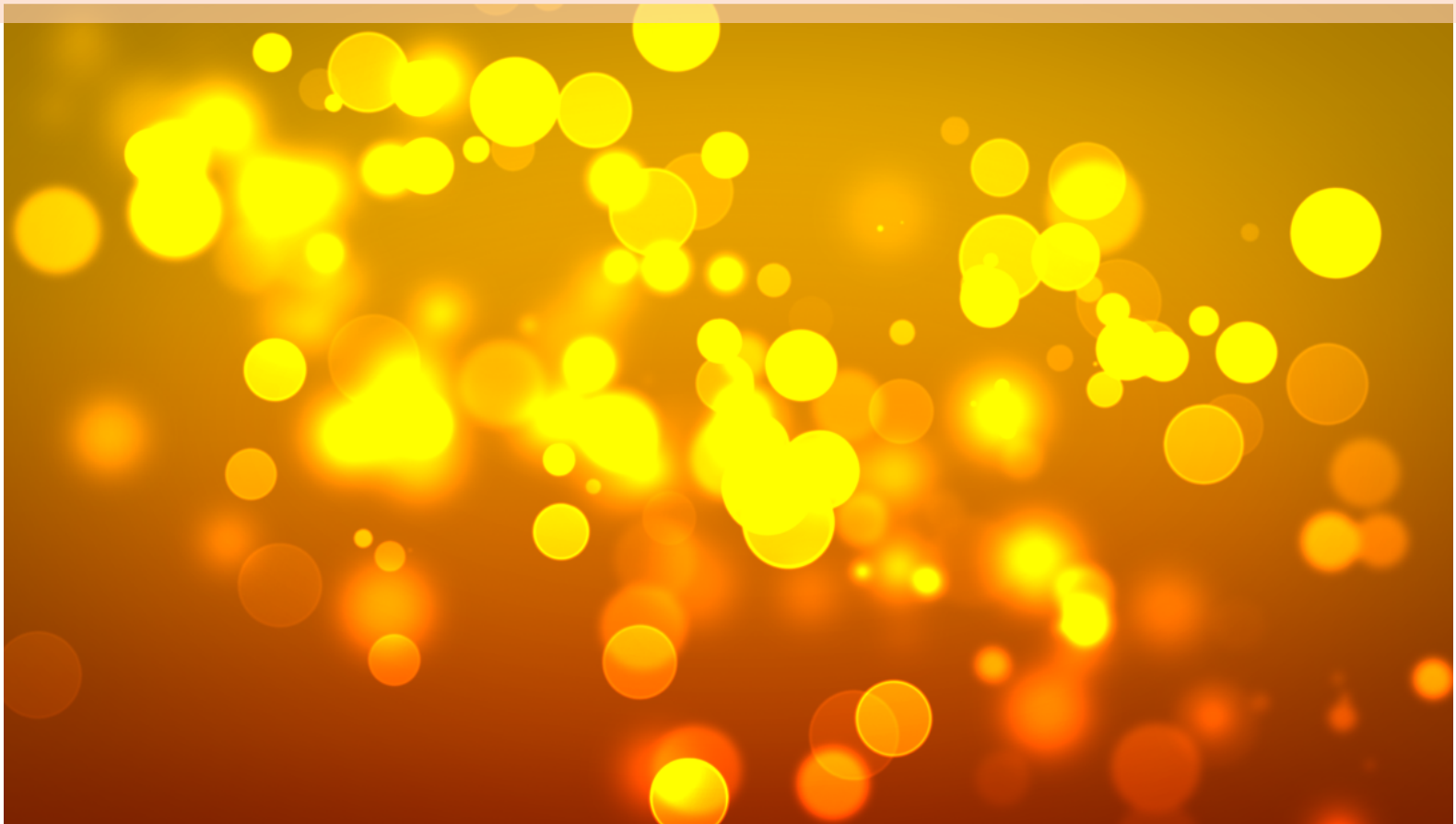
Algèbre et arithmétique 1

Bernard Le Stum

7 juillet 2025



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

Réalisé en LaTeX à partir du modèle Legrand Orange Book

Table des matières

Introduction

Nous commençons par l'étude des nombres complexes. Nous définissons ces nouveaux nombres à partir des nombres réels que l'on supposera donc déjà connus. Nous utiliserons de manière informelle un certain nombre de notions et de notations issues de la logique mathématique ainsi que de la théorie des ensembles bien que celles-ci ne seront vraiment présentées que plus tard dans le cours. Il est essentiel d'apprendre à manipuler formellement ces nouveaux nombres et de n'utiliser leurs formes algébrique ou exponentielle que lorsque cela est nécessaire. Nous verrons de nombreux exemples d'application à la géométrie plane.

Nous poursuivons par une introduction à la logique mathématique et à la théorie des ensembles. Le but d'un mathématicien est de démontrer des théorèmes, ou en d'autres termes, d'énoncer et de valider des propositions. Le calcul propositionnel est un outil qui structure les raisonnements permettant d'obtenir un théorème à partir de résultats connus. Afin d'appliquer ces méthodes en mathématiques, on introduit le vocabulaire ensembliste. De notre point de vue, il s'agira simplement de rassembler des éléments dans ce qu'on appelle un ensemble. On réalise alors que les opérations logiques ont une interprétation naturelle dans ce contexte, ce qui permet de traiter avec une grande rigueur les problèmes mathématiques.

Nous concluons avec l'arithmétique. Il s'agit de l'étude des nombres entiers qu'il est important de considérer en tant que tels et non pas comme des réels particuliers. Un entier naturel n'est jamais que le successeur de celui qui le précède. En partant de ce postulat, on peut définir les opérations classiques (addition, multiplication et ordre) et établir leurs propriétés. C'est ensuite que nous attaquerons l'arithmétique proprement dite : division euclidienne, nombres premiers, etc. Nous établirons avec une grande rigueur de nombreux résultats classiques.

La présentation ci-dessus peut inquiéter par son aspect théorique mais tous ces chapitres seront chacun illustrés par de nombreux exercices. Il n'est pas demandé aux étudiants de digérer tous les concepts introduits en cours. Celui qui saura faire

ou même refaire parfaitement les exercices aura montré qu'il maîtrise suffisamment les techniques nécessaires. Mais avant de considérer qu'un exercice est effectivement terminé, il ne suffit pas d'en donner la réponse, même illustrée de calculs. Il faut rédiger une démonstration complète et rigoureuse, laquelle à partir de résultats déjà établis, permet de conclure. En cela, le cours peut et doit servir de modèle. La résolution d'un exercice se fait donc en deux parties qui peuvent cependant s'imbriquer : l'expérimentation scientifique consiste à retourner le problème dans tous les sens jusqu'à sa résolution, et la rédaction relève elle de la littérature scientifique. Il est alors essentiel de respecter toutes les règles littéraires. En particulier, l'utilisation d'abréviation devra être totalement maîtrisée sinon absente et les symboles logiques réservés à l'écriture d'énoncés.

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

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

Merci à Julien Sebag et Nicolas Charpenay pour les remarques et suggestions qui m'ont permis d'améliorer le texte original.

1. Les quatre premiers chapitres du cours http ://exo7.emath.fr/cours/livre-algebre-1.pdf sont assez proches du notre même si l'organisation est sensiblement différente.

1. Nombres complexes

Vous savez résoudre une équation réelle du second degré de la forme $ax^2+bx+c=0$: il est nécessaire que $\Delta := b^2-4ac \geq 0$, et on aura alors

$$x = \frac{-b \pm \delta}{2a} \quad \text{avec} \quad \delta = \sqrt{\Delta}.$$

Ceci est bien connu depuis l'antiquité. C'est en cherchant à étendre cette méthode aux équations du troisième degré que les mathématiciens de la renaissance ont inventé les nombres complexes. En effet, même si une équation réelle du troisième degré a toujours une solution réelle, il est nécessaire pour la trouver de considérer des équations intermédiaires du second degré avec parfois $\Delta < 0$. L'exemple le plus simple d'une telle équation est $x^2+1=0$. Pour celle-ci, il suffit d'*imaginer* qu'il existe une solution qu'on appelle [1] i et de poursuivre les calculs comme si i était un « vrai nombre ». On peut donc multiplier i par un nombre réel b et obtenir ce qu'on appelle un *nombre imaginaire pur* ib. On peut ajouter un nombre réel a et un nombre imaginaire pur ib et obtenir un *nombre complexe* $a+ib$. Enfin, on peut aussi être amenés à multiplier i par lui même, mais comme i est solution de $x^2+1=0$, on aura $i^2=-1$. Ces règles élémentaires se prolongent naturellement en des opérations sur tous les nombres complexes. On dispose alors du magnifique théorème de d'Alembert-Gauss [2] qui dit qu'une équation algébrique à coefficients complexes a toujours au moins une solution complexe.

1. On utilise la lettre j en électricité.
2. Que nous ne démontrerons pas ici.

1.1 Addition

On commence par donner la définition formelle d'un nombre complexe :

Définition 1.1.1 Un *(nombre) complexe*[a] est un nombre de la forme $z =$"$a + ib$" avec $a, b \in \mathbb{R}$. On dit que a est la *partie réelle* de z et on écrit $a = \mathrm{Re}(z)$. On dit que b est la *partie imaginaire* de z et on écrit $b = \mathrm{Im}(z)$.

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

On désigne par $\mathbb{C}$ l'ensemble de tous les nombres complexes. Ainsi,

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

Remarque

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

Exemple

1. Les nombres 0, 1, -1, $\sqrt{2}$ et π sont des nombres réels, et donc aussi des nombres complexes.
2. Les nombres $i := i1$, $-i := i(-1)$ et $2\pi i := i2\pi$ (on écrit aussi bi au lieu de ib) sont des nombres imaginaires purs, et donc aussi complexes.
3. Les nombres $1 + i$, $j := -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ sont des nombres imaginaires, et donc aussi complexes, mais ce ne sont pas des imaginaires purs.
4. Le nombre 0 est l'unique nombre qui est à la fois réel et imaginaire pur (mais pas imaginaire !).

Proposition 1.1.2 Si $z, w \in \mathbb{C}$, on a

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

Démonstration. Cela signifie que $a + ib = c + id$ avec $a, b, c, d \in \mathbb{R}$ si et seulement si $a = c$ et $b = d$. ■

Définition 1.1.3 Si $z = a + ib$ avec $a, b \in \mathbb{R}$ et $w = c + id$ avec $c, d \in \mathbb{R}$, sont deux nombres complexes, leur *somme* est le nombre complexe

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

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

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

Proposition 1.1.4 Si $z, w \in \mathbb{C}$, on a

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

Démonstration. Résulte immédiatement des définitions (exercice). ■

Proposition 1.1.5 On a
1. $\forall z_1, z_2 \in \mathbb{C}, \quad z_1 + z_2 = z_2 + z_1$,
2. $\forall z_1, z_2, z_3 \in \mathbb{C}, \quad (z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$,
3. $\forall z \in \mathbb{C}, \quad z + 0 = z$,
4. $\forall z \in \mathbb{C}, \exists - z \in \mathbb{C}, \quad z + (-z) = 0$.

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

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

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

(la *soustraction* est l'opération qui associe à deux *termes* leur *différence*).

- Si v_1 et v_2 sont deux vecteurs d'affixes z_1 et z_2, alors l'affixe de $v_1 \pm v_2$ est $z_1 \pm z_2$. Faire un dessin.
- Si M, N sont deux points d'affixes z, w, alors le vecteur $\overrightarrow{MN}$ a pour affixe $w - z$. Faire un dessin.
- La *translation* de vecteur u correspond à l'addition de l'affixe de u. Faire un dessin.
- Les points M_1, M_2, M_3, M_4 d'affixes respectifs z_1, z_2, z_3, z_4 forment un *parallélogramme* si et seulement si $z_1 - z_2 + z_3 - z_4 = 0$. Faire un dessin.

Définition 1.1.6 Si $z = a + ib$ avec $a, b \in \mathbb{R}$ et $k \in \mathbb{R}$, leur *produit (externe)* est $kz := ka + ikb$.

Remarque

- On a alors toujours

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

- Si $k \in \mathbb{R}_{\neq 0}$, on écrit aussi $\dfrac{z}{k} := \dfrac{1}{k}z$.
- On dispose des propriétés suivantes :
  1. $\forall z \in \mathbb{C}, \quad 1z = z$,
  2. $\forall z, w \in \mathbb{C}, \forall k \in \mathbb{R}, \quad k(z + w) = kz + kw$,
  3. $\forall z \in \mathbb{C}, \forall k, l \in \mathbb{R}, \quad (k + l)z = kz + lz$,
  4. $\forall z \in \mathbb{C}, \forall k, l \in \mathbb{R}, \quad (kl)z = k(lz)$.
- $\mathbb{C}$ est un *espace vectoriel réel* (groupe abélien ainsi que ces quatre propriétés).
- Si u est le vecteur d'affixe z, alors ku a pour affixe kz. Faire un dessin.
- L'*homothétie* de rapport k correspond à la multiplication par k sur l'affixe. Faire un dessin.
- Si M_1 et M_2 ont pour affixe z_1 et z_2, alors leur *milieu* a pour affixe $\dfrac{z_1 + z_2}{2}$. Le *centre de gravité* des points M_1, M_2, M_3 d'affixes respectifs z_1, z_2, z_3 a pour affixe $\dfrac{z_1 + z_2 + z_3}{3}$.

Définition 1.1.7 Si $z = a + ib$ avec $a, b \in \mathbb{R}$, alors son *conjugué* est $\overline{z} := a - ib$.

Proposition 1.1.8 On a

1. $\forall z \in \mathbb{C}, \quad \mathrm{Re}(\overline{z}) = \mathrm{Re}(z)$ et $\mathrm{Im}(\overline{z}) = -\mathrm{Im}(z)$,
2. $\forall z \in \mathbb{C}, \quad z = \mathrm{Re}(z) + i\mathrm{Im}(z)$ et $\overline{z} = \mathrm{Re}(z) - i\mathrm{Im}(z)$,
3. $\forall z \in \mathbb{C}, \quad \mathrm{Re}(z) = \dfrac{z + \overline{z}}{2}$ et [a] $\mathrm{Im}(z) = \dfrac{z - \overline{z}}{2i}$,
4. $\forall z, w \in \mathbb{C}, k \in \mathbb{R} \quad \overline{kz + lw} = k\overline{z} + l\overline{w}$,
5. $\forall z \in \mathbb{C}, \quad \overline{\overline{z}} = z$.

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

Démonstration. Résulte immédiatement des définitions (exercice). ■

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

1.2 Multiplication

La description de la multiplication des nombres complexes sous leur forme algébrique ne semble pas très naturelle :

Définition 1.2.1 Si $z = a + ib$ avec $a, b \in \mathbb{R}$ et $w = c + id$ avec $c, d \in \mathbb{R}$ sont deux nombres complexes, leur *produit* est le nombre complexe

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

Remarque
- La *multiplication* est l'opération qui associe à deux *facteurs* leur *produit*.
- En pratique, on écrira $zw := z \times w$ exactement comme pour les réels. On a bien $ib = i \times b$, ce qui fait qu'il n'y a pas d'ambiguïté dans les notations.
- On remarquera que $i^2 = i \times i = -1$.
- Comme toujours, par convention, la multiplication sera prioritaire sur l'addition.

Proposition 1.2.2 On a

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

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

$$z^{-1} = \frac{a}{a^2 + b^2} + i\frac{-b}{a^2 + b^2}$$

et on calcule :

$$\begin{aligned} z \times z^{-1} &= (a + ib) \times \left(\frac{a}{a^2 + b^2} + i\frac{-b}{a^2 + b^2} \right) \\ &= \left(a\frac{a}{a^2 + b^2} - b\frac{-b}{a^2 + b^2} \right) + i \left(a\frac{-b}{a^2 + b^2} + b\frac{a}{a^2 + b^2} \right) \\ &= \frac{a^2 + b^2}{a^2 + b^2} + i\frac{a^2 - b^2}{a^2 + b^2} \\ &= 1. \end{aligned}$$

■

Remarque

- On écrira tout simplement $z_1 \times z_2 \times z_3$ sans mettre de parenthèses car il n'y a pas d'ambiguïté.
- $\mathbb{C}$ est un *corps* (groupe abélien ainsi que ces cinq propriétés : $\mathbb{C}^\times := \mathbb{C}_{\neq 0}$ est un groupe abélien pour la multiplication et la distributivité).
- On dispose comme dans tout corps de l'équivalence importante

$$\forall z, w \in \mathbb{C}, \quad z \times w = 0 \Leftrightarrow z = 0 \text{ ou } w = 0.$$

- On définit le *quotient*[3] de deux nombre complexes z et $w \neq 0$ par la formule

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

(l'opération correspondante est la *division* du *dividende* par le *diviseur*).
- Si $z \neq 0$, on dit que z^{-1} (ou de manière équivalente $1/z$) est l'*inverse* de z. On a toujours $(z^{-1})^{-1} = z$ et $(z \times w)^{-1} = z^{-1} \times w^{-1}$.
- Deux vecteurs u_1 et u_2 d'affixes z_1 et z_2 sont *colinéaires* (resp. *orthogonaux*) si et seulement si z_2/z_1 est réel (resp. imaginaire pur) ou si $z_1 = 0$. Faire un dessin.
- Les points M_1, M_2, M_3 d'affixes respectifs z_1, z_2, z_3 sont *alignés* (resp. forment un *triangle rectangle* en M_1) si et seulement si $\dfrac{z_3 - z_1}{z_2 - z_1}$ est réel (resp. imaginaire pur) ou bien $z_1 = z_2$. Faire un dessin.
- Une *droite affine* à pour équation complexe $\mathrm{Re}(\overline{\omega} z) = c$ ou $\omega \in \mathbb{C}^\times$ et $c \in \mathbb{R}$ (si l'équation est $ax + by = c$, alors $\omega = a + ib$).

Exemple

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

Proposition 1.2.3 On a $\forall z, w \in \mathbb{C}, \quad \overline{z \times w} = \overline{z} \times \overline{w}$.

