

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 télescopiques	7
1.4	Puissances	7
2	Ensembles et applications	9
2.1	Ensembles	9
2.2	Applications	11
3	Logique	13
3.1	Opérations sur les prédicats	13
3.1.1	Négation	13
4	Nombres complexes	15
4.1	Vision algébrique des nombres complexes	15
4.2	Vision géométrique des nombres complexes	17
4.3	Géométrie des nombres complexes	19
4.3.1	Equation d'une droite	20
5	Arithmétique	21
5.1	Divisibilité	21
5.2	PGCD et PPCM	22
5.3	Algorithme d'Euclide	23

Chapitre 1

Calcul Algébrique

1.1 Point sur les ensembles de nombres

Définition 1.1.1 (Ensemble des nombres entiers naturels).

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

Définition 1.1.2 (Ensemble des nombres entiers relatifs).

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

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 :

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

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 :

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

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

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).

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

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 $m \leq n$ et $a_k \in \mathbb{R}$, $m \leq k \leq n$

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

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 $m \leq n$ et $a_k, b_k \in \mathbb{R}$, $m \leq k \leq n$

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

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

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

□

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

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

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

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

□

1.3.1 Quelques sommes importantes

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

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

$$S = a + ar + \cdots + ar^{n-1}$$

$$rS = ar + ar^2 + \cdots + ar^n$$

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

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

□

1.3.2 Sommes télescopiques

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

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

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

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

□

1.4 Puissances

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

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

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. $\frac{a^n}{a^m} = a^{n-m}, a \neq 0$

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

$$5. a^0 = 1$$

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

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

□

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

$$(a^m)^n = \underbrace{\underbrace{(a \times a \times \cdots \times a)}_{m \text{ fois}} \times \underbrace{(a \times a \times \cdots \times a)}_{m \text{ fois}} \times \cdots \times \underbrace{(a \times a \times \cdots \times a)}_{m \text{ fois}}}_{n \text{ fois}} = \underbrace{a \times a \times \cdots \times a}_{m \times n \text{ fois}}$$

□

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

$$\frac{a^n}{a^m} = \frac{\underbrace{a \times a \cdots \times a}_{n \text{ fois}}}{\underbrace{a \times a \cdots \times a}_{m \text{ fois}}} = \underbrace{a \times a \times \cdots \times a}_{n-m \text{ fois}}$$

□

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).

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).

Deux ensembles E et F sont égaux $\iff E \subset F$ et $F \subset E$

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

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

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

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

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

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

1. Associativité :

$$\begin{aligned} A \cup (B \cup C) &= (A \cup B) \cup C \\ A \cap (B \cap C) &= (A \cap B) \cap C \end{aligned}$$

2. Élément neutre :

$$\begin{aligned} A \cup \emptyset &= A \\ A \cap A &= A \end{aligned}$$

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).

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

Remarque 2.1.1. Soient E, F des ensembles.

- $(E \setminus F) \subset E$
- $(E \setminus F) \cap F = \emptyset$
- $E \setminus F \neq F \setminus E$

Remarque 2.1.2. Soient E et A des ensembles.

$$A \subset E$$

$$A^C = E \setminus A$$

$$(A^C)^C = A$$

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.

\square 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 :

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

\supseteq 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 :

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

\square

Démonstration. 2

Soient A et B des ensembles et x un élément quelconque.

\square 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 :

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

\square 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 :

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

\square

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. $f : E \rightarrow F$ est une application si pour chaque $x \in E$, on associe un élément de F noté $f(x)$

Définition 2.2.2 (Injectivité). Soit $f : E \rightarrow F$, 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 :

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

Définition 2.2.3 (Surjectivité). Soit $f : E \rightarrow F$, 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 :

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

Définition 2.2.4 (Bijectivité). Soit $f : E \rightarrow F$, 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 :

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

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

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

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

comme étant la réciproque de f .

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

Définition 2.2.8 (Image directe et image réciproque). Soient $f : E \rightarrow F$ 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 $f : E \rightarrow F$ une application et A, B des parties de F .

1. $f^{-1}(F \setminus A) = E \setminus f^{-1}(A)$
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 : $\exists x \in A \cap B, y = f(x)$

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

d'où $y \in f(A) \cap f(B)$ □

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 ou 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 $\text{non}(P) \text{ ou } Q$
2. $\text{non}(P \text{ ou } Q)$ est équivalent à $\text{non}(P) \text{ et } \text{non}(Q)$
3. $\text{non}(P \text{ et } Q)$ est équivalent à $\text{non}(P) \text{ ou } \text{non}(Q)$

Remarque 3.1.1.

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

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

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 .

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

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.

