit sur l'application initiale représentée à gauche : il n'existe pas de point $a \in A$ satisfaisant $f(a) = b$. En d'autres termes b n'est pas dans l'image de la relation G_f. Cela conduit à la définition.

Définition 1.5.3. Soit $f : A \to B$ une application. L'image de f, notée $Im(f)$ ou $f(A)$ est égale à l'image de G_f. L'application f est surjective [c] si $Im(f) = B$.

Donnons tout de suite quelques exemples et contre-exemples.

Exemple 1.5.2. 1. L'application $f_1 : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$ n'est pas surjective. En effet, le nombre -1 n'est pas dans l'image de f_1.

c. On dit aussi que f est une surjection.

2. L'application $f_2 : \mathbb{R} \to [0, +\infty[: x \mapsto x^2$ est surjective. Il s'agit d'une propriété des nombres réels, que vous avez admise, mais que vous serez à même de démontrer à l'issue du cours d'analyse.
3. L'application $f_3 : \mathbb{N} \to \mathbb{N}_0 : n \mapsto n+1$ est surjective, puisque tout nombre naturel non nul est le successeur d'un nombre naturel. Nous reverrons sous peu cette propriété.
4. L'application $f_4 : \mathbb{R} \to \mathbb{R} : x \mapsto \sin(x)$ n'est pas surjective puisque par exemple, 2 n'est le sinus d'aucun nombre réel.
5. L'application $f_5 : \mathbb{R} \to [-1, 1] : x \mapsto \sin(x)$ est surjective. Ici encore, je vous renvoie au cours d'analyse pour une démonstration rigoureuse, mais vous pouvez vous convaincre de ce fait sur le cercle trigonométrique.

Nous avons bien sûr des résultats analogues à ceux concernant les applications injectives.

Proposition 1.5.5. *Une application $f : A \to B$ est surjective si, et seulement si, on a $\mathrm{dom}(G_f^{-1}) = B$.*

Démonstration. On sait que $\mathrm{dom}(G_f^{-1}) = Im(G_f) = Im(f)$. Donc l'assertion de l'énoncé est équivalente à $Im(f) = B$, c'est-à-dire à la surjectivité de f. □

La traduction en termes d'équations est également simple.

Proposition 1.5.6. *Une application $f : A \to B$ est surjective si, et seulement si, pour tout $b \in B$, l'équation*

$$f(x) = b, \quad (x \in A) \tag{1.2}$$

admet au moins une solution.

Démonstration. Il suffit de traduire la condition de l'énoncé. Le fait que l'équation (2.7) admette une solution est équivalent au fait que b soit dans l'image de f. La condition d'existence d'une solution pour tout $b \in B$ s'écrit donc $B = Im(f)$. □

Enfin, il est utile de remarquer que l'on peut toujours rendre une application quelconque surjective par restriction de l'ensemble d'arrivée.

Proposition 1.5.7. *Pour tout application $f : A \to B$, l'application $f : A \to Im(f) = f(A)$ est surjective.*

Démonstration. C'est évident. □

Passons maintenant à quelques propriétés des bijections. D'après ce que nous venons de voir, on a le résultat suivant.

Proposition 1.5.8. *Les assertions suivantes sont équivalentes :*

1. *L'application $f : A \to B$ est une bijection ;*
2. *L'application $f : A \to B$ est une injection et une surjection.*
3. *L'application $f : A \to B$ est telle que G_f^{-1} est de type application.*

Bien entendu, nous avons déjà démontré toutes les équivalences. La dernière donne lieu à une autre définition.

Définition 1.5.4. Soit $f : A \to B$ une bijection. La relation réciproque G_f^{-1} est de type application. On note cette application $f^{-1} : B \to A$, définie par $G_{f^{-1}} = G_f^{-1}$ et on l'appelle application réciproque de f [d].

Vous avez déjà rencontré des applications réciproques. En voici une petite liste.

d. On dit aussi application inverse de f.

Exemple 1.5.3. 1. L'application $f : [0, +\infty[\to [0, +\infty[: x \mapsto x^2$ est une bijection. La réciproque est l'application racine carrée : $\sqrt{\cdot} : [0, +\infty[\to [0, +\infty[: y \mapsto \sqrt{y}$.

2. L'application sinus $\sin : [-\frac{\pi}{2}, \frac{\pi}{2}] \to [-1, 1]$ est une bijection[e]. L'application réciproque est l'application arc sinus $\arcsin : [-1, 1] \to [-\frac{\pi}{2}, \frac{\pi}{2}]$.
3. L'application cosinus $\cos : [0, \pi] \to [-1, 1]$ est une bijection. Sa réciproque est l'application arc cosinus $\arccos : [-1, 1] \to [0, \pi]$.

Il est utile de pouvoir caractériser l'application réciproque.

Proposition 1.5.9. *Si $f : A \to B$ est une bijection, alors pour tous $a \in A$, $b \in B$, on a $f(a) = b$ si, et seulement si, $a = f^{-1}(b)$.*

Démonstration. Revenons à la définition des relations réciproques. On a alors les équivalences suivantes

$$b = f(a) \Leftrightarrow aG_f b \Leftrightarrow bG_f^{-1} a \Leftrightarrow bG_{f^{-1}} a \Leftrightarrow a = f^{-1}(b),$$

ce qui achève la preuve. □

Pour ce qui suit, nous avons besoin de définir l'égalité de deux applications.

Définition 1.5.5. Deux applications f et g sont égales si

1. Elles ont même domaine A ;
2. Pour tout $a \in A$, on a $f(a) = g(a)$.

Pour tout ensemble A, on définit l'application identique de A, notée id_A par $\mathrm{id}_A(a) = a$ pour tout $a \in A$.

On a alors le résultat suivant.

Proposition 1.5.10. *Si $f : A \to B$ est une bijection, alors on a $f^{-1} \circ f = \mathrm{id}_A$, $f \circ f^{-1} = \mathrm{id}_B$ et $(f^{-1})^{-1} = f$.*

Démonstration. On sait que $f^{-1} \circ f$ est une application définie sur A, tout comme id_A. Il reste maintenant à calculer $(f^{-1} \circ f)(a)$ pour tout $a \in A$ et à montrer que c'est a. Mais on a $(f^{-1} \circ f)(a) = b$ si, et seulement si $f^{-1}(f(a)) = b$, qui est équivalent à $f(a) = f(b)$, ou encore à $a = b$, puisque f est injectif.

La deuxième égalité se démontre comme la première, ou en appliquant la première à $f^{-1} : B \to A$, une fois que l'on a démontré que $(f^{-1})^{-1} = f$. Pour montrer que $f^{-1} : B \to A$ est une bijection et calculer son inverse, on peut procéder comme plus haut et montrer que pour tout $a \in A$, il existe un unique $b \in B$ tel que $f^{-1}(b) = a$. Alors b sera égal à $(f^{-1})^{-1}(a)$. Mais encore une fois par la proposition 1.5.9, l'assertion $f^{-1}(b) = a$ est équivalente à $b = f(a)$, ce qui suffit. □

Proposition 1.5.11. *La composée de deux bijections est une bijection. Plus précisément, si $f : A \to B$ et $g : B \to C$ sont des bijections, alors $g \circ f : A \to C$ est une bijection. De plus, on a la relation $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Démonstration. On sait déjà que la composée $g \circ f : A \to C$ est une application. Il reste à montrer que pour tout $c \in C$, il existe un unique $a \in A$ tel que $(g \circ f)(a) = c$. Si tel est le cas, $g \circ f$ sera une bijection et l'élément a satisfaisant cette condition sera par définition $(g \circ f)^{-1}(c)$. Mais on a les équivalences suivantes :

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

La première équivalence vient de la caractérisation de la composée d'applications. La deuxième et la troisième découlent de la proposition 1.5.9. □

e. On a restreint l'ensemble d'arrivée de sinus pour le rendre injectif, ce n'est pas la seule façon de faire, comme nous le verrons bientôt. On a également restreint l'ensemble d'arrivée pour rendre cette application surjective.

1.6 Images et pré-images de sous-ensembles

Dans cette courte section, nous donnons quelques définitions très importantes dans tous les cours. Il s'agit des images et des pré-images (ou images inverses) de sous-ensembles.

Définition 1.6.1. Soit $f : A \to B$ une application, soient X un sous-ensemble de A et Y un sous ensemble de B. Alors l'image de X par f est l'ensemble

$$f(X) = \{f(x) : x \in X\}.$$

La pré-image de Y par f, ou l'image inverse de Y par f est l'ensemble

$$f^{-1}(Y) = \{x \in A : f(x) \in Y\}.$$

L'ensemble $f(X)$ est donc constitué des images par f de tous les points de X, tandis que $f^{-1}(Y)$ est l'ensemble de tous les points dont l'image appartient à Y.

Remarque 1.5.
1. La notation $f^{-1}(Y)$ est dangereuse elle pourrait vous faire penser qu'il faut que f soit une bijection pour que cet ensemble soit défini. Ce n'est pas le cas : cet ensemble existe toujours, et ce n'est en général pas l'image de Y par f^{-1}, qui n'existe que si f est bijectif.
2. Nous avons associé à une application $f : A \to B$ deux nouvelles applications : $f : \mathcal{P}(A) \to \mathcal{P}(B) : X \mapsto f(X)$ et $f^{-1} : \mathcal{P}(B) \to \mathcal{P}(A) : Y \mapsto f^{-1}(Y)$.

Voici quelques exemples.

Exemple 1.6.1.
1. Soit $f : \mathbb{R} \to \mathbb{R} : x \mapsto \sin(x)$, alors $f([0, \frac{\pi}{2}]) = \{\sin(x) : x \in [0, \frac{\pi}{2}]\} = [0, 1]$.
2. Pour la même application, on a

$$f^{-1}([0, 1]) = \{x \in \mathbb{R} : \sin(x) \in [0, 1]\} = [0, \pi] \cup [2\pi, 3\pi] \cup \cdots = \cup_{k\in\mathbb{Z}}[2k\pi, (2k + 1)\pi].$$

3. Pour la même application, on a

$$f^{-1}([\frac{1}{2}, \frac{3}{2}]) = \{x \in \mathbb{R} : \sin(x) \geqslant \frac{1}{2}\} = \cup_{k\in\mathbb{Z}}[\frac{\pi}{6} + 2k\pi, \frac{5\pi}{6} + 2k\pi].$$

4. Soit $p_1 : \mathbb{R}^2 \to \mathbb{R} : (x, y) \mapsto x$. On a

$$p_1^{-1}(]\frac{1}{2}, 1[) = \{(x, y) \in \mathbb{R}^2 : x \in]\frac{1}{2}, 1[\} =]\frac{1}{2}, 1[\times\mathbb{R}.$$

On a le résultat suivant pour le comportement de l'image et de la pré-image vis-à-vis des unions et intersections. Vous pouvez retenir qu'il n'y a que l'image d'une intersection qui ne se comporte pas bien.

Proposition 1.6.1. *Soit $f : A \to B$ une application. On a alors*
1. $f^{-1}(Y \cup Z) = f^{-1}(Y) \cup f^{-1}(Z)$, *pour tous* $Y, Z \subset B$;
2. $f^{-1}(Y \cap Z) = f^{-1}(Y) \cap f^{-1}(Z)$, *pour tous* $Y, Z \subset B$
3. $f(Y \cup Z) = f(Y) \cup f(Z)$, *pour tous* $Y, Z \subset A$;
4. $f(Y \cap Z) \subset f(Y) \cap f(Z)$, *pour tous* $Y, Z \subset A$.

En général, la dernière inclusion est stricte.

Démonstration. On procède par double inclusion. Montrons par exemple la première égalité. Soit $a \in f^{-1}(Y \cup Z)$. Par définition, le point $f(a)$ appartient à $Y \cup Z$. Si $f(a) \in Y$, alors $a \in f^{-1}(Y) \subset f^{-1}(Y) \cup f^{-1}(Z)$. Si $f(a) \in Z$, alors $a \in f^{-1}(Z) \subset f^{-1}(Y) \cup f^{-1}(Z)$.

On montre l'autre inclusion : soit $a \in f^{-1}(Y) \cup f^{-1}(Z)$. Si $a \in f^{-1}(Y)$, alors $f(a) \in Y \subset Y \cup Z$ et donc a appartient à $f^{-1}(Y \cup Z)$. On fait de même si $a \in f^{-1}(Z)$.

Montrons la dernière inclusion. Si b appartient à $f(Y \cap Z)$, alors il existe $a \in Y \cap Z$ tel que $b = f(a)$. Mais puisque a appartient à Y, b appartient à $f(Y)$. De même, puisque $a \in Z$, b appartient à $f(Z)$. Au total, b appartient à $f(Y) \cap f(Z)$.