Démonstration. Clair (exercice). ■

Remarque

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

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

lorsque $w \neq 0$.
- On introduira plus tard le *module* de $z = a + ib$ par la formule $|z| := \sqrt{a^2 + b^2}$. On a alors

$$z \times \overline{z} = (a + ib)(a - ib) = a^2 + b^2 = |z|^2$$

et donc

$$z^{-1} = \frac{\overline{z}}{|z|^2} \quad \text{si } z \neq 0.$$

3. On ne parlera pas de *fraction* (*numérateur* sur *dénominateur*) qui est une notion plus subtile.

- Si u est un vecteur d'affixe z, alors sa *norme* est $\|u\| = |z|$. Si M, N sont deux points d'affixes z, w, on dispose de la *longueur* $MN = |w - z|$.

Définition 1.2.4 Si $z \in \mathbb{C}$ et $n \in \mathbb{N}$, alors la *puissance* n-ème de z est

$$z^n := \underbrace{z \times \cdots \times z}_{n \text{ fois}}.$$

Si $z \neq 0$, la *puissance* $(-n)$-ème de z est

$$z^{-n} := \underbrace{\frac{1}{z} \times \cdots \times \frac{1}{z}}_{n \text{ fois}}.$$

Remarque Formellement, la *puissance* n-ème de z est définie par récurrence en posant $z^0 = 1$ et $z^{n+1} = z^n \times z$. La puissance $(-n)$-ème de z est alors définie par $z^{-n} := (z^{-1})^n$.

Exemple 1. $i^4 = 1$.

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

Proposition 1.2.5 1. $\forall z \in \mathbb{C}^\times, \forall m, n \in \mathbb{Z}, \quad z^{m+n} = z^m \times z^n$,

2. $\forall z \in \mathbb{C}^\times, \forall m, n \in \mathbb{Z}, \quad (z^m)^n = z^{mn}$,

3. $\forall z, w \in \mathbb{C}^\times, \forall n \in \mathbb{Z}, \quad (z \times w)^n = z^n \times w^n$.

Démonstration. La démonstration de ces résultats utilise uniquement le fait que $\mathbb{C}$ est un corps et pas une seule fois la définition des nombres complexe. La démonstration est donc identique en tout point à celle de la proposition analogue sur $\mathbb{R}$. ■

Remarque

- On peut aussi montrer que

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

- On peut inclure le cas $z = 0$ dans les différentes formules si on se limite aux entiers positifs.

1.3 Sommes et produits

Comme de nombreux résultats déjà vus, ce qui suit reste valable sur $\mathbb{R}, \mathbb{Z}\ldots$

Définition 1.3.1 Si $m, n \in \mathbb{Z}$, alors *somme* de $z_m, z_{m+1}, \ldots, z_n \in \mathbb{C}$ est

$$\sum_{k=m}^{n} z_k = z_m + z_{m+1} + \cdots + z_n.$$

Remarque

- Formellement, on définit ces sommes par récurrence :

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

- On définit de la même manière les *produits*

$$\prod_{k=m}^{n} z_k = z_m \times z_{m+1} \times \ldots \times z_n \quad (= 1 \text{ si } n < m).$$

- Plus généralement, si I est un ensemble fini, on peut définir $\sum_{i\in I} z_i$ et $\prod_{i\in I} z_i$. Dans notre cas, $I = \{m, m+1, \ldots, n\}$.
- $\sum_{\emptyset} = 0$ et $\prod_{\emptyset} = 1$.

Exemple

1. Pour tout $n \in \mathbb{N} \setminus \{0\}$,

$$\sum_{k=1}^{n} 0 = 0, \quad \sum_{k=1}^{n} 1 = n, \quad \prod_{k=1}^{n} 0 = 0, \quad \text{et} \quad \prod_{k=1}^{n} 1 = 1.$$

2. Pour tout $n \in \mathbb{N}$ et $z \in \mathbb{C}$

$$\sum_{k=1}^{n} z = nz \quad \text{et} \quad \prod_{k=1}^{n} z = z^n.$$

3. Pour tout $n \in \mathbb{N}$,

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

Proposition 1.3.2

1. Si $z_m, \ldots, z_n, w_m, \ldots w_n \in \mathbb{C}$, alors

$$\sum_{k=m}^{n} z_k + \sum_{k=m}^{n} w_k = \sum_{k=m}^{n}(z_k + w_k).$$

2. Si $z_m, \ldots, z_n, w \in \mathbb{C}$, alors

$$\left(\sum_{k=m}^{n} z_k\right) w = \sum_{k=m}^{n} z_k w.$$

3. Si $z_m, \ldots, z_n \in \mathbb{C}$, alors (relation de Chasles)

$$\sum_{k=m}^{n} z_k = \sum_{k=m}^{p} z_k + \sum_{k=p+1}^{n} z_k.$$

Démonstration. Ces formules sont obtenues par récurrence. ■

Remarque

- Dans la formule d'une somme ou d'un produit, on dit que k est une variable *muette*. On a par exemple

$$\sum_{k=m}^{n} z_k = \sum_{l=m}^{n} z_l, \quad \sum_{k=m}^{n} z_k = \sum_{k=-n}^{-m} z_{-k} \quad \text{ou} \quad \sum_{k=m}^{n} z_k = \sum_{k=m+l}^{n+l} z_{k-l}.$$

- Téléscopage : on a

$$\begin{aligned}&\sum_{k=m}^{n}(z_k - z_{k+1})\\ &= (z_m - z_{m+1}) + (z_{m+1} - z_{m+2}) + \ldots + (z_{n-1} - z_n) + (z_n - z_{n+1})\\ &= z_m - z_{n+1}.\end{aligned}$$

- Toutes ces propriétés ont un analogue multiplicatif (produits).

Proposition 1.3.3 $\forall z \in \mathbb{C}_{\neq 1}, \forall n \in \mathbb{N}, \quad \displaystyle\sum_{k=0}^{n} z^k = \frac{1-z^{n+1}}{1-z}.$

Démonstration. Par telescopage :

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

■

Remarques

- On a plus généralement

$$\sum_{k=m}^{n} z^k = \frac{z^m - z^{n+1}}{1-z} \quad \left(\text{et } \sum_{k=0}^{n} w^{n-k} z^k = \frac{w^{n+1} - z^{n+1}}{w-z}\right).$$

- On dit que $w_0, w_1, \ldots, w_n$ sont en *progression arithmétique* (resp. *géométrique*) s'il existe $z \in \mathbb{C}$ tel que $w_{k+1} = w_k + z$ (resp. $w_{k+1} = zw_k$) pour $k = 0, \ldots, n-1$. On a alors

$$\sum_{k=0}^{n} w_k = (n+1)\left(w_0 + \frac{n}{2}z\right) \quad \left(\text{resp. } \sum_{k=0}^{n} w_k = \frac{1-z^{n+1}}{1-z} w_0\right).$$

On *rappelle* la notion de *factorielle* pour $n \in \mathbb{N}$:

$$n! = \prod_{k=1}^{n} k.$$

On a donc $0! = 1$, $1! = 1$; $2! = 3$, $3! = 6$, $4! = 24$, ...

On *rappelle* la notion de *coefficient binomial* définie pour $n, k \in \mathbb{Z}$ par

$$\binom{n}{k} := 0 \text{ sauf si } 0 \leq k \leq n, \quad \binom{0}{0} := 1,$$

et ensuite par récurrence :

$$\binom{n+1}{k} := \binom{n}{k-1} + \binom{n}{k}.$$

On dispose ainsi du *triangle de Pascal* :

$\binom{n}{k}$	$k=0$	$k=1$	$k=2$	$k=3$	$k=4$
$n=0$	1				
$n=1$	1	1			
$n=2$	1	2	1		
$n=3$	1	3	3	1	
$n=4$	1	4	6	4	1

On peut alors montrer que si $n, k \in \mathbb{N}$, alors

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\dots(n-k+1)}{k(k-1)\dots 1}.$$

C'est le nombre de façons de choisir k objets parmi n.

Théoreme 1.3.4 Soient $z, w \in \mathbb{C}$ et $n \in \mathbb{N}$. Alors,

$$\begin{aligned}(z+w)^n &= \sum_{k=0}^{n} \binom{n}{k} z^{n-k} w^k \\ &= z^n + nz^{n-1}w + \frac{n(n-1)}{2} z^{n-2}w^2 + \ldots + nzw^{n-1} + w^n.\end{aligned}$$

Démonstration. On procède par récurrence (informelle) sur n, le cas $n = 0$ étant immédiat. On aura donc

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

■

Exemple Avec $j := -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, on a (formule du binôme)

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

On en déduit que

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

On voit alors que

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

1.4 Exponentielle complexe

La définition de l'exponentielle d'un nombre complexe peut sembler un peu étrange :

Définition 1.4.1 Si $z = a + ib$ avec $a, b \in \mathbb{R}$ est un nombre complexe, alors l'*exponentielle* de z est

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

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

On rappelle les formules trigonométriques

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

Proposition 1.4.2
1. $e^0 = 1$,
2. $\forall z, w \in \mathbb{C}, \quad e^{z+w} = e^z \times e^w$,

Démonstration. La première assertion est immédiate. Pour la seconde, si $z = a + ib$ avec $a, b \in \mathbb{R}$ et $w = c + id$ avec $c, d \in \mathbb{R}$, on aura d'un coté

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

et de l'autre

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

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

$$\mathbb{C} \to \mathbb{C}^\times, \quad z \mapsto e^z$$

(avec l'addition sur la source et la multiplication sur le but). Le corollaire qui suit résulte *formellement* de ces propriétés.

- Pour tout $z \in \mathbb{C}$, on a $\overline{e^z} = e^{\overline{z}}$.
- Si $x \in \mathbb{R}$, alors
$$\overline{e^{ix}} = e^{\overline{ix}} = e^{-ix} = \left(e^{ix}\right)^{-1}.$$

Corollaire 1.4.3
1. $\forall z \in \mathbb{C}, \quad e^z \neq 0$ et $e^{-z} = \dfrac{1}{e^z}$,
2. $\forall z, w \in \mathbb{C}, \quad e^{z-w} = \dfrac{e^z}{e^w}$,
3. $\forall z \in \mathbb{C}, \forall n \in \mathbb{Z}, \quad e^{nz} = (e^z)^n$.

Démonstration.
1. On a $e^z \times e^{-z} = e^{z-z} = e^0 = 1$. On a donc bien $e^z \neq 0$ et $e^{-z} = \dfrac{1}{e^z}$.
2. On a alors $e^{z-w} = e^z \times e^{-w} = e^z \times \frac{1}{e^w} = \dfrac{e^z}{e^w}$.
3. Le cas $n \geq 0$ se traite par récurrence : on a $e^0 = 1 = (e^z)^0$ et si $e^{nz} = (e^z)^n$ alors
$$e^{(n+1)z} = e^{nz+z} = e^{nz} \times e^z = (e^z)^n \times e^z = (e^z)^{n+1}.$$
Lorsque $n < 0$ (si bien que $-n > 0$), on aura donc
$$e^{nz} = \frac{1}{e^{-nz}} = \frac{1}{(e^z)^{-n}} = (e^z)^n.$$
■

Remarque On dispose des *formules de Moivre* pour $x \in \mathbb{R}$
$$e^{ix} = \cos(x) + i\sin(x) \quad \text{et} \quad e^{-ix} = \cos(x) - i\sin(x)$$
ainsi que des *formules d'Euler*
$$\cos(x) = \frac{e^{ix} + e^{-ix}}{2} \quad \text{et} \quad \sin(x) = \frac{e^{ix} - e^{-ix}}{2i}.$$

Exemple
1. Avec les formules de Moivre :
$$\cos(3x) + i\sin(3x) = e^{3ix} = (e^{ix})^3 = (\cos(x) + i\sin(x))^3 = \cos^3(x) + 3i\cos^2(x)\sin(x) - 3\cos(x)\sin^2(x) - i\sin^3(x).$$
On en déduit que
$$\begin{cases} \cos(3x) &= \cos^3(x) - 3\cos(x)\sin^2(x) &= 4\cos^3(x) - 3\cos(x) \\ \sin(3x) &= 3\cos^2(x)\sin(x) - \sin^3(x) &= 3\sin(x) - 4\sin^3(x). \end{cases}$$
2. Avec les formules d'Euler :
$$\begin{aligned} \cos^3(x) &= \left(\frac{e^{ix} + e^{-ix}}{2}\right)^3 \\ &= \frac{1}{8}(e^{3ix} + 3e^{ix} + 3e^{-ix} + e^{-3ix}) \\ &= \frac{1}{4}\left(\frac{e^{3ix} + e^{-3ix}}{2} + 3\frac{e^{ix} + e^{-ix}}{2}\right) \\ &= \frac{1}{4}(\cos(3x) + 3\cos(x)). \end{aligned}$$
On peut faire la même chose avec $\sin^3(x)$.

1.5 Module et argument

Proposition 1.5.1 Si $z \in \mathbb{C}^\times$, il existe un unique $r \in \mathbb{R}_{>0}$ et un unique $\theta \in \mathbb{R}$ modulo 2π tels que $z = re^{i\theta}$.

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

$$z = a + ib = r\cos(\theta) + ir\sin(\theta) = re^{i\theta}.$$ ■

Remarque

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

  $$\mathbb{C} \to \mathbb{C}^\times, \quad z \mapsto e^z$$

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

Définition 1.5.2 On dit alors que r est le *module* de z, et on écrit $|z| = r$, et que $\theta \mod 2\pi$ est son *argument*, et on écrit $\arg(z) \equiv \theta \mod 2\pi$. On pose aussi $|0| = 0$ (mais l'argument de 0 est indéfini).

Exemple

1. $|1| = 1$ et $\arg(1) \equiv 0 \mod 2\pi$,
2. $|-1| = 1$ et $\arg(-1) \equiv \pi \mod 2\pi$,
3. $|i| = 1$ et $\arg(i) \equiv \pi/2 \mod 2\pi$,
4. $|1 + i| = \sqrt{2}$ et $\arg(1 + i) \equiv \pi/4 \mod 2\pi$.

Remarque

- Si $z = a \in \mathbb{R}$, alors $|z| = |a|$ (le module d'un nombre réel est égal à sa valeur absolue). Il n'y a donc pas d'ambiguïté dans la notation.
- Si $z, w \in \mathbb{C}^\times$, on a

  $$z = w \Leftrightarrow \begin{cases} |z| = |w| \\ \arg(z) \equiv \arg(w) \mod 2\pi \end{cases}$$

- Les réels r et θ sont exactement les coordonnées *polaires* du vecteur d'affixe z. Faire un dessin.

Proposition 1.5.3 1. Si $z, w \in \mathbb{C}^\times$, alors

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

2. Si $z \in \mathbb{C}^\times$, alors

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

3. Si $z, w \in \mathbb{C}^\times$, alors

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

4. Si $z \in \mathbb{C}^\times$ et $n \in \mathbb{Z}$, alors

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

5. Si $z \in \mathbb{C}^\times$, alors

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

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

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

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

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

et que

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

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

Remarque

- Les résultats concernant les modules sont encore valides si z (ou w) est nul.
- On a
$$\begin{cases} |-z| = |z \times (-1)| = |z| \times |-1| = |z| \times 1 = |z| & \text{et} \\ \arg(-z) \equiv \arg(z \times (-1)) \equiv \arg(z) + \arg(-1) \equiv \arg(z) + \pi \mod 2\pi \end{cases}$$
- Attention : si $\arg(z^n) \equiv \theta \mod 2\pi$, alors $\arg(z) \equiv \dfrac{\theta}{n} \mod \dfrac{2\pi}{n}$.
- Attention : on peut comparer les *modules* de deux nombres complexes z et w et écrire par exemple $|z| \leq |w|$ mais on ne compare *jamais* deux nombres complexes : on réserve la notation $x \leq y$ aux nombres *réels*.
- Pour représenter le produit de deux nombres complexes, on multiplie les rayons et on ajoute les angles. Faire un dessin.
- La *rotation* d'angle θ correspond à la multiplication par $e^{i\theta}$ sur l'affixe. Faire un dessin.

Proposition 1.5.4 $\forall z \in \mathbb{C}, \quad |z|^2 = z \times \overline{z} = \mathrm{Re}(z)^2 + \mathrm{Im}(z)^2$.

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

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

et, si $z \neq 0$,

$$\arg(z \times \overline{z}) \equiv \arg(z) + \arg(\overline{z}) \equiv \arg(z) - \arg(z) \equiv 0 \mod 2\pi. \qquad \blacksquare$$

Remarque
- Plus prosaïquement, si $z = a + ib$ avec $a, b \in \mathbb{R}$, alors $|z| = \sqrt{a^2 + b^2}$.
- On a toujours $|\mathrm{Re}(z)| \leq |z|$ (resp. $|\mathrm{Im}(z)| \leq |z|$) avec égalité si et seulement si z est réel (resp. imaginaire pur).

Proposition 1.5.5 On a

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

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

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

Remarque
- On a utilisé le fait que deux nombres *positifs* sont dans le même ordre que leurs carrés.
- On a *égalité* triangulaire $|z + w| = |z| + |w|$ si et seulement si $\arg(z) \equiv \arg(w) \mod 2\pi$ si et seulement si $w = kz$ avec $k \in \mathbb{R}_{\geq 0}$.
- On aura aussi toujours $||z| - |w|| \leq |z - w|$.
- Les trois propriétés de la proposition définissent ce qu'on appelle *une valeur absolue*.

On peut faire le lien avec la géométrie.

Remarque
- Si on désigne par u le vecteur d'affixe z, on a $\|u\| = |z|$ (norme).
- Si on désigne par M et N les points d'affixes respectifs z et w, alors $MN = |w - z|$ (distance).

