Algèbre 1 pour les informaticiens

Année scolaire 2022-2023

Table des matières

1 Calcul Algébrique **2**
1.1 Point sur les ensembles de nombres . . . 2
1.1.1 Axiomatique . . . 2
1.2 Opérations sur les fractions . . . 3
1.3 Sommes . . . 5
1.3.1 Quelques sommes importantes . . . 6
1.3.2 Sommes téléscopiques . . . 7
1.4 Puissances . . . 7

2 Ensembles et applications **9**
2.1 Ensembles . . . 9
2.2 Applications . . . 11

3 Logique **14**
3.1 Opérations sur les prédicats . . . 14
3.1.1 Négation . . . 14

4 Nombres complexes **16**
4.1 Vision algébrique des nombres complexes . . . 16
4.2 Vision géométrique des nombres complexes . . . 18
4.3 Géométrie des nombres complexes . . . 21
4.3.1 Equation d'une droite . . . 21

5 Arithmétique **23**
5.1 Divisibilité . . . 23
5.2 PGCD et PPCM . . . 24
5.3 Algorithme d'Euclide . . . 25
5.4 Nombres premiers . . . 26
5.5 Congruences . . . 28

Chapitre 1

Calcul Algébrique

1.1 Point sur les ensembles de nombres

Définition 1.1.1 (Ensemble des nombres entiers naturels).

$$\mathbb{N} = \{0; 1; ...\}$$

Définition 1.1.2 (Ensemble des nombres entiers relatifs).

$$\mathbb{Z} = \{...; -1; 0; 1; ...\}$$

Définition 1.1.3 (Ensemble des nombres rationnels).

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{N}^* \right\}$$

Définition 1.1.4. Ensemble des nombres réels

$$\mathbb{R} =]-\infty; +\infty[$$

1.1.1 Axiomatique

Ici $\mathbb{K}$ désigne soit $\mathbb{N}$, soit $\mathbb{Z}$, soit $\mathbb{Q}$, soit $\mathbb{R}$

Proposition 1.1.1 (Loi de composition $+$).

1. Associativité :

$$\forall (a, b, c) \in \mathbb{K}^3,\ a + (b + c) = (a + b) + c$$

2. Commutativité :

$$\forall (a, b) \in \mathbb{K}^2,\ a + b = b + a$$

3. Existence d'un élément neutre :

$$\forall a \in \mathbb{K},\ a + 0 = a$$

4. Symétrie :

$$\forall (a, a') \in \mathbb{K}^2,\ a + a' = 0 \text{ avec } a' = -a$$

Remarque : Cette propriété ne s'applique pas dans $\mathbb{N}$

Proposition 1.1.2 (Loi de composition $\cdot$)**.**

1. Associativité :

$$\forall(a,b,c)\in\mathbb{K}^3,\ (a\cdot b)\cdot c = a\cdot(b\cdot c)$$

2. Commutativité :

$$\forall(a,b)\in\mathbb{K}^3,\ a\cdot b = b\cdot a$$

3. Existence d'un élément neutre : $\forall a\in\mathbb{K}$

$$a\cdot 1 = a$$
$$a\cdot 0 = 0$$

4. Distributivité : $\forall(a,b,c)\in\mathbb{K}^3$

$$a\cdot(b+c) = a\cdot b + a\cdot c$$
$$(a+b)\cdot c = a\cdot c + b\cdot c$$

1.2 Opérations sur les fractions

Proposition 1.2.1 (Addition sur les fractions)**.**

$$\forall(a,b,c,d)\in\mathbb{Z}^4,\ \frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$$

Démonstration.
$\forall(a,b,c,d,a',b',c',d')\in\mathbb{Z}^8$
D'après la proposition on a :

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$$

et :

$$\frac{a'}{b'}+\frac{c'}{d'}=\frac{a'd'+b'c'}{b'd'}$$

Montrons que :

$$\frac{ad+bc}{bd}=\frac{a'd'+b'c'}{b'd'}$$

On suppose que :

$$\frac{a}{b}=\frac{a'}{b'} \iff a'b=ab'$$
$$\frac{c}{d}=\frac{c'}{d'} \iff c'd=cd'$$

On aurait donc :

$$\frac{ad+bc}{bd}=\frac{a'd'+b'c'}{b'd'}$$
$$\iff (ad+bc)b'd' = bd(a'd'+b'c')$$
$$\iff (ad+bc)b'd' - bd(a'd'+b'c') = 0$$

$$\begin{aligned}(ad+bc)b'd' - bd(a'd'+b'c') &= (adb'd' + bcb'd') - (bda'd' + bdb'c') \\ &= adb'd' + bcb'd' - bda'd' - bdb'c' \\ &= adb'd' - a'd'bd + bcb'd' - b'c'bd \\ &= ab'dd' - a'bdd' + cd'bb' - c'dbb' \\ &= (ab' - a'b)dd' + (cd' - c'd)dd'\end{aligned}$$

D'après l'hypothèse de départ :

$$\begin{aligned}ab' = a'b &\iff ab' - a'b = 0 \\ cd' = c'd &\iff cd' - c'd = 0\end{aligned}$$

Donc :

$$(\underbrace{ab' - a'b}_{0})dd' + (\underbrace{cd' - c'd}_{0})dd' = 0$$

On obtient alors :

$$(ad+bc)b'd' - bd(a'd'+b'c') = 0$$

□

Proposition 1.2.2 (Multiplication sur les fractions)**.**

$$\forall (a,b,c,d) \in \mathbb{Z}^4,\ \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$$

Démonstration.
$\forall (a,b,c,d,a',b',c',d') \in \mathbb{Z}^8$
D'après la proposition on a :

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

et :

$$\frac{a'}{b'} \cdot \frac{c'}{d'} = \frac{a'c'}{b'd'}$$

Montrons que :

$$\frac{ac}{bd} = \frac{a'c'}{b'd'}$$

On suppose que :

$$\begin{aligned}\frac{a}{b} = \frac{a'}{b'} &\iff a'b = ab' \\ \frac{c}{d} = \frac{c'}{d'} &\iff c'd = cd'\end{aligned}$$

On aurait donc :

$$\begin{aligned}&\frac{ac}{bd} = \frac{a'c'}{b'd'} \\ &\iff acb'd' = bda'c' \\ &\iff acb'd' - bda'c' = 0\end{aligned}$$

$$\begin{aligned}acb'd' - bda'c' &= (ab')(cd') - (a'b)(c'd) \\ &= (ab')(cd') - (a'b)(cd') + (a'b)(cd') - (a'b)(c'd) \\ &= (ab' - a'b)(cd') + (cd' - c'd)(a'b)\end{aligned}$$

D'après l'hypothèse de départ :

$$\begin{aligned} ab' = a'b &\iff ab' - a'b = 0 \\ cd' = c'd &\iff cd' - c'd = 0 \end{aligned}$$

Donc :

$$(\underbrace{ab' - a'b}_{0})(cd') + (\underbrace{cd' - c'd}_{0})(a'b) = 0$$

On obtient alors :

$$acb'd' - bda'c' = 0$$

□

1.3 Sommes

Définition 1.3.1 (Définition de la somme)**.** $\forall m, n \in \mathbb{N}$ avec $m \leqslant n$ et $a_k \in \mathbb{R},\ m \leqslant k \leqslant n$

$$\sum_{k=m}^{n} a_k = a_m + a_{m+1} + \cdots + a_n$$

Remarque 1.3.1. L'indice de sommation est important car :

$$\sum_{k=m}^{n} a_l = \underbrace{a_l + a_l + \cdots + a_l}_{n-m+1 \text{termes}} = (n - m + 1)a_l$$

Proposition 1.3.1 (Linéarité de la somme)**.** $\forall m, n \in \mathbb{N}$ avec $m \leqslant n$ et $a_k, b_k \in \mathbb{R},\ m \leqslant k \leqslant n$

$$\sum_{k=m}^{n} (a_k + b_k) = \sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k$$