Le deux autres égalités se montrent de manière analogue. □

On peut montrer sur un exemple simple que la dernière inclusion de la proposition précédente est stricte. Considérons la projection $p_1 : \mathbb{R}^2 \to \mathbb{R}$. Soient les sous ensembles $X = [0,1] \times [0,1]$ et $Y = [0,1] \times [2,3]$ dans $\mathbb{R}^2$. Ils sont disjoints : on a $X \cap Y = \varnothing$, donc $p_1(X \cap Y) = p_1(\varnothing) = \varnothing$. Par contre $p_1(X) = p_1(Y) = [0,1]$, donc $p_1(X) \cap p_1(Y) = [0,1]$.

Etant donné $f : A \to B$, on peut également se demander comment se composent les applications f et f^{-1} définies entre $\mathcal{P}(A)$ et $\mathcal{P}(B)$. La notation suggère qu'elles sont inverses l'une de l'autre, mais ce n'est pas le cas. Voici un résultat cependant utile.

Proposition 1.6.2. *Soit $f : A \to B$ une application. Pour tout $X \subset A$ et tout $Y \subset B$,*

1. *On a $X \subset f^{-1}(f(X))$, l'égalité ayant lieu notamment si f est injectif;*
2. *On a $f(f^{-1}(Y)) \subset Y$, l'égalité ayant lieu notamment si f est surjectif.*

Démonstration. On montre la première inclusion de manière classique : soit $x \in X$ et montrons que $x \in f^{-1}(f(X))$. Par définition, cela est vrai si $f(x) \in f(X)$. Mais cette dernière assertion est vraie par définition de $f(X)$, puisque x appartient à X. Supposons maintenant f injectif et montrons l'autre inclusion. Soit $a \in f^{-1}(f(X))$. Par définition, $f(a)$ appartient à $f(X)$. Il existe donc $X \in X$ tel que $f(a) = f(x)$. Mais puisque f est injectif, cela implique $a = x$, donc $a \in X$.

Pour la deuxième inclusion, on considère $z \in f(f^{-1}(Y))$. Il existe $x \in f^{-1}(Y)$ tel que $z = f(x)$. Mais puisque x appartient à $f^{-1}(Y)$, on doit avoir $f(x) \in Y$. Donc z appartient à Y. Supposons f surjectif et montrons l'autre inclusion. Soit $y \in Y$. Puisque f est surjectif, il existe $a \in A$ tel que $f(a) = y$. Puisque $f(a) \in Y$, le point a appartient à $f^{-1}(Y)$, donc y est l'image d'un point de $f^{-1}(Y)$ et appartient donc à $f(f^{-1}(Y))$. □

Chapitre 2

Nombres complexes

2.1 Introduction

Dans ce chapitre, nous commençons par une révision rapide des équations du second degré dans $\mathbb{R}$ et des quelques résultats associés. Nous en profitons pour illustrer une technique, la complétion des carrés, qui est utile dans d'autres domaines. Nous constatons que certaines équations du second degré (et de degré supérieur) n'ont pas de solution dans $\mathbb{R}$, parce que les nombres négatifs ne sont pas des carrés. Nous faisons alors une extension de l'ensemble des nombres, et des opérations, pour obtenir les nombres complexes. Comme cela a été le cas dans le premier chapitre, nous construisons ces nombres à partir de ceux que nous connaissons [a]. Cette construction est importante car elle permet de prouver l'existence d'un ensemble de nombres ayant les propriétés voulues, mais il est encore plus important de pouvoir calculer avec les nombres complexes, et la construction classique de ces nombres ne permet pas de calculer facilement. Heureusement, nous trouvons deux façons de se donner des nombres complexes qui permettent de calculer facilement. Au passage, elles permettent, via l'exponentielle complexe, de récupérer facilement des résultats de trigonométrie, via par exemple, la formule de Moivre.

On pourrait croire que c'est encore un chapitre qui ne sert pas à grand chose et se demander si c'est bien raisonnable d'étendre encore les ensembles de nombres, après tout, si certaines équations n'ont pas de solution, elles n'ont pas de solution, un point c'est tout. Vous verrez dans la suite du cours d'algèbre que le travail avec les nombres complexes est paradoxalement plus simple qu'avec les nombres réels. Cela est dû au fait que non seulement toutes les équations du second degré auront deux solutions complexes (éventuellement confondues), mais en fait toutes les équations polynomiales de degré $n \geqslant 1$ admettent n solutions complexes (comptées avec leurs multiplicités). Pour les mathématiciens, les nombres complexes sont donc ceux qui permettent d'obtenir les résultats les plus simples et d'apporter des solutions efficaces à de nombreux problèmes. Pour les physiciens, ils sont la pierre angulaire de bon nombre de théories. Citons par exemple cette équation qui a fait couler pas mal d'encre au 20e siècle :

$$i\hbar\frac{\mathrm{d}}{\mathrm{dt}}|\Psi(t)\rangle = \hat{H}|\Psi(t)\rangle.$$

Elle commence par l'unité complexe i. Vous la découvrirez bientôt, sous cette forme ou sous une autre. Plus généralement, la mécanique quantique est construite sur des espaces de Hilbert, fait appel à des opérateurs linéaires hermitiens, et tout cela ne peut être construit sans nombres complexes. Tout cela répond à la question que vous vous posiez certainement : *"Quand est-ce que j'en aurai fini avec les nombres complexes ?"*... Jamais. Alors autant s'y mettre tout de suite.

a. Nous nous sommes entendus sur le fait que je ne définirai pas les nombres réels. Cela fait partie des cours d'analyse, mais vous les connaissez raisonnablement.

2.2 Equations du second degré et complétion des carrés

Les équations du second degré sont des équations ayant la forme générale :

$$ax^2 + bx + c = 0, \quad a \in \mathbb{R}_0, b, c \in \mathbb{R}. \tag{2.1}$$

Ces équations sont très simples à résoudre quand $b = 0$: par exemple $x^2 - 7 = 2$ a pour ensemble de solutions $\{-3; 3\}$, comme chacun sait. Mais attardons nous quelques secondes sur les étapes que l'on peut parcourir pour arriver à cette conclusion. Nous avons en fait procédé par équivalences :

$$x^2-7 = 2 \Leftrightarrow x^2-7-2 = 2+(-2) \Leftrightarrow x^2-9 = 0 \Leftrightarrow (x+3)(x-3) = 0 \Leftrightarrow x+3 = 0 \,\text{ou}\, x-3 = 0...$$

Les équivalences (vraies) ont le même sens qu'au premier chapitre : elles indiquent que les deux assertions ont même valeur de vérité, c'est-à-dire que ces équations ont le même ensemble de solutions. Mais nous avons utilisé, pour cette simple équation, que 2 admet un *opposé* pour l'addition ; cet opposé est le nombre qui permet d'avoir le *neutre* pour l'addition, à savoir 0. Nous avons, sans l'écrire, déplacé les parenthèses, donc utilisé l'*associativité* de l'addition. Ensuite, nous avons utilisé l'identité remarquable $(a+b)(a-b) = a^2-b^2$, qui résulte facilement du fait que la *multiplication distribue l'addition*, et du fait que la multiplication est *commutative*. Ensuite, nous avons utilisé la "règle du produit nul" ($ab = 0$ ssi $a = 0$ ou $b = 0$), qui se déduit facilement du fait que *tout nombre non nul admet un inverse* (et de la distributivité, qui rend 0 absorbant). En bref, nous avons utilisé pratiquement toutes les propriétés bien connues des nombres réels.

Voici un deuxième exemple encore assez simple : on considère l'équation suivante (pour $x \in \mathbb{R}$)

$$3(x + 5)^2 = 21. \tag{2.2}$$

On a la même résolution que ci-dessus :

$$3(x+5)^2 = 21 \Leftrightarrow 3(x+5)^2-21 = 0 \Leftrightarrow 3[(x+5)^2-7] = 0 \Leftrightarrow 3[(x+5)+\sqrt{7}][(x+5)-\sqrt{7}] = 0$$

Donc l'ensemble des solutions est $S = \{-5 + \sqrt{7}, -5 - \sqrt{7}\}$. Evidemment, vous me direz que je ne prends que des équations simples, qui mènent tout de suite à une factorisation car on a une différence de deux carrés. Je suis bien d'accord, mais en développant l'équation (2.2), nous venons en fait de résoudre

$$3x^2 + 30x + 54 = 0. \tag{2.3}$$

Tout le problème consiste à passer de l'équation (2.3), contenant un terme du premier degré en x à l'équation (2.2). C'est en fait assez simple : on met d'abord le facteur 3 en évidence et on se ramène à $3(x^2 + 10x + 18) = 0$. La seule façon de grouper x^2 et $10x$ pour former un carré est que $10x$ soit un double produit (c'est $2.5.x$), donc on souhaite avoir $x^2 + 10x + 25$, et on écrit donc

$$3(x^2 + 10x + 18) = 3(x^2 + 10x + 18 + 7 - 7) = 3[(x^2 + 2.5.x + 25) - 7] = 3[(x + 5)^2 - 7].$$

On a donc complété $x^2 + 10x$ pour obtenir un carré parfait et faire ainsi disparaître le terme du premier degré qui nous posait problème.

Dans le cas général, on procède de la même façon pour faire "disparaître" ce même terme dans le trinôme $ax^2 + bx + c$. On peut toujours le faire en complétant le carré :

$$\begin{aligned} ax^2 + bx + c &= a(x^2 + \frac{b}{a}x + \frac{c}{a}) = a(x^2 + 2\frac{b}{2a}x + \frac{c}{a}) = a(x^2 + 2\frac{b}{2a}x + (\frac{b}{2a})^2 - (\frac{b}{2a})^2 + \frac{c}{a}) \\ &= a((x + \frac{b}{2a})^2 - \frac{b^2 - 4ac}{4a^2}). \end{aligned} \tag{2.4}$$

Selon le signe de $b^2 - 4ac$ on a une différence de deux carrés ou une somme de deux carrés. Ce nombre détermine donc l'existence des solutions. On l'appelle le *réalisant* ou *discriminant* de l'équation, et on le note ρ ou Δ (je choisirai Δ).

La forme (2.4) du trinôme ax^2+bx+c obtenue ci-dessus permet alors, via la factorisation et la "règle du produit nul" d'obtenir tous les résultats ci-dessous. Elle sera également utile pour étudier les fonctions du second degré.

Proposition 2.2.1. *La structure des solutions de l'équation* (2.1) *dépend du signe de* Δ *:*

1. *si* $\Delta > 0$*, l'équation admet deux solutions distinctes : on a*
$$S = \{\frac{-b-\sqrt{\Delta}}{2a}, \frac{-b+\sqrt{\Delta}}{2a}\}.$$
2. *si* $\Delta = 0$*, l'équation admet une solution unique :* $S = \{\frac{-b}{2a}\}$*. La solution* $\frac{-b}{2a}$ *est dite double.*
3. *si* $\Delta < 0$*, l'équation est incompatible :* $S = \varnothing$*.*

Démonstration. Si Δ est positif ou nul, alors c'est un carré, le carré de $\sqrt{\Delta}$, donc on a

$$ax^2+bx+c = a[(x+\frac{b}{2a})^2-\frac{(\sqrt{\Delta})^2}{4a^2}] = a[(x+\frac{b}{2a})^2-(\frac{\sqrt{\Delta}}{2a})^2] = a(x+\frac{b}{2a}+\frac{\sqrt{\Delta}}{2a})(x+\frac{b}{2a}-\frac{\sqrt{\Delta}}{2a}),$$

et on conclut via la règle du produit nul.

On constate que les deux solutions sont distinctes si $\Delta > 0$ et qu'elles se confondent (d'où l'appellation solution double) si $\Delta = 0$.

Si Δ est strictement négatif, alors on a quand-même

$$ax^2 + bx + c = a((x + \frac{b}{2a})^2 - \frac{\Delta}{4a^2}).$$

Le premier terme $(x+\frac{b}{2a})^2$ est positif ou nul, tandis que le deuxième, $-\frac{\Delta}{4a^2}$, est strictement positif, quel que soit x. Donc la somme est strictement positive, pour tout x, et n'est donc jamais nulle. □

Tant que nous y sommes, rappelons un théorème sur la somme et le produit des solutions. Nous avons déjà fait une partie de la preuve, pour trouver les solutions des équations du second degré.