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

$$\widehat{(u_1, u_2)} \equiv \arg\left(\frac{z_2}{z_1}\right) \mod 2\pi.$$

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

$$\widehat{M_2M_1M_3} \equiv \arg\left(\frac{z_3 - z_1}{z_2 - z_1}\right) \mod 2\pi.$$

1.6 Equations algébriques

Proposition 1.6.1 Si $\alpha = re^{i\theta}$ avec $r \in \mathbb{R}_{>0}$ et $\theta \in \mathbb{R}$, $n \in \mathbb{N}$ et $z \in \mathbb{C}$, alors

$$z^n = \alpha \quad \Leftrightarrow \quad \exists k \in \{0, \dots, n-1\}, z = r^{1/n} e^{i\frac{\theta + k2\pi}{n}}$$

Démonstration. On aura

$$\begin{aligned} z^n = \alpha &\Leftrightarrow |z^n| = |\alpha| \text{ et } \arg(z^n) \equiv \arg(\alpha) \mod 2\pi \\ &\Leftrightarrow |z|^n = r \text{ et } n\arg(z) \equiv \theta \mod 2\pi \\ &\Leftrightarrow |z| = r^{1/n} \text{ et } \arg(z) \equiv \theta/n \mod \frac{2\pi}{n}. \end{aligned}$$

Enfin, $\arg(z) \equiv \theta/n \mod \frac{2\pi}{n}$ signifie que $\arg(z) \equiv \theta/n + k2\pi/n \mod 2\pi$ avec $k \in \mathbb{Z}$. Mais il suffit de prendre $k \in \{0, \dots, n-1\}$. ■

Corollaire 1.6.2 $\forall \zeta \in \mathbb{C}, \forall n \in \mathbb{N}, \quad \zeta^n = 1 \Leftrightarrow \exists k \in \{0, \dots, n-1\}, \zeta = e^{\frac{2ik\pi}{n}}$. ■

Remarque
- On dit alors que ζ est une *racine n-ème de l'unité* (et avant que z est une racine *racine n-ème de α*).
- En faisant varier k entre 0 et $n-1$, cela correspond géométriquement aux sommets du polygone régulier à n cotés. Faire un dessin.
- Si $\zeta^n = 1$ et $\zeta \neq 1$, alors

$$1 + \zeta + \zeta^2 + \cdots + \zeta^{n-1} = \frac{1 - \zeta^n}{1 - \zeta} = 0.$$

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

Corollaire 1.6.3 Tout $\alpha \in \mathbb{C}^\times$ possède exactement deux racines carrées (opposées) dans $\mathbb{C}^\times$.

Démonstration. Les racines carrées de $\alpha = re^{i\theta}$ sont $\sqrt{r}e^{i\theta/2}$ et $\sqrt{r}e^{i(\theta/2+\pi)} = -\sqrt{r}e^{i\theta/2}$. ■

Remarque
- La *racine carrée* d'un réel *positif* x est l'*unique* réel *positif* dont le carré vaut x. On le note $\sqrt{x}$. On utilise *jamais* cette notation si $x \notin \mathbb{R}_{\geq 0}$.
- Il n'y a pas d'ordre sur les racines carrées en général. Par exemple, si on écrit $-i = e^{-i\pi/2}$, on trouve d'abord $e^{-i\pi/4}$ et ensuite $e^{-i\pi/4+i\pi} = e^{i3\pi/4}$. Mais si on écrit $-i = e^{i3\pi/2}$, on trouve d'abord $e^{i3\pi/4}$ et ensuite $e^{i3\pi/4+i\pi} = e^{i7\pi/4} = e^{-i\pi/4}$.

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

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

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

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

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

et

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

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

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

on est ramenés à résoudre

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

On en déduit immédiatement que $a^2 = 4$ is bien que $a = \pm 2$ et donc que $b = \mp 2$ si bien que les racines sont $2 - 2i$ et $-2 + 2i$.

Proposition 1.6.4 Soient $\alpha, \beta, \gamma \in \mathbb{C}$ avec $\alpha \neq 0$. Soit $\Delta := \beta^2 - 4\alpha\gamma$ et δ une racine de Δ. Alors l'équation $\alpha z^2 + \beta z + \gamma = 0$ a pour solutions

$$\frac{-\beta + \delta}{2\alpha} \quad \text{et} \quad \frac{-\beta - \delta}{2\alpha}.$$

Démonstration. Classique : on écrit

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

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

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

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

et on se souvient que ses racines sont $2 - 2i$ et $-2 + 2i$. On en déduit que les solutions de l'équation sont

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

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

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

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

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

En particulier, on a (somme et produit des racines) :

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

1.7 Géométrie (faire des dessins)

On rappelle d'abord les résultats vus jusqu'à présent :

Définition 1.7.1 L'*affixe* du vecteur u de composantes (resp. du point M de coordonnées) (a, b) est le nombre complexe $z = a + ib$.

1.
   - Si u, v sont deux vecteurs d'affixes respectifs z et w et $k, l \in \mathbb{R}$, alors l'affixe de $ku + lv$ est $kz + lw$.
   - Si M, N sont deux points d'affixes z, w, alors le vecteur $\overrightarrow{MN}$ a pour affixe $w - z$.
   - Les points M_1, M_2, M_3, M_4 d'affixes respectifs z_1, z_2, z_3, z_4 forment un parallélogramme si et seulement si $z_1 - z_2 + z_3 - z_4 = 0$.
   - Si M, N sont deux points d'affixes z, w, alors le milieu de $\{M, N\}$ a pour affixe $\frac{z+w}{2}$.
   - Deux vecteurs u et v d'affixes z et w sont colinéaires (resp. orthogonaux) si et seulement si z/w est réel (resp. imaginaire pur) ou si $w = 0$.

- Si M_1, M_2, M_3 ont pour affixes z_1, z_2, z_3, alors le triangle $\{M_1, M_2, M_3\}$ est plat (resp.rectangle en M_1) si et seulement si $\dfrac{z_3 - z_1}{z_2 - z_1}$ est réel (resp. imaginaire pur) ou bien $z_1 = z_2$.
- Une droite affine à pour équation complexe $\mathrm{Re}(\overline{\omega} z) = c$ ou $\omega \in \mathbb{C}$ et $c \in \mathbb{R}$.
- Les sommets du polygone régulier à n cotés ont pour affixes $e^{2i\pi k/n}$ avec $k = 0, \ldots, n-1$.

2.
- Les réels $|z|$ et $\arg(z)$ sont les coordonnées *polaires* du vecteur d'affixe z.
- La norme d'un vecteur u d'affixe z est $\|u\| = |z|$.
- La distance entre deux points M et N d'affixes z et w est $MN = |z - w|$.
- Le *cercle* (resp. *disque*) de centre M_0 d'affixe z_0 et de rayon $r \geq 0$ a pour équation $|z - z_0| = r$ (resp. $|z - z_0| \leq r$).
- La *médiatrice* des points M_1 et M_2 d'affixes respectifs z_1 et z_2 a pour équation $|z - z_1| = |z - z_2|$.
- Si on désigne par u et v les vecteurs d'affixes respectifs z et w et $u \neq 0$, alors

$$\widehat{(u, v)} \equiv \arg\left(\frac{w}{z}\right).$$

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

$$\widehat{M_2 M_1 M_3} \equiv \arg\left(\frac{z_3 - z_1}{z_2 - z_1}\right).$$

3.
- La projection verticale correspond à la partie réelle.
- La projection horizontale correspond à la partie imaginaire.
- La symétrie centrale correspond à l'opposé.
- La reflexion verticale correspond au conjugué.
- La translation de vecteur u d'affixe w correspond à l'addition de w.
- L'homothétie de rapport $k \in \mathbb{R}$ correspond à la multiplication par k.
- La rotation d'angle $\theta \in \mathbb{R}$ correspond à la multiplication par $e^{i\theta}$.

Définition 1.7.2 Une *similitude directe* est une transformation qui conserve les angles (orientés).

Cela signifie que si M, N, P distincts sont respectivement transformés en M', N', P', alors M', N', P' sont distincts et

$$\widehat{N'M'P'} = \widehat{NMP}.$$

Exemple 1. La translation de vecteur u est caractérisée par $\overrightarrow{MM'} = u$,

2. l'homothétie de centre Ω et de rapport $k \in \mathbb{R}$ est caractérisée par $\overrightarrow{\Omega M'} = k\overrightarrow{\Omega M}$,
3. la rotation de centre Ω et d'angle $\theta \in \mathbb{R}$ est caractérisée par $\widehat{M\Omega M'} = \theta$ et $\Omega M' = \Omega M$.

4. La réflexion par rapport à une droite Δ n'est pas une similitude directe (c'est une similitude indirecte).

Remarque 1. Une *similitude (directe ou indirecte)* est une transformation qui conserve les angles *géométriques* (en valeur absolue).
2. Une *isométrie* est une transformation qui conserve les distances (c'est automatiquement une similitude).
3. Les *similitudes fondamentales* sont les *translations*, les *rotations*, les *homothéties* (directes) et les *réflexions* (indirectes). À part les homothéties, ce sont toutes des isométries.
4. L'identité est une similitude (directe). Si on compose deux similitudes (directes), on obtient une similitude (directe). De même, la réciproque d'une similitude (directe) est aussi une similitude (directe). Même chose avec les isométries.

Lemme 1.7.3 Une transformation est une similitude si et seulement si elle conserve les proportions.

Cela signifie que les transformés M', N', P' de trois points distincts M, N, P sont aussi distincts et que

$$\frac{M'P'}{M'N'} = \frac{MP}{MN}.$$

Démonstration. En effet, les triangles (ordonnés) (M, N, P) et (M', N', P') ont les mêmes angles géométriques si et seulement si ils sont proportionnels [4]. Cela résulte de la règle des sinus :

$$\frac{\sin \widehat{M}}{NP} = \frac{\sin \widehat{N}}{MP} = \frac{\sin \widehat{P}}{MN}$$

(qui s'obtient aisément en considérant les hauteurs) et du fait que $\widehat{M}+\widehat{N}+\widehat{P} = \pi$. ■

Théoreme 1.7.4 Une transformation plane est une similitude directe si et seulement si il existe $\alpha, \beta \in \mathbb{C}$ avec $\alpha \neq 0$ tels que le point d'affixe z est transformé en le point d'affixe [a] $z' = \alpha z + \beta$.

a. Pour une similitude indirecte, c'est $z' = \alpha \overline{z} + \beta$.

Démonstration. On se donne trois points distincts M_1, M_2, M_3 d'affixes z_1, z_2, z_3 et on note M_1', M_2', M_3' leurs transformées d'affixes z_1', z_2', z_3'. C'est une similitude directe si et seulement si on a toujours

$$\arg\left(\frac{z_3' - z_1'}{z_2' - z_1'}\right) = \arg\left(\frac{z_3 - z_1}{z_2 - z_1}\right).$$

On aura aussi obligatoirement

$$\frac{|z_3' - z_1'|}{|z_2' - z_1'|} = \frac{|z_3 - z_1|}{|z_2 - z_1|}$$

4. On dit alors qu'ils sont *semblables*.

puisqu'une similitude conserve les proportions. La condition s'écrit donc (même module et même argument)

$$\frac{z'_3 - z'_1}{z'_2 - z'_1} = \frac{z_3 - z_1}{z_2 - z_1}.$$

Si la transformation est donnée par $z \mapsto z' := \alpha z + \beta$, on a bien

$$\frac{z'_3 - z'_1}{z'_2 - z'_1} = \frac{(\alpha z_3 + \beta) - (\alpha z_1 + \beta)}{(\alpha z_2 + \beta) - (\alpha z_1 + \beta)} = \frac{z_3 - z_1}{z_2 - z_1}.$$

Réciproquement, on considère les points d'affixes $0, 1, z$ et les affixes β, γ, z' de leurs transformés. La condition sur ces points s'écrit alors

$$\frac{z' - \beta}{\gamma - \beta} = \frac{z - 0}{1 - 0}.$$

En posant $\alpha = \gamma - \beta$, on trouve $z' = \alpha z + \beta$. ■

Exemple
1. $z' = z + 1$: c'est la translation de vecteur $u(1, 0)$.
2. $z' = 2z$: c'est l'homothétie de centre $O(0, 0)$ et de rapport 2.
3. $z' = iz$: c'est la rotation de centre $O(0, 0)$ et d'angle $\pi/2$.

Remarque
1. La translation de vecteur u est caractérisée par $M' = M + u$. Cela s'écrit encore $z' = z + \beta$ ou β est l'affixe de u.
2. L'homothétie de rapport k centrée en Ω est caractérisée par $\overrightarrow{\Omega M'} = k\overrightarrow{\Omega M}$. Cela s'écrit encore $z' - \omega = k(z - \omega)$ ou ω désigne l'affixe de Ω. On trouve donc $\alpha = k$ et $\beta = (1 - k)\omega$.
3. La rotation d'angle θ centrée en Ω est caractérisée par $\Omega M' = \Omega M$ et $\widehat{M\Omega M'} = \theta$. Cela s'écrit encore $|z' - \omega| = |z - \omega|$, c'est à dire $\left|\frac{z'-\omega}{z-\omega}\right| = 1$, et $\arg\left(\frac{z'-\omega}{z-\omega}\right) = \theta$. C'est équivalent à $\frac{z'-\omega}{z-\omega} = e^{i\theta}$ ou encore $z' - \omega = e^{i\theta}(z - \omega)$. On trouve donc $\alpha = k$ et $\beta = (1 - e^{i\theta})\omega$.

Proposition 1.7.5 On considère une similitude directe donnée par $z \mapsto \alpha z + \beta$ avec $\alpha \neq 0$.
1. Si $\alpha = 1$, on trouve la translation de vecteur u d'affixe β.
2. Sinon, le point Ω d'affixe $\omega := \beta/(1 - \alpha)$ est l'unique point fixe et la similitude est composée de la rotation de centre Ω et d'angle $\theta = \arg(\alpha)$ avec l'homothétie de même centre Ω et de rapport $k := |\alpha|$.

Démonstration. Si $\alpha \neq 1$, l'équation $z = \alpha z + \beta$ est équivalente à $z = \beta/(1 - \alpha)$, ce qui montre que le point Ω d'affixe $\omega := \beta/(1 - \alpha)$ est l'unique point fixe. Si le point M d'affixe z est transformé en le point M' d'affixe z', on aura

$$z' - \omega = \alpha z + \beta - \omega = \alpha(z - \omega) = ke^{i\theta}(z - \omega).$$

Il s'agit donc bien de composer l'homothétie de rapport k et la rotation d'angle θ centrées en Ω. ■

Remarque
- L'ordre de la composition n'a pas d'importance.
- On trouve une rotation si et seulement si $|\alpha| = 1$ (et $\alpha \neq 1$ ou $\beta = 0$).
- On trouve une homothétie si et seulement si $\alpha \in \mathbb{R}$ (et $\alpha \neq 0$).

Exemple
1. Avec $z' = \frac{i}{2}z + 2 - i$, on trouve $\Omega = (2, 0)$, $k = 1/2$ et $\theta = \pi/2$.
2. Avec
$$z' = \frac{3 + i\sqrt{3}}{4}z + \frac{1 - i\sqrt{3}}{2},$$
on trouve $\Omega = (2, 0)$, $k = \sqrt{3}/2$ et $\theta = \pi/6$.

Proposition 1.7.6 Étant donné une similitude directe, il existe un unique réel strictement positif k (resp. un unique réel $\theta \mod 2\pi$) tel que, si deux points distincts M, N sont transformés en M', N', alors
$$\frac{M'N'}{MN} = k \quad \left(\text{resp. } (\overrightarrow{MN}, \overrightarrow{M'N'}) \equiv \theta \mod 2\pi\right).$$
Si ce n'est pas une translation, alors il existe un unique point fixe Ω.

Démonstration. Si on désigne par z, w les affixes de M et N, alors les affixes de M' et N' s'écrivent respectivement $z' = \alpha z + \beta$ et $w' = \alpha w + \beta$. On aura alors
$$\frac{w' - z'}{w - z} = \frac{(\alpha w + \beta) - (\alpha z + \beta)}{w - z} = \alpha.$$
On voit donc que $\theta = \arg(\alpha)$ et $k = |\alpha|$. ■

Définition 1.7.7 On dit que θ est l'*angle*, que k est le *rapport* et que Ω est le *centre* de la similitude. Ce sont les *invariants géométriques* de la similitude.

Remarques
1. Si la similitude est une translation de vecteur u, on remplace le centre Ω par u dans les invariants géométriques (on aura donc 1, 0 et u).
2. Le rapport d'homothétie est un réel quelconque mais le rapport de similitude est un réel positif. Cela signifie qu'une similitude de rapport $k > 0$ et d'angle $\theta \in \mathbb{R}$ est une homothétie lorsque $\theta \equiv 0 \mod \pi$.
3. L'identité est à la fois une translation, une homothétie et une rotation.
4. Une symétrie centrale est à la fois une rotation d'angle π et une homothétie de rapport -1.

Proposition 1.7.8 La composée de deux similitudes directes de rapports respectifs k et k' et d'angles respectifs θ et θ' est une similitude directe de rapport kk' et d'angle $\theta + \theta'$.

Démonstration. On compose $z \mapsto z' = \alpha z + \beta$ avec $z' \mapsto z'' = \alpha' z' + \beta'$. On aura donc

$$z'' = \alpha'(\alpha z + \beta) + \beta' = (\alpha\alpha')z + (\beta\alpha' + \beta').$$

On a bien $|\alpha\alpha'| = kk'$ et $\arg(\alpha\alpha') = \theta + \theta'$. ■

Proposition 1.7.9 Étant donnnés quatre points M, N, M', N' avec $M \neq N$ et $M' \neq N'$, il existe une unique similitude directe qui transforme M en M' et N en N'.

Démonstration. On désigne par z, w, z', z' les affixes respectifs de M, N, M', N'. On doit donc résoudre

$$\alpha, \beta \in \mathbb{C}, \quad \begin{cases} z' = \alpha z + \beta \\ w' = \alpha w + \beta \end{cases}$$

(avec $\alpha \neq 0$). Et on trouve

$$\alpha = \frac{z' - w'}{z - w} \quad \text{et} \quad \beta = \frac{zw' - wz'}{z - w}.$$ ■

Exemple

1. Il existe une unique similitude directe qui échange deux points M et N, c'est la symétrie centrée au milieu I de $\{M, N\}$.
2. Il existe une unique similitude directe centrée en un point Ω qui transforme un point donné $M \neq \Omega$ en un point fixé $N \neq \Omega$.

1.8 Exercices (7 juillet 2025)

Exercice 1.1 Représenter les points M_k d'affixes z_k pour $k = 1, \dots, 5$ avec

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

Exercice 1.2 Montrer que les diagonales d'un parallélogramme se coupent en leur milieu.

Exercice 1.3 Déterminer les formes algébriques de :

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

Exercice 1.4 Résoudre les équations suivantes :

1. $z + 2i = iz - 1$,
2. $(3+2i)(z-1) = i$,
3. $(2-i)z + 1 = (3+2i)z - i$,
4. $(4-2i)z^2 = (1+5i)z$.

Exercice 1.5 Déterminer l'ensemble des points M d'affixe z tels que les points d'affixes z, z^2, z^4 sont alignés ?