Démonstration. $\forall m, n \in \mathbb{N}$ avec $m \leqslant n$ et $a_k, b_k \in \mathbb{R},\ m \leqslant k \leqslant n$

$$\begin{aligned} \sum_{k=m}^{n} (a_k + b_k) &= (a_m + b_m) + (a_{m+1} + b_{m+1}) + \cdots (a_n + b_n) \\ &= (a_m + a_{m+1} + \cdots + a_n) + (b_m + b_{m+1} + \cdots + b_n) \\ &= \sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k \end{aligned}$$

□

Proposition 1.3.2 (Linéarité de la multiplication de la somme par une constante)**.** $\forall m, n \in \mathbb{N}$ avec $m \leqslant n$ et $a_k, \lambda \in \mathbb{R},\ m \leqslant k \leqslant n$

$$\sum_{k=m}^{n} (\lambda a_k) = \lambda \sum_{k=m}^{n} a_k$$

Démonstration. $\forall m, n \in \mathbb{N}$ avec $m \leqslant n$ et $a_k, \lambda \in \mathbb{R},\ m \leqslant k \leqslant n$

$$\begin{aligned} \sum_{k=m}^{n} (\lambda a_k) &= \lambda a_m + \lambda a_{m+1} + \cdots + \lambda a_n \\ &= \lambda(a_m + a_{m+1} + \cdots + a_n) \end{aligned}$$

□

1.3.1 Quelques sommes importantes

1. $\displaystyle\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ avec $n \in \mathbb{N}$
2. $\displaystyle\sum_{k=1}^{n} (a + (k-1)\,d) = \frac{1}{2}n\,(2a + (n-1)\,d)$ avec $n \in \mathbb{N}$ et $a, d \in \mathbb{R}$
3. $\displaystyle\sum_{k=0}^{n-1} ar^k = \sum_{k=1}^{n} ar^{k-1} = a \cdot \frac{1-r^n}{1-r}$ avec $n \in \mathbb{N}$ et $a, r \in \mathbb{R}$

Démonstration. 1 On pose $\mathrm{S} = \displaystyle\sum_{k=1}^{n} k$ avec $n \in \mathbb{N}$

On a donc :

$$\begin{aligned} S =& 1 + 2 + \cdots + (n-1) + n \\ & n + (n-1) + \cdots + 2 + 1 = S \end{aligned}$$

En additionnant les termes du "dessus" et du "dessous" on obtient :

$$\begin{aligned} 2S &= n \cdot (n+1) \\ S &= \frac{n(n+1)}{2} \end{aligned}$$

□

Démonstration. 2 On pose $\mathrm{S} = \displaystyle\sum_{k=1}^{n} (a + (k-1)\,d)$ avec $n \in \mathbb{N},\ a, d \in \mathbb{R}$

$$\begin{aligned} S = \sum_{k=1}^{n} (a + (k-1)\,d) &= \sum_{k=1}^{n} (a - d + dk) \\ &= \sum_{k=1}^{n} (a-d) + \sum_{k=1}^{n} dk \\ &= \sum_{k=1}^{n} (a-d) + d\sum_{k=1}^{n} k \\ &= n(a-d) + d\frac{n(n+1)}{2} \\ &= n\left((a-d) + \frac{d(n+1)}{2}\right) \\ &= \frac{1}{2}n\,(2\,(a-d)) + d(n+1)) \\ &= \frac{1}{2}n(2a - 2d + nd + d) \\ &= \frac{1}{2}n(2a - d + nd) \\ &= \frac{1}{2}n(2a + (n-1)d) \end{aligned}$$

□

Démonstration. 3 On pose S $= \sum_{k=0}^{n-1} ar^k$ avec $n \in \mathbb{N},\ a, r \in \mathbb{R}$

$$\begin{aligned} S &= a + ar + \cdots + ar^{n-1} \\ rS &= ar + ar^2 + \cdots + ar^n \end{aligned}$$

$$\begin{aligned} S - rS = (a &+ ar + \cdots + ar^{n-1}) \\ &-(ar + \cdots + ar^{n-1} + ar^n) \end{aligned}$$

$$\begin{aligned} (1-r)S &= a - ar^n \\ S &= a \cdot \frac{1-r^n}{1-r} \end{aligned}$$

□

1.3.2 Sommes téléscopiques

Proposition 1.3.3 (Somme téléscopique)**.** $\forall m, n \in \mathbb{N}$ avec $m \leqslant n,\ a_k \in \mathbb{R}$ avec $m \leqslant k \leqslant n$

$$\sum_{k=m}^{n} (a_k - a_{k-1}) = a_n - a_{m-1}$$

Démonstration. $\forall m, n \in \mathbb{N}$ avec $m \leqslant n,\ a_k \in \mathbb{R}$ avec $m \leqslant k \leqslant n$

$$\begin{aligned} \sum_{k=m}^{n} (a_k + a_{k-1}) = &(\underline{a_m} - a_{m-1}) \\ &+(\underline{a_{m+1}} - \underline{a_m}) \\ &+(a_{m+2} - \underline{a_{m+1}}) \\ &\vdots \\ &+(\underline{a_{n-1}} - \underline{a_{n-2}}) \\ &+(a_n - \underline{a_{n-1}}) \\ \sum_{k=m}^{n} (a_k + a_{k-1}) = &\ a_n - a_{m-1} \end{aligned}$$

□

1.4 Puissances

Définition 1.4.1 (Puissance d'un réel)**.** $\forall a \in \mathbb{R},\ \forall n \in \mathbb{N}$

$$a^n = \underbrace{a \times a \times \cdots \times a}_{nfois}$$

Proposition 1.4.1 (Propriétés des puissances)**.** $\forall a \in \mathbb{R},\ \forall m, n \in \mathbb{N}$

1. $a^m \times a^n = a^{m+n}$
2. $(a^m)^n = a^{mn}$
3. $\dfrac{a^n}{a^m} = a^{n-m}, a \neq 0$

4. $a^{-m} = \dfrac{1}{a^m}, a \neq 0$
5. $a^0 = 1$

Démonstration. 1 $\forall a \in \mathbb{R},\ \forall n, m \in \mathbb{N}$

$$\begin{aligned} a^m \times a^n &= \underbrace{(a \times a \times \cdots \times a)}_{mfois} \times \underbrace{(a \times a \times \cdots \times a)}_{nfois} \\ &= \underbrace{a \times a \times \cdots \times a}_{m+nfois} \end{aligned}$$

□

Démonstration. 2 $\forall a \in \mathbb{R},\ \forall n, m \in \mathbb{N}$

$$(a^m)^n = \underbrace{\underbrace{(a \times a \times \cdots \times a)}_{mfois} \times \underbrace{(a \times a \times \cdots \times a)}_{mfois} \times \cdots \times \underbrace{(a \times a \times \cdots \times a)}_{mfois}}_{nfois} = \underbrace{a \times a \times \cdots \times a}_{m \times nfois}$$

□

Démonstration. 3 $\forall a \in \mathbb{R}^*,\ \forall n, m \in \mathbb{N}$

$$\frac{a^n}{a^m} = \frac{\overbrace{a \times a \cdots \times a}^{nfois}}{\underbrace{a \times a \cdots \times a}_{mfois}} = \underbrace{a \times a \times \cdots \times a}_{n-mfois}$$

□

Démonstration. 4 $\forall a \in \mathbb{R}^*,\ \forall m \in \mathbb{N}$

$$\begin{aligned} a^{-m} &= a^{0-m} \\ &= \frac{a^0}{a^m} \\ &= \frac{1}{a^m} \end{aligned}$$

□

Démonstration. 5 $\forall a \in \mathbb{R}$

$$\begin{aligned} a^1 &= a \\ a^0 &= \frac{a}{a} = 1 \end{aligned}$$

□

Chapitre 2

Ensembles et applications

2.1 Ensembles

Définition 2.1.1 (Définition intuitive d'un ensemble)**.** Un ensemble E est une collection d'objets appelés éléments. Si E contient un élément x, on dit que x appartient à E, noté $x \in E$

Définition 2.1.2 (Ensemble vide)**.** L'ensemble vide noté $\emptyset$ est l'ensemble ne contenant aucun élément.