Proposition 2.2.2. *Si* $\Delta \geqslant 0$*, alors l'équation du second degré* $ax^2+bx+c = 0$ *admet les solutions* x_1 *et* x_2 *(éventuellement égales). De plus, le trinôme correspondant se factorise :*

$$ax^2 + bx + c = a(x - x_1)(x - x_2) \quad \forall x \in \mathbb{R}.$$

Enfin, on a $x_1 + x_2 = \frac{-b}{a}$ *et* $x_1x_2 = \frac{c}{a}$*.*

Cette proposition permet par exemple de vérifier les solutions que l'on a trouvé à peu de frais : on peut calculer leur produit et comparer à $\frac{c}{a}$. Ce n'est pas une vérification exacte, mais elle permet de détecter des erreurs : si vous avez fait une faute de calcul, il y a peu de chances que le produit de vos solutions donne quand-même la bonne valeur. Ce résultat permet aussi de trouver la deuxième solution si on connaît la première, en ramenant l'équation du second degré à une équation du premier degré. Par exemple, sachant que l'équation $x^2 - 5x + 6 = 0$ admet $x_1 = 2$ comme solution, la deuxième solution x_2 satisfait $2x_2 = 6$, donc c'est 3.

Démonstration. La factorisation est acquise dans la preuve de la proposition 2.2.1. Pour la somme et le produit des solutions, on peut procéder à partir de leur expression : $\frac{-b\pm\sqrt{\Delta}}{2a}$. Dans la somme, les racines se simplifient, et on a donc $\frac{-2b}{2a}$. Pour le produit, on a

$$x_1x_2 = \frac{1}{4a^2}(-b-\sqrt{\Delta})(-b+\sqrt{\Delta}) = \frac{1}{4a^2}(b^2-\Delta) = \frac{c}{a},$$

et la preuve est terminée. □

Ce n'est cependant pas la preuve la plus instructive, alors j'en donne une deuxième.

Démonstration. Puisque le trinôme se factorise, on a

$$ax^2 + bx + c = a(x - x_1)(x - x_2) = ax^2 - a(x_1 + x_2)x + ax_1x_2,$$

quel que soit x. En identifiant les coefficients de chaque degré, on obtient directement $b = -a(x_1 + x_2)$ et $c = ax_1x_2$. □

Cette preuve est efficace, mais elle soulève une question : comment sait-on que l'on peut identifier les coefficients, quand deux fonctions polynomiales sont égales ? Autrement dit, peut-on affirmer que $ax^2 + bx + c = a'x^2 + b'x + c'$ (pour tout $x \in \mathbb{R}$) implique $a = a'$, $b = b'$ et $c = c'$? En soustrayant le membre de droite, on voit que cette question est équivalente à la suivante : l'assertion "$(a-a')x^2 + (b-b')x + (c-c') = 0$, pour tout $x \in \mathbb{R}$" implique-t-elle $a - a' = b - b' = c - c' = 0$? On peut encore écrire cette implication sous la forme

$$a''x^2 + b''x + c'' = 0 \quad \forall x \in \mathbb{R} \Rightarrow a'' = b'' = c'' = 0.$$

C'est un problème d'indépendance linéaire, comme vous le verrez dans la suite du cours d'algèbre. Dans notre cas, il y a plusieurs façon de se convaincre que l'implication est vraie. Par exemple, en exprimant que l'équation est satisfaite pour trois valeurs de x (0, 1 et -1), on obtient un système d'équations en a'', b'' et c'' qui n'admet que la solution nulle. On peut aussi se souvenir qu'une vraie équation du second degré admet au plus 2 solutions. Donc celle-ci doit être une "fausse" équation du second degré : on doit avoir $a'' = 0$, mais alors on a $b''x + c'' = 0$ pour tout $x \in \mathbb{R}$, et on trouve de même $b'' = 0$, puis $c'' = 0$. On peut aussi utiliser les dérivées : si une fonction est nulle sur $\mathbb{R}$, elle est nulle en 0, et sa dérivée aussi sur $\mathbb{R}$, donc en 0,... Ces arguments se généralisent à des fonctions polynomiales de degré supérieur à 2.

Cette proposition admet une réciproque, que je cite pour être complet.

Proposition 2.2.3. *Si n_1 et n_2 sont deux nombres dont la somme est s et le produit p, alors ces nombres sont solutions de l'équation*

$$x^2 - sx + p = 0.$$

Démonstration. Il suffit d'exprimer les conditions sur n_1 et n_2 ($n_1 + n_2 = s$ et $n_1n_2 = p$) et de résoudre ce système d'équations. □

Pour terminer cette section, voici quelques utilisations possibles de la complétion des carrés :

1. Dans un repère orthonormé, l'équation du cercle de centre $C : (c_1, c_2)$ et de rayon r (pour la distance euclidienne) est donnée par

   $$(x - c_1)^2 + (y - c_2)^2 = r^2,$$

   ou un multiple non nul. On peut ramener un certain nombre d'équations du second degré à cette forme et ainsi trouver le centre et le rayon du cercle d'équation

   $$4x^2 + 4y^2 + 6x - 12y - 25 = 0.$$

   De manière générale, on peut appliquer cette méthode à l'équation

   $$ax^2 + ay^2 + bx + cy + d = 0 \quad (a \neq 0).$$

2. Si ne demande pas d'avoir un cercle, on peut appliquer la même méthode à

   $$4x^2 + 2y^2 + 6x - 12y - 25 = 0.$$

   On obtient l'équation canonique d'une ellipse dont les axes sont parallèles à ceux du repère.

3. On peut même avoir des doubles produits en xy, c'est la même méthode (y est un nombre, après tout) :

$$4x^2 + 4xy + 2y^2 + 6x - 12y - 25 = 0.$$

4. La complétion des carrés permet également de factoriser dans $\mathbb{R}$ la fonction polynomiale $P(x) = x^4 + 4$, bien que celle-ci n'admette pas de zéros dans $\mathbb{R}$. On doit ici compléter le carré en ajoutant et en soustrayant le double produit adéquat.
5. Enfin, on peut aussi démontrer que l'expression $Q(x_1, x_2) = 7x_1^2 + 2x_2^2 + 4x_1x_2$ est positive ou nulle, quels que soient $x_1, x_2 \in \mathbb{R}$, en écrivant cette expression comme une somme de deux carrés.

2.3 Nombres complexes, introduction et définition

Nous venons de revoir les équations du second degré dans $\mathbb{R}$. Nous savons donc que l'équation

$$x^2 + 4x + 8 = 0 \tag{2.5}$$

n'admet pas de solution. Cela peut se voir de deux façons : d'une part en calculant le réalisant du trinôme du second degré en question : $\Delta = 16 - 32 = -16 < 0$, d'autre part en notant que l'équation s'écrit encore

$$(x + 2)^2 + 4 = 0 \quad \text{ou encore} \quad (x + 2)^2 - (-4) = 0.$$

Si nous voulons résoudre cette équation comme pour les équations réelles, cela revient, d'après la dernière formule à trouver un (ou plusieurs) nombre(s) z tel que $z^2 = -4$. On sait que ce n'est pas possible dans les nombres réels, puisque le carré de tout nombre réel est positif ou nul. La solution consiste à *étendre* l'ensemble des réels en ajoutant un nombre supplémentaire le nombre i tel que

$$i^2 = -1.$$

Cela vous paraît abstrait ? Absurde ? Pourtant, cela ne vous a pas tracassé que l'on ajoute un nombre aux rationnels, que l'on a appelé $\sqrt{2}$ pour résoudre l'équation $(x+2)^2 - 2 = 0$. On aurait pu appeler ce nombre j, et demander que $j^2 = 2$ [a]. Cela vous semble naturel, mais cela ne l'était pas pour Pythagore, par exemple. On pourrait alors obtenir

$$(2i)^2 = (2i)(2i) = -4,$$

moyennant le fait qu'on puisse définir le nombre $2i$ et faire le produit de deux tels nombres, avec les règles habituelles. On aurait alors également

$$(-2i)^2 = -4$$

et donc deux solutions à l'équation (2.5), à savoir :

$$x = -2 + 2i \quad \text{et} \quad x = -2 - 2i.$$

Pour que ces nombres soient solutions de l'équation (2.5), encore faut-il que l'on puisse calculer $(-2 + 2i)^2$, comme d'habitude (avec un produit bien défini, commutatif et associatif,...). Cela permettra de calculer $(-2+2i)^2 + 4(-2+2i) + 8$ et de montrer que c'est 0. Nous avons déjà remarqué toutes les propriétés nécessaires à la résolution des équations

a. La construction que je vais détailler ci-dessous s'adapte pour définir le champ $\mathbb{Q}(\sqrt{2})$, qui est l'ensemble des nombres de la forme $a + b\sqrt{2}$, où a et b sont rationnels.

du premier et du second degré dans $\mathbb{R}$. Il serait de bon ton que ces propriétés soient également satisfaites pour les nombres de la forme $a+ib$. Si ces propriétés étaient satisfaites, on aurait alors

$$(a+ib)+(a'+ib') = (a+a')+i(b+b'),\ (a+ib)(a'+ib') = aa'+bb'i^2+(ab'+a'b)i = (aa'-bb')+(ab'+a'b)i, \tag{2.6}$$

par associativité de $+$, distributivité et commutativité de l'addition et de la multiplication.

On pourrait alors donner comme définition des nombres complexes

$$\mathbb{C} = \{a+ib : a,b \in \mathbb{R}\},$$

où les opérations sont définies par (2.6), et où $i^2 = -1$. Mais si on procède de la sorte, comme sait-on qu'un tel nombre i existe, quel statut donner au $+$ entre a et ib, comment ib est-il d'ailleurs défini ? L'écriture $a+ib$ est-elle unique ? Il y a plusieurs façon de présenter une définition qui répond à toutes ces questions. J'en choisis une qui me paraît intuitive à ce stade : dans $a+ib$, je ne sais ni ce qu'est ce $+$, ni ce qu'est ce i, tout ce que je sais, c'est qu'il y a a et b, donc j'écris plutôt (a,b), en pensant très fort que je veux que ce soit $a+ib$. Je vais ensuite définir la somme et le produit pour obtenir ce qui est écrit à l'équation (2.6), mais en utilisant les couples au lieu d'expressions $a+ib$ pas encore définies. J'arrive donc à la définition.

Définition 2.3.1. On définit l'ensemble des nombres complexes par

$$\mathbb{C} = \{(a,b) : a,b \in \mathbb{R}\}.$$

En tant qu'ensemble, on a donc $\mathbb{C} = \mathbb{R}^2$. On passe maintenant aux opérations en gardant en tête l'équation (2.6).

Définition 2.3.2. L'addition des nombres complexes est définie par

$$+ : \mathbb{C}\times\mathbb{C} \to \mathbb{C} : ((a,b),(a',b')) \mapsto (a+a', b+b'),$$

et la multiplication est donnée par

$$\cdot : \mathbb{C}\times\mathbb{C} \to \mathbb{C} : ((a,b),(a',b')) \mapsto (aa'-bb', ab'+a'b),$$

pour tous $a,a',b,b' \in \mathbb{R}$.

Les nombres complexes sont donc simplement des couples de nombres réels. l'addition est bien connue : c'est celle des composantes de vecteurs du plan. Seule la multiplication est nouvelle. Nous vérifions maintenant que l'addition et la multiplication munissent $\mathbb{C}$ d'une structure de champ. Nous découpons ces propriétés en celles relatives à l'addition, celles de la multiplication et la distributivité.

Proposition 2.3.1. *L'addition des nombres complexes a les propriétés suivantes :*

1. *elle est associative : on a* $(z+z')+z'' = z+(z'+z'') \quad \forall z,z',z'' \in \mathbb{C}$ *;*
2. *elle admet un neutre* $e=(0,0)$ *: on a* $z+e = e+z = z \quad \forall z \in \mathbb{C}$ *;*
3. *tout élément admet un opposé :* $\forall z \in \mathbb{C}, \exists z' \in \mathbb{C} : z+z' = z'+z = e$.
4. *elle est commutative : on a* $z+z' = z'+z, \quad \forall z,z' \in \mathbb{C}$.

Démonstration. C'est une simple vérification. On a par exemple

$$((x,y)+(x',y'))+(x'',y'') = (x+x', y+y')+(x'',y'') = ((x+x')+x'', (y+y')+y'')$$

et

$$(x,y)+((x',y')+(x'',y'')) = (x,y)+(x'+x'', y'+y'') = (x+(x'+x''), y+(y'+y'')).$$

On est donc ramené à l'associativité de la somme des nombres réels. De la même façon, on a

$$(x, y) + (0, 0) = (x + 0, y + 0) = (x, y) = (0, 0) + (x, y),$$

car 0 est neutre pour l'addition dans $\mathbb{R}$. On vérifie ensuite que l'opposé du nombre complexe (x, y) est $(-x, -y)$, et on montre la commutativité comme plus haut. Dans chaque cas, on est ramené à la propriété correspondante dans $\mathbb{R}$. □

Remarque 2.1. a) L'élément $e = (0, 0)$ est plus simplement noté 0, l'opposé d'un élément $z \in \mathbb{C}$ est noté $-z$.

b) Cette proposition signifie que la structure mathématique $(\mathbb{C}, +, 0)$ est un *groupe* (les propriétés (1), (2) et (3)) *commutatif* (la propriété (4)).