Exercice 1.6 On considère le nombre complexe $z = \dfrac{1}{2} + i\dfrac{\sqrt{3}}{2}$.

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

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

Exercice 1.7 Montrer que si $z \in \mathbb{C}$ satisfait $|1 + iz| = |1 - iz|$, alors $z \in \mathbb{R}$.

Exercice 1.8

1. Montrer que

$$\forall z, w \in \mathbb{C}, \quad |z + w|^2 + |z - w|^2 = 2(|z|^2 + |w|^2).$$

2. En déduire que, dans un parallélogramme, la somme des carrés des cotés est égale à la somme des carrés des diagonales [a].

a. Si z_1, z_2, z_3, z_4 désignent les affixes des sommets, on pourra poser $z = z_2 - z_1$ et $w = z_4 - z_1$.

Exercice 1.9 Calculer $\sum_{k=0}^{7} (1+i)^k$.

Exercice 1.10 Soit $z \in \mathbb{C}$. Calculer $S_n := \sum_{k=0}^{n} kz^k$ en développant $(1-z)S_n$.

Exercice 1.11 On pose $z = 2e^{i\pi/4}$. Déterminer les formes exponentielles de $\overline{z}$, z^{-1}, $-z$ et iz. et les représenter tous ces nombres dans le plan complexe.

Exercice 1.12 Donner la forme exponentielle des nombres complexes suivants :

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

Exercice 1.13 Utiliser les formules d'Euler pour linéariser les expressions suivantes :

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

Exercice 1.14 Montrer que $e^{i\frac{\pi}{12}} = \dfrac{e^{i\frac{\pi}{3}}}{e^{i\frac{\pi}{4}}}$. En déduire les valeurs de $\cos(\pi/12)$ et $\sin(\pi/12)$.

Exercice 1.15 Déterminer la forme exponentielle des nombres suivants :

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

Exercice 1.16 Déterminer la forme exponentielle de

1. $z = 1 + e^{ia}$ avec $|a| \leq \pi$,
2. $z = e^{ia} + e^{ib}$ avec $|b - a| \leq \pi$.

Exercice 1.17

1. Montrer que si $x \not\equiv 0 \mod 2\pi$, alors

$$\sum_{k=0}^{n} e^{ikx} = \frac{\sin\left(\frac{(n+1)x}{2}\right)}{\sin\left(\frac{x}{2}\right)} e^{i\frac{nx}{2}}.$$

2. En déduire $\sum_{k=0}^{n} \cos(kx)$ et $\sum_{k=0}^{n} \sin(kx)$.

Exercice 1.18 Représenter dans le plan complexe l'ensemble des points M dont l'affixe z vérifie la condition suivante :

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

Exercice 1.19

1. Montrer que si $a, b \in \mathbb{R}$ avec $a > 0$, alors

$$\arg(a + ib) \equiv \arctan(b/a) \mod 2\pi.$$

2. Calculer $z := (1+i)(1+2i)(1+3i)$.
3. En déduire que $\arctan(1) + \arctan(2) + \arctan(3) = \pi$.

Exercice 1.20 Déterminer les racines carrées des nombres complexes suivants :

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

Exercice 1.21 Résoudre dans $\mathbb{C}$ les équations suivantes

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

Exercice 1.22 Montrer que si $s, p, z_1, z_2 \in \mathbb{C}$, alors z_1 et z_2 sont les solutions de l'équation $z^2 - sz + p = 0$ si et seulement si $z_1 + z_2 = s$ et $z_1 z_2 = p$.

Exercice 1.23 Déterminer les racines n-èmes de z dans les cas suivants :

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

Exercice 1.24 On désigne par $\mathbb{Z}[i]$ l'ensemble des *entiers de Gauss*, c'est-à-dire les nombres qui s'écrivent $m + in$ avec $m, n \in \mathbb{Z}$.

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

Exercice 1.25

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

Exercice 1.26 Déterminer les invariants géométriques de la similitude donnée par :

1. $z' = z + 3 - i$,
2. $z' = 2z + 3$,
3. $z' = iz + 1$,
4. $z' = (1-i)z + 2 + i$.

Exercice 1.27 1. Déterminer les invariants géométriques de la similitude donnée par

$$z' = \frac{3+i\sqrt{3}}{4}z + \frac{1-i\sqrt{3}}{2}.$$

2. Montrer que si Ω désigne son centre et que M est transformé en M', alors le triangle $\{\Omega, M, M'\}$ est rectangle en M'.

Exercice 1.28 Déterminer la forme complexe de la similitude directe de centre Ω, d'angle θ et de rapport k :

1. $\Omega(1,1)$, $\theta = \pi/2$ et $k = 2$,
2. $\Omega(0,0)$, $\theta = \pi/3$ et $k = \sqrt{3}$,
3. $\Omega(1,-2)$, $\theta = \pi/4$ et $k = 2\sqrt{2}$.

Exercice 1.29 Déterminer les invariants géométriques de la similitude directe

1. qui transforme $M(1,0)$ en $M'(1,1)$ et $N(0,2)$ en $N'(-3,-1)$,
2. qui transforme $M(5,-4)$ en $M'(-1,-4)$ et M' en $M''(-4,-1)$,
3. de centre $O(0,0)$ qui transforme $M(-\sqrt{2},\sqrt{2})$ en $M'(-2\sqrt{3},-2)$.

Exercice 1.30 1. Montrer que la composée d'une homothétie et d'une translation est une homothétie ou une translation.

2. Montrer que la composée d'une rotation et d'une translation est une rotation ou une translation.
3. Montrer que la composée de deux homothéties est une homothétie ou une translation.
4. Montrer que la composée de deux rotations est une rotation ou une translation.

Exercice 1.31 Déterminer les formes complexes des transformations planes suivantes :

1. La translation de vecteur $(1,-1)$.
2. L'homothétie de centre $(1,-1)$ et de rapport 2.
3. La symétrie de centre $(0,0)$.
4. La symétrie de centre $(1,-1)$.
5. La rotation de centre $(0,0)$ et d'angle $\pi/2$.
6. La rotation de centre $(1,-1)$ et d'angle $\pi/2$.
7. La reflexion verticale par rapport à la droite $y = 0$.
8. La reflexion verticale par rapport à la droite $y = -1$.
9. La reflexion horizontale par rapport à la droite $x = 0$.
10. La reflexion horizontale par rapport à la droite $x = 1$.

2. Logique et ensembles

Nous avons ici une approche extrêmement naïve de la logique mathématique qui vise seulement à inculquer les principes de base et présenter la mécanique sous-jacente au raisonnement. Nous aurons aussi une vision concrète de la notion d'ensemble et ne traiterons pas du tout de la Théorie des ensembles proprement dite qui permet d'interpréter tous les objets mathématiques comme étant eux-même des ensembles. Pour une approche plus sérieuse, nous renvoyons par exemple vers [Kri07] ou [Bou70].

2.1 Opérateurs logiques

Définition 2.1.1 Un *théorème* est un énoncé mathématique dont on sait qu'il est vrai [a]. Une *proposition* est un énoncé mathématique qui peut être vrai (ou faux sinon) selon les valeurs des variables éventuelles [b].

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

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

Exemple

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

Remarque

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

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

Définition 2.1.2 Une *démonstration* consiste à décider [a] si une proposition (qui ne dépend pas des variables) est un théorème.

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

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

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

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

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

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

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

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

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

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

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

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

alors

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

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

Définition 2.1.3 La *logique*[a] consiste à déterminer la vérité d'une proposition en fonction de la vérité des propositions qui la composent.

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

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

Définition 2.1.4

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

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

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

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

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

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

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

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

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

par la table de vérité suivante :

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

Exemple La proposition "$2 > 3$" est fausse et la proposition "$1 < 4$" est vraie, donc

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

Remarque

- La nature statique des connecteurs logiques contraste avec la nature dynamique des démonstrations :
  1. Pour montrer que $\mathcal{P}$ est fausse, on montre que "non $\mathcal{P}$" est vraie.
  2. Pour montrer que "$\mathcal{P}$ et $\mathcal{Q}$" est vraie, on montrer successivement que $\mathcal{P}$ est vraie puis que $\mathcal{Q}$ est vraie.
  3. Pour montrer que "$\mathcal{P}$ ou $\mathcal{Q}$" est vraie, on suppose que $\mathcal{P}$ est fausse et on montre que $\mathcal{Q}$ est vraie.
  4. Pour montrer que "$\mathcal{P} \Rightarrow \mathcal{Q}$" est vraie, on suppose que $\mathcal{P}$ est vraie et on montre que $\mathcal{Q}$ est vraie.
  5. Pour montrer que "$\mathcal{P} \Leftrightarrow \mathcal{Q}$" est vraie, on montre que $\mathcal{P}$ est vraie si et seulement si $\mathcal{Q}$ est vraie.
- En logique pure, on utilise plutôt les symboles $\neg$, $\wedge$, $\vee$, $\rightarrow$ et $\leftrightarrow$.
- Convention pour l'utilisation des parenthèses dans les formules :

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

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

Proposition 2.1.5 Si $\mathcal{P}$, $\mathcal{Q}$ et $\mathcal{R}$ sont des propositions, on a

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

8. $\mathcal{P}$ et ($\mathcal{Q}$ ou $\mathcal{R}$) $\Leftrightarrow$ ($\mathcal{P}$ et $\mathcal{Q}$) ou ($\mathcal{P}$ et $\mathcal{R}$),
9. $\mathcal{P}$ ou ($\mathcal{Q}$ et $\mathcal{R}$) $\Leftrightarrow$ ($\mathcal{P}$ ou $\mathcal{Q}$) et ($\mathcal{P}$ ou $\mathcal{R}$),
10. ($\mathcal{P} \Rightarrow \mathcal{Q}$) $\Leftrightarrow$ non $\mathcal{P}$ ou $\mathcal{Q}$,
11. non($\mathcal{P} \Rightarrow \mathcal{Q}$) $\Leftrightarrow$ $\mathcal{P}$ et non $\mathcal{Q}$ (*),
12. ($\mathcal{P} \Rightarrow \mathcal{Q}$) $\Leftrightarrow$ (non $\mathcal{Q} \Rightarrow$ non $\mathcal{P}$),
13. ($\mathcal{P} \Leftrightarrow \mathcal{Q}$) $\Leftrightarrow$ ($\mathcal{Q} \Leftrightarrow \mathcal{P}$),
14. ($\mathcal{P} \Leftrightarrow \mathcal{Q}$) $\Leftrightarrow$ (($\mathcal{P} \Rightarrow \mathcal{Q}$) et ($\mathcal{Q} \Rightarrow \mathcal{P}$)),
15. ($\mathcal{P} \Leftrightarrow \mathcal{Q}$) $\Leftrightarrow$ (non $\mathcal{P} \Leftrightarrow$ non $\mathcal{Q}$).

Démonstration. Il suffit d'élaborer les tables de vérité. Montrons par exemple la tautologie numérotée 11) :

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

Les autres sont laissées en exercice. ■

Remarque
- La *règle du tiers exclu* est la tautologie "$\mathcal{P}$ ou non $\mathcal{P}$" (à laquelle il faut rajouter le principe de non-contradiction "non($\mathcal{P}$ et non $\mathcal{P}$)").
- La *règle d'inférence* est la tautologie "$\mathcal{P}$ et ($\mathcal{P} \Rightarrow \mathcal{Q}$) $\Rightarrow \mathcal{Q}$".
- Le *raisonnement par l'absurde* est la tautologie "non non $\mathcal{P} \Rightarrow \mathcal{P}$".
- La *disjonction des cas* est la tautologie "($\mathcal{P} \Rightarrow \mathcal{Q}$) et (non $\mathcal{P} \Rightarrow \mathcal{Q}$) $\Rightarrow \mathcal{Q}$".

Exemple On veut montrer par disjonction des cas que pour tout entier naturel n, $n^2 + n$ est pair. On a $n^2 + 1 = n(n + 1)$. Si n est pair, c'est gagné. Sinon, c'est $n + 1$ qui est pair et on gagne aussi.

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

Exemple 1. La contraposée de l'implication "$n < 2 \Rightarrow n \leq 3$" est l'implication "$n > 3 \Rightarrow n \geq 2$" (qui est *aussi* vraie - attention, il faut un quantificateur pour dire ça).

2. La réciproque de l'implication "$n < 2 \Rightarrow n \leq 3$" est l'implication "$n \leq 3 \Rightarrow n < 2$" (qui elle est *fausse*).
3. La négation de l'implication "$n < 2 \Rightarrow n \leq 3$" est "$n < 2$ et $n > 3$" (qui est bien sûr fausse).
4. Il *suffit* que $n < 2$ pour que $n \leq 3$ et il est *nécessaire* que $n \leq 3$ pour que $n < 2$.
5. Pour que $n > 2$, il est nécessaire et suffisant que $n \geq 3$.

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

2.2 Quantificateurs

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

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

Définition 2.2.1 Si $\mathcal{P}$ est une proposition, alors

1. la proposition "$\forall x\ \mathcal{P}(x)$" est vraie si la proposition $\mathcal{P}(x)$ est toujours vraie (quelle que soit la valeur de x),
2. la proposition "$\exists x\ \mathcal{P}(x)$" est vraie si la proposition $\mathcal{P}(x)$ est parfois vraie (pour au moins une valeur de x).

Remarque

- Pour que cette définition en soit effectivement une (c'est-à-dire qu'elle introduit du nouveau vocabulaire), il faut mentionner que $\forall$ est le *quantificateur universel* et que $\exists$ est le *quantificateur existentiel*.
- Ne pas confondre la proposition "$\forall x\ \mathcal{P}(x)$" qui ne dépend *pas* de x (et idem avec $\exists$) et la proposition $\mathcal{P}(x)$, qui elle dépend de x (on dira parfois *propriété* au lieu de proposition pour insister sur ce fait).
- Il est parfois pratique [1] d'écrire "$\exists! x\ \mathcal{P}(x)$" pour exprimer qu'il existe un *unique* x qui satisfait la propriété $\mathcal{P}$. Cela signifie donc que

$$\exists x \left(\mathcal{P}(x) \text{ et } (\forall y\ \mathcal{P}(y) \Rightarrow y = x)\right).$$

1. Attention, ce n'est pas un quantificateur.

Proposition 2.2.2 Si $\mathcal{P}$ est une proposition, alors

1. non $(\forall x\ \mathcal{P}(x)) \Leftrightarrow (\exists x$ non $\mathcal{P}(x))$ et
2. non $(\exists x\ \mathcal{P}(x)) \Leftrightarrow (\forall x$ non $\mathcal{P}(x))$.

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

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

■

Remarques

1. En anticipant sur la section suivante, on écrira
   (a) "$\forall x \in E, \mathcal{P}(x)$" au lieu de "$\forall x\ x \in E \Rightarrow \mathcal{P}(x)$" et
   (b) "$\exists x \in E, \mathcal{P}(x)$" au lieu de "$\exists x\ x \in E$ et $\mathcal{P}(x)$".
2. On écrira parfois [2] $\forall x, y \in E$ au lieu de $\forall x \in E, \forall y \in E$ et idem avec $\exists$.
3. On aura donc
   (a) non $(\forall x \in E, \mathcal{P}(x)) \Leftrightarrow (\exists x \in E,$ non $\mathcal{P}(x))$,
   (b) non $(\exists x \in E, \mathcal{P}(x)) \Leftrightarrow (\forall x \in E,$ non $\mathcal{P}(x))$.

Exemple La négation de

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

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

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

Pour montrer que la fonction

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

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

On peut aussi considérer les fonctions

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

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

On conclut avec le raisonnement par récurrence :

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

Théoreme 2.2.3 Si $\mathcal{P}$ est une proposition qui dépend de $n \in \mathbb{N}$, alors

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

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

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

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

Remarque

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

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

$$(\forall n \in \mathbb{N}, \mathcal{P}(n)) \Leftrightarrow (\forall n \in \mathbb{N}, ((\forall m \in \mathbb{N}, m < n \Rightarrow \mathcal{P}(m)) \Rightarrow \mathcal{P}(n)).$$

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

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

Exemple

1. On veut montrer par récurrence que $n^2 + n$ est toujours pair, c'est à dire que $\forall n \in \mathbb{N}, \exists k \in \mathbb{N}, n^2 + n = 2k$. On a bien $0^2 + 0 = 2 \times 0$. Soit $n \in \mathbb{N}$. Soit $k \in \mathbb{N}$ tel que $n^2 + n = 2k$. (Posons $l = k + n + 1$). On a alors

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

2. On veut montrer que $100! \geq 2^{100}$. On va montrer en fait par récurrence sur l'entier naturel $n \geq 4$ que $n! \geq 2^n$. On a $4! = 24 \geq 16 = 2^4$ et si $n \geq 4$ est un entier naturel qui satisfait $n! \geq 2^n$, on aura bien

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

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

3. On veut montrer par récurrence descendante que $\sqrt{2}$ est irrationnel. Soit $n \in \mathbb{N}$ tel que $\sqrt{2} = n/m$ avec $m \in \mathbb{N}$. Alors, $n^2 = 2m^2$ et donc n est pair (et non nul) si bien que $n = 2p$ avec $p < n$. On a alors $m^2 = 2p^2$ si bien que m aussi est pair et donc $m = 2q$. On a ainsi $\sqrt{2} = p/q$ avec $p < n$.

2.3 Ensembles

Définition 2.3.1 Un *ensemble*[a] E est une « collection d'objets » x appelés les *éléments* de E. On dit alors que x *appartient* à E et on écrit $x \in E$. Sinon, on écrit $x \notin E$.

a. Ce que nous définissons ici est en fait la relation d'appartenance.

Remarque
- Deux ensembles sont égaux si et seulement si ils ont les mêmes éléments[3] : $E = F \Leftrightarrow (\forall x, x \in E \Leftrightarrow x \in F)$.
- On peut décrire un ensemble :
  1. en *extension* : en donnant une liste de ses éléments,
  2. en *compréhension* : en donnant une propriété qui les caractérise.
- Passer d'une écriture en compréhension à une écriture en extension (trouver la solution à un problème) ou le contraire (modéliser un problème) forment les deux défis principaux à relever en mathématiques.
- On représente généralement les ensembles à l'aide de *diagrammes de Venn*, appelés aussi communément des *patates*.

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

Définition 2.3.2 Un ensemble E est *contenu* (ou *inclus*) dans un ensemble F si tout élément de E est aussi un élément de F. On écrit alors $E \subset F$ et on dit aussi que E est une *partie* ou un *sous-ensemble* de F. Sinon, on écrit $E \not\subset F$.