Définition 2.1.3 (Inclusion)**.**

$$\text{Un ensemble F est inclus dans un ensemble E} \iff \forall x \in F,\ x \in E.$$

On note : $F \subset E$ On dit aussi que F est un sous-ensemble, une partie de E

Définition 2.1.4 (Egalité d'ensembles)**.**

$$\text{Deux ensembles E et F sont égaux} \iff E \subset F \text{ et } F \subset E$$

Définition 2.1.5 (Singleton)**.** Un singleton est un ensemble de ne contenant qu'un seul élément (noté entre accolades).

Définition 2.1.6 (Réunion d'ensembles)**.** Soient E et F deux ensembles.

$$E \cup F \text{ (lu E union F) } = \{\forall x,\ x \in E \text{ ou } x \in F\}$$

Définition 2.1.7 (Intersection d'ensembles)**.** Soient E et F deux ensembles.

$$E \cap F \text{ (lu E inter F) } = \{\forall x,\ x \in E \text{ et } x \in F\}$$

Proposition 2.1.1 (Propriétés sur les ensembles)**.** Soient A, B, C, E des ensembles

1. Associativité :

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

2. Elément neutre :

$$A \cup \emptyset = A$$
$$A \cap A = A$$

3. Intersection d'un ensemble et d'une partie :

$$A \subset E \iff A \cap E = E \cap A = A$$

4. Commutativité :

$$A \cup B = B \cup A$$
$$A \cap B = B \cap A$$

5. Distributivité :

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

Définition 2.1.8 (Complémentaire d'un ensemble)**.**

$$E \backslash F = \{\forall x,\ x \in E \text{ et } x \notin F\}$$

Remarque 2.1.1. Soient E, F des ensembles.
— $(E \backslash F) \subset E$
— $(E \backslash F) \cap F = \emptyset$
— $E \backslash F \neq F \backslash E$

Remarque 2.1.2. Soient E et A des ensembles.

$$A \subset E$$
$$A^C = E \backslash A$$
$$(A^C)^C = A$$

Proposition 2.1.2 (Lois de Morgan)**.** Soient A et B des ensembles.
1. $(A \cup B)^C = A^C \cap B^C$
2. $(A \cap B)^C = A^C \cup B^C$

Démonstration. 1
Soient A et B des ensembles et x un élément quelconque.
$\boxed{\subset}$ Par définition du complémentaire :

$$x \in (A \cup B)^C \iff x \notin (A \cup B)$$

$x \notin A$ car $A \subset (A \cup B)$ ce qui impliquerait que $x \in (A \cup B)$ et donc il y aurait une contradiction. On obtient une contradiction similaire si on suppose que $x \in B$. Ainsi on a $x \in A^C$ et $x \in B^C$, donc par la définition de l'intersection on a :

$$x \in (A^C \cap B^C)$$

d'où :

$$(A \cup B)^C \subset (A^C \cap B^C)$$

$\boxed{\supset}$ Par définition de l'intersection :

$$\begin{aligned} x \in (A^C \cap B^C) &\iff x \in A^C \text{ et } x \in B^C \\ &\iff x \notin A \text{ et } x \notin B \\ &\iff x \in (A \cup B)^C \end{aligned}$$

d'où :

$$(A^C \cap B^C) \subset (A \cup B)^C$$

Ainsi :

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

□

Démonstration. 2
Soient A et B des ensembles et x un élément quelconque.
$\boxed{\subset}$ Par définition du complémentaire :

$$\begin{aligned} x \in (A \cap B)^C &\iff x \notin (A \cap B) \\ &\iff x \notin A \text{ et } x \notin B \\ &\iff x \in A^C \text{ et } x \in B^C \\ &\iff x \in (A^C \cap B^C) \end{aligned}$$

Sachant que :

$$(A^C \cap B^C) \subset (A^C \cup B^C)$$

On a :

$$x \in (A^C \cap B^C) \implies x \in (A^C \cup B^C)$$

d'où :

$$(A \cap B)^C \subset (A^C \cup B^C)$$

$\boxed{\supset}$ Par définition de la réunion :

$$\begin{aligned} x \in (A^C \cup B^C) &\iff x \in A^C \text{ ou } x \in B^C \\ &\iff x \notin A \text{ ou } x \notin B \\ &\iff x \notin (A \cap B) \\ &\iff x \in (A \cap B)^C \end{aligned}$$

Ainsi :

$$(A^C \cap B^C) \subset (A \cup B)^C$$

Donc :

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

□

Définition 2.1.9 (Produit cartésien)**.** Soient E et F des ensembles
- $E \times F = \{(x, y),\ x \in E,\ y \in F\}$
- $E \times E = E^2$
- $E \times E \times E = E^3$

2.2 Applications

Définition 2.2.1 (Application)**.** Soient E et F deux ensembles. $f : E \to F$ est une application si pour chaque $x \in E$, on associe un élément de F noté $f(x)$

Définition 2.2.2 (Injectivité)**.** Soit $f : E \to F$, on dit que f est injective si pour chaque élément de F, il y a au plus un élément de E qui y est associé. Autrement dit :

$$\text{f injective} \iff \{\forall (x_1, x_2) \in E^2, f(x_1) = f(x_2) \implies x_1 = x_2\}$$

Définition 2.2.3 (Surjectivité)**.** Soit $f : E \to F$, on dit que f est surjective si pour chaque élément de F, il y a au moins un élément de E qui y est associé. Autrement dit :

$$\text{f surjective} \iff \{\forall y \in F, \exists x \in E, y = f(x)\}$$

Définition 2.2.4 (Bijectivité)**.** Soit $f : E \to F$, on dit que f est bijective si elle est injective et surjective, c'est-à-dire que pour chaque élément de F, il y a exactement un élément de E qui y est associé. Autrement dit :

$$\text{f bijective} \iff \{\forall y \in F, \exists! x \in E, y = f(x)\}$$

Définition 2.2.5 (Ensemble fini)**.** Un ensemble E est un ensemble fini non-vide si et seulement si pour tout entier $n \geqslant 1$, il existe une application bijective de $\{1, 2, \ldots, n\}$ dans E.

Définition 2.2.6 (Fonction réciproque)**.** Soient E et F deux ensembles. Supposons que $f : E \to F$ est une application bijective. On peut définir l'application

$$f^{-1} : \begin{cases} F & \to E \\ y & \mapsto x \end{cases}$$

comme étant la réciproque de f.

Définition 2.2.7 (Composition)**.** Soient f et g deux applications telles que : $f : E \to F$ et $g : F \to G$ on a l'application $g \circ f : E \to G$ qui est définie comme étant la composée de f et de g.

Définition 2.2.8 (Image directe et image réciproque)**.** Soient $f : E \to F$ une application, A une partie de E et B une partie de F. Nous avons :
- $f(A) = \{f(x), x \in A\}$: image directe
- $f^{-1}(B) = \{x \in E, f(x) \in B\}$: image réciproque

Proposition 2.2.1 (Propriétés sur les images directes et réciproques)**.** Soient $f : E \to F$ une application et A, B des parties de F.
1. $f^{-1}(F \backslash A) = E \backslash f^{-1}(A)$
2. $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$
3. $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$
4. $f(A \cup B) = f(A) \cup f(B)$
5. $f(A \cap B) \subset f(A) \cap f(B)$

Démonstration. 5 : $f(A \cap B) \subset f(A) \cap f(B)$

Soit $y \in f(A \cap B) = \{f(x), x \in A \cap B\}$, par définition : $\exists x \in A \cap B, y = f(x)$

$$\begin{aligned} x \in A \cap B &\iff x \in A \wedge x \in B \\ x \in A &\implies y = f(x) \subset f(A) \\ x \in B &\implies y = f(x) \subset f(B) \end{aligned}$$

d'où $y \in f(A) \cap f(B)$ $\square$

Remarque 2.2.1.

$$f(A \cap B) \neq f(A) \cap f(B)$$

Chapitre 3

Logique

Définition 3.0.1 (Assertion)**.** Une **assertion** est une affirmation mathématique qui peut être vraie pou fausse.