On a des propriétés analogues pour la multiplication, qui montrent qu'elle se comporte comme la multiplication des nombres réels.

Proposition 2.3.2. *La multiplication des nombres complexes a les propriétés suivantes :*

1. *elle est associative : on a*

$$(z.z').z'' = z.(z'.z'') \quad \forall z, z', z'' \in \mathbb{C};$$

2. *elle admet un neutre* $1 = (1, 0)$ *: on a*

$$1.z = z.1 = z \quad \forall z \in \mathbb{C};$$

3. *tout élément non nul admet un inverse :*

$$\forall z \in \mathbb{C}^* = \mathbb{C} \setminus \{0\}, \exists z' \in \mathbb{C} : z.z' = z'.z = 1.$$

4. *elle est commutative : on a*

$$z.z' = z'.z, \quad \forall z, z' \in \mathbb{C}.$$

Démonstration. Les points 1.,2.,et 4. se démontrent comme plus haut et sont laissés à titre d'exercice. Seule l'existence d'un inverse demande une justification. Soit $z = (x, y) \neq (0, 0)$. Un inverse de z est alors $z' = (x', y')$ satisfaisant

$$\begin{cases} xx' - yy' &= 1 \\ yx' + xy' &= 0 \end{cases}$$

On résout le système, par exemple par la méthode du pivot (il faut discuter si $x = 0$ ou $y = 0$), et on trouve que l'inverse de $z = (x, y)$ est $z' = (\frac{x}{x^2+y^2}, -\frac{y}{x^2+y^2})$. □

Remarque 2.2. a) L'inverse d'un élément non nul z est généralement noté z^{-1} ou $\frac{1}{z}$. Cela permet de définir la division des nombres complexes : si $z' \neq 0$, $\frac{z}{z'}$ est ne nombre par lequel il faut multiplier z' pour obtenir z. C'est donc zz'^{-1}. Cela permet aussi de vérifier qu'on peut "multiplier en haut et en bas : $\frac{z}{z'} = \frac{wz}{wz'}$, pour tout $w \neq 0$.

Une dernière propriété lie l'addition et la multiplication des nombres complexes. La démonstration est ici encore une simple vérification et est laissée comme exercice.

Proposition 2.3.3. *La multiplication des nombres complexes distribue l'addition : on a*

$$z.(z' + z'') = z.z' + z.z'' = (z' + z'').z,$$

pour tous $z, z', z'' \in \mathbb{C}$.

Remarque 2.3. Les neuf propriétés que nous venons de lister dans les trois propositions ci-dessus sont résumées en une phrase, "La structure $(\mathbb{C}, +, 0, \cdot, 1)$ est un *champ*". Elles signifient qu'on peut additionner et multiplier les nombres complexes **comme on a l'habitude de le faire avec les nombres réels.**

En particulier les "produits remarquables" que nous avons vus jusqu'à présent, ou encore la théorie des systèmes linéaires, sont exactement identiques, que l'on travaille avec des nombres réels ou des nombres complexes.

2.4 Plongement de $\mathbb{R}$, nombre i, représentation, forme algébrique et nombres associés

Lors des extensions précédentes, nous avons écrit des inclusions $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$. En fait, ces inclusions ne sont obtenues qu'à partir d'identifications : les éléments de $\mathbb{Z}$ s'écrivent $+n$ ou $-n$, pour $n \in \mathbb{N}$. On identifie alors n à $+n$. De même, les rationnels sont définis comme des fractions (à équivalence près) $\frac{a}{b}$. Les nombres entiers sont des fractions : $3 = \frac{3}{1}$. On identifie alors ces deux nombres et on plonge $\mathbb{Z}$ dans $\mathbb{Q}$. Pour obtenir l'inclusion $\mathbb{R} \subset \mathbb{C}$, il faut faire de même. On connaît l'identification parce que c'est celle utilisée en géométrie analytique : quand on a deux axes dans le plan, on porte des nombres sur les axes, et pas des couples de nombres (par exemple, on note 1 pour l'unité sur l'axe des abscisses au lieu de $(1, 0)$). Pourtant ces points sont sur les axes, mais aussi dans le plan.

Définition 2.4.1. Le plongement de $\mathbb{R}$ dans $\mathbb{C}$ est défini par

$$j : \mathbb{R} \to \mathbb{C} : x \mapsto (x, 0).$$

Dans la suite, on ne notera plus cette identification, et on écrira x pour $(x, 0)$, exactement comme dans $\mathbb{Q}$, on écrit 3 au lieu de $\frac{3}{1}$. On peut alors écrire $\mathbb{R} \subset \mathbb{C}$. Il est cependant important de vérifier que cette identification a les propriétés adéquates : des nombres réels différents ne peuvent pas coïncider une fois qu'on les considère dans $\mathbb{C}$, et la multiplication et l'addition de deux nombres réels ne doit pas dépendre du fait que l'on considère ces nombres comme appartenant à $\mathbb{R}$ ou à $\mathbb{C}$. C'est l'objet du résultat suivante.

Proposition 2.4.1. *L'application j est injective. Elle définit donc une bijection de $\mathbb{R}$ sur son image. De plus,*

1. *$j(x + x') = j(x) + j(x')$ pour tous $x, x' \in \mathbb{R}$;*
2. *$j(x.x') = j(x).j(x')$ pour tous $x, x' \in \mathbb{R}$;*

Démonstration. Montrons que j est injectif. On a $j(x) = j(x') \Leftrightarrow (x, 0) = (x', 0)$, et cette condition implique visiblement $x = x'$. De même,

$$j(x+x') = (x+x', 0) = (x, 0)+(x', 0) = j(x)+j(x'), \quad \text{et} \quad j(xx') = (xx', 0) = (x, 0).(x', 0) = j(x).j(x'),$$

pour tous $x, x' \in \mathbb{R}$. □

En utilisant cette identification, nous pouvons écrire des expressions du type $a.z$, où $a \in \mathbb{R}$ et $z \in \mathbb{C}$. Si $z = (x, y)$, on a

$$a.z = (a, 0).(x, y) = (ax - 0y, ay + 0x) = (ax, ay).$$

La première égalité est obtenue en identifiant a à $j(a)$, la seconde en appliquant la définition du produit. La multiplication d'un nombre complexe par un nombre réel correspond donc à la multiplication usuelle des éléments de $\mathbb{R}^2$ par les nombres réels.

Remarque 2.4. Dans la suite nous ne noterons plus le point pour la multiplication.

Il est maintenant grand temps de revenir aux préoccupations que nous avions dans l'introduction de cette section. Nous nous rappelons que nous voulions définir $a + ib$, mais que nous avons dû nous rabattre sur le couple (a, b). Naturellement, le couple $(0, 1)$ devrait correspondre au nombre $0 + i1 = i$. Cela amène la définition suivante.

Définition 2.4.2. Nous notons i le nombre complexe $(0, 1)$. On l'appelle unité imaginaire. [a]

Cette simple définition nous permet d'arriver au but recherché.

a. Cette notation remonte à Leonhard Euler (1707-1783).

Proposition 2.4.2. *Tout nombre complexe z s'écrit de manière unique $x+iy$ ($x, y \in \mathbb{R}$). On a $i^2 = -1$.*

Démonstration. Par définition, tout nombre complexe z s'écrit de manière unique $z = (x, y)$. De plus,

$$(x, y) = (x, 0) + (0, y) = x(1, 0) + y(0, 1) = x1 + yi = x + iy.$$

On a utilisé la multiplication dans $\mathbb{C}$ et l'identification de $\mathbb{R}$ à un sous-ensemble de $\mathbb{C}$. L'unicité est évidente : si $x + iy = x' + iy'$, alors $(x, y) = (x', y')$, donc $x = x'$ et $y = y'$. De plus, $i^2 = (0, 1)(0, 1) = (-1, 0) = -1$. □

Définition 2.4.3. Si x, y sont réels, l'écriture $x + iy$ est l'écriture sous *forme algébrique* du nombre complexe (x, y).

Nous pouvons donc maintenant utiliser cette écriture unique pour calculer avec les nombres complexes. Il suffit de retenir que l'addition et la multiplication munissent $\mathbb{C}$ d'une structure de champ, et que $i^2 = -1$. La proposition suivante insiste bien sur ce mode de calcul, que nous avions espéré dans la relation (2.6).

Proposition 2.4.3. *On a*

$$(x + iy) + (x' + iy') = x + x' + i(y + y') \quad \text{et} \quad (x + iy)(x' + iy') = xx' - yy' + i(xy' + x'y)$$

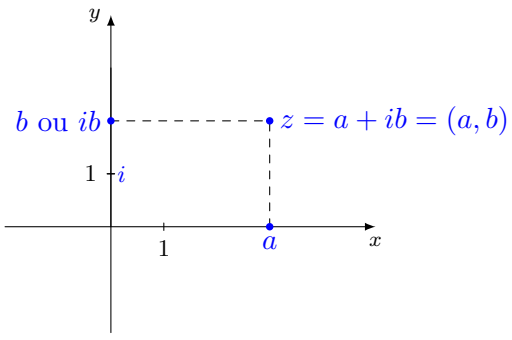
quels que soient x, x', y, y' dans $\mathbb{R}$

Démonstration. L'addition est commutative et associative, de plus la multiplication distribue l'addition, et $i^2 = -1$. □

Cette proposition est très importante, car elle vous permet d'additionner et multiplier les nombres complexes, comme si vous le faisiez avec les nombres réels, à l'exception du fait que le nombre i a un statut spécial, et qu'il faut tenir compte de la seule relation $i^2 = -1$.

Exemple 2.4.1. Calculer $5.(3 + 2i)$, $(2 + i)^2$, $(1 + 3i)^2$, $(-2 + 2i)^2 + 4(-2 + 2i) + 8$. [b]

Enfin, puisque les nombres complexes sont des couples de nombres réels, on peut les *représenter* dans le plan, alors appelé plan complexe (on parle aussi de plan d'Argand, ou de diagramme d'Argand), comme on a l'habitude de le faire en géométrie analytique :



Remarquons que le nombre b sur l'axe des *ordonnées* indique que l'on reporte le nombre réel b sur cet axe gradué, mais le point en question représente le nombre complexe $ib = (0, b)$. Cela ne créera pas de confusion pour la suite de noter b ou ib sur le deuxième axe. Les nombres correspondants sont les multiples réels de i. Ils sont appelés imaginaires purs.

Nous définissons ici des nombres naturellement associés à tout nombre complexe.

b. Solutions : $15 + 10i$, $3 + 4i$, $-8 + 6i$, 0.

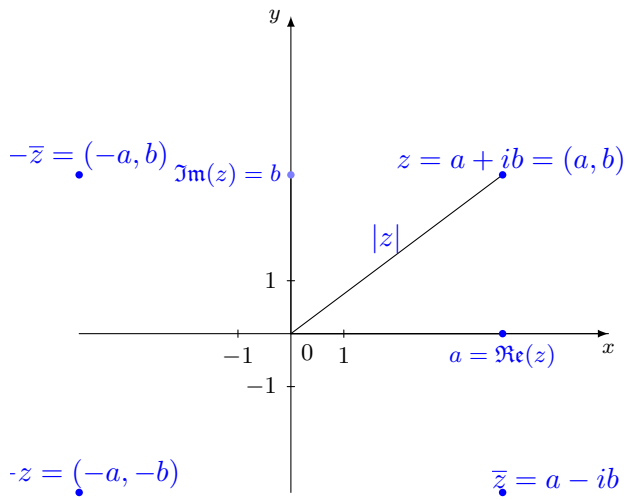
Définition 2.4.4. Pour tout nombre complexe $z = a + ib$ $(a, b \in \mathbb{R})$, on définit

1. la partie réelle de z par $\mathfrak{Re}(z) = a$;
2. la partie imaginaire de z par $\mathfrak{Im}(z) = b$;
3. le nombre conjugué de z par $\overline{z} = a - ib$;
4. le module de z par $|z| = \sqrt{a^2 + b^2} = \sqrt{z \cdot \overline{z}}$;

Remarque 2.5. Attention, la partie imaginaire de z est bien b, et pas ib. Ici on a fait un choix.

Le module n'est pas défini comme la valeur absolue des nombres réels. En effet, il n'y a pas d'ordre naturel sur $\mathbb{C}$ et la tentative de définition $\max\{-z, z\}$ n'aurait simplement pas de sens. Cependant, nous savons que la valeur absolue du nombre réel x mesure la distance de x à 0. C'est cette propriété qui est généralisée. Cela permet de montrer que le module du nombre réel x tel que défini ici correspond à sa valeur absolue. Cela découle aussi de la définition : Si x est réel, on a $|(x, 0)| = \sqrt{x^2} = |x|$.