Remarque
- On a donc

$$E \subset F \Leftrightarrow (\forall x \ x \in E \Rightarrow x \in F).$$

3. Attention : la collection de tous les ensembles n'est pas un ensemble (paradoxe de Russel).

- On a toujours $\emptyset \subset E$.
- On écrit aussi $E \subsetneq F$ pour $E \subset F$ et $E \neq F$.
- Ne pas confondre $\in$ et $\subset$. Ne pas confondre $\not\subset$ et $\subsetneq$.

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

Proposition 2.3.3 Si E, F et G sont trois ensembles, alors
1. $E \subset E$,
2. $E \subset F$ et $F \subset G \Rightarrow E \subset G$,
3. $E \subset F$ et $F \subset E \Leftrightarrow E = F$.

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

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

Exemple Pour montrer que les ensembles $E := \{x \in \mathbb{R} \ / \ x^2 = 1\}$ et $F := \{1, -1\}$ sont égaux, on montre :
1. que $E \subset F$ (analyse) : si $x^2 = 1$, alors $(x-1)(x+1) = x^2 - 1 = 0$ si bien que $x - 1 = 0$ ou $x + 1 = 0$ et donc $x = 1$ ou $x = -1$,
2. puis que $F \subset E$ (synthèse) : on a $1^2 = 1$ et $(-1)^2 = 1$.

2.4 Opérations sur les ensembles

Définition 2.4.1 Soient E et F deux ensembles. Alors,
1. leur *intersection* est l'ensemble $E \cap F$ des éléments qui sont à la fois dans E et dans F,
2. leur *union* est l'ensemble $E \cup F$ des éléments qui sont soit dans E ou dans F (ou dans les deux).

Remarque • On a donc

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

et

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

- On a bien sûr

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

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

Proposition 2.4.2 Si E, F et G sont des ensembles, alors

1. $E \cap \emptyset = \emptyset$,
2. $E \cap E = E$,
3. $E \cap F = F \cap E$,
4. $(E \cap F) \cap G = E \cap (F \cap G)$,
5. $E \cup \emptyset = E$,
6. $E \cup E = E$,
7. $E \cup F = F \cup E$,
8. $(E \cup F) \cup G = E \cup (F \cup G)$,
9. $E \cap (F \cup G) = (E \cap F) \cup (E \cap G)$,
10. $E \cup (F \cap G) = (E \cup F) \cap (E \cup G)$.

Démonstration. Tous ces résultats sont conséquences immédiates de tautologies. Il suffit de désigner respectivement par $\mathcal{P}$, $\mathcal{Q}$ et $\mathcal{R}$ les conditions $x \in E$, $x \in F$ et $x \in G$. L'assertion 9 par exemple résulte alors de

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

En effet, le membre de droite s'écrit à $x \in E \cap (F \cup G)$ et celui de gauche : $x \in (E \cap F) \cup (E \cap G)$. Les autres assertions sont laissées en exercice. ■

Remarque

- On écrira $E \cap F \cap G$ et $E \cup F \cup G$ sans les parenthèses puisqu'il n'y a pas d'ambiguïté.
- On dit que E et F sont *disjoints* si $E \cap F = \emptyset$.
- On définit aussi leur *différence* comme étant l'ensemble $E \setminus F$ des éléments qui sont dans E mais pas dans F (on réservera en pratique cette notation au cas $F \subset E$).
- On considère aussi parfois la *différence symétrique*

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

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

Définition 2.4.3 Si A est une partie d'un ensemble E, son *complémentaire* dans E est l'ensemble

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

des éléments qui sont dans E mais pas dans A.

Remarque

- On a donc

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

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

Exemple 1. Si $E = \{1, 2\}$ et $A = \{1\}$, alors $A^{\mathrm{c}} = \{2\}$.

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

Proposition 2.4.4 1. Si A est une partie d'un ensemble E, on a $(A^c)^c = A$,

2. Si A et B sont deux parties d'un ensemble E, alors

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

3. Si A et B sont deux parties d'un ensemble E, alors (lois de De Morgan)

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

Démonstration. Conséquences immédiates de tautologies en désignant respectivement par $\mathcal{P}$ et $\mathcal{Q}$ les conditions $x \in A$ et $x \in B$ (détails en exercice). ■

Définition 2.4.5 Le *produit (cartésien)* de deux ensembles E et F est l'ensemble $E \times F$ des *couples*[a] (x, y) avec $x \in E$ et $y \in F$.

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

Remarque

- On a donc[4] $(x, y) \in E \times F \Leftrightarrow x \in E$ et $y \in F$.
- On a $(x, y) = (x', y') \Leftrightarrow x = x'$ et $y = y'$.
- Ne pas confondre paire et couple : on a $(1, 2) \neq (2, 1)$ et $(1, 1)$ est bien un couple.
- On a $E \times F \neq F \times E$ sauf s'ils sont égaux ou si l'un des deux est vide : $E \times \emptyset = \emptyset \times F = \emptyset$.
- On peut aussi considérer l'ensemble $E \times F \times G$ des triplets si G est un autre ensemble (et au delà).

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

2. $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$.
3. On dispose de l'axe des abscisses

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

et de l'axe des ordonnées

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

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

4. Ne pas confondre avec $x \in E \cap F \Leftrightarrow x \in E$ et $x \in F$.

2.5 Applications

Définition 2.5.1 Une *application*[a] $f : E \to F$ est une méthode qui permet d'associer à *tout* élément x de E *un* élément $f(x)$ de F. On dit que E est la *source* ou l'*ensemble de départ* de f et que F le *but* ou l'*ensemble d'arrivée*. On dit que $f(x)$ est l'*image* de x et que x est un *antécédent* de $f(x)$. Au lieu de $y = f(x)$, on écrira aussi $f : x \mapsto y$ (ne pas confondre avec $f : E \to F$).

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

Exemple 1. On peut définir une application

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

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

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

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

- Le *graphe* d'une application f est l'ensemble $\{(x, f(x)) : x \in E\} \subset E \times F$. Une fois fixés E et F, il revient au même de se donner f ou son graphe.
- Ne pas confondre une application avec une *fonction* qui associe à *certains* éléments de E un élément de F (on rencontre aussi des fonctions *multivaluées* qui peuvent associer *plusieurs* éléments de F au même élément de E).
- Au lieu d'écrire $f(x)$, on devrait écrire $x.f$ comme font les informaticiens pour indiquer que la variable x subit la méthode f.

Définition 2.5.2 Une application $f : E \to F$ est

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

Remarque • Le fait qu'une application soit injective, surjective ou bijective dépend de E et de F et pas seulement de la méthode pour déduire $f(x)$ de x.

- L'injectivité dit que deux éléments distincts ne peuvent pas avoir la même image,
- la surjectivité dit que tout élément du but a au moins un antécédent,

- la bijectivité dit que tout élément du but a exactement un antécédent (voir ci-dessous).

Exemple
1. L'application $\exp : \mathbb{R} \to \mathbb{R}$ est injective mais pas surjective,
2. L'application $\mathbb{R} \to \mathbb{R}, x \mapsto x^3 - x$ est surjective mais pas injective,
3. L'application $\mathbb{R} \to \mathbb{R}, x \mapsto x^3$ est bijective,
4. L'application $\mathbb{R} \to \mathbb{R}, x \mapsto x^2$ n'est ni injective, ni surjective,
5. L'application $\mathbb{R}_{\geq 0} \to \mathbb{R}, x \mapsto x^2$ est injective (pas surjective) et l'application $\mathbb{R} \to \mathbb{R}_{\geq 0}, x \mapsto x^2$ est surjective (pas injective).

Proposition 2.5.3 Une application $f : E \to F$ est bijective si et seulement si pour tout $y \in F$, il existe un unique $x \in E$ tel que $f(x) = y$.

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

Définition 2.5.4 Si f est bijective, alors l'application $f^{-1} : F \to E$ qui envoie $y \in F$ sur son unique antécédent $x \in E$ par l'application f est l'*application réciproque* de F.

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

Remarque
- Si f est bijective, on a

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

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

2.6 Composition

Définition 2.6.1 Si $f : E \to F$ et $g : F \to G$, sont deux applications, leur *composée* est l'application $g \circ f : E \to G$ définie par

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

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

- Si $E \subset F$, la *restriction* à E de $g : F \to G$ est la composée

$$g_{|E} = g \circ f : E \overset{f}{\hookrightarrow} F \overset{g}{\to} G.$$

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

Exemple 1. Considérons

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

et

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

On aura alors

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

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

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

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

Proposition 2.6.2 1. Si $f : E \to F$ est une application, on a

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

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

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

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

$$(h \circ (g \circ f))(x) = h(g(f(x))) = ((h \circ g) \circ f)(x). \qquad \blacksquare$$

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

Proposition 2.6.3 La composée de deux applications injectives (resp. surjectives, resp. bijectives) l'est aussi.

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

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

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

Exemple Les applications

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

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

Proposition 2.6.4 Une application $f : E \to F$ est bijective si et seulement s'il existe une application $g : F \to E$ telle que $g \circ f = \mathrm{Id}_E$ et $f \circ g = \mathrm{Id}_F$. On a alors $g = f^{-1}$.

Démonstration. Montrons tout d'abord que l'on aura nécessairement $g = f^{-1}$. En effet, si $y \in F$, on aura $f(g(y)) = (f \circ g)(y) = y$ et donc (par définition de f^{-1}) $g(y) = f^{-1}(y)$. Supposons maintenant que f est bijective. Si $x \in E$, on a $f(x) = f(x)$ et donc $f^{-1}(f(x)) = x$ si bien que $f^{-1} \circ f = \mathrm{Id}_E$. De même, si $y \in F$, on a $f^{-1}(y) = f^{-1}(y)$ et donc $f(f^{-1}(y)) = y$ is bien que $f \circ f^{-1} = \mathrm{Id}_F$. Réciproquement, supposons l'existence de g. Si $y \in F$ et qu'on pose $x = g(y)$, on aura $f(x) = f(g(y)) = y$, ce qui montre que f est surjective. Et si $x, x' \in E$ satisfont $f(x) = f(x')$, on aura $x = g(f(x)) = g(f(x')) = x'$ et f est aussi injective. ■

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

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

Proposition 2.6.5
1. Si $f : E \to F$ est bijective, alors f^{-1} aussi et $(f^{-1})^{-1} = f$,
2. si $f : E \to F$ et $g : F \to G$ sont bijectives, alors $(g \circ f$ aussi et on a) $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

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

2. En effet, on aura bien

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

ainsi que

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

Exemple 1. Puisque $\mathbb{R} \to \mathbb{R}, x \mapsto x^3$ est bijective de réciproque $\mathbb{R} \to \mathbb{R}, x \mapsto \sqrt[3]{x}$, alors $\mathbb{R} \to \mathbb{R}, x \mapsto \sqrt[3]{x}$ est bijective de réciproque $\mathbb{R} \to \mathbb{R}, x \mapsto x^3$.

2. Puisque $\ln : \mathbb{R}_{>0} \to \mathbb{R}$ est bijective de réciproque $\exp : \mathbb{R} \to \mathbb{R}_{>0}$, alors $\exp : \mathbb{R} \to \mathbb{R}_{>0}$ est bijective de réciproque $\ln : \mathbb{R}_{>0} \to \mathbb{R}$. Mais attention, $\exp : \mathbb{R} \to \mathbb{R}$ n'est *pas* bijective.

3. L'application $\mathbb{R}_{>0} \to \mathbb{R}, x \mapsto (\ln x)^3$ est bijective de réciproque $\mathbb{R} \to \mathbb{R}_{>0}, x \mapsto e^{\sqrt[3]{x}}$

2.7 Exercices (7 juillet 2025)

Exercice 2.1 Les propositions suivantes sont elles des tautologies ?

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

Exercice 2.2 Parmi les propositions suivantes, quelle est la négation de "$\mathcal{P} \Rightarrow \mathcal{Q}$" ?

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

Exercice 2.3

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

Exercice 2.4 Parmi les assertions suivantes relatives à une application $f : \mathbb{R} \to \mathbb{R}$, quelle est la contraposée de "f croissante $\Rightarrow f(3) \geq f(2)$" ?

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

Exercice 2.5 La proposition $\forall x \in \mathbb{R}, x > 1 \Rightarrow x^2 > 1$ est elle vraie ? Qu'en est-il des propositions

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

Exercice 2.6 Pour chacune des formules suivantes, expliciter sa négation et décider (démonstration) si cela a un sens de leur validité respective :

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

Exercice 2.7 If M is an absolute ∇-module on R, then both

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

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

Exercice 2.8 Montrer par contraposition les propriétés suivantes :

1. “Un entier naturel dont le carré est pair est automatiquement pair lui même”,
2. “Un nombre réel dont le carré vaut deux est toujours strictement inférieur à deux”.

Exercice 2.9 Montrer par l'absurde les assertions suivantes :

1. “Zéro est le seul réel positif qui est inférieur à tout réel strictement positif”,
2. “La racine carrée de deux n'est pas un nombre entier”.

Exercice 2.10 On considère la propriété $\mathcal{P}$:=“$2^n > n^2$”.

1. Montrer que pour tout entier $n \geq 3$, on a $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$.
2. Pour quelles valeurs de l'entier naturel n a-t-on $\mathcal{P}(n)$?

Exercice 2.11

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

Exercice 2.12 Montrer par récurrence que pour tout réel positif x et pour tout entier naturel n, on a $(1+x)^n \geq 1 + nx$.

Exercice 2.13 Montrer par récurrence que les formules suivantes sont valides pour tout entier naturel n (non nul en ce qui concerne la dernière) :

1. $\displaystyle\sum_{k=0}^{n}(2k+1) = (n+1)^2$,
2. $\displaystyle\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$,
3. $\displaystyle\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$,
4. $\displaystyle\sum_{k=0}^{n}(-1)^k k^2 = (-1)^n \frac{n(n+1)}{2}$,
5. $\displaystyle\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1} \quad (n \neq 0)$.

Exercice 2.14 Soient E, F, G trois ensembles.

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

Exercice 2.15 Soient A et B deux parties de $\mathbb{N}$ qui se rencontrent (ne sont pas disjointes).

1. Le plus petit élément de $A \cap B$ est-il nécessairement le plus petit élément de A et de B ?
2. Le plus petit élément de $A \cup B$ est-il nécessairement le plus petit élément de A ou de B ?

Exercice 2.16 Soient A et B deux parties d'un ensemble E.

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

Exercice 2.17 Soient A, B deux parties d'un ensemble E. Montrer que

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

Exercice 2.18 Soient A, B, C trois parties d'un ensemble E. Montrer que

1. $(A \cap B \subset A \cap C \text{ et } A \cup B \subset A \cup C) \Rightarrow B \subset C$,
2. $(A \cap B = A \cap C \text{ et } A \cup B = A \cup C) \Rightarrow B = C$.

Exercice 2.19 Soient A, B, C trois parties d'un ensemble E. Montrer que

$$A \cup B = B \cap C \Leftrightarrow A \subset B \subset C.$$

Exercice 2.20 Soient E et F deux ensembles.

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

Exercice 2.21 Montrer que le disque unité dans $\mathbb{R}^2$ ne peut pas s'écrire comme produit de deux parties de $\mathbb{R}$.

Exercice 2.22 Les applications suivantes sont-elles injectives ? surjectives ? bijectives ?

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

Exercice 2.23 Soient $f : E \to F$ et $g : F \to G$ deux applications.

1. Si $g \circ f$ est surjective, f est elle automatiquement surjective ?
2. Si $g \circ f$ est surjective, g est elle automatiquement surjective ?

3. Si $g \circ f$ est injective, f est elle automatiquement injective ?
4. Si $g \circ f$ est injective, g est elle automatiquement injective ?

Exercice 2.24
1. Soient $f : E \to F$ et $g_1, g_2 : F \to G$ trois applications telles que $g_1 \circ f = g_2 \circ f$. A-t-on toujours $g_1 = g_2$? Et si f est injective ? Et si f est surjective ?
2. Soient $f_1, f_2 : E \to F$ et $g : F \to G$ trois applications telles que $g \circ f_1 = g \circ f_2$. A-t-on toujours $f_1 = f_2$? Et si g est injective ? Et si g est surjective ?

Exercice 2.25 On considère les applications $f, g : \mathbb{N} \to \mathbb{N}$ définies respectivement par

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

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

Exercice 2.26 Si $f : E \to E$ est une application et $n \in \mathbb{N}$, on définit f^n par récurrence en posant :

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

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

Exercice 2.27
1. Déterminer une bijection entre $\mathbb{Z}_{\geq 1}$ et $\mathbb{Z}_{\geq 2}$,
2. en déduire une bijection entre $A_1 := \{\frac{1}{n} : n \in \mathbb{Z}_{\geq 1}\}$ et $A_2 := \{\frac{1}{n} : n \in \mathbb{Z}_{\geq 2}\}$,
3. montrer que $[0,1] \setminus A_1 = [0,1[\setminus A_2$,
4. en déduire une bijection entre $[0,1]$ et $[0,1[$.

Exercice 2.28
1. établir une bijection entre $\mathbb{N}$ et $\mathbb{Z}$ (on pourra compter alternativement les nombres positifs et les nombres négatifs).
2. établir une bijection entre $\mathbb{N}$ et $\mathbb{N} \times \mathbb{N}$ (on pourra compter les couples en oblique),
3. établir une bijection entre $\mathbb{N}$ et $\mathbb{Q}_{\geq 0}$ (on pourra sauter les fractions qu'on aura déjà comptées).