Définition 3.0.2 (Prédicat)**.** Un **prédicat** est une "assertion" dépendant d'une ou plusieurs variables.

Exemple 3.0.1.
— "Tous les entiers sont des nombres rationnels" est une assertion.
— "L'entier n est pair" est un prédicat.
— "Le réel x est le carré d'un nombre réel" est un prédicat.

3.1 Opérations sur les prédicats

P	Q	P et Q	P ou Q	non(P)	P $\implies$ Q
V	V	V	V	F	V
V	F	F	V	F	F
F	V	F	V	V	V
F	F	F	F	V	V

3.1.1 Négation

1. $P \implies Q$ est équivalent à non(P) ou Q
2. non(P ou Q) est équivalent à non(P) et non(Q)
3. non(P et Q) est équivalent à non(P) ou non(Q)

Remarque 3.1.1.
1. Pour contredire "tous les éléments de E ont une propriété P", il suffit de trouver un contre-exemple

$$non(\forall x \in E, P(x)) \iff \exists x \in E, non(P(x))$$

2. Pour contredire "il existe un élément de E vérifiant une propriété P", il faut montrer que tous les éléments de E ne vérifient pas la propriété P.

$$non(\exists x \in E, P(x)) \iff \forall x \in E, non(P(x))$$

3. Une affirmation de type :

$$\exists! x \in E, P(x) \iff \begin{cases} \exists x \in E, P(x) \\ \text{Si } P(x) \text{ et } P(y) \text{ sont vrais, alors } x = y \end{cases}$$

Remarque 3.1.2.
$\{(a_n)\}_{n\in\mathbb{N}} \subset \mathbb{R}$, $\lim\limits_{n\to+\infty} a_n = \alpha \in \mathbb{R}$
A. Cauchy :

$$\forall \varepsilon > 0, \exists N, |a_n - \alpha| < \varepsilon, \forall n \geqslant N$$

Chapitre 4

Nombres complexes

$$(\mathbb{N}, +, \times) \subset (\mathbb{Z}, +, \times) \subset (\mathbb{Q}, +, \times) \subset (\mathbb{R}, +, \times) \subset (\mathbb{C}, +, \times)$$

L'ensemble des nombres complexes est adapté à la résolution des équations algébriques.

4.1 Vision algébrique des nombres complexes

Définition 4.1.1 (Forme algébrique des nombres complexes)**.**

$$\mathbb{C} = \{a + ib \mid (a, b) \in \mathbb{R}^2\}, \text{ avec } i = \sqrt{-1}$$

Proposition 4.1.1 (Opérations sur les nombres complexes)**.**

1. Somme : Soient $z = a + ib \in \mathbb{C}, \omega = c + id \in \mathbb{C}, (a, b, c, d) \in \mathbb{R}^4$

$$z + \omega = a + c + i(b + d)$$

   (a) Associativité : $(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3), (z_1, z_2, z_3) \in \mathbb{C}^3$
   (b) Elément neutre : $0 = 0 + i0 \implies z + 0 = 0 + z = z,\ z \in \mathbb{C}$
   (c) Symétrique : $\forall z \in \mathbb{C}, \exists z', z + z' = z' + z = 0, z' = -z$

$$z = a + ib \implies -z = -a + i(-b)$$

   (d) Commutativité : $z + \omega = \omega + z$

2. Produit : Soient $z = a + ib \in \mathbb{C}, \omega = c + id \in \mathbb{C}, (a, b, c, d) \in \mathbb{R}^4$

$$z \cdot \omega = (ac - bd) + i(ad + bc)$$

   (a) Associativité :

$$(z_1 \cdot z_2) \cdot z_3 = z_1 \cdot (z_2 \cdot z_3), \forall (z_1, z_2, z_3) \in \mathbb{C}^3$$

   (b) Elément neutre :

$$1 = 1 + i0 \implies z \times 1 = 1 \times z = z$$
$$\forall z \in \mathbb{C} \backslash \{0\}, \exists z' \in \mathbb{C}, z \cdot z' = z' \cdot z = 1$$

   (c) Commutativité :

$$z \cdot \omega = \omega \cdot z, \forall (z, \omega) \in \mathbb{C}^2$$

   (d) Distributivité :

$$(z_1 + z_2) \cdot \omega = z_1 \cdot \omega + z_2 \cdot \omega$$
$$z \cdot (\omega_1 + \omega_2) = z \cdot \omega_1 + z \cdot \omega_2$$
$$\forall (z, z_1, z_2, \omega, \omega_1, \omega_1) \in \mathbb{C}^6$$

Démonstration. Produit

$$\begin{aligned} z\cdot\omega &= (a+ib)\cdot(c+id) \\ &\text{“=”}\ a\cdot(c+id)+ib\cdot(c+id) \\ &\text{“=”}\ a\cdot c+a\cdot id+ib\cdot c+ib\cdot id \\ &\text{“=”}\ ac+i(ad)+i(bc)+i^2bd \\ &\text{“=”}\ ac-bd+i(ad+bc) \end{aligned}$$

□

Remarque 4.1.1. $(\mathbb{C},+,\times)$ est un corps commutatif

Définition 4.1.2 (Conjugué d'un nombre complexe)**.** Soit $z=a+ib$ un nombre complexe, le nombre $\overline{z}=a-ib$ est dit le conjugué de z.

Proposition 4.1.2. Soient $z=a+ib, z'=a-ib, (a,b)\in\mathbb{R}^2, z\in\mathbb{C}$

$$z\cdot z'=a^2+b^2$$

Démonstration.

$$\begin{aligned} z\cdot z' &= (a+ib)(a-ib) \\ &= a^2-iab+iab-i^2b^2 \\ &= a^2+b^2 \end{aligned}$$

□

Définition 4.1.3 (Module d'un nombre complexe)**.** Soit $z=a+ib$ un nombre complexe, on définit son module comme étant :

$$|z|=\sqrt{a^2+b^2}$$

Proposition 4.1.3 (Propriétés des modules)**.** Soient $z=a+ib$ et $z=a'+ib'$ des nombres complexes, on a les propriétés suivantes sur les modules :
- $|z\cdot z'|=|z|\cdot|z'|$
- $\left|\frac{z}{z'}\right|=\frac{|z|}{|z'|}$
- $|z+z'|\leqslant|z|+|z'|$
- $|z|^2=z\cdot\overline{z}=a^2+b^2$
- $|z|\geqslant 0$
- $|z|=0 \iff z=0$
- $|z|=|\overline{z}|=|-z|=|-\overline{z}|$

Définition 4.1.4 (Partie réelle et partie imaginaire)**.** Soit $z=a+ib\in\mathbb{C}, (a,b)\in\mathbb{R}^2$

$$\begin{aligned} \Re(z) &= Re(z)=a \text{ (Partie réelle)} \\ \Im(z) &= Im(z)=b \text{ (Partie imaginaire)} \end{aligned}$$

Proposition 4.1.4.
- $z+\overline{z}=(a+ib)+(a-ib)=2a \implies \Re(z)=\dfrac{z+\overline{z}}{2}$
- $z-\overline{z}=(a+ib)-(a-ib)=2ib \implies \Im(z)=\dfrac{z-\overline{z}}{2i}$

4.2 Vision géométrique des nombres complexes

Définition 4.2.1 (Argument d'un nombre complexe)**.** Soit z un nombre complexe, l'argument de z, noté $\arg(z)$ représente l'angle entre la droite des réels et celle issue de l'origine et passant par z.