On a donc pour tout nombre complexe z, $z = \mathfrak{Re}(z) + i\mathfrak{Im}(z)$. Un nombre est dit *réel* si sa partie imaginaire est nulle. Si sa partie réelle est nulle, il est dit *imaginaire pur*. Tous ces nombres se représentent facilement dans le plan complexe :



Exemple 2.4.2. Calculer la partie réelle, la partie imaginaire, le module et le conjugué de

1. $z_0 = i$,
2. $z_1 = -2$,
3. $z_2 = 1 + \sqrt{3}i$,
4. $z_3 = 1 + i$,
5. $z_4 = 3 + 2i$.

On applique simplement les définitions. On peut bien sûr aussi représenter ces nombres pour "voir" le solutions, que voici :

- $\mathfrak{Re}(z_0) = 0$
- $\mathfrak{Im}(z_0) = 1$
- $|z_0| = 1$
- $\overline{z_0} = -i$

- $\mathfrak{Re}(z_1) = -2$
- $\mathfrak{Im}(z_1) = 0$
- $|z_1| = 2$
- $\overline{z_1} = -2$

- $\mathfrak{Re}(z_2) = 1$
- $\mathfrak{Im}(z_2) = \sqrt{3}$
- $|z_2| = 2$
- $\overline{z_2} = 1 - \sqrt{3}i$

- $\mathfrak{Re}(z_3) = 1$
- $\mathfrak{Im}(z_3) = 1$
- $|z_3| = \sqrt{2}$
- $\overline{z_3} = 1 - i$

- $\mathfrak{Re}(z_4) = 3$
- $\mathfrak{Im}(z_4) = 2$
- $|z_4| = \sqrt{13}$
- $\overline{z_4} = 3 - 2i$

Il est important de pouvoir travailler avec ces nombres associés, c'est-à-dire de connaître les propriétés de cette association. C'est l'objet des propriétés suivantes.

Proposition 2.4.4 (Egalité)**.** *Si z_1, z_2 sont des nombres complexes, on a*

$$z_1 = z_2 \Leftrightarrow \begin{cases} \mathfrak{Re}(z_1) = \mathfrak{Re}(z_2) \\ \mathfrak{Im}(z_1) = \mathfrak{Im}(z_2) \end{cases}$$

Démonstration. Cela provient directement de l'unicité de la décomposition $z = \mathfrak{Re}(z) + i\mathfrak{Im}(z)$, valable pour tout nombre complexe. □

Proposition 2.4.5 (Conjugué)**.** *Pour tous nombres complexes z_1 et z_2, on a*

1. $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$, $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$ *et* $\overline{\overline{z_1}} = z_1$;
2. *Si* $z_2 \neq 0$, *alors* $\overline{(\frac{z_1}{z_2})} = \frac{\overline{z_1}}{\overline{z_2}}$;
3. *Si* $z_1 \neq 0$, *on a* $\frac{1}{z_1} = \frac{\overline{z_1}}{|z_1|^2}$.

Remarque 2.6. Les premières formules sont faciles à retenir : "conjugué d'une somme, d'un produit ou d'un quotient égale somme, produit, quotient des conjugués." Il reste à savoir que conjuguer deux fois revient à ne rien faire, puis la formule la plus importante : le produit d'un nombre par son conjugué vaut son module au carré.

Démonstration. Pour la première assertion, c'est un simple calcul : on écrit $z_1 = a_1 + ib_1$ et $z_2 = a_2 + ib_2$, pour a_1, a_2, b_1, b_2 dans $\mathbb{R}$ et on calcule.

Pour la deuxième assertion, on peut calculer de la même manière. Mais on peut aussi remarquer que $\overline{(\frac{z_1}{z_2})} = \frac{\overline{z_1}}{\overline{z_2}}$ est équivalente à $\overline{z_2}\overline{(\frac{z_1}{z_2})} = \overline{z_1}$. Cette dernière égalité est vraie puisque le produit des conjugués vaut le conjugué du produit (par 1.). La troisième assertion est équivalente à $z_1\overline{z_1} = |z_1|^2$. Avec les notations que nous avons choisies, $z_1\overline{z_1} = (a_1 + ib_1)(a_1 - ib_1) = a_1^2 + b_1^2 = |z_1|^2$. □

Le nombre complexe conjugué permet de mettre sous forme algébrique le quotient de deux nombres complexes dont le dénominateur n'est pas nul, en utilisant le dernier point de la proposition précédente, ce qui revient à multiplier haut et bas par le conjugué du dénominateur : $\frac{z_1}{z_2} = \frac{z_1\overline{z_2}}{z_2\overline{z_2}} = \frac{z_1\overline{z_2}}{|z_2|^2}$.

Exemple 2.4.3. Mettre sous forme algébrique les quotients

1. $\frac{3+i}{4-i}$, 2. $\frac{i+5}{i-5}$, 3. $\frac{1}{i}$, 4. $\frac{5+3i}{4i+3}$.

On applique la formule, ou on multiple haut et bas par le conjugué (ou un multiple réel du conjugué) et on obtient

$$\frac{3+i}{4-i} = \frac{(3+i)(4+i)}{(4-i)(4+i)} = \frac{11+7i}{17}, \quad \frac{i+5}{i-5} = \frac{(i+5)(i+5)}{(i-5)(i+5)} = -\frac{24+10i}{26}.$$

De même, on trouve $\frac{1}{i} = -i$ et $\frac{5+3i}{4i+3} = \frac{1}{25}(27 - 11i)$.

Proposition 2.4.6 (Parties réelles et imaginaires)**.** *Soit z un nombre. Alors,*

1. *On a* $\mathfrak{Re}(z) = \frac{z+\overline{z}}{2}$ *et* $\mathfrak{Im}(z) = \frac{z-\overline{z}}{2i}$;
2. *Le nombre z est réel ssi* $\mathfrak{Im}(z) = 0$ *ssi* $z = \overline{z}$;
3. *Le nombre z est imaginaire pur ssi* $\mathfrak{Re}(z) = 0$ *ssi* $z = -\overline{z}$.

Démonstration. On considère $z = a + ib$, où a, b sont réels, et on calcule $z + \overline{z} = 2a$, $z - \overline{z} = 2ib$. Pour la deuxième assertion, , par définition z est réel si $b = 0$, c'est-à-dire si $\mathfrak{Im}(z) = 0$. On peut encore écrire cette condition $\frac{z-\overline{z}}{2i} = 0$, ou $z = \overline{z}$. On prouve la troisième assertion de la même façon. □

Passons maintenant aux propriétés du module.

Proposition 2.4.7 (Module)**.** *Pour tous nombres complexes z_1, z_2*

1. $|z_1 z_2| = |z_1||z_2|$ *et si* $z_2 \neq 0$, $|\frac{z_1}{z_2}| = \frac{|z_1|}{|z_2|}$ *et* $|\overline{z_1}| = |z_1|$;
2. $|z_1|^2 = z_1\overline{z_1}$,
3. $|z_1 + z_2|^2 = |z_1|^2 + |z_2|^2 + 2\mathfrak{Re}(z_1\overline{z_2})$

On a donc de bonne propriétés pour le module d'un produit, d'un quotient, et du conjugué. La deuxième propriété est déjà connue, mais c'est également une propriété du module. Enfin, puisque le module d'un nombre complexe correspond à la norme d'un élément de $\mathbb{R}^2$. On ne peut pas s'attendre à ce que le module d'une somme soit la somme des modules. Mais on a un théorème qui ressemble assez bien au théorème d'Al Kashi, ou aux propriétés du produit scalaire et de la norme. Ce n'est pas étonnant.

Démonstration. Pour la première propriété, il suffit de calculer, en prenant $z_1 = a_1 + ib_1$ et $z_2 = a_2 + ib_2$. On peut démontrer l'égalité entre les carrés. On a

$$|z_1 z_2|^2 = (a_1a_2 - b_1b_2)^2 + (a_1b_2 + a_2b_1)^2 \quad \text{et} \quad |z_1|^2|z_2|^2 = (a_1^2 + b_1^2)(a_2^2 + b_2^2).$$

On développe les deux expression et on constate qu'elles sont égales.

On peut calculer aussi pour la propriétés sur les quotients, mais on peut aussi constater qu'elle est équivalente à $|z_2||\frac{z_1}{z_2}| = |z_1|$. Cette dernière propriété est vraie, puisque le produit des modules est égal au module du produit. Enfin, $|a_1 - ib_1| = \sqrt{a_1^2 + (-b_1)^2} = |a_1 + ib_1|$.

Nous avons déjà démontré la deuxième assertion.

Pour la troisième, on peut encore calculer les deux membres en utilisant les mêmes notations. Je vous laisse le faire. Mais on peut aussi calculer comme ceci :

$$|z_1 + z_2|^2 = (z_1 + z_2)(\overline{z_1 + z_2}) = (z_1 + z_2)(\overline{z_1} + \overline{z_2}) = z_1\overline{z_1} + z_2\overline{z_2} + (z_1\overline{z_2} + z_2\overline{z_1}).$$

Mais on a la relation $z_2\overline{z_1} = \overline{z_1\overline{z_2}}$, donc la dernière parenthèse vaut $z_1\overline{z_2} + \overline{z_1\overline{z_2}}$, ce qui donne le résultat annoncé vu la proposition 2.4.6. □

Remarque 2.7. Il est quand-même intéressant de calculer $\mathfrak{Re}(z_1\overline{z_2})$, avec les notations habituelles : on a alors

$$z_1\overline{z_2} = (a_1 + ib_1)(a_2 - ib_2) = a_1a_2 + b_1b_2 + i(a_2b_1 - a_1b_2)$$

Donc $\mathfrak{Re}(z_1\overline{z_2}) = a_1b_1 + a_2b_2$ n'est rien d'autre que le produit scalaire standard des éléments z_1 et z_2 de $\mathbb{R}^2$.

Enfin, nous terminons par quelques inégalités qui seront utiles par la suite. Il est également intéressant de réfléchir à l'interprétation géométrique de ces inégalités. Pour les premières, on a un triangle rectangle et pour la seconde, un triangle quelconque.

Proposition 2.4.8 (Inégalités)**.** *Soient des nombres complexes z, z_1, z_2.*

1. *On a $|\mathfrak{Re}(z)| \leqslant |z|$, $|\mathfrak{Im}(z)| \leqslant |z|$;*
2. *On a l'inégalité triangulaire $|z_1 + z_2| \leqslant |z_1| + |z_2|$.*
3. *De plus $|z_1 - z_2| \geqslant ||z_1| - |z_2||$*

Démonstration. On écrit comme d'habitude $z = a + ib$ où a, b sont réels. La première inégalité s'écrit alors $|a| \leqslant \sqrt{a^2 + b^2}$. Elle est équivalente, puisqu'il s'agit de nombres positifs, à $a^2 \leqslant a^2 + b^2$. L'inégalité concernant la partie imaginaire se démontre de la même façon.

Pour la deuxième assertion, il est équivalent de démontrer $|z_1 + z_2|^2 \leqslant (|z_1| + |z_2|)^2$. Mais le membre de gauche vaut $|z_1|^2 + |z_2|^2 + 2\mathfrak{Re}(z_1\overline{z_2})$ et celui de droite $|z_1|^2 + |z_2|^2 + 2|z_1||z_2|$. L'inégalité à démontrer se réduit donc à $\mathfrak{Re}(z_1\overline{z_2}) \leqslant |z_1||z_2| = |z_1||\overline{z_2}|$, ou encore à $\mathfrak{Re}(z_1\overline{z_2}) \leqslant |z_1\overline{z_2}|$. Cette dernière inégalité résulte du point 1.

Pour la troisième assertion, il y a un truc : $z_1 = (z_1 - z_2) + z_2$, donc $|z_1| \leqslant |z_1 - z_2| + |z_2|$, par le point 2. On a donc $|z_1 - z_2| \geqslant |z_1| - |z_2|$. Par symétrie, on obtient aussi $|z_1 - z_2| \geqslant |z_2| - |z_1|$. □

Remarque 2.8. La deuxième inégalité porte aussi le nom d'inégalité de Minkowski.

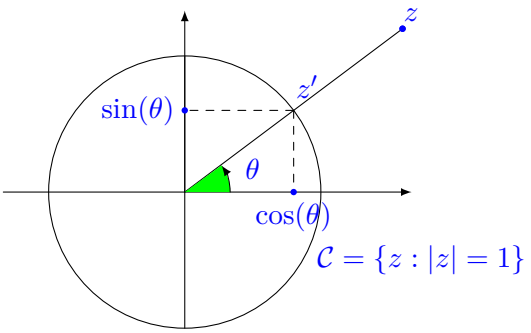
2.5 Forme trigonométrique, formule de Moivre

Jusqu'à présent, nous avons défini les nombres complexes comme des couples de nombres réels, et obtenu la représentation algébrique. Nous les avons représentés dans le plan muni d'un repère orthonormé, au moyen de *coordonnées cartésiennes*. Il existe cependant d'autre systèmes de coordonnées du plan. Les plus connues sont les coordonnées polaires. Elles correspondent à une autre écriture des nombres complexes, appelée forme trigonométrique.