3. Arithmétique

3.1 Nombres entiers

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

Définition 3.1.1 L'ensemble des *entiers naturels*[a] (resp. *relatifs*) est

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

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

Remarque

- Tout entier naturel s'obtient de manière unique en un nombre fini d'étapes à partir de 0 en associant à un entier naturel p son *successeur* que l'on notera « $p + 1$ » (c'est une notation, nous n'avons pas encore introduit l'addition des nombres entiers).
- En théorie des ensembles, on définit les entiers naturels par la méthode de von Neumann en posant

$$0 = \emptyset, \quad 1 := \{0\}, \quad 2 := \{0, 1\}, \quad \ldots \quad , \quad p := \{0, 1, \ldots, p-1\}, \quad \ldots$$

- Un entier relatif est, soit un entier naturel $n = p$, soit l'*opposé* $n = -p$ d'un entier naturel non nul.
- On pose $-0 := 0$ et si p est un entier naturel non nul, $-(-p) := p$ et on dit que c'est l'*opposé* de $-p$.
- On a

$$\forall n \in \mathbb{Z}, \quad -(-n) = n$$

et

$$\forall n \in \mathbb{Z}, \quad n \in \mathbb{N} \text{ et } -n \in \mathbb{N} \Leftrightarrow n = 0.$$

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

Définition 3.1.2 L'*addition* des entiers est l'opération qui associe à $m, n \in \mathbb{Z}$ leur *somme* $m+n$ définie

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

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

Proposition 3.1.3
1. $\forall m, n \in \mathbb{Z}, \quad m+n = n+m.$
2. $\forall n_1, n_2, n_3 \in \mathbb{Z}, \quad (n_1+n_2)+n_3 = n_1+(n_2+n_3),$
3. $\forall n \in \mathbb{Z}, \quad n+0 = n,$
4. $\forall n \in \mathbb{Z}, \quad -n+n = 0.$

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

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

- On montre par récurrence que $(m+n)+p = m+(n+p)$ lorsque $p \in \mathbb{N}$: on a $(m+n)+0 = m+n = m+(n+0)$, et si on suppose que $(m+n)+p = m+(n+p)$, on aura

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

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

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

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

Remarque • Comme nous l'avons déjà fait au cours de la démonstration, on écrira $n_1+n_2+n_3$ sans les parenthèses puisqu'il n'y a pas d'ambiguïté.

- $\mathbb{Z}$ est un groupe abélien pour l'addition (ces quatre propriétés).
- Simplification : si $m+n=m+n'$, alors $-m+m+n=-m+m+n'$ et donc $n=n'$.
- Si $p,q\in\mathbb{N}$, alors $p+q\in\mathbb{N}$ (les trois premières propriétés sont toujours satisfaites mais leur démonstration est dans ce cas bien plus élémentaire).

Définition 3.1.4 La *multiplication* des entiers est l'opération qui associe à $m,n\in\mathbb{Z}$ leur *produit* mn défini

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

Proposition 3.1.5
1. $\forall m,n\in\mathbb{Z},\quad mn=nm,$
2. $\forall n_1,n_2,n_3\in\mathbb{Z},\quad (n_1n_2)n_3=n_1(n_2n_3),$
3. $\forall n\in\mathbb{Z},\quad 1n=n,$
4. $\forall n_1,n_2,n_3\in\mathbb{Z},\quad n_1(n_2+n_3)=n_1n_2+n_1n_3,$
5. $\forall m,n\in\mathbb{Z},\quad mn=0\Leftrightarrow m=0$ ou $n=0.$

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

Remarque
- On écrira $n_1n_2n_3$ sans les parenthèses puisqu'il n'y a pas d'ambiguïté.
- $\mathbb{Z}$ est un *anneau intègre* (groupe abélien pour l'addition plus ces quatre propriétés).
- On a $0n=(0+0)n=0n+0n$ et donc $0n=0$. De même, on a $n+(-1)n=1n+(-1)n=(1+(-1))n=0n=0$ et donc $(-1)n=-n$.
- Si $p,q\in\mathbb{N}$, alors $pq\in\mathbb{N}$ (et les propriétés se démontrent bien plus facilement). En, fait, si $p\in\mathbb{N}$ et $p\neq 0$, alors $mp\in\mathbb{N}\Leftrightarrow m\in\mathbb{N}$.

Définition 3.1.6 L'opération *puissance* associe à $m\in\mathbb{Z}$ et $p\in\mathbb{N}$ la *puissance p-ème de m* définie par récurrence sur p par
$$m^0:=1 \quad \text{et} \quad m^{p+1}=m^pm.$$

Proposition 3.1.7
1. $\forall m\in\mathbb{Z},p,q\in\mathbb{N},\quad m^{p+q}=m^pm^q,$
2. $\forall m\in\mathbb{Z},p,q\in\mathbb{N},\quad m^{pq}=(m^p)^q,$
3. $\forall m,n\in\mathbb{Z},p\in\mathbb{N},\quad (mn)^p=m^pn^p.$

Démonstration. Exercice de récurrence. ■

Proposition 3.1.8 Pour tout $m, n \in \mathbb{Z}$ et $p \in \mathbb{N}$:

- $(m+n)^p = \sum_{k=0}^{p} \binom{p}{k} m^{p-k} n^k$,
- $m^{p+1} - n^{p+1} = (m-n) \sum_{k=0}^{p} m^{p-k} n^k$.

Démonstration. Ça se démontre par récurrence. Pour la seconde, on a déjà $m^1 - n^1 = (m-n)m^0 n^0$. Soit maintenant $p \in \mathbb{N}$ tel que la formule est satisfaite. On aura alors

$$\begin{aligned} m^{p+2} - n^{p+2} &= mm^{p+1} - mn^{p+1} + mn^{p+1} - nn^{p+1} \\ &= m(m^{p+1} - n^{p+1}) + (m-n)n^{p+1} \\ &= m(m-n) \sum_{k=0}^{p} m^{p-k} n^k + (m-n)n^{p+1} \\ &= (m-n) \sum_{k=0}^{p} m^{p+1-k} n^k + (m-n)n^{p+1} \\ &= (m-n) \sum_{k=0}^{p+1} m^{p+1-k} n^k. \end{aligned}$$

■

Remarque On en déduit que

$$\forall m, n \in \mathbb{N}, p \in \mathbb{N} \setminus \{0\}, \quad m = n \Leftrightarrow m^p = n^p.$$

Définition 3.1.9 L'*ordre* dans $\mathbb{Z}$ est la relation définie par

$$m \leq n \Leftrightarrow n - m \in \mathbb{N}.$$

Remarque

- On dit alors que m est *inférieur (ou égal)* à n.
- On dira que m est *strictement inférieur* à n et on écrira $m < n$ si, de plus, $m \neq n$.
- On utilise aussi le vocabulaire et les notations symétriques ($\geq, >$: supérieur et supérieur strict).

Proposition 3.1.10

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

Démonstration.

1. $n - m \in \mathbb{N}$ ou $-(n-m) \in \mathbb{N}$,
2. $n_3 - n_1 = (n_3 - n_2) + (n_2 - n_1) \in \mathbb{N}$,
3. $n - m \in \mathbb{N}$ et $-(n-m) \in \mathbb{N}$, donc $n - m = 0$.

■

Remarque Ces propriétés définissent une *relation d'ordre total* sur $\mathbb{Z}$ (totale, transitive, antisymétrique).

Proposition 3.1.11 1. $\forall n_1, n_2, n_3 \in \mathbb{Z}, \quad n_1 + n_3 \leq n_2 + n_3 \Leftrightarrow n_1 \leq n_2$,
2. $\forall m, n \in \mathbb{Z}, \forall p \in \mathbb{N} \setminus \{0\}, \quad mp \leq np \Leftrightarrow m \leq n$.

Démonstration. Laissé en exercice. ■

Remarque • On a

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

- On peut montrer aussi que

$$\forall m, n \in \mathbb{N}, p \in \mathbb{N} \setminus \{0\}, \quad m \leq n \Leftrightarrow m^p \leq n^p.$$

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

Définition 3.1.12 Soit $E \subset \mathbb{Z}$.

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

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

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

Exemple 1. Soit $E := \{3, 5, 6\}$. Alors, mais 6 et 8 sont des majorants. 1, 4 et 5 ne sont pas des majorants. En fait, 6 est le plus grand élément.

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

Remarque • Si E possède un majorant (resp. minorant), on dit que E est *majorée* (resp. *minorée*). Si les deux conditions sont remplies, on dit que E est *bornée*.

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

Théoreme 3.1.13 Toute partie majorée (resp. minorée) non vide de $\mathbb{Z}$ possède un plus grand (resp. plus petit) élément.

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

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

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

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

3.2 Division et congruence

Dans la suite, et sauf mention explicite du contraire, toutes les lettres représentent des entiers relatifs.

Définition 3.2.1 On dit que b est un *diviseur* de a ou que a est un *multiple* de b et on écrit $b \mid a$ s'il existe $q \in \mathbb{Z}$ tel que $a = bq$. Sinon, on écrit $b \nmid a$.

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

Remarque
- On a donc $b \mid a \Leftrightarrow (\exists q \in \mathbb{Z}, a = qb)$.
- Attention : tout entier divise 0 mais 0 est l'unique multiple de 0.
- On a $b \mid a \Leftrightarrow |b| \mid |a|$.
- Si $b \mid a$ et $a \neq 0$, alors $|b| \leq |a|$.
- Lorsque $b \neq 0$, on a $a/b \in \mathbb{Q}$ et $b \mid a \Leftrightarrow a/b \in \mathbb{Z}$. On évitera en fait ce genre de considération.
- Un entier est dit *pair* s'il c'est un multiple de 2 et *impair* sinon.

Théoreme 3.2.2 Si $b \in \mathbb{Z}_{\neq 0}$, alors il existe $q, r \in \mathbb{Z}$ uniques tels que $a = bq + r$ et $0 \leq r < |b|$.

Démonstration.

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

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

L'ensemble E minoré par $-|a|$. En effet, soit $q \in E$. Si $q + 1 \geq 0$, alors $-|a| \leq -1 \leq q$ (puisque $a \neq 0$). Et si $q+1 < 0$, alors $-|a| \leq a < b(q+1) < q+1$ (puisque $b > 0$).
L'ensemble E n'est pas vide car $|a| \in E$. En effet, $a \leq |a| < |a| + 1 \leq b(|a| + 1)$ (puisque $b > 0$ encore).
L'ensemble E étant minoré et non-vide possède donc un plus petit élément qu'on notera q. On a alors $q \in E$ et $q - 1 \notin E$ si bien que

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

et il suffit alors de poser $r = a - bq$. Lorsque $b < 0$, on écrit $a = |b|q' + r$ et on pose $q = -q'$.

- Unicité : supposons que $bq_1 + r_1 = bq_2 + r_2$ avec $0 \leq r_1, r_2 < |b|$. On a alors $|b||q_2 - q_1| = |r_2 - r_1|$ si bien que $0 \leq |b||q_2 - q_1| < |b|$. Puisque $b \neq 0$, cela signifie que $0 \leq |q_2 - q_1| < 1$ et donc $q_2 = q_1$. On a alors aussi $r_2 = r_1$. ■

Définition 3.2.3 On dit alors que q est le *quotient* et que r est le *reste* de la *division euclidienne* de a par b.

Exemple Effectuons la division euclidienne de 733 par 13 :

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

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

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

Remarque

- Si $b \neq 0$, alors $b \mid a$ si et seulement si le reste dans la division euclidienne de a par b est 0.
- Un entier n est pair (resp. impair) si et seulement si il existe $q \in \mathbb{Z}$ tel que $n = 2q$ (resp. $n = 2q + 1$).

Proposition 3.2.4

1. $a \mid a$,
2. $a \mid b$ et $b \mid c \Rightarrow a \mid c$,
3. $a \mid b$ et $b \mid a \Leftrightarrow |a| = |b|$.

Démonstration. 1. $a = 1a$,

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

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

Proposition 3.2.5 1. $a \mid b$ et $a \mid c \Rightarrow a \mid (b + c)$,
2. $a \mid b \Rightarrow ac \mid bc$.

Démonstration. 1. Si $b = pa$ et $c = qa$, alors $b + c = (p + q)a$.
2. Si $b = pa$, alors $bc = pac$. ■

Remarque Comme conséquence, on voit que :

- si $a \mid b$ et $a \mid c$, alors $a \mid b - c$,
- si $a \mid b$, alors $a \mid c \Leftrightarrow a \mid (b + c)$,
- $ac \mid bc \Leftrightarrow (a \mid b$ ou $c = 0)$,
- si $a \mid b$, alors $a^k \mid b^k$ (on verra la réciproque plus tard).

Définition 3.2.6 Deux entiers a et b sont *congrus* modulo un entier n si n divise $b - a$. On écrit alors $a \equiv b \mod n$.

Exemple On a $9 \equiv 5 \mod 2$ mais aussi $9 \equiv 3 \mod 2$. On a $9 \equiv 5 \mod 4$ mais $9 \not\equiv 3 \mod 4$. On a $25 \equiv -1 \mod 13$.

Remarque

- En d'autres termes, $a \equiv b \mod n \Leftrightarrow \exists k \in \mathbb{Z}, b = a + kn$.
- Plus prosaïquement, « congrus modulo n » signifie comme toujours : « égaux quitte à ajouter un multiple entier de n ».
- On a $b \mid a \Leftrightarrow a \equiv 0 \mod b$.

Proposition 3.2.7 1. $a \equiv a \mod n$,
2. $a \equiv b \mod n$ et $b \equiv c \mod n \Rightarrow a \equiv c \mod n$,
3. $a \equiv b \mod n \Leftrightarrow b \equiv a \mod n$.

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

■

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

Proposition 3.2.8 $$\left\{\begin{array}{rcll} a & \equiv & a' & \mod n \\ b & \equiv & b' & \mod n \end{array}\right. \Rightarrow \left\{\begin{array}{rcll} a+b & \equiv & a'+b' & \mod n \\ ab & \equiv & a'b' & \mod n. \end{array}\right.$$

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

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

Proposition 3.2.9 Supposons $b \neq 0$. Alors,

1. le reste dans la division euclidienne de a par b est le plus petit entier naturel r tel que $a \equiv r \mod b$,
2. on a $a \equiv a' \mod b$ si et seulement si a et a' ont même reste dans la division euclidienne par b.

Démonstration. On effectue la division euclidienne $a = bq + r$ avec $0 \leq r < |b|$.

On a alors bien $a \equiv r \mod b$. Supposons que $a \equiv r' \mod b$ avec $0 \leq r' < r$. Alors, $r \equiv r' \mod b$ et donc $b \mid (r-r')$ si bien que $|b| \leq r-r' < |b|$. Contradiction.

On effectue maintenant la division euclidienne $a' = bq' + r'$ avec $0 \leq r' < |b|$. On a alors $a' \equiv r' \mod b$ et $|r-r'| < |b|$. On en déduit que

$$a \equiv a' \mod b \Leftrightarrow r \equiv r' \mod b \Leftrightarrow b \mid (r-r') \Leftrightarrow r-r' = 0 \Leftrightarrow r = r'.$$ ■

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

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

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

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

puis

$$9^3 = 9 \times 9^2 \equiv 9 \times 3 = 27 = 13 \times 2 + 1 \equiv 1 \mod 13 \text{ (bon)}.$$

On a $1000 = 3 \times 333 + 1$ et on en déduit que

$$100^{1000} \equiv 9^{1000} = 9^{3\times 333+1} = (9^3)^{333} \times 9 \equiv 1^{333} \times 9 = 1 \times 9 = 9$$

si bien que le reste est 9.

3.3 pgcd et ppcm

On dit que d est un *diviseur commun* à a et à b si $d \mid a$ et $d \mid b$. On dit que m est un *multiple commun* à a et à b si $a \mid m$ et $b \mid m$.

Lemme 3.3.1 Il existe

1. un *plus grand diviseur commun (pgcd)* à a et b si on suppose que $a \neq 0$ ou $b \neq 0$ que l'on note $a \wedge b$,
2. un plus *petit multiple commun strictement positif (ppcm)* à a et b si on suppose que $a \neq 0$ et $b \neq 0$ que l'on note $a \vee b$.

Par *convention*, $0 \wedge 0 = 0$ et $a \vee 0 = 0 \vee b = 0$.

Démonstration. 1. L'ensemble des diviseurs communs est majoré (par $|a|$ par exemple si c'est a qui est non nul) et non-vide (puisqu'il contient toujours 1). Il possède donc un plus grand élément.

2. Les multiples communs strictement positifs forment un ensemble minoré (par 0) et non-vide (puisqu'il contient $|ab|$). Celui-ci possède donc un plus petit élément. ■

Exemple 1. $24 \wedge 36 = 12$ et $24 \vee 36 = 72$.

2. $95 \wedge 57 = 19$ et $95 \vee 57 = 285$.
3. $1 \wedge 99 = 1$ et $1 \vee 99 = 99$.
4. $0 \wedge 99 = 99$ et $0 \vee 99 = 0$.

Proposition 3.3.2 1. $a \wedge b = b \wedge a$ et $a \vee b = b \vee a$,

2. $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ et $(a \vee b) \vee c = a \vee (b \vee c)$,
3. $a \wedge 0 = |a|$ et $a \vee 0 = 0$,
4. $a \wedge 1 = 1$ et $a \vee 1 = |a|$.

Démonstration. Exercice. ■

Remarque

- $a \wedge b = 0 \Leftrightarrow (a = 0 \text{ et } b = 0)$ et $a \vee b = 0 \Leftrightarrow (a = 0 \text{ ou } b = 0)$.
- $a \wedge b := |a| \wedge |b|$ et $a \vee b := |a| \vee |b|$.
- $a \mid b \Leftrightarrow a \wedge b = |a| \Leftrightarrow a \vee b = |b|$.
- On écrira $a \wedge b \wedge c$ et $a \vee b \vee c$ puisqu'il n'y a pas d'ambiguïté. Notons que c'est en fait le plus plus grand diviseur commun (resp. plus petit multiple commun strictement positif) à a, b et c (ou 0).

Lemme 3.3.3 Si $a = bq + r$ alors $a \wedge b = b \wedge r$.