Proposition 4.2.1 (Propriétés des arguments)**.** Soient $z, z_1, z_2 \in \mathbb{C}^3, n \in \mathbb{N}$
- $\arg(z_1 \cdot z_2) = \arg z_1 + \arg z_2$
- $\arg z^n = n \arg z$
- $\arg \frac{z_1}{z_2} = \arg z_1 - \arg z_2$
- $\arg \frac{1}{z} = -\arg z$

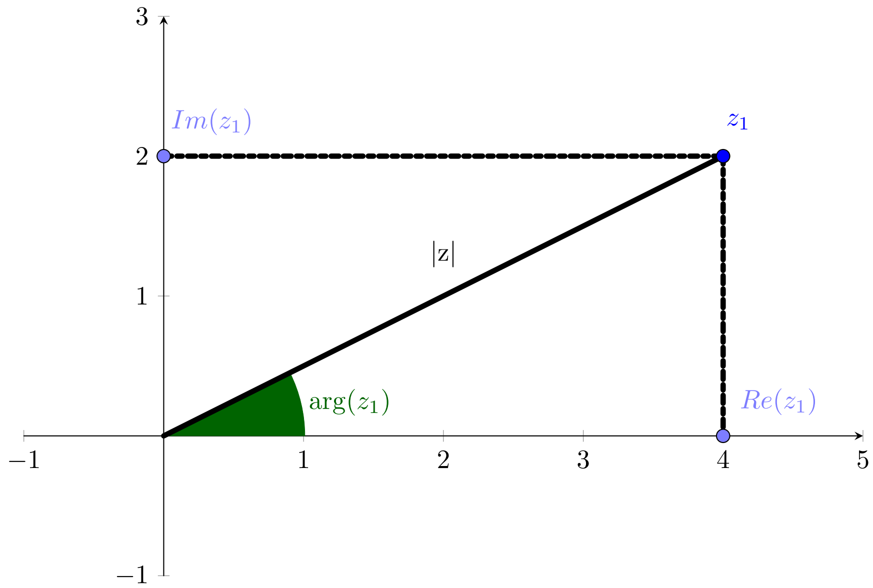

FIGURE 4.1 – Vision géométrique des nombres complexes (Base du code par : [2])

Définition 4.2.2 (Forme trigonométrique d'un nombre complexe)**.** Soit z un nombre complexe, on peut l'écrire sous sa forme trigonométrique ainsi :

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

Avec :
- $r = |z|$
- $\theta = \arg(z)$

Proposition 4.2.2. Soient $z_1 = r_1(\cos(\theta_1) + i \sin(\theta_1))$ et $z_2 = r_2(\cos(\theta_2) + i \sin(\theta_2))$, deux nombres complexes. Nous avons la propriété suivante :

$$z_1 z_2 = r_1 r_2(\cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2))$$

Démonstration.

$$\begin{aligned}
z_1 z_2 &= (r_1(\cos(\theta_1) + i\sin(\theta_1))(r_2(\cos(\theta_2) + i\sin(\theta_2)) \\
&= (r_1\cos\theta_1 + ir_1\sin\theta_1)(r_2\cos\theta_2 + ir_2\sin\theta_2) \\
&= (r_1\cos\theta_1 \cdot r_2\cos\theta_2) + (r_1\cos\theta_1 \cdot ir_2\sin\theta_2) + (ir_1\sin\theta_1 \cdot r_2\cos\theta_2) + (ir_1\cos\theta_1 + ir_2\sin\theta_2) \\
&= (r_1\cos\theta_1)(r_2\cos\theta_2) - (r_1\sin\theta_1)(r_2\sin\theta_2) + i((r_1\cos\theta_1)(r_2\sin\theta_2) + (r_1\sin\theta_1)(r_2\cos\theta_2)) \\
&= r_1r_2((\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2) + i(\sin\theta_1\cos\theta_2 + \cos\theta_1\sin\theta_2)) \\
&= r_1r_2(\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2))
\end{aligned}$$

□

Proposition 4.2.3 (Formule de Moivre)**.**

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

Définition 4.2.3 (Forme exponentielle d'un nombre complexe)**.** On peut écrire un nombre complexe sous une forme exponentielle :

$$z = r(\cos\theta + i\sin\theta) = re^{i\theta}$$

Proposition 4.2.4 (Identité d'Euler)**.**

$$e^{i\pi} = -1$$

Proposition 4.2.5 (Formules d'Euler)**.**

$$\cos\theta = \frac{e^{i\theta} + e^{-i\theta}}{2} \qquad \sin\theta = \frac{e^{i\theta} - e^{-i\theta}}{2i}$$

Démonstration.

$$\begin{aligned}
e^{i\theta} + e^{-i\theta} &= (\cos\theta + i\sin\theta) + (\cos\theta - i\sin\theta) \\
&= 2\cos\theta \\
\frac{e^{i\theta} + e^{-i\theta}}{2} &= \cos\theta
\end{aligned}$$

$$\begin{aligned}
e^{i\theta} - e^{-i\theta} &= (\cos\theta + i\sin\theta) - (\cos\theta - i\sin\theta) \\
&= 2i\sin\theta \\
\frac{e^{i\theta} - e^{-i\theta}}{2i} &= \sin\theta
\end{aligned}$$

□

Remarque 4.2.1 (Passer de la forme algébrique à la forme trigonométrique)**.**
Soit $z = a + ib, (a,b) \in \mathbb{R}^2$ un nombre complexe sous sa forme algébrique, on peut passer sous la forme trigonométrique ainsi :

$$\cos\theta = \frac{a}{|z|} \qquad \sin\theta = \frac{b}{|z|}$$

Exemple 4.2.1. $z = 1 + i$
On a : $|z| = \sqrt{1^2 + 1^2}$

On a donc :

$$\cos\theta = \frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2} \qquad \sin\theta = \frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2}$$

On en déduit donc que $\theta = \frac{\pi}{4}$.
Ainsi $z = \sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right)$

Définition 4.2.4 (Racine n-ième d'un nombre complexe)**.** Soit $z \in \mathbb{C}$. On appelle racine n-ième du nombre complexe z tout nombre complexe $\omega \in \mathbb{C}$ vérifiant :

$$\omega^n = z$$

Proposition 4.2.6. Un complexe non nul $z = \rho e^{i\theta}$ $(\rho = |z|)$ admet n racines n-ièmes données par :

$$\omega = \rho^{\frac{1}{n}} e^{i\left(\frac{\theta}{n} + \frac{2k\pi}{n}\right)}$$

Démonstration. On cherche à résoudre

$$\omega^n = z,\ (n \in \mathbb{N})$$

Posons

$$\begin{cases} \omega = |\omega| e^{i\theta_1} \\ z = |z| e^{i\theta_2} \end{cases} \iff \begin{cases} \omega^n = |\omega^n| e^{in\theta_1} \\ z = |z| e^{i\theta_2} \end{cases}$$

Par identification :

$$\begin{cases} |\omega|^n = |z| \\ n\theta_1 = \theta_2 + 2k\pi,\ (k \in \mathbb{Z}) \end{cases} \iff \begin{cases} |\omega| = |z|^{\frac{1}{n}} \\ \theta_1 = \frac{\theta_2}{n} + \frac{2k\pi}{n},\ (k \in \mathbb{Z}) \end{cases}$$

En posant :

$$\begin{cases} \rho = |z| \\ \theta_2 = \theta \end{cases}$$

on obtient :

$$\omega = \rho^{\frac{1}{n}} e^{i\left(\frac{\theta}{n} + \frac{2k\pi}{n}\right)},\ (k \in \mathbb{Z})$$