Tout d'abord, rappelons que l'ensemble des nombres complexes de module égal à 1 est exactement le cercle trigonométrique. Tout nombre complexe z tel que $|z| = 1$ s'écrit donc de manière unique

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

pour $\theta \in [0, 2\pi[$. On peut de la même manière repérer tout nombre complexe z non nul, au moyen de l'angle entre le premier vecteur associé au repère et z, et du module de z. Voici l'idée :



La droite déterminée par 0 et z coupe le cercle en z', qui a pour coordonnées $(\cos(\theta), \sin(\theta))$. Donc $z' = \cos(\theta) + i\sin(\theta)$. Pour obtenir z, on doit multiplier z' par un nombre positif ρ. Si $z = \rho z'$, alors $|z| = \rho|z'| = \rho$. L'idée géométrique est claire, mais comment décrire cette transformation sous forme algébrique ? C'est l'objet de la proposition suivante.

Proposition 2.5.1. *Si $z = a + ib$ est un nombre complexe non nul, alors il existe un unique $\theta \in [0, 2\pi[$ et un unique $\rho \in]0, +\infty[$ tels que $z = \rho(\cos(\theta) + i\sin(\theta))$. De plus θ et ρ sont donnés par les équations suivantes :*

$$\begin{cases} \rho & = |z| = \sqrt{a^2 + b^2} \\ \cos(\theta) & = \frac{a}{\sqrt{a^2+b^2}} \\ \sin(\theta) & = \frac{b}{\sqrt{a^2+b^2}} \end{cases}$$

Remarque 2.9. Cette écriture du nombre complexe z est appelée forme trigonométrique de z.

Démonstration. Il suffit d'écrire les conditions demandées : on a $a+ib = \rho(\cos(\theta)+i\sin(\theta))$ si, et seulement si, les parties réelles et imaginaires de ces deux nombres sont égales. On peut aussi ajouter la condition d'égalité des modules de ces nombres, qui est une conséquence des deux autres. On a donc les conditions équivalentes

$$\begin{cases} a & = & \rho\cos(\theta) \\ b & = & \rho\sin(\theta) \\ \sqrt{a^2 + b^2} & = & \rho|cos(\theta) + i\sin(\theta)| = \rho. \end{cases}$$

On obtient directement l'existence d'un unique θ, puisque $(\frac{a}{\sqrt{a^2+b^2}}, \frac{b}{\sqrt{a^2+b^2}})$ a un module égal à 1. □

Définition 2.5.1. 1. L'angle θ de la proposition précédente est appelé *l' argument principal* de z. Par extension, on appellera aussi argument de z tout angle θ' tel que $z = \rho(\cos(\theta') + i\sin(\theta'))$, c'est-à-dire tel que $\theta' - \theta = 2k\pi$, $k \in \mathbb{Z}$. [a]

2. Un nombre complexe z écrit sous la forme $z = \rho(\cos\theta + i\sin\theta)$ est mis sous *forme trigonométrique.*

3. On note $e^{i\theta}$ le nombre $\cos(\theta)+i\sin(\theta)$. La forme trigonométrique est alors $z = \rho e^{i\theta}$. [b]

Exemple 2.5.1. Trouver les formes trigonométrique de

1. $z_0 = 1 + i$,
2. $z_1 = -1$,
3. $z_2 = 2 + 3i$,
4. $z_3 = -2 - 3i$,
5. $z_4 = 1 + \sqrt{3}i$.

Détaillons la solution pour $z_0 = 1 + i$ (on peut le représenter pour voir l'angle). On a $\rho = |z_0| = \sqrt{2}$. On cherche alors θ tel que

$$\begin{cases} \rho\cos(\theta) &= 1 \\ \rho\sin(\theta) &= 1, \end{cases}$$

ou encore

$$\begin{cases} \cos(\theta) &= \frac{\sqrt{2}}{2} \\ \sin(\theta) &= \frac{\sqrt{2}}{2} \end{cases}$$

Dès lors, on a $z_0 = \sqrt{2}e^{i\frac{\pi}{4}}$.

On procède de la même façon pour obtenir $z_1 = e^{i\pi}$, $z_2 = \sqrt{13}e^{i\arccos\left(\frac{2}{\sqrt{13}}\right)}$, $z_3 = \sqrt{13}e^{i(2\pi-\arccos\left(\frac{-2}{\sqrt{13}}\right))}$ et $z_4 = 2e^{i\frac{\pi}{3}}$.

Ces formes alternatives permettent de **calculer plus facilement les produits et inverses** des nombres complexes, comme le montre la proposition suivante.

Proposition 2.5.2. *Si $z_1 = \rho_1 e^{i\theta_1}$ et $z_2 = \rho_2 e^{i\theta_2}$ alors on a*

$$z_1 \cdot z_2 = \rho_1\rho_2 e^{i(\theta_1+\theta_2)}$$

Si $z_2 \neq 0$, alors on a

$$\frac{z_1}{z_2} = \frac{\rho_1}{\rho_2}e^{i(\theta_1-\theta_2)}.$$

Enfin, on a

$$z_1^n = \rho_1^n e^{in\theta_1} \quad et \quad \overline{z_1} = \rho_1 e^{-i\theta_1}.$$

Démonstration. On prouve la première formule en utilisant les définitions de $e^{i\theta_1}$ et $e^{i\theta_2}$, et les formules d'addition pour le sinus et le cosinus, en effet, on a

$$z_1 \cdot z_2 = \rho_1\rho_2 e^{i\theta_1}e^{i\theta_2}.$$

De plus

$$\begin{aligned} e^{i\theta_1}e^{i\theta_2} &= (\cos(\theta_1) + i\sin(\theta_1))(\cos(\theta_2) + i\sin(\theta_2)) \\ &= (\cos(\theta_1)\cos(\theta_2) - \sin(\theta_1)\sin(\theta_2)) + i(\cos(\theta_1)\sin(\theta_2) + \sin(\theta_1)\cos(\theta_2)) \\ &= \cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2) \\ &= e^{i(\theta_1+\theta_2)}. \end{aligned}$$

a. Le choix de considérer l'angle θ dans $[0, 2\pi[$ est arbitraire, on aurait pu le choisir dans $]-\pi, \pi]$ par exemple. La correspondance se fait en ajoutant des multiples de 2π si nécessaire.

b. Cette notation sera justifiée par les propriétés de ces nombres vis-à-vis de la multiplication, des puissances et du passage à l'inverse. Notez que dans certains exposés, on prend le problème dans l'autre sens : on définit l'exponentielle de tout nombre complexe, puis seulement le sinus et le cosinus.

Toutes les autres formules s'en déduisent : la deuxième assertion est équivalente à

$$z_1 = \frac{\rho_1}{\rho_2} e^{i(\theta_1-\theta_2)} \rho_2 e^{i\theta_2},$$

qui est vraie par le point 1. L'expression de z_1^n est obtenue par récurrence directe, et $\overline{z_1} = \rho_1(\cos(\theta_1) - i\sin(\theta_1))$. □

Le résultat est donc obtenu a partir des formules de trigonométrie. Il peut vous permettre de les retrouver, simplement en vous souvenant que $e^{i\theta}$ a les propriétés bien connues de l'exponentielle. [c] Comme cas particulier des formules précédentes, on obtient le résultat suivant.

Corollaire 2.5.1 (Formule de Moivre (Abraham de Moivre (1667-1754)))**.** *On a*

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

pour tout $\theta \in \mathbb{R}$ et tout n entier.

Cette formule permet, en développant le membre de gauche, d'exprimer $\cos(n\theta)$ et $\sin(n\theta)$ au moyen d'expressions polynomiales en $\sin(\theta)$ et $\cos(\theta)$. Par exemple, on a

$$\begin{aligned}\cos(3\theta) &= \mathfrak{Re}(\cos\theta + i\sin\theta)^3 = \mathfrak{Re}(\cos^3(\theta) + 3i\cos^2(\theta)\sin(\theta) - 3\cos(\theta)\sin^2(\theta) - i\sin^3(\theta)) \\ &= \cos^3(\theta) - 3\cos(\theta)\sin^2(\theta).\end{aligned}$$

De même, $\sin(3\theta) = 3\cos^2(\theta)\sin(\theta) - \sin^3(\theta)$.

Si on veut obtenir des formules qui permettent de transformer des produits, ou des puissances de sinus et cosinus, en sinus ou cosinus d'angles multiples, on peut utiliser la proposition suivante.

Proposition 2.5.3. *On a les formules*

$$\cos(x) = \mathfrak{Re}(e^{ix}) = \frac{e^{ix} + e^{-ix}}{2}, \quad \textit{et} \quad \sin(x) = \mathfrak{Im}(e^{ix}) = \frac{e^{ix} - e^{-ix}}{2i}$$

pour tout $x \in \mathbb{R}$.

A l'aide de ces formules, on peut :

1. Récupérer les formules de Carnot (développer $\cos^2(x) = (\frac{e^{ix}+e^{-ix}}{2})^2$)
2. Exprimer $\cos^3(x)$ en fonction de $\cos(3x)$ et $\cos(x)$ (développer $\cos^3(x) = (\frac{e^{ix}+e^{-ix}}{2})^3$).
3. Faire de même avec $\sin^3(x)$ (développer $\sin^3(x) = (\frac{e^{ix}-e^{-ix}}{2i})^3$).
4. Se souvenir des formules d'addition : $\cos(x+y) = \mathfrak{Re}(e^{i(x+y)})$, de même avec le sinus.

2.6 Un mot sur la forme exponentielle

Nous avons jusqu'à présent défini l'exponentielle d'un nombre complexe imaginaire pur : $e^{ib} = \cos(b) + i\sin(b)$. Nous connaissons aussi l'exponentielle des nombres réels (c'est l'exponentielle classique du nombre réel a, notée e^a). Si on veut définir l'exponentielle sur les nombres complexes, et qu'elle garde la propriété de transformer les sommes en produits, on est amené naturellement à la définition suivante.

Définition 2.6.1. Si $z = a + ib$, où $a, b \in \mathbb{R}$, on définit

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

c. Le comportement en question est $e^a e^b = e^{a+b}$, quels que soient a et b. Dans la plupart des textes mathématiques, les exponentielles complexes sont définies avant les sinus et cosinus, et les propriétés de ces derniers se déduisent de cette propriété fondamentale des exponentielles.

Cette définition permet d'obtenir un résultat similaire à celui sur les formes trigonométriques.

Proposition 2.6.1. *Tout nombre complexe non nul z s'écrit e^w pour un $w \in \mathbb{C}$. Ce nombre complexe w n'est pas unique.*

Démonstration. On sait que z admet une forme trigonométrique $z = \rho e^{i\theta} = \rho(\cos(\theta) + i\sin(\theta))$. Puisque ρ est strictement positif, on a $\rho = e^{\ln(\rho)}$, donc $z = e^{\ln(\rho)+i\theta}$. Cette forme n'est pas unique puisqu'on peut ajouter à θ tout multiple de 2π sans changer la valeur de l'exponentielle. □

La notation exponentielle est justifiée par les propriétés suivantes, que l'on démontrer sans difficulté.

Proposition 2.6.2. *Pour tous nombres complexes z, z_1, z_2, on a*

1. $e^{z_1}e^{z_2} = e^{z_1+z_2}$;
2. $\frac{1}{e^z} = e^{-z}$;
3. $(e^z)^n = e^{nz}, \forall z \in \mathbb{N}$.
4. *Pour tout $x \in \mathbb{R}$, on a $|e^{ix}| = 1$.*

2.7 Interprétation géométrique de l'addition et de la multiplication

Nous avons défini les opérations d'addition et de multiplication dans $\mathbb{C}$. Nous avons constaté que l'addition était celle des composantes de vecteurs. Elle a donc un interprétation géométrique simple. L'addition d'un élément fixe de $\mathbb{C}$ est une transformation du plan bien connue : c'est une translation. En passant à la forme trigonométrique, nous pouvons aussi interpréter la multiplication par un élément fixe de $\mathbb{C}$ comme une transformation de $\mathbb{C}$. Voici les définitions et résultats formels

Définition 2.7.1. Pour tout $z_0 \in \mathbb{C}$ définissons les applications

1. $s_{z_0} : \mathbb{C} \to \mathbb{C} : z \mapsto z + z_0$
2. $m_{z_0}\mathbb{C} \to \mathbb{C} : z \mapsto zz_0$

Ainsi définie, s_{z_0} est la "somme avec z_0", tandis que m_{z_0} est la "multiplication par z_0". Ces deux applications peuvent être inversées (si $z_0 \neq 0$ dans le second cas), comme l'indique la proposition suivante.