Démonstration. Si $a = b = 0$ ou si $b = r = 0$, c'est clair. Sinon, si on suppose que $d \mid b$, on aura $d \mid bq$ et donc $d \mid a \Leftrightarrow d \mid r$ si bien que $d \mid a$ et $d \mid b \Leftrightarrow d \mid b$ et $d \mid r$. En d'autres termes, a, b d'une part et b, r d'autre part ont les mêmes diviseurs. Donc le même pgcd. ■

Remarque On en déduit l'*algorithme d'Euclide* pour déterminer le pgcd de deux entiers naturels a et b : on pose $d_0 := a, d_1 := b$ puis on définit d_{n+1} par la récurrence

$$d_{n-1} = q_n d_n + d_{n+1} \quad \text{avec } 0 \leq d_{n+1} < d_n$$

jusqu'à ce que $d_{n+1} = 0$; on aura alors

$$a \wedge b = d_0 \wedge d_1 = d_1 \wedge d_2 = \cdots = d_n \wedge d_{n+1} = d_n \wedge 0 = d_n.$$

Exemple On a $598 \wedge 414 = 46$:

$$\begin{aligned} 598 &= 414 \times 1 + 184, \\ 414 &= 184 \times 2 + 46, \\ 184 &= 46 \times 4 + 0. \end{aligned}$$

Théoreme 3.3.4 — de Bézout. $|d| = a \wedge b \Leftrightarrow \begin{cases} d \mid a, d \mid b \text{ et} \\ \exists u, v \in \mathbb{Z}, au + bv = d. \end{cases}$

Démonstration. Si $a = b = 0$, c'est clair. Sinon, on peut supposer que $d > 0$. La condition est clairement suffisante : si $c \mid a$ et $c \mid b$, alors $c \mid d = au + bv$ et donc $c \leq |d|$. Pour montrer qu'elle est nécessaire, on étend l'algorithme d'Euclide en définissant deux suites finies $u_n, v_n \in \mathbb{Z}$ telles que $d_n = au_n + bv_n$. On pose tout d'abord

$$u_0 := 1, \quad v_0 := 0, \quad u_1 := 0, \quad v_1 := 1$$

On a donc bien $d_0 = a$ et $d_1 = b$. Si $d_{n+1} = 0$, on a $d_n = d$ et il suffit donc de poser $u := u_n$ et $v := v_n$. Sinon, on a $d_{n-1} = q_n d_n + d_{n+1}$ avec $0 \leq d_{n+1} < d_n$. On pose alors

$$u_{n+1} := u_{n-1} - q_n u_n \quad \text{et} \quad v_{n+1} = v_{n-1} - q_n v_n.$$

On a aura bien

$$\begin{aligned} au_{n+1} + bv_{n+1} &= a(u_{n-1} - q_n u_n) + b(v_{n-1} - q_n v_n) \\ &= au_{n-1} + bv_{n-1} - q_n(au_n + bv_n) \\ &= d_{n-1} - q_n d_n \\ &= d_{n+1}. \end{aligned}$$

■

Exemple

1. On a $1 \times 3 - 1 \times 2 = 1$, $1 \times 4 - 1 \times 2 = 2$, $1 \times 4 - 1 \times 3 = 1$, $1 \times 5 - 2 \times 2 = 1$, etc.
2. On a $-2 \times 598 + 3 \times 414 = 46$:

$$\begin{aligned} 598 &= 1 \times 598 + 0 \times 414 \\ 414 &= 0 \times 598 + 1 \times 414 \quad (-1 \times -) \\ 184 &= 1 \times 598 - 1 \times 414 \quad (-2 \times -) \\ 46 &= -2 \times 598 + 3 \times 414. \end{aligned}$$

3. Alternative à l'algorithme d'Euclide étendu : on détermine la suite d_n comme d'habitude en posant $d_0 := a, d_1 := b$ puis par récurrence

$$d_{n-1} = q_n d_n + d_{n+1} \quad \text{avec } d_{n+1} < d_n$$

jusqu'à ce que $d_n = a \wedge b$. On remonte ensuite par récurrence en posant $u_1 = 0$ et $u_2 = 1$, puis $u_{k+2} = u_k - q_{n-k}u_{k+1}$, de telle sorte que $d_n = u_k d_{n-k} + u_{k-1}d_{n-k+1}$ et il suffit de prendre $k = n$. Sur l'exemple précédent, la division euclidienne usuelle nous fournit

$$\begin{aligned} 598 &= 1 \times 414 + 184, \\ 414 &= 2 \times 184 + 46. \end{aligned}$$

On en déduit

$$\begin{aligned} 46 &= 414 - 2 \times 184 \\ &= 414 - 2 \times (598 - 1 \times 414) \\ &= -2 \times 598 + 3 \times 414. \end{aligned}$$

Définition 3.3.5 Deux entiers a et b sont *premiers entre eux* si $a \wedge b = 1$.

Exemple On a $2 \wedge 3 = 1$, $1000 \wedge 1001 = 1$, $10000 \wedge 59 = 1$.

Corollaire 3.3.6 $a \wedge b = 1 \Leftrightarrow \exists u, v \in \mathbb{Z}, au + bv = 1$. ■

Théoreme 3.3.7 Si $a \wedge b = 1$, alors

1. (lemme de Gauss) $a \mid bc \Leftrightarrow a \mid c$,
2. $(a \mid c \text{ et } b \mid c) \Leftrightarrow ab \mid c$.

Démonstration. Dans chaque cas, la condition est clairement suffisante et il reste à montrer qu'elle est nécessaire. On écrit $au + bv = 1$ et on a donc $acu + bcv = c$ si bien que,

1. si $a \mid bc$, alors $a \mid bcv$ et comme $a \mid acu$, on voit que $a \mid c$,
2. si $a \mid c$ alors $ab \mid bcv$, et si $b \mid c$ alors $ab \mid acu$, et on a donc $ab \mid c$. ■

Exemple Montrer que $99 \mid 5247$. On a $9 \mid 5247$ car $5 + 2 + 4 + 7 = 18$ et $1 + 8 = 9$. On a $11 \mid 5247$ car $5 - 2 + 4 - 7 = 0$. Il suffit alors de remarquer que $99 = 9 \times 11$ et que $9 \wedge 11 = 1$.

Corollaire 3.3.8 — « Théorème chinois ». Si $m \wedge n = 1$, alors

1. $\forall a, b \in \mathbb{Z}, \quad \begin{cases} a \equiv b \mod m \\ a \equiv b \mod n \end{cases} \Leftrightarrow a \equiv b \mod mn$,
2. $\forall a, b \in \mathbb{Z}, \exists c \in \mathbb{Z}, \quad \begin{cases} c \equiv a \mod m \\ c \equiv b \mod n \end{cases}$.

Démonstration. Pour la première partie, on a $m \mid b-a$ et $n \mid b-a$ si et seulement si $mn \mid b-a$. Pour la seconde, on écrit $um+vn=1$ et on pose $c=bum+avn$. ■

Proposition 3.3.9 1. $(a \wedge b)(a \vee b) = |ab|$,
2. $c \mid (a \wedge b) \Leftrightarrow c \mid a$ et $c \mid b$,
3. $(a \vee b) \mid c \Leftrightarrow a \mid c$ et $b \mid c$,
4. $ac \wedge bc = (a \wedge b) \times |c|$,
5. $ac \vee bc = (a \vee b) \times |c|$.

Démonstration. Si $a=0$ ou $b=0$, tout est clair. Quitte à remplacer a, b et c par leurs valeurs absolues, on peut donc supposer que $a, b > 0$ et $c \geq 0$. On pose $d := a \wedge b$ et $m = a \vee b$. On rappelle que l'on peut écrire $d = au + bv$ avec $d \mid a$ et $d \mid b$.

On commence par l'assertion 2). Seule la réciproque nécessite un argument mais si $c \mid a$ et $c \mid b$, alors $c \mid au + bv = d$.

On montre ensuite l'assertion 4). On a $dc = acu + bcv$ avec $dc \mid ac$ et $dc \mid bc$ et on conclut avec la réciproque du théorème de Bézout.

On montre maintenant simultanément les l'assertions 3) et 1). Puisque $d \mid a$ et $d \mid b$, on peut écrire $a = da'$ et $b = db'$. Il résulte alors de l'assertion 4) que $a' \wedge b' = 1$. Supposons que c est un multiple commun à a et b, c'est à dire que $a \mid c$ et $b \mid c$. Alors, en particulier, $d \mid c$ et on peut donc écrire $c = dc'$. En simplifiant par d, on trouve donc que $a' \mid c'$ et $b' \mid c'$. Puisque $a' \wedge b' = 1$, il en résulte que $a'b' \mid c'$ et donc $da'b' \mid c$. Cela s'applique en particulier au cas $c = m$ et ça implique que $da'b' \leq m$. Mais on sait aussi que $a \mid ab' = da'b'$ et $b \mid a'b = da'b'$ si bien que $da'b'$ est un multiple commun à a et b et donc $da'b' \geq m$. On a donc $m = da'b'$. On en déduit d'une part l'assertion 1), c'est à dire que $dm = (da')(db') = ab$, mais aussi que $m = da'b' \mid c$, c'est à dire la réciproque de l'assertion 3). Le sens direct est immédiat.

Enfin, pour l'assertion 5), on sait par l'assertion 4) que $dc = ac \wedge bc$ et on applique ensuite l'assertion 1) à ac et bc, ce qui donne

$$(dc)(ac \vee bc) = (ac \wedge bc)(ac \vee bc) = (ac)(bc) = abc^2 = dmc^2$$

et on simplifie par dc (c'est trivial si $c=0$). ■

Proposition 3.3.10 Si $n \in \mathbb{N}$, alors $a^n \wedge b^n = (a \wedge b)^n$.

Démonstration. On suppose d'abord que $a \wedge b = 1$, on écrit $1 = au + bv$, puis

$$\begin{aligned} 1 &= (au+bv)^{2n} \\ &= \sum_{i=0}^{2n} \binom{2n}{i} (au)^{2n-i}(bv)^i \\ &= \left(\sum_{i=0}^{n-1} \binom{2n}{i} a^{n-i} u^{2n-i} (bv)^i \right) a^n + \left(\sum_{i=n}^{2n} \binom{2n}{i} (au)^{2n-i} b^{i-n} v)^i \right) b^n. \end{aligned}$$

Cela montre que $a^n \wedge b^n = 1$. En général, on écrit $a = da'$ et $b = db'$ avec $a' \wedge b' = 1$. On a alors $a^n \wedge b^n = d^n a'^n \wedge d^n b'^n = d^n(a'^n \wedge b'^n) = d^n$. ■

Remarque On en déduit que $a \mid b \Leftrightarrow a^n \mid b^n$ si $n > 0$.

3.4 Nombres premiers

Définition 3.4.1 Un entier p est *premier* s'il possède un unique diviseur plus grand que 2. On dit *nombre premier* si $p \in \mathbb{N}$.

Remarque
- L'unique diviseur plus grand que 2 est nécessairement $|p|$.
- Un entier p est premier si et seulement si $|p|$ est premier.
- Les nombres 0 et 1 ne sont pas premiers (tous les entiers divisent 0 et seulement 1 et -1 divisent 1).
- La définition correcte d'*entier premier* est en fait la condition (équivalente) du lemme d'Euclide que nous verrons plus bas. La définition ci-dessus est plutôt celle d'un entier *irréductible* (qui est en fait équivalente).

Exemple
1. $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, \ldots$
2. $3, 5, 17, 257, 65537$ (nombres de Fermat).
3. $3, 7, 127, 8191$ (nombres de Mersenne).

Lemme 3.4.2 Si $a \neq 1, -1$, alors il existe un nombre premier p tel que $p \mid a$. Si $a \neq 0$ et a n'est pas premier, on peut supposer $p^2 \leq |a|$.

Démonstration. Le cas $a = 0$ étant clair, quitte à remplacer a par sa valeur absolue, on peut supposer $a > 1$. Soit p le plus petit diviseur de a avec $p > 1$. Puisque tout diviseur de p est aussi un diviseur de a, p est nécessairement premier. On écrit ensuite $a = pq$. Si a n'est pas premier, on a nécessairement $q > 1$. Comme q est un diviseur de a et que $q > 1$, on doit avoir $p \leq q$ si bien que $p^2 \leq pq = a$. ■

Remarque
- Le *crible d'ératosthène* est un algorithme qui permet de trouver tous les nombres premiers (inférieurs à $n > 1$ fixé). On fait la liste croissante de tous les entiers entre 2 et n. On pose $p = 2$ et on commence la boucle. On raye tous les autres multiples de p. Soit q le prochain entier qui n'est pas rayé. Si $q^2 > n$, on arrête. Sinon, on pose $p := q$ et on reprend la boucle.
- Il existe une infinité de nombres premiers : par l'absurde, si $p_1, \ldots, p_r$ étaient les seuls nombres premiers, alors il existerait $i \in \{1, \ldots, r\}$ tel que $p_i \mid p_1 \ldots p_r + 1$ et donc $p_i \mid 1$.

Exemple Le nombre 167 est premier. On vérifie facilement qu'il n'est pas divisible par $2, 3, 5, 11$. On a $167 \equiv -1 \mod 7$. Enfin, $13^2 = 169 > 167$.

Corollaire 3.4.3 On a $a \wedge b \neq 1$ si et seulement si il existe un nombre premier p tel que $p \mid a$ et $p \mid b$.

Démonstration. Soit $d = a \wedge b$. Si $d = 0$, c'est clair. Sinon, $d > 1$ si et seulement s'il existe p premier avec $p \mid d$. Cela signifie que $p \mid a$ et $p \mid b$. ■

Lemme 3.4.4 Un entier p est premier si et seulement si

$$p \wedge a = 1 \Leftrightarrow p \nmid a$$

(a est premier avec p si et seulement si a n'est pas un multiple de p).

Démonstration. Supposons que p est premier. Si $p \mid a$, alors $p \wedge a = |p| > 1$ puisque p est premier. Réciproquement, si $p \wedge a = d > 1$, alors $d \mid p$ et donc $|p| = d$ puisque p est premier si bien que $p \mid a$. La preuve que la condition implique que p est premier est laissée en exercice. ■

Lemme 3.4.5 — d'Euclide. Un entier p est premier si et seulement si $p \neq 0, 1, -1$ et

$$p \mid ab \Leftrightarrow p \mid a \text{ ou } p \mid b$$

(p divise un produit si et seulement si il divise un des facteurs).

Démonstration. On vient de voir que si p est premier et $p \nmid a$, alors $p \wedge a = 1$. Il résulte alors du lemme de Gauss que si $p \mid ab$, alors nécessairement $p \mid b$. La réciproque est automatique. La preuve que la condition implique que p est premier est laissée en exercice. ■

Remarque On voit donc par récurrence sur $n \geq 1$ que si p est premier, alors $p \mid a^n \Leftrightarrow p \mid a$.

Lemme 3.4.6 Si p est un nombre premier et $0 < k < p$, alors $\binom{p}{k}$ est un multiple de p.

Démonstration. On a

$$k\binom{p}{k} = k\frac{p!}{k!(p-k)!} = p\frac{(p-1)!}{(k-1)!(p-k)!} = p\binom{p-1}{k-1}.$$

Puisque $0 < k < p$, on a $p \nmid k$ et on conclut avec le lemme d'Euclide. ■

Remarque C'est faux si p n'est pas premier comme le montre le cas de $\binom{4}{2} = 6$ qui n'est pas un multiple de 4.

Théoreme 3.4.7 — de Fermat (petit). Si p est un nombre premier, alors

$$p \nmid a \Leftrightarrow p \mid a^{p-1} - 1$$

Démonstration. Clairement, $p \mid a$ et $p \mid a^{p-1} - 1$ aboutit à une contradiction. Pour conclure, il suffit donc de montrer, grâce au lemme d'Euclide, que $a^p \equiv a \mod p$ car on aura alors $p \mid a(a^{p-1} - 1)$. Pour $a \geq 0$, on procède par récurrence, le cas $a = 0$ étant trivial. Grâce au lemme, on aura

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k \equiv a^p + 1 \equiv a + 1 \mod p.$$

D'autre part, $(-1)^p = -1$ si p est impair et $(-1)^p = 1 \equiv -1 \mod 2$. Donc, $(-a)^p \equiv (-1)^p a^p \equiv (-1) \times a \equiv -a$. ■

Remarque

- En termes de congruences, le théorème s'écrit

$$a \not\equiv 0 \mod p \quad \Leftrightarrow \quad a^{p-1} \equiv 1 \mod p.$$

  On peut préférer la forme compacte $a^p \equiv a \mod p$.
- Le test de primalité de Fermat permet de dire si un nombre p est *probablement premier* en regardant si 2^{p-1}, 3^{p-1}, etc. sont congrus à 1 modulo p. Par exemple, $2^8 = 256 \equiv 4 \mod 9$ donc 9 n'est pas premier.
- Le grand théorème de Fermat (démontré seulement en 1992 par Andrew Wiles) stipule que si $a, b, c \in \mathbb{N} \setminus \{0\}$, alors $a^n + b^n \neq c^n$ pour $n > 2$.

3.5 Valuation

Définition 3.5.1 Si p est un nombre premier, la *valuation p-adique*[a] de $a \neq 0$, que l'on note $v_p(a)$, est le plus grand entier naturel v tel que $p^v \mid n$.

a. La terminologie n'est pas au programme mais la notion l'est.

Si besoin, on pose $v_p(0) := +\infty$.

Exemple

1. $v_2(1000) = v_5(1000) = 3$ et $v_p(1000) = 0$ sinon.
2. $v_7(1001) = v_{11}(1001) = v_{13}(1001) = 1$ et $v_p(1001) = 0$ sinon.
3. $v_2(1002) = v_3(1002) = v_{167}(1002) = 1$ et $v_p(1002) = 0$ sinon.

Remarque

- La valuation p-adique de a est bien définie car les v tels que $p^v \mid a$ sont majorés pour $a \neq 0$. En fait, on a

$$v_p(a) \leq \frac{\ln(|a|)}{\ln(p)}.$$

- Par définition,

$$\forall v \in \mathbb{N}, \quad v \leq v_p(a) \Leftrightarrow p^v \mid a.$$

- On a $v = v_p(a)$ si et seulement si $a = p^v b$ avec $p \nmid b$.
- On a $v_p(a) > 0 \Leftrightarrow p \mid a$.
- Pour a fixé, on a $v_p(a) = 0$ pour presque tout (tous sauf pour un nombre fini) nombre premier p : si $p \mid a$, alors $p \leq |a|$.
- On a $v_p(a) = 0$ pour tout nombre premier p si et seulement si $a = 1$ ou $a = -1$.

Proposition 3.5.2 Soit p un nombre premier. Alors,

1. $v_p(1) = 0$ (et $v_p(0) = +\infty$),
2. $v_p(a + b) \geq \min(v_p(a), v_p(b))$,
3. $v_p(ab) = v_p(a) + v_p(b)$.

Démonstration. 1. Clair.

2. Si $v = \min(v_p(a), v_p(b))$, alors $p^v \mid a$ et $p^v \mid b$ si bien que $p^v \mid a + b$ et donc $v \leq v_p(a + b)$.
3. Posons $v = v_p(a)$ et $w = v_p(b)$. On a alors $a = p^v a'$ et $b = p^w b'$ avec $p \nmid a'$ et $p \nmid b'$. On en déduit que $ab = p^{v+w} a'b'$ et $p \nmid a'b'$ grâce au lemme d'Euclide.