□

Définition 4.2.5 (Racine n-ième de l'unité)**.** On appelle racine n-ième de l'unité, une racine n-ième de 1, on notera $\mathbb{U}_n$ l'ensemble des racines n-ièmes de l'unité :

$$\mathbb{U}_n = \{z \in \mathbb{C} | z^n = 1\}$$

Proposition 4.2.7. Les racines n-ièmes de l'unité sont de la forme :

$$\omega_k = e^{\frac{2ik\pi}{n}}, k \in [\![0, n-1]\!]$$

Démonstration. On cherche à résoudre

$$z^n = 1,\ n \in \mathbb{N}$$

Posons $z = |z|e^{i\theta}$. On obtient donc en elevant à la puissance n

$$\begin{aligned} & z^n = |z^n|e^{in\theta} = 1 \\ \iff\ & |z|^n e^{in\theta} = e^{i0} \end{aligned}$$

Par identification

$$\begin{cases} |z| = 1 \\ n\theta = 0 + 2k\pi,\ (k \in \mathbb{Z}) \end{cases}$$

On obtient alors

$$\theta = \frac{2k\pi}{n},\ (k \in \mathbb{Z})$$

Finalement on obtient bien

$$z = e^{i\frac{2k\pi}{n}},\ (k \in \mathbb{Z})$$

que l'on peut également écrire

$$z = e^{i\frac{2k\pi}{n}},\ (k \in [\![0, n-1]\!])$$

car il y a un cycle. □

4.3 Géométrie des nombres complexes

- $z \mapsto z + a, (a \in \mathbb{C})$: translation de vecteur $\vec{u}$ d'affixe a
- $z \mapsto az, (a \in \mathbb{R}^*)$: homothétie de rapport a
- $z \mapsto e^{i\theta}z, (\theta \in \mathbb{R})$: rotation d'angle θ et de centre 0
- $z \mapsto \overline{z}$: réflexion par rapport à l'axe des réels
- $z \mapsto a + e^{i\theta}(z - a)$: rotation d'angle θ de centre a
- $z \mapsto e^{2i\theta} \cdot \overline{z}$: réflexion par rapport à la droite formant un angle θ avec l'axe des réels.

4.3.1 Equation d'une droite

- L'axe des réels : $\overline{z} = z$
- Un axe formant un angle θ avec l'axe des réels : $\overline{e^{-i\theta}z} = e^{-i\theta}z$
- L'asymptote verticale de partie réelle a : $z + \overline{z} = 2a$

Exemple 4.3.1. $z \mapsto \frac{1}{z}$
On pose : $\omega = \frac{1}{z}$
On a donc : $z = \frac{1}{\omega}$
$z + \overline{z} = 2 \implies \frac{1}{\omega} + \overline{\frac{1}{\omega}} = 2 \implies \frac{1}{\omega} + \frac{1}{\overline{\omega}} = 2$
$\omega\overline{\omega}\left(\frac{1}{\omega} + \frac{1}{\overline{\omega}}\right) = 2\omega\overline{\omega}$
On a donc : $\overline{\omega} + \omega = 2\omega\overline{\omega} \implies 2\omega\overline{\omega} - \omega - \overline{\omega} = 0$
C'est à dire : $\omega\overline{\omega} - \frac{1}{2}\omega - \frac{1}{2}\overline{\omega} = \left(\omega - \frac{1}{2}\right)\left(\overline{\omega} - \frac{1}{2}\right) - \frac{1}{4} = 0$
Ce qui équivaut à $\left|\omega - \frac{1}{2}\right|^2 = \left(\frac{1}{2}\right)^2 \iff \left|\omega - \frac{1}{2}\right| = \left(\frac{1}{2}\right)$

Exemple 4.3.2. $P = \{z \in \mathbb{C}, \Im(z) > 0\}$: le demi-plan de Poincaré
Déterminer l'image de P par la transformation $z \mapsto \frac{z-i}{z+i}$

1. $\omega = \frac{z-i}{z+i}$, exprimer z en fonction de ω.

$$\begin{aligned} &\omega = \frac{z-i}{z+i} \\ \iff &\omega(z+i) = z - i \\ \iff &\omega(z+i) + i = z \\ \iff &\omega z + \omega i + i = z \\ \iff &\omega z - z = -\omega i - i \\ \iff &z(\omega+1) = -\omega i - i \\ \iff &z = \frac{-\omega i - i}{\omega + 1} \\ \iff &z = \frac{-i(\omega+1)}{\omega+1} \end{aligned}$$

2. $z \in P \iff \Im(z) > 0$
   $z = x + iy$, $\overline{z} = x - iy$, on a : $z - \overline{z} = 2iy$
   Si on a $\Im(z) = y > 0 \iff \frac{1}{2i}(z - \overline{z}) > 0$
   A la fin on obtient : $\omega\overline{\omega} < 1 \implies |\omega| < 1$

Chapitre 5

Arithmétique

5.1 Divisibilité

Définition 5.1.1. Soient $a \in \mathbb{Z}, b \in \mathbb{Z}^*$. On dit que :
- a est un multiple de $b \iff \exists q \in \mathbb{Z}, a = bq$
- b est un diviseur de $a \iff \exists q \in \mathbb{Z}, a = bq$
- b divise $a \iff b \mid a$

Théorème 5.1.1 (Division euclidienne)**.** Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$. Alors

$$\exists!(q, r) \in \mathbb{Z}^2, a = bq + r, \ (0 \leqslant r < |b|)$$

Vocabulaire :
- a est appelé le *dividende*
- b est appelé le *diviseur*
- q est appelé le *quotient*
- r est appelé le *reste*

Démonstration. [1] Nous devons montrer deux choses, *l'existence* et *l'unicité* du couple (q, r)

1. **Existence**
   Montrons que (q, r) existe.
   Supposons $a \in \mathbb{N}$ et considérons $M = \{n \in \mathbb{N} \mid nb \leqslant a\}$ l'ensemble des multiples de b inférieurs à a. M est une partie de $\mathbb{N}$. Nous avons deux propriétés :
   (a) M est non vide car 0 est un multiple de b inférieur à a
   (b) M est majoré par a d'après sa définition.

   Ainsi, M admet un plus grand élément que l'on notera q, vérifiant :
   (a) $qb \leqslant a$ car $q \in M$
   (b) $(q + 1)b > a$ car $q + 1 > q$ sachant que q est le plus grand élément de M, $q + 1 \notin M$.

   Posons $r = a - bq \iff a = bq + r$. Sachant que $a \geqslant bq$, $r \geqslant 0$.
   On a $r < b$ car $b = (q + 1)b - qb > a - bq = r$.
   Supposons que $a \in \mathbb{Z}$. Si a est positif, on se ramène au cas précédent.
   Dans le cas où $a < 0$, $-a \geqslant 0$, ainsi, $\exists(q', r') \in \mathbb{Z}^2$ tel que

$$\begin{aligned} & -a = bq' + r' \text{ avec } 0 \leqslant r' < |b| \\ \iff & \ a = b(-q') - r' \end{aligned}$$

   Si $r' = 0$, on pose $q = -q'$ et $r = 0$ et on obtient le couple recherché.
   Si $r' \neq 0$, $r' \in [\![1, b - 1]\!]$ et $a = b(-q' - 1) + (b - r')$, on pose $q = -q' - 1$ et $r = b - r'$ et on obtient le couple recherché.