Proposition 2.7.1. *Pour tout $z_0 \in \mathbb{C}$, s_{z_0} est une bijection de $\mathbb{C}$ dans $\mathbb{C}$. C'est aussi le cas pour m_{z_0} si $z_0 \neq 0$.*

Démonstration. On constate que l'inverse de s_{z_0} est s_{-z_0} et que l'inverse de m_{z_0} est $m_{z_0^{-1}}$. □

Remarque 2.10. On n'a pas du tout utilisé les structures spécifiques de $\mathbb{C}$ dans cette preuve. On a juste utilisé la structure de groupe de $(\mathbb{C}, +, 0)$ et de $(\mathbb{C}_0, \cdot, 1)$. Ce résultat se généralise donc à n'importe quel groupe.

Puisque $\mathbb{C}$ a été identifié au plan, les applications s_{z_0} et m_{z_0} peuvent être vues comme de transformations du plan. Il reste à identifier ces transformations.

Proposition 2.7.2. *Si $z_0 = a_0 + ib_0 = \rho_0 e^{i\theta_0}$, alors la bijection s_{z_0} est une translation de vecteur z_0 (ou $\overrightarrow{Oz_0}$), et m_{z_0} est une similitude, c'est la composée d'une rotation centrée à l'origine du repère et d'angle θ_0 et d'une homothétie de rapport ρ_0), également centrée à l'origine.*

Démonstration. On calcule $s_{z_0}(z)$ en considérant $z = a+ib$. On a $s_{z_0}(z) = a+a_0+i(b+b_0)$. En termes géométriques, z_{z_0} transforme le point de coordonnées (a, b) en le point de coordonnées $(a + a_0, b + b_0)$. On a donc bien une translation.

On calcule $m_{z_0}(z)$ en considérant $z = \rho e^{i\theta}$. On a $m_{z_0}(z) = \rho_0 e^{i(\theta+\theta_0)}$. On a donc ajouté θ_0 à l'argument de z, ce qui correspond bien à une rotation, puis multiplié par $\rho_0 \in \mathbb{R}$, ce qui correspond à une homothétie. □

Cette interprétation permet de "voir" certains résultats algébriques. Par exemple, le nombre $e^{i\theta}$ correspond à une rotation d'angle θ. Alors son carré correspond à appliquer deux fois cette rotation, donc à une rotation d'angle 2θ, sa puissance n-ème à une rotation d'angle $n\theta$. On voit donc la formule de Moivre. De même, multiplier par -1 consiste à appliquer une rotation d'angle π. On n'est donc pas surpris d'avoir $-1 = e^{i\pi}$...

2.8 Racines carrées et équations du second degré

Il est maintenant grand temps de revenir à nos moutons. Nous avons quand même introduit les nombres complexes pour obtenir des racines carrées. [a]. Nous allons montrer dans cette section que toute équation du second degré à coefficients complexes admet des solutions dans l'ensemble des nombres complexes. Passons toute de suite à la définition des racines carrées.

Définition 2.8.1. Si z est un nombre complexe, alors on appelle une racine carrée de z tout nombre complexe z' tel que $z'^2 = z$.

Nous avons construit les nombres complexes pour donner des racines aux nombres négatifs. On a en fait obtenu bien plus, comme l'indique le résultat suivant.

Proposition 2.8.1. *Tout nombre complexe z non nul admet exactement deux racines carrées opposées. Le nombre complexe $z = 0$ admet une seule racine 0. Cette racine est dite double.*

Démonstration. Si $z \neq 0$, nous avons constaté que la forme trigonométrique était plus adaptée à la multiplication. On considère donc $z = \rho e^{i\theta}$ et on cherche $z' = \rho' e^{i\theta'}$ tel que $z'^2 = z$. Cette condition s'écrit encore $\rho'^2 e^{i2\theta'} = \rho e^{i\theta}$. On obtient donc les conditions équivalentes

$$\begin{cases} \rho'^2 & = & \rho \\ \cos(2\theta') & = & \cos(2\theta) \\ \sin(2\theta') & = & \sin(2\theta) \end{cases}$$

Cela donne directement $\rho' = \sqrt{\rho}$ et $2\theta' = \theta + 2k\pi$, $k \in \mathbb{Z}$. Si on remarque que $e^{i2\pi} = 1$, on peut se limiter à $k \in \{0, 1\}$ et on trouve les solutions $\sqrt{\rho}e^{i\frac{\theta}{2}}$ et $\sqrt{\rho}e^{i\frac{\theta}{2}+i\pi} = -\sqrt{\rho}e^{i\frac{\theta}{2}}$. Le cas de $z = 0$ est évident. □

Remarque 2.11.

1. Dans le plan complexe, il devient délicat de privilégier naturellement une des deux racines, pour définir une expression du type $\sqrt{z}$. On peut le faire en prenant les précautions, mais on ne peut plus garantir que cette racine ait les même propriétés que dans $\mathbb{R}$, comme par exemple $\sqrt{a}\sqrt{b} = \sqrt{ab}$ quand ces expressions sont définies. On n'utilisera donc pas le symbole $\sqrt{z}$, quand z est complexe. On ne l'utilisera que quand le radicand est réel et positif. C'est déjà le cas dans les lignes qui suivent.
2. Il est important d'insister sur le fait qu'il s'agit d'une preuve constructive. Les racines de $z = \rho e^{i\theta}$sont
$$\pm\sqrt{\rho}e^{i\frac{\theta}{2}}.$$

a. En fait, les nombres complexes n'ont pas été introduits à cet effet. Ils sont apparus comme un artifice de calcul pour résoudre certaines équations du troisième de degré.

3. Dans la preuve, il n'était pas nécessaire de passer aux équations trigonométriques : on a $e^{i\theta} = e^{i\theta'}$ si et seulement si $\theta - \theta' = 2k\pi$, pour un $k \in \mathbb{Z}$.

Exemple 2.8.1. Déterminer les racines carrés de $1 + i$ et de $3 + 4i$

Solution : on calcule la forme trigonométrique de $1 + i$, et on obtient $\sqrt{2}e^{i\frac{\pi}{4}}$. Les racines carrées sont donc $\pm\sqrt[4]{2}e^{i\frac{\pi}{8}}$. Si on le souhaite, on peut développer l'exponentielle pour revenir à une forme algébrique.

On fait de même pour $3+4i$. Il s'écrit $5e^{i\arccos(\frac{3}{5})}$. Donc les racines sont $\pm\sqrt{5}e^{i\arccos(\frac{3}{5})/2}$. Il reste alors à calculer la forme algébrique en développant $\cos(\frac{1}{2}\arccos(\frac{3}{5}))$ et $\sin(\frac{1}{2}\arccos(\frac{3}{5}))$. Les formules de Carnot donnent une solution : on a $1+\cos(2a) = 2\cos^2(a)$ et $1-\cos(2a) = 2\sin^2(a)$, donc $\cos^2(\frac{a}{2}) = \frac{1}{2}(1 + \cos(a))$ et $\sin^2(\frac{a}{2}) = \frac{1}{2}(1 - \cos(a))$. Donc finalement

$$\cos(\arccos(\frac{3}{5})/2) = \sqrt{\frac{1}{2}(1 + \frac{3}{5})} = \frac{2}{\sqrt{5}} \quad \text{et} \quad \sin(\arccos(\frac{3}{5})/2) = \frac{1}{\sqrt{5}}.$$

Donc les racines de $3 + 4i$ sont $\pm(2 + i)$.

L'exemple précédent montre qu'il serait utile de pouvoir calculer directement les racines carrées à partir de la forme algébrique.

Proposition 2.8.2. *Les racines carrées du nombre complexe $z = a + ib$ sont les nombres $x + iy$ où x, y sont solutions du système d'équations*

$$\begin{cases} x^2 - y^2 &= a \\ 2xy &= b \\ x^2 + y^2 &= \sqrt{a^2 + b^2}. \end{cases}$$

Démonstration. Un nombre complexe $z' = x + iy$ est une racine de z ssi on a $z'^2 = z$. On exprime que ces deux nombres sont égaux, c'est-à-dire qu'ils ont même partie réelle et même partie imaginaire. Puisque $z'^2 = (x^2 - y^2) + 2ixy$, ces conditions sont équivalentes à

$$\begin{cases} x^2 - y^2 &= a \\ 2xy &= b. \end{cases}$$

On peut ajouter une équation : les nombres z'^2 et z sont égaux ssi, ils ont des même partie réelle, même partie imaginaire et même module. La condition sur le module est une conséquence des deux autres, mais elle sera bien utile pour résoudre le système d'équations. Puisque $|z'^2| = |z'|^2$, on a l'équation supplémentaire $x^2 + y^2 = \sqrt{a^2 + b^2}$ et on obtient le résultat annoncé. □

Ce théorème est facile à retenir : on cherche $z' = x + iy$ tel que $z'^2 = z$. On exprime que ces nombres ont même partie réelle, même partie imaginaire et même module.

Exemple 2.8.2. Revenons à $z = 3 + 4i$. Les racines carrées sont les nombres $x + iy$ satisfaisant

$$\begin{cases} x^2 - y^2 &= 3 \\ 2xy &= 4 \\ x^2 + y^2 &= 5. \end{cases}$$

La première et la dernière équation nous permettent, en additionnant et en soustrayant membre à membre, d'obtenir le système équivalent

$$\begin{cases} x^2 &= 4 \\ y^2 &= 1 \\ 2xy &= 4. \end{cases}$$

Les solutions des deux premières équations sont $x = \pm 2$ et $y = \pm 1$. Cela fait quatre possibilités. Mais la dernière équation indique que x et y ont même signe. On trouve donc $x = 2$ et $y = 1$ ou $x = -2$ et $y = -1$. C'est quand-même plus facile.

Il est très simple de retenir les trois équations ci-dessus. On peut systématiser la résolution du système d'équations et obtenir une formule pour les racines. C'est l'objet du résultat suivant, que je donne à titre indicatif.

Proposition 2.8.3. *Les racines du nombre complexe $z = a + ib$ sont données par*

1. *Si $b \neq 0$, $\pm(\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}} + \operatorname{sgn}(b)\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}i)$, où $\operatorname{sgn}(b)$ est le signe de b.*
2. *Si $b = 0$ et $a \geqslant 0$, $\pm\sqrt{a}$;*
3. *Si $b = 0$ et $a \leqslant 0$, $\pm i\sqrt{-a}$.*

Démonstration. On reprend le système d'équations obtenu à la proposition précédente et on additionne et soustrait, membre à membre, la première et la troisième équation. On obtient alors le système équivalent

$$\begin{cases} 2x^2 &= \sqrt{a^2+b^2}+a \\ 2y^2 &= \sqrt{a^2+b^2}-a \\ 2xy &= b. \end{cases}$$

Les membres de droite des deux premières équations sont positifs car $|a| \leqslant \sqrt{a^2+b^2}$ pour tous a, b réels. Cela permet de déterminer x et y, au signe près (on a en général deux solutions pour x et deux pour y). Si $b \neq 0$, la dernière équation permet d'éliminer deux possibilités sur les quatre et d'obtenir le résultat annoncé. Si $b = 0$, les équations se simplifient et donnent directement le résultat annoncé. □

Voici encore un exemple.

Exemple 2.8.3. Si on cherche les racines complexes de $5 + 12i$, on les cherche sous la forme $x + iy$. On exprime l'équation $(x + iy)^2 = 5 + 12i$, que l'on développe pour obtenir

$$\begin{cases} x^2 - y^2 &= 5 \\ 2xy &= 12. \end{cases}$$

On n'oublie pas la troisième équation, qui est $x^2 + y^2 = |5 + 12i| = \sqrt{169} = 13$. On résout le système

$$\begin{cases} x^2 - y^2 &= 5 \\ 2xy &= 12 \\ x^2 + y^2 &= 13. \end{cases}$$

En additionnant et en soustrayant les première et troisième équation, on obtient $x^2 = 9$ et $y^2 = 4$. On a donc $x = \pm 3$ et $y = \pm 2$. Mais puisque le produit xy doit être positif, soit on choisit les deux solutions positives, soit les deux négatives. Les racines carrées sont donc $-3 - 2i$ et $3 + 2i$.

Maintenant que nous connaissons l'existence des racines carrées et que nous pouvons les calculer, nous pouvons également résoudre les équations du second degré à coefficients complexes.

Définition 2.8.2. Une équation du type

$$az^2 + bz + c = 0, \quad a \in \mathbb{C} \setminus \{0\}, b, c \in \mathbb{C} \tag{2.7}$$

est appelée équation du second degré à coefficients complexes.