■

Remarque

- Si $k \in \mathbb{N}$, alors $v_p(a^k) = kv_p(a)$.
- Si $v_p(a) < v_p(b)$, alors $v_p(a + b) = \min(v_p(a), v_p(b))$.
- On dispose de formules analogues pour les degrés des polynômes :
  1. $\deg(1) = 0$ et $\deg(0) = -\infty$,
  2. $\det(P + Q) \leq \max(\deg(P), \deg(Q))$,
  3. $\deg(PQ) = \deg(P) + \deg(Q)$.

Proposition 3.5.3 $a \mid b$ si et seulement si $v_p(a) \leq v_p(b)$ pour tout nombre premier p.

Démonstration. Supposons que $b = ac$. Alors, $v_p(b) = v_p(a) + v_p(c) \geq v_p(a)$. Pour la réciproque, on se ramène rapidement au cas $a \geq 1$ que l'on traite par récurrence forte sur a (avec b quelconque). Si $a = 1$, la condition est vide. Si $a \geq 2$, il existe p premier tel que $p \mid a$ et puisque $1 \leq v_p(a) \leq v_p(b)$, on aura aussi $p \mid b$. On peut donc écrire $a = pa'$ et $b = pb'$ si bien que $v_p(a') = v_p(a) - 1 \leq v_p(b) - 1 = v_p(b')$. Par récurrence forte, puisque $1 \leq a' < a$, on a $a' \mid b'$ et donc $a = pa' \mid pb' = b$. ■

Proposition 3.5.4 Si p est un nombre premier, alors

$$\begin{cases} v_p(a \wedge b) = \min(v_p(a), v_p(b)) \\ v_p(a \vee b) = \max(v_p(a), v_p(b)). \end{cases}$$

Démonstration. Posons $d = a \wedge b$ et $m = a \vee b$. Puisque $d \mid a$ et $d \mid b$, on a $v_p(d) \leq v_p(a)$ et $v_p(d) \leq v_p(b)$ si bien que $v_p(d) \leq \min(v_p(a), v_p(b))$. D'autre part, on peut écrire

$d = au + bv$ et on a donc $v_p(d) \geq \min(v_p(a) + v_p(u), v_p(b) + v_p(v) \geq \min(v_p(a), v_p(b))$. Enfin, comme $md = ab$, alors

$$v_p(m) = v_p(a) + v_p(b) - \min(v_p(a), v_p(b)) = \max(v_p(a), v_p(b))$$

puisqu'on a toujours $x + y = \min(x, y) + \max(x, y)$. ■

Remarques
- $|a| = |b|$ si et seulement si $v_p(a) = v_p(b)$ pour tout nombre premier p.
- $a \wedge b = 1$ si et seulement si $v_p(a)v_p(b) = 0$ pour tout nombre premier p.
- On voit facilement que si $n > 0$, alors $a \mid b \Leftrightarrow a^n \mid b^n$. Il suffit de remarquer que $v_p(a) \leq v_p(b) \Leftrightarrow nv_p(a) \leq nv_p(b)$.
- On voit facilement que $a^n \wedge b^n = (a \wedge b)^n$ et $a^n \vee b^n = (a \vee b)^n$. Il suffit de remarquer que $\min(nv_p(a), nv_p(b)) = n \min(v_p(a), v_p(b))$. Et idem pour le ppcm.

Théoreme 3.5.5 Tout entier $n > 1$ s'écrit de manière unique sous la forme

$$n = \prod_{i=1}^{r} p_i^{v_i}$$

avec $1 < p_1 < \cdots < p_r$ premiers et $v_1, \ldots, v_r > 0$.

Démonstration. Si p est un nombre premier, on a

$$v_p\left(\prod_{i=1}^{r} p_i^{v_i}\right) = \sum_{i=1}^{r} v_p(p_i^{v_i}) = \sum_{i=1}^{r} v_i v_p(p_i) = \begin{cases} v_i \text{ si } p = p_i \\ 0 \text{ sinon.} \end{cases}$$

- Unicité : on aura nécessairement $p_i \mid n$ et $v_i = v_{p_i}(n)$.
- Existence : on désigne par $1 < p_1 < \cdots < p_r$ les nombres premiers qui divisent n et on pose $v_i := v_{p_i}(n)$. ■

Remarque
- On dit que $\mathbb{Z}$ est un anneau *factoriel*.
- On en déduit que le nombre de diviseurs positifs de n est

$$d(n) := \prod_{i=1}^{r} (v_i + 1).$$

- On peut réécrire les formules sous la forme

$$\forall n > 0, \quad n = \prod_{p \text{ premier}} p^{v_p(n)} \quad \text{et} \quad d(n) := \prod_{p \text{ premier}} (v_p(n) + 1)$$

(puisque $v_p(n)$ est presque toujours nul et $p^{v_p(n)}$ vaut donc presque toujours 1).

Exemple
1. $2 = 2^1$, $3 = 3^1$, $4 = 2^2$, $5 = 5^1$, $6 = 2^1 \times 3^1$, $7 = 7^1$, $8 = 2^3$, $9 = 3^2$, $10 = 2^1 \times 5^1$, $11 = 11^1$, $12 = 2^2 \times 3$, etc.
2. $1000 = 2^3 \times 5^3$, $1001 = 7 \times 11 \times 13$, $1002 = 2 \times 3 \times 167$.
3. On a $12 = 2^2 \times 3^1$ si bien que $d(12) = (2 + 1)(1 + 1) = 6$ et 12 a donc six diviseurs positifs. En effet, ce sont $1, 2, 3, 4, 6, 12$.

Corollaire 3.5.6 Si $n = \prod_{i=1}^{r} p_i^{v_i}$ et $m = \prod_{i=1}^{r} p_i^{w_i}$ avec $p_1, \ldots, p_r$ premiers distincts, alors

$$n \wedge m = \prod_{i=1}^{r} p_i^{\min(v_i, w_i)} \quad \text{et} \quad n \vee m = \prod_{i=1}^{r} p_i^{\max(v_i, w_i)}. \quad \blacksquare$$

Exemple On a $n := 231868 = 2^2 \times 7^3 \times 13^2$ et $m := 8190 = 2 \times 3^2 \times 5 \times 7 \times 13$ donc $n \wedge m = 2 \times 7 \times 13 = 182$ et $n \vee m = 2^2 \times 3^2 \times 7^3 \times 13^2$.

Remarque Dans le dernier example, on pourrait demander de « calculer » ce ppcm. Mais que veut dire calculer ? Pour nous, cela signifie exprimer ce nombre en base dix (dans l'alphabet des chiffres usuels). Or cela n'est plus nécessaire puisqu'on dispose maintenant d'un alphabet universel et naturel : les nombres premiers.

3.6 Exercices (7 juillet 2025)

La calculette pourra être utilisée comme outil d'aide à la décision mais en aucun cas comme argument scientifique.

Exercice 3.1 1. Je suis un nombre à quatre chiffres. Mon chiffre des dizaines est le double de mon chiffre des milliers. Mon chiffre des centaines est le triple de celui de mes unités. La somme de mes chiffres vaut onze. Qui suis-je ?

2. Vérifier que la prochaine date qui s'écrit avec huit chiffres différents est le 17 06 2345. Quelle était la dernière ?

Exercice 3.2 Effectuer les divisions euclidiennes suivantes :

1. 100001 par 101, 2. 656665 par 11, 3. 66227 par 13.

Exercice 3.3 Sachant que $12079233 = 75968 \times 159 + 321$, déterminer le reste de la division euclidienne de 12079233 par 75968 puis par 159.

Exercice 3.4 Déterminer selon la parité de $n > 0$ le reste dans la division euclidienne par n de la somme S_n des n premiers entiers naturels non nuls ?

Exercice 3.5 1. Montrer que si $n \in \mathbb{Z}$, alors $2 \mid n(n+1)$.

2. Montrer de même que $3 \mid n(n+1)(n+2)$.

3. Montrer de même que $8 \mid n(n+1)(n+2)(n+3)$.

Exercice 3.6 Montrer par récurrence sur $n \in \mathbb{N}$ que

1. 11 divise $4^{4n+2} - 3^{n+3}$,
2. 17 divise $3 \times 5^{2n+1} + 2^{3n+1}$.

Exercice 3.7 Montrer par récurrence sur $n \in \mathbb{N}$ que $40^n n! \mid (5n)!$ (on pourra utiliser l'exercice 3.5.3).

Exercice 3.8 1. Déterminer les $n \in \mathbb{Z}$ tels que $2n - 3$ est divisible par $n - 2$?

2. Même question avec $3n - 7$ et $n - 4$?

Exercice 3.9 Résoudre les equations suivantes dans $\mathbb{N}$:

1. $x^2 - y^2 = 1$, 2. $xy = x + y$,
3. $xy = 2x + 2y$, 4. $2xy = x + y$.

Exercice 3.10 1. Déterminer en fonction de $n \in \mathbb{N}$ le reste dans la division euclidienne de 2^n par 5.

2. Même question avec 3^n et 7.

3. Même question avec 38^n et 7.

Exercice 3.11 1. Pour quelles valeurs de l'entier naturel n le nombre $4^n + 2^n + 1$ est il divisible par 7 ?

2. Même question avec $9^n + 3^n + 1$ et 13.
3. Même question avec $25^n + 5^n + 1$ et 31.

Exercice 3.12 Déterminer en fonction de la parité de l'entier naturel n le reste dans la division de $7^n + 1$ par 8.

Exercice 3.13 Montrer que la somme de trois cubes consécutifs est divisible par 9.

Exercice 3.14 Soient $a, b \in \mathbb{Z}$ et $n \geq 2$. Montrer que si $a \equiv b \mod n$, alors $a^n \equiv b^n \mod n^2$.

Exercice 3.15
1. Montrer que $3^{126} + 5^{126}$ est divisible par 13.
2. Montrer que si n est un entier naturel, alors $3^{2n+1} + 2^{4n+2}$ est divisible par 7.

Exercice 3.16
1. Quel est le reste de la division euclidienne de 247^{349} par 7 ?
2. Quel est le reste de la division euclidienne de 1357^{2013} par 5 ?

Exercice 3.17
1. Montrer que si $n > 0$, alors $6^n \equiv 6 \mod 10$.
2. En déduire le chiffre des unités du nombre 123456^{789}.
3. Montrer que $56^6 \equiv 56 \mod 100$.
4. Quel est le chiffre des dizaines de 123456^{789}.

Exercice 3.18
1. Déterminer les trois derniers chiffres de 49^2 et de 401^5 en utilisant la formule du binôme.
2. En déduire les trois derniers chiffres de 7^{20} puis de 7^{1001}.

Exercice 3.19
1. Calculer le pgcd de 231868 et 8190. En déduire leur ppcm.
2. Même question avec 23145 et 17.
3. Même question avec 12345 et 678.
4. Même question avec $2^{445} + 7$ et 15.

Exercice 3.20 Déterminer deux entiers u et v tels que

1. $23u + 35v = 1$,
2. $27u + 25v = 1$.

Exercice 3.21
1. Déterminer le pgcd d de $a := 2873$ et $b := 1001$ ainsi que deux entiers relatifs u et v tels que $au + bv = d$.
2. Peut-on trouver deux entiers u et v tels que $au + bv = 15$?

Exercice 3.22
1. Montrer que tout entier pair a vérifie $a^2 \equiv 0 \mod 4$.
2. Montrer que tout entier impair a vérifie $a^2 \equiv 1 \mod 8$.
3. Soient a, b, c trois entiers *impairs*.
   (a) Quel est le reste de la division de $a^2 + b^2 + c^2$ par 8 ? En déduire que ce n'est pas un carré d'un entier.
   (b) En développant $(a + b + c)^2$, montrer que $ab + bc + ac \equiv 3 \mod 4$. En déduire que ce n'est pas non plus le carré d'un entier.

Exercice 3.23
1. Montrer que si $n \in \mathbb{Z}$, alors $6 \mid n(n+1)(n+2)$.
2. Montrer de même que $24 \mid n(n+1)(n+2)(n+3)$.

Exercice 3.24
1. Montrer que si a et b sont premiers entre eux alors a et $a+b$ sont aussi premiers entre eux.
2. Montrer que si a est premier avec b et c, alors a est premier avec bc
3. Montrer que si a et b sont premiers entre eux, alors pour tous entiers naturels k et l, a^k et b^l sont aussi premiers entre eux.

Exercice 3.25 Peut-on mettre les nombres 1 à 30 dans les cases d'un tableau de 5 lignes et 6 colonnes de sorte qu'en additionnant les nombres de chaque colonne on trouve toujours la même somme ? Et avec un tableau à 6 lignes et 5 colonnes ?

Exercice 3.26
1. Montrer que si n est un entier quelconque, alors $8n+7$ et $6n+5$ sont toujours premiers entre eux.
2. Même question avec $2n+3$ et n^2+3n+2.
3. Même question avec $5^{n+1}+6^{n+1}$ et 5^n+6^n.

Exercice 3.27
1. Résoudre dans $\mathbb{Z}$ l'équation $6a+11b=0$.
2. Résoudre dans $\mathbb{Z}$ l'équation $6a+11b=1$.
3. Résoudre dans $\mathbb{Z}$ l'équation $6a+12b=5$.

Exercice 3.28 Résoudre

$$a, b \in \mathbb{N}, \quad a \wedge b = 18 \text{ et } a \vee b = 360?$$

Exercice 3.29 On veut résoudre

$$a, b \in \mathbb{Z}_{>0}, \quad \begin{cases} a+b=51 \\ a \vee b = 216. \end{cases} \tag{3.1}$$

1. Décomposer 51, 72 et 216 en produits de facteurs premiers.
2. Quel est le pgcd de 51 et 216 ?
3. Déterminer toutes les décompositions de 72 et 216 en produits d'entiers naturels premiers entre eux.
4. Montrer que si a et b sont solutions du système (3.1), alors leur pgcd divise celui de 51 et 216.
5. Conclure.

Exercice 3.30
1. Montrer que si $a, b \geq 2$ sont premiers entre eux, alors $\dfrac{\ln(a)}{\ln(b)}$ est irrationnel.
2. Montrer que si $a, b \in \mathbb{Q}$ sont tels que $ab, a+b \in \mathbb{Z}$, alors $a, b \in \mathbb{Z}$.

Exercice 3.31 Les nombres 111, 1111, 11111 (persévérer), 111111 sont ils premiers ?

Exercice 3.32 Décomposer en produit de facteurs premiers les entiers 46848, 2379, 1001 et 2873.

Exercice 3.33 Montrer que l'intervalle $[n!+2, n!+n]$ ne contient aucun nombre premier. Montrer que l'on peut trouver mille nombres entiers consécutifs qui ne sont pas premiers.

Exercice 3.34 Montrer que si $10 \leq n \leq 120$, alors n est premier si et seulement si $n \wedge 210 = 1$.

Exercice 3.35

1. Montrer que si p premier divise à la fois $a+b$ et ab, alors p divise nécessairement a et b.
2. En déduire que si a et b sont premiers entre eux, alors $a+b$ et ab sont aussi premiers entre eux.

Exercice 3.36 — Nombres de Fermat.

1. Montrer que si $q \in \mathbb{N}$ est *impair*, alors
$$x^q + 1 = (x+1)\sum_{k=0}^{q-1}(-1)^k x^k.$$
2. Montrer que, pour $m > 0$, si $2^m + 1$ est premier, alors $m = 2^n$ avec $n \in \mathbb{N}$.
3. Montrer que $2^{16} = 65536 \equiv 154 \mod 641$. En déduire que $2^{32} + 1 \equiv 0 \mod 641$ n'est pas premier.

Exercice 3.37 — Nombres de Mersenne.

1. Montrer que si $a^n - 1$ est premier et $a, n \geq 2$, alors $a = 2$ et n est premier.
2. Montrer que $2^{11} - 1 \equiv 0 \mod 23$ n'est pas premier.

Exercice 3.38

1. Soit $a \in \mathbb{N}$ et $n \in \mathbb{N}$. Montrer qu'il existe $b \in \mathbb{N}$ tel que $a = b^n$ si et seulement si $n \mid v_p(a)$ pour tout nombre premier p.
2. Montrer que si $a \in \mathbb{N}$ est à la fois un carré et un cube, alors c'est une puissance sixième.
3. Soient $a, b \in \mathbb{N}$ premiers entre eux. Montrer que si ab est un carré, alors a et b aussi.

Exercice 3.39

1. Montrer (par l'absurde) que si $n \equiv 3 \mod 4$, alors il existe un nombre premier p tel que $p \mid n$ et $p \equiv 3 \mod 4$.
2. Montrer que si $p_1, \ldots, p_r$ sont des entiers, alors $4p_1 \ldots p_r - 1 \equiv 3 \mod 4$.
3. En déduire qu'il existe une infinité de nombres premiers de la forme $4k-1$ avec $k \in \mathbb{N}$.

Bibliographie

[BS09] Stéphane Balac et François Sturm. *Algèbre et analyse : cours de mathématiques de première année avec exercices corrigés*. Presses polytechniques et universitaires romandes, 2009.

[Bou70] Nicolas Bourbaki. *Éléments de mathématique. Théorie des ensembles*. Hermann, Paris, 1970, 349 pp. (not consecutively paged) (cf. page 35).

[Esc16] Jean-Pierre Escofier. *Toute l'algèbre pour la licence*. Dunod, 2016.

[Hal67] Paul Halmos. *Introduction à la théorie des ensembles*. Eyrolles, 1967.

[Kri07] Jean-Louis Krivine. *Théorie des ensembles*. 2e édition. Numéro 5. Paris : Cassini, 2007 (cf. page 35).

[LM03a] François Liret et Dominique Martinais. *Algèbre - 1re année*. Dunod, 2003.

[LM03b] François Liret et Dominique Martinais. *Algèbre et géométrie - 2e année*. Dunod, 2003.

[RW13] Jean-Pierre Ramis et André Warusfel. *Mathématiques Tout en un pour la Licence 1 - 2e édition*. Dunod, 2013.

[ST77] Ian Stewart et David Tall. *The foundations of mathematics*. Oxford University Press, 1977.

[Was08] Pierre Wassef. *Arithmétique*. Vuibert, 2008.