2. **Unicité**
   Pour cette partie, il suffit de supposer deux couples $(q, r) \in \mathbb{Z}^2$ et $(q', r') \in \mathbb{Z}^2$ et de montrer que $q = q'$ et $r = r'$.
   Commençons par $a = bq + r,\ (0 \leqslant r < |b|)$ et $a = bq' + r',\ (0 \leqslant r' < |b|)$. Comme $0 \leqslant r < b$ et $0 \leqslant r' < b$, on a :

$$b|q' - q| = |r' - r| < b$$

   ce qui n'est possible que si $|q' - q| = 0$ ce qui implique que $q = q'$. Ceci entraîne donc $r = r'$ et donc on a montré que $(q, r) = (q', r')$

□

5.2 PGCD et PPCM

Définition 5.2.1 (PPCM et PGCD)**.** Soit $(a, b) \in \mathbb{Z}^2 \backslash \{(0, 0)\}$ tel que $ab \neq 0$

$$\mathcal{M}:\ = \{m \in \mathbb{Z} \mid a \mid m \text{ et } b \mid m\} \Rightarrow \mathcal{M} \neq \phi \text{ car } ab \in \mathcal{M}$$

$$\mathcal{M} \cap \mathbb{N}^* \leftarrow \text{ il y a le plus petit commun multiple (PPCM)}$$

$$\mathcal{D} = \{d \in \mathbb{Z} \mid d \mid a \text{ et } d \mid b\} \Rightarrow \mathcal{D} \neq \emptyset \text{ car } 1 \in \mathcal{D}$$

On a : $d \mid a, b \implies |d| \leqslant m \min(|a|, |b|)$ et $\mathrm{Card}(\mathcal{D}) < \infty$ Il y a le plus grand élément $\leftarrow$ le plus grand commun diviseur (PGCD)

Théorème 5.2.1 (PPCM)**.** Soit $(a, b) \in \mathbb{Z}^* \times \mathbb{Z}^*$ et $m \in \mathbb{Z},\ a \mid m$ et $b \mid m$. Alors $\mathrm{ppcm}(a, b) \mid m$

Démonstration. Posons $\ell = \mathrm{ppcm}(a, b)$

$$\begin{aligned} &\exists!(q, r) \in \mathbb{Z}^2,\ m = q\ell + r,\ 0 \leqslant r < \ell \\ &\iff r = m - q\ell,\ m \text{ et } \ell \text{ sont multiples de } a \text{ et} \\ &\qquad r \text{ est aussi un multiple de } a \text{ et } b \end{aligned}$$

Par la minimalité de ℓ, $r = 0 \implies m = q\ell$ □

Théorème 5.2.2 (PGCD)**.** Soit $(a, b) \in \mathbb{Z}^* \times \mathbb{Z}^*$ et $d \in \mathbb{Z},\ d \mid a$ et $d \mid b$. Alors $d \mid \mathrm{pgcd}(a, b)$

Démonstration. Posons $m = \mathrm{pgcd}(a, b)$. Il suffit de montrer que

$$\mathrm{pgcd}(m, d) = m$$

Soit $\ell = \mathrm{ppcm}(m, d)$, $\ell \geqslant m$, a et b sont multiples de m et d
D'après le théorème précédent :

$$\ell \mid a \text{ et } \ell \mid b,\ l \leqslant m$$

Sachant qu'on a $\ell \geqslant m$ et $\ell \leqslant m$, on en conclut que $\ell = m$ □

Théorème 5.2.3. Soit $(a, b) \in (\mathbb{N}^*)^2 \implies ab = \mathrm{pgcd}(a, b)\mathrm{ppcm}(a, b)$

Définition 5.2.2 (Nombres premiers entre eux)**.** Soit $(a, b) \in (\mathbb{Z}^*)^2$

$$a \text{ et } b \text{ premiers entre eux } \iff \mathrm{pgcd}(a, b) = 1$$

5.3 Algorithme d'Euclide

Proposition 5.3.1 (Algorithme d'Euclide)**.** Soient $a \in \mathbb{Z}^*$, $b \in \mathbb{Z}^*$ tel que

$$|a| > |b| \implies \exists!(q,r) \in \mathbb{Z}^2, a = bq + r, 0 \leqslant r < |b|$$
$$\text{pgcd}(a,b) = \text{pgcd}(b,a) = \text{pgcd}(b, a - qb) = \text{pgcd}(b,r)$$

$$\text{pgcd}(a,b) = \text{pgcd}(b,r)$$

Si $r = 0 \implies a = qb,\ \text{pgcd}(a,b) = b$ Supposons que $r = 0$:

$$\exists!(q_1, r_1),\ b = q_1 r + r_1,\ 0 \leqslant r_1 < r$$

Si $r_1 \neq 0 \implies \exists!(q_2, r_2),\ r = q_2 r_1 + r_2,\ 0 \leqslant r_2 < r_1$
$\vdots$
Si $r_{n-2} \neq 0 \implies \exists!(q_{n-1}, r_{n-1}),\ r_{n-3} = q_{n-1} r_{n-2} + r_{n-1},\ 0 \leqslant r_{n-1} < r_{n-2}$

$$\exists q_n,\ r_{n-2} = q_n r_{n-1}$$

$$\begin{aligned}
\text{pgcd}(a,b) &= \text{pgcd}(b,r) \\
&= \text{pgcd}(r, r_1) \\
&= \text{pgcd}(r_1, r_2) \\
&\vdots \\
&= \text{pgcd}(r_{n-2}, r_{n-1}) \\
&= \text{pgcd}(q_n r_{n-1}, r_{n-1}) = r_{n-1}
\end{aligned}$$

Exemple 5.3.1.

1. $\text{pgcd}(72, 58)$

$$\begin{aligned}
72 &= 58 \times 1 + 14 \\
58 &= 14 \times 4 + 2 \\
14 &= 2 \times 7 + 0
\end{aligned}$$

   On en conclut que $\text{pgcd}(72, 58) = 2$

2. $\text{pgcd}(625, 216)$

$$\begin{aligned}
625 &= 216 \times 2 + 193 \\
216 &= 193 \times 1 + 23 \\
193 &= 23 \times 8 + 9 \\
23 &= 9 \times 2 + 5 \\
9 &= 5 \times 1 + 4 \\
5 &= 4 \times 1 + 1
\end{aligned}$$

   On en conclut que $\text{pgcd}(625, 216) = 1$

Théorème 5.3.1 (Identité de Bézout)**.** Soient $(a,b) \in \mathbb{Z}^2$

$$\exists (u,v) \in Z^2 \text{ tel que } au + bv = \text{pgcd(a, b)}$$

Corollaire 5.3.1. Soient $(a, b) \in (\mathbb{Z}^*)^2$, $d \in \mathbb{Z}$

$$\exists (u, v) \in \mathbb{Z}^2 \text{ tel que } au + bv = d \iff \text{pgcd}(a, b) \mid d$$

Trouver les $(x, y) \in \mathbb{Z}$ tels que $ax + by = d$ et $\text{pgcd}(a, b) \mid d$
Théorème de Bézout : $\exists (x_0, y_0) \in \mathbb{Z}^2$ tel que $ax_0 + by_0 = d$

$$\begin{cases} ax + by = d \\ ax_0 + by_0 = d \end{cases} \implies a(x - x_0) + b(y - y_0) = 0 \iff a(x - x_0) = b(y_0 - y) \text{ multiple } k \text{ ppcm}(a, b)$$

$$\exists k \in \mathbb{Z} \text{ tq } a(x - x_0) = b(y - y_0) = \text{ppcm}(a, b)k$$

$$\begin{cases} x = x_0 + \frac{\text{ppcm}(a,b)k}{a} \\ y = y_0 - \frac{\text{ppcm}(a,b)k}{b} \end{cases}$$

d'où

$$\{(x, y) \in \mathbb{Z}^2 \mid ax + by = d\} = (x_0, y_0) + \mathbb{Z}\left(\frac{\text{ppcm}(a, b)}{a}, \frac{\text{ppcm}(a, b}{b}\right)$$

Exemple 5.3.2. $a = 75$ et $b = 42$

$$\begin{aligned} 75 &= 42 \cdot 1 + 33 \\ 42 &= 33 \cdot 1 + 9 \\ 33 &= 9 \cdot 3 + 6 \\ 9 &= 6 \cdot 1 + 3 \\ 6 &= 3 \cdot 2 + 0 \end{aligned}$$