La fonction $P : \mathbb{C} \to \mathbb{C} : z \mapsto az^2 + bz + c$ est appelée *fonction trinôme du second degré.*

A ce trinôme on associe le nombre complexe $\Delta = b^2 - 4ac$.

Proposition 2.8.4. *Toute équation du second degré à coefficients complexes admet deux solutions complexes distinctes (si $\Delta \neq 0$) ou une seule solution complexe, dite double (si $\Delta = 0$). Ces solutions sont données par*

$$\frac{-b \pm \delta}{2a} \quad \text{où} \quad \delta^2 = \Delta.$$

Remarque 2.12. On peut simplifier le résultat en indiquant qu'il y a deux solutions, comptées avec leurs multiplicités. Le concept de multiplicité sera approfondi dans la suite du cours d'algèbre. On notera aussi que la formule est identique à celle que l'on connaît dans les nombres réels. On ne note pas $\sqrt{\Delta}$, et cela explique la notation δ.

Démonstration. On procède comme dans le cas des équation à coefficients réels. On a encore

$$az^2 + bz + c = a((z + \frac{b}{2a})^2 - \frac{\Delta}{4a^2}).$$

Puisque Δ est toujours un carré, on peut écrire $\Delta = \delta^2$ et continuer la factorisation.

$$az^2 + bz + c = a((z + \frac{b}{2a})^2 - (\frac{\delta}{2a})^2) = a(z + \frac{b}{2a} + \frac{\delta}{2a})(z + \frac{b}{2a} - \frac{\delta}{2a}).$$

L'équation admet donc les solutions de l'énoncé. □

Les résultats sur la factorisation du trinôme, et la somme et le produit des solutions se généralisent.

Proposition 2.8.5. *L'équation du second degré $az^2 + bz + c = 0$ admet des solutions z_1 et z_2 (éventuellement égales). Le trinôme correspondant se factorise :*

$$az^2 + bz + c = a(z - z_1)(z - z_2) \quad \forall z \in \mathbb{C}.$$

De plus, on a $z_1 + z_2 = \frac{-b}{a}$ et $z_1 z_2 = \frac{c}{a}$.

Démonstration. Nous avons déjà obtenu la factorisation. La preuve pour la somme et le produit est identique à celle du cas réel. □

2.9 Généralisations : puissances n-èmes et racines n-èmes

Pour calculer la puissance n-ème d'un nombre complexe, on peut utiliser une des formes que l'on a à disposition : algébrique ou trigonométrique. La forme trigonométrique est évidemment la plus simple à utiliser. En effet, calculer une puissance n-ème d'une forme algébrique $a + ib$ donne lieu à l'expression $(a + ib)^n$. C'est quelque peu pénible, mais cela peut être mené à bien grâce à la formule du binôme de Newton, que je rappelle ici. Tout d'abord, voici la définition des coefficients binomiaux.

Définition 2.9.1. Pour tous $k, n \in \mathbb{N}$ tels que $0 \leqslant k \leqslant n$, on définit le coefficient binomial

$$C_n^k = \frac{n!}{k!(n-k)!}.$$

Remarque 2.13.
1. Par convention, on pose $0! = 1$, donc $C_n^0 = C_n^n = 1$.
2. Le nombre C_n^k est le nombre de façons de choisir k objets parmi n objets distincts, sans remise, et l'ordre n'ayant pas d'importance.

Ces nombres satisfont la règle de construction connue sous le nom de triangle de Pascal.

Proposition 2.9.1. *Pour tout $n \geqslant 1$ et tout k tel que $0 \leqslant k \leqslant n - 1$,*

$$C_n^k + C_n^{k+1} = C_{n+1}^{k+1}$$

Démonstration. Il suffit de calculer le membre de gauche, en mettant en évidence tout ce que l'on peut. □

Remarque 2.14. Il y a une preuve moins calculatoire : considérons $n + 1$ objets distincts et marquons le premier, disons o_1. Pour choisir les $k + 1$ objets, soit on sélectionne o_1, soit on ne le sélectionne pas. Dans le premier cas, il reste à choisir k objets parmi les n objets restants (C_n^k possibilités). Dans le deuxième cas, on doit choisir $k + 1$ objets parmi les n objets restants (C_n^{k+1} possibilités).

Voici une version du triangle de Pascal : sur la ligne n, on porte C_n^k pour $k \in \{0, \dots, n\}$. Les valeurs extrêmes sont égales à 1. Les autres sont obtenues en utilisant la formule de la proposition précédente : on additionne les valeurs adéquates de la ligne précédente :

$$
\begin{array}{lccccccccccc}
n=0: & & & & & & 1 & & & & & \\
n=1: & & & & & 1 & & 1 & & & & \\
n=2: & & & & 1 & & 2 & & 1 & & & \\
n=3: & & & 1 & & 3 & & 3 & & 1 & & \\
n=4: & & 1 & & 4 & & 6 & & 4 & & 1 & \\
n=4: & 1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}
$$

Proposition 2.9.2 (Formule du binôme de Newton)**.** *Pour tous nombres complexes w et z, et tout $n \in \mathbb{N}$, on a*

$$(w+z)^n = \sum_{k=0}^{n} C_n^k w^k z^{n-k}.$$

Démonstration. La preuve la plus systématique se fait par récurrence. Pour $n = 0, 1, 2$ le résultat est facile à obtenir. Supposons que le résultat soit vrai pour $n \in \mathbb{N}$ et montrons qu'il est vrai pour $n+1$. On a

$$(w+z)^{n+1} = (w+z)(w+z)^n = (w+z)\sum_{k=0}^{n} C_n^k w^k z^{n-k} = \sum_{k=0}^{n} C_n^k w^{k+1} z^{n-k} + \sum_{k=0}^{n} C_n^k w^k z^{n-k+1}.$$

Si on garde en tête la formule à prouver pour $n+1$, la deuxième somme contient les bons monômes $w^k z^{n-k+1}$. On fait un changement d'indice ($k' = k+1$, donc $k = k'-1$) dans la première somme, pour obtenir

$$\sum_{k=0}^{n} C_n^k w^{k+1} z^{n-k} = \sum_{k'=1}^{n+1} C_n^{k'-1} w^{k'} z^{n-k'+1} = \sum_{k=1}^{n+1} C_n^{k-1} w^k z^{n-k+1}.$$

On a donc

$$\begin{aligned}(w+z)^{n+1} &= \sum_{k=1}^{n+1} C_n^{k-1} w^k z^{n-k+1} + \sum_{k=0}^{n} C_n^k w^k z^{n-k+1} \\ &= C_n^n w^{n+1} z^0 + C_0^0 w^0 z^{n+1} + \sum_{k=1}^{n} (C_n^{k-1} + C_n^k) w^k z^{n-k+1}.\end{aligned}$$

On conclut en utilisant le triangle de Pacal et en notant que $C_n^n = 1 = C_{n+1}^{n+1}$. □

Remarque 2.15. Un seul cas de base suffit, évidemment. Mais regarder ce qui se passe pour $n = 2$ ou $n = 3$ permet au lecteur débutant d'anticiper les manipulations des sommes qui apparaissent dans la preuve.

Il existe d'autres démonstrations plus rapides, mais moins systématiques. Par exemple, on peut se dire que $(w+z)^n$ est le produit de n facteurs suivants : $(w+z)\dots(w+z)$. Pour développer ce produit, on distribue chaque terme. A chaque distribution, on est donc amené à choisir entre z et w. Dans le développement, on a donc des monômes de la forme $w^k z^l$, mais avec la condition $k+l = n$, ou $l = n-k$, car il y a n facteurs. Reste à déterminer le coefficient de ce monôme. Il correspond à toutes les façons distinctes de choisir les k facteurs où on développe sur w et non z. C'est évidemment C_n^k.

Il existe bien sûr d'innombrables généralisations de cette formule. On peut aussi noter que la preuve n'a pas fait appel aux définitions spécifiques des opérations dans $\mathbb{C}$. On a distribué, permuté des sommes, utilisé la commutativité... La formule est donc certainement vraie dans tout anneau commutatif.

Mais bon, revenons à nos moutons. On peut définir les racines n-èmes d'un nombre complexe :

Définition 2.9.2. Une racine n-ème d'un nombre complexe z est un nombre complexe w tel que $w^n = z$.

En utilisant la forme trigonométrique des nombres complexes, on obtient directement le résultat suivant. La preuve est un copier coller de celle qui concerne les racines carrées.

Proposition 2.9.3. *Tout nombre complexe non nul z admet n racines n-èmes distinctes.*

Démonstration. On considère donc $z = \rho e^{i\theta}$ et on cherche $z' = \rho' e^{i\theta'}$ tel que $z'^n = z$. Cette condition s'écrit encore $\rho'^n e^{in\theta'} = \rho e^{i\theta}$. On obtient donc les conditions équivalentes

$$\begin{cases} \rho'^n &= \rho \\ n\theta' &= \theta + 2k\pi, \quad k \in \mathbb{Z} \end{cases}$$

Cela donne directement $\rho' = \sqrt[n]{\rho}$. De plus, si on remarque que $e^{i2\pi} = 1$, on peut se limiter à $k \in \{0, \dots, n-1\}$ et on trouve les solutions $\sqrt[n]{\rho} e^{i(\frac{\theta}{n} + \frac{2k\pi}{n})}$, $k \in \{0, \dots, n-1\}$. □

Un cas particulier intéressant est le suivant.

Définition 2.9.3. On appelle racine n-ème de l'unité tout nombre complexe w tel que $w^n = 1$.

Le résultat suivant est en grande partie un corollaire de la proposition 2.9.3, plus précisément de la forme des racines n-èmes trouvée dans la preuve de cette proposition.

Proposition 2.9.4. *Les racines n-èmes de l'unité sont les nombres*

$$e^{i\frac{2k\pi}{n}}, \quad k \in \{0, \dots, n-1\}.$$

On en déduit directement les propriétés suivantes.

Proposition 2.9.5.
- *Les racines n-èmes de l'unité sont les puissances successives de $\omega_n = e^{i\frac{2\pi}{n}}$.*
- *Si $n \geqslant 2$, la somme des racines n-èmes de l'unité est nulle.*
- *Les racines n-èmes de l'unité ont un module égal à 1.*
- *Les racines n-èmes de l'unité sont les sommets d'un polygone régulier à n côtés, inscrit dans le cercle trigonométrique.*
- *L'ensemble des racines n-èmes de l'unité est un sous-groupe de $(\mathbb{C}_0, \cdot, 1)$, noté U_n.*
- *L'ensemble des racines n-èmes de w s'écrit $\{w_0 \omega_n^k : k \in \{0, \dots, n-1\}\}$, si w_0 est une racine n-ème de w.*

Terminons cette section par une petite discussion sur les racines n-èmes primitives de l'unité.

Définition 2.9.4. Une racine n-ème primitive de l'unité est une racine de l'unité ω telle que n soit le plus petit $t \in \mathbb{N}_0$ tel que $\omega^t = 1$.

Exemple 2.9.1. Le nombre -1 n'est pas une racine *quatrième primitive* de l'unité. Parce que bien sûr $(-1)^4 = 1$, mais on a aussi $(-1)^2 = 1$, donc 4 n'est pas la plus petite puissance de -1 qui soit égale à 1. Mais i et $-i$ sont bien des racines quatrièmes primitives.

Proposition 2.9.6. *Si ω est une racine n-ème primitive de l'unité, alors*

$$U_n = \{\omega, \omega^2, \dots, \omega^n = 1\}.$$

Démonstration. Il est facile de démontrer que les nombres $\omega, \omega^2, \dots, \omega^n$ sont des racines n-èmes de l'unité : $(\omega^k)^n = (\omega^n)^k = 1^k = 1$. Pour terminer il suffit de montrer que ces nombres sont tous distincts. Mais si il existe k, l distincts compris entre 1 et n tels que $\omega^k = \omega^l$, si $l > k$, on a alors $\omega^{l-k} = 1$, et $k - l < n$, ce qui est contraire à l'hypothèse. □

On a aussi assez directement ce dernier résultat, qui permet de déterminer les racines n-èmes primitives de l'unité.

Proposition 2.9.7. *Si $w = e^{i\frac{2k\pi}{n}}$ est une racine n-ème primitive, alors k et n n'ont pas de facteur commun.*

Démonstration. Si k et n ont un facteur commun q, on a $k = k'q$ et $n = n'q$, où $n < n'$. Alors $e^{i\frac{2k\pi}{n}} = e^{i\frac{2k'\pi}{n'}}$, ce qui montre que w est une racine n'-ème de l'unité et n'est donc pas une racine n-ème primitive. □

Remarque 2.16. La réciproque de cette proposition est vraie, mais elle est plus délicate à établir.

Table des matières