On remonte dans l'algorithme d'Euclide

$$\begin{aligned} 3 &= 9 - 6 \\ 3 &= (42 - 33) - (33 - 9 \cdot 3) \\ 3 &= (42 - (75 - 42)) - ((75 - 42) - (42 - 33)3) \\ 3 &= (42 - (75 - 42)) - ((75 - 42) - (42 - (75 - 42))3) \\ 3 &= 75 \cdot (-5) + 42 \cdot 9 \end{aligned}$$

Lemme 5.3.1 (Lemme de Gauss)**.** $(a, b) \in \mathbb{Z}^*$ tels que a et b sont premiers entre eux (leur pgcd est 1)

$$c \in \mathbb{Z} \text{ tq } a \mid bc \implies a \mid c$$

Démonstration.

$$\begin{aligned} \text{pgcd}(a, b) = 1 &\implies \exists (u, v) \in \mathbb{Z}^2 \text{ tq } au + bv = 1 \\ &\implies a(cu) + b(cv) = c \\ &\implies \text{pgcd}(a, bc) \mid c \end{aligned}$$

□

5.4 Nombres premiers

Définition 5.4.1 (Nombres premiers)**.** $p \in \mathbb{N}^*$ est dit premier si

$$\exists d \in \mathbb{N}^* \text{ tq } d \mid p \implies d \in \{1, p\}$$

Exemple 5.4.1. $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37$ sont des nombres premiers

Remarque 5.4.1. $F_n = 2^{2^n} + 1$ est une suite composée exclusivement de nombres premiers.

Théorème 5.4.1 (Théorème d'Euclide)**.** Il existe une infinité de nombres premiers.

Démonstration. Supposons qu'il existe k nombres premiers $p_1, p_2, \cdots, p_k$

$$N := p_1 p_2 \cdots p_k + 1 \implies p_i \nmid N$$

□

Lemme 5.4.1. Soit $n \in \mathbb{N}$ tq $n \geqslant 2$.
Soit p le plus petit diviseur de n tq $p > 2 \implies p$ premier

Démonstration. Si p n'était pas premier : $1 < \exists d < p$ tq $d \mid p$
$d \mid p$ et $p \mid n \implies d \mid n$ ce qui reviendrait à contredire la minimialité de p □

Théorème 5.4.2 (Décomposition en facteurs premiers)**.** Soit $n \in \mathbb{N}^*$ tq $n \geqslant 2$. Il existe une unique écriture de n sous la forme de :

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

1. p_i premiers
2. $\alpha_i \in \mathbb{N}^*$
3. $p_1 < p_2 < \cdots < p_k$

Démonstration. **Existence** : On procède par récurrence forte en utilisant le Lemme de Gauss
Unicité : On utilise le Lemme de Gauss □

Proposition 5.4.1 (PGCD à partir de la décomposition en facteurs premiers)**.** Soient $(a, b) \in \mathbb{Z}^2$, pour déterminer leur PGCD, on peut se servir de leurs décomposition en facteurs premiers.

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} (k \in \mathbb{N})$$
$$b = n_1^{\beta_1} n_2^{\beta_2} \cdots p_i^{\beta_i} (i \in \mathbb{N})$$

pgcd(a, b) correspond aux produits des facteurs premiers communs.

Remarque 5.4.2 (Décomposer en facteurs premiers)**.** Pour décomposer facilement un nombre en facteurs premiers.

1. On divise par le diviseur premier le plus faible tel que le reste soit nul
2. On refait de même avec le quotient, il faut que le diviseur premier soit supérieur ou égal au précédent.
3. On continue jusqu'à finir avec un quotient premier

Exemple 5.4.2. Décomposons 423 en facteurs premiers.

$$\frac{423}{3} = 141$$
$$\frac{141}{3} = 47$$

Sachant que 47 est premier, on obtient la décomposition

$$423 = 3 \times 3 \times 47 = 3^2 \times 47$$

Exemple 5.4.3. Calculons le PGCD de 624 et 408.
On a :

$$624 = 2^4 \times 3 \times 13$$
$$408 = 2^3 \times 3 \times 17$$

On remarque que 2^3 et 3 sont communs aux deux décompositions.

$$\text{pgcd}(624, 408) = 2^3 \times 3 = 24$$

5.5 Congruences

Définition 5.5.1 (Congruence)**.** Soient $(a, b) \in \mathbb{Z}^2$ et $n \in \mathbb{N}, n \geqslant 2$
On dit que a et b sont congrus modulo n s'il existe un $k \in \mathbb{Z}$ tel que :

$$n \mid a - b \iff a - b = kn$$

On note :

$$a \equiv b\ [n] \iff a = b \pmod{n}$$

Exemple 5.5.1.

$$9 \equiv 2[7] \iff 9 \equiv 9[7]$$

Proposition 5.5.1. Pour $(a, b, c) \in \mathbb{Z}^3$ et $n \in \mathbb{N}, n \geqslant 2$

1. $a \equiv a\ [n]$ (Réflexivité)
2. $a \equiv b\ [n] \implies b \equiv a\ [n]$ (Symétrie)
3. $a \equiv b\ [n],\ b \equiv c\ [n] \implies a \equiv c\ [n]$ (Transitivité)
4. $a \equiv b\ [n],\ c \equiv d\ [n] \implies a + c \equiv b + d\ [n]$
5. $a \equiv b\ [n],\ c \equiv d\ [n] \implies ac \equiv bc\ [n]$
6. $a \equiv b\ [n] \implies a^k \equiv b^k\ [n], (k \in \mathbb{N})$

Démonstration. On revient à la définition de congruence

1. $a - a = 0 = 0 \times n \implies a \equiv a\ [n]$
2. $a \equiv b\ [n] \iff a - b = kn,\ (k \in \mathbb{Z})$ puis $b \equiv c\ [n] \implies b = c + k'n,\ (k' \in \mathbb{Z})$ On a donc

$$\begin{aligned} a - (c + k'n) = kn &\iff a - c - k'n = kn \\ &\iff a - c = (k + k')n \end{aligned}$$

En posant $(k + k') = K$, $K \in \mathbb{Z}$ par stabilité, ainsi on retrouve

$$a - c = Kn \iff a \equiv c\ [n]$$

□

Exemple 5.5.2.

$$8^{5000} - 6^{4787} \text{ modulo } 7$$

On a : $\begin{cases} 8 \equiv 1\ [7] \\ 6 \equiv -1\ [7] \end{cases} \implies \begin{cases} 8^{5000} \equiv 1\ [7] \\ 6^{4787} \equiv -1\ [7] \end{cases} \implies \begin{cases} 8^{5000} - 6^{4787} \equiv 2\ [7] \end{cases}$

Exemple 5.5.3. Trouver les $x \in \mathbb{Z}$ tels que

$$3x \equiv 5\ [7]$$

On a une solution particulière $x_0 = 4$
On a ensuite

$$\begin{aligned} 3x &\equiv 5\ [7] \\ 6x &\equiv 10\ [7] \\ 6x &\equiv 3\ [7] \\ 6x &\equiv -x_0\ [7] \end{aligned}$$

$$-x_0 \equiv 3\ [7] \iff x_0 \equiv -3\ [7] \equiv 4\ [7]$$

On a ensuite

$$\begin{aligned} 3x &\equiv 5\ [7] \\ 3x_0 &\equiv 5\ [7] \iff 3 \times 4 \equiv 5\ [7] \end{aligned}$$

On a donc :

$$\begin{aligned} 3(x - x_0) &\equiv 0\ [7] \\ 3(x - 4) &\equiv 0\ [7] \end{aligned}$$

Bibliographie

[1] Alain Soyeur et François Capaces et Emmanuel Vieillard-Baron et Sésamath et les mathematiques.net. *Cours de Mathématiques Sup MPSI PCSI PTSI TSI* `http://les.mathematiques.free.fr/pdf/livre.pdf`.

[2] Logiciel Geogebra. `https://www.geogebra.org/?lang=fr`.