$\{(a_n)\}_{n \in \mathbb{N}} \subset \mathbb{R}, \lim_{n \rightarrow +\infty} a_n = \alpha \in \mathbb{R}$

A. Cauchy :

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

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) Élément 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) Élément neutre :

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

(c) Commutativité :

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

(d) Distributivité :

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

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 $\bar{z} = a - ib$ 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 :

$$\begin{aligned}- & |z \cdot z'| = |z| \cdot |z'| \\ - & \left| \frac{z}{z'} \right| = \frac{|z|}{|z'|} \\ - & |z + z'| \leq |z| + |z'| \\ - & |z|^2 = z \cdot \bar{z} = a^2 + b^2 \\ - & |z| \geq 0 \\ - & |z| = 0 \iff z = 0 \\ - & |z| = |\bar{z}| = |-z| = |-\bar{z}|\end{aligned}$$

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

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

Proposition 4.1.4.

$$\begin{aligned}- & z + \bar{z} = (a + ib) + (a - ib) = 2a \implies \Re(z) = \frac{z + \bar{z}}{2} \\ - & z - \bar{z} = (a + ib) - (a - ib) = 2ib \implies \Im(z) = \frac{z - \bar{z}}{2i}\end{aligned}$$

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 $z, z_1, z_2 \in \mathbb{C}^3, n \in \mathbb{N}$

- $\arg(z_1 \cdot z_2) = \arg z_1 + \arg z_2$
- $\arg z^n = n \arg z$
- $\arg \frac{z_1}{z_2} = \arg z_1 - \arg z_2$
- $\arg \frac{1}{z} = -\arg z$

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.

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

□

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 :

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

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.

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

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

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

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

□

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 :

$$\begin{aligned} \cos \theta &= \frac{1}{\sqrt{2}} \\ &= \frac{\sqrt{2}}{2} \end{aligned} \qquad \begin{aligned} \sin \theta &= \frac{1}{\sqrt{2}} \\ &= \frac{\sqrt{2}}{2} \end{aligned}$$

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

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

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 :

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

En posant :

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

on obtient :

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

□

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 :

$$\omega_k = e^{\frac{2ik\pi}{n}}, k \in \llbracket 0, n-1 \rrbracket$$

Démonstration. On cherche à résoudre

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

Posons $z = |z|e^{i\theta}$. On obtient donc en élevant 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

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

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
- $z \mapsto \bar{z}$: réflexion par rapport à l'axe des réels
- $z \mapsto a + e^{i\theta}(z - a)$: rotation d'angle θ de centre a
- $z \mapsto e^{2i\theta} \cdot \bar{z}$: 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 : $\bar{z} = z$
- 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 : $z + \bar{z} = 2a$

Exemple 4.3.1. $z \mapsto \frac{1}{z}$

On pose : $\omega = \frac{1}{z}$

On a donc : $z = \frac{1}{\omega}$

$$z + \bar{z} = 2 \implies \frac{1}{\omega} + \frac{1}{\bar{\omega}} = 2 \implies \frac{1}{\omega} + \frac{1}{\bar{\omega}} = 2$$

$$\omega \bar{\omega} \left(\frac{1}{\omega} + \frac{1}{\bar{\omega}} \right) = 2\omega \bar{\omega}$$

$$\text{On a donc : } \bar{\omega} + \omega = 2\omega \bar{\omega} \implies 2\omega \bar{\omega} - \omega - \bar{\omega} = 0$$

$$\text{C'est à dire : } \omega \bar{\omega} - \frac{1}{2}\omega - \frac{1}{2}\bar{\omega} = \left(\omega - \frac{1}{2}\right) \left(\bar{\omega} - \frac{1}{2}\right) - \frac{1}{4} = 0$$

$$\text{Ce qui équivaut à } \left|\omega - \frac{1}{2}\right|^2 = \left(\frac{1}{2}\right)^2 \iff \left|\omega - \frac{1}{2}\right| = \left(\frac{1}{2}\right)$$

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 .

$$\omega = \frac{z-i}{z+i}$$

$$\iff \omega(z+i) = z-i$$

$$\iff \omega(z+i) + i = z$$

$$\iff \omega z + \omega i + i = z$$

$$\iff \omega z - z = -\omega i - i$$

$$\iff z(\omega + 1) = -\omega i - i$$

$$\iff z = \frac{-\omega i - i}{\omega + 1}$$

$$\iff z = \frac{-i(\omega + 1)}{\omega + 1}$$

2. $z \in P \iff \Im(z) > 0$

$$z = x + iy, \bar{z} = x - iy, \text{ on a : } z - \bar{z} = 2iy$$

$$\text{Si on a } \Im(z) = y > 0 \iff \frac{1}{2i}(z - \bar{z}) > 0$$

$$\text{A la fin on obtient : } \omega \bar{\omega} < 1 \implies |\omega| < 1$$

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

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

Vocabulaire :

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

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

1. Existence

Supposons $a \in \mathbb{N}$ et considérons $M = \{n \in \mathbb{N} \mid nb \leq a\}$ 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) $qb \leq a$ 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 $a \geq bq$, $r \geq 0$.

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 $a < 0$, $-a \geq 0$, ainsi, $\exists(q', r') \in \mathbb{Z}^2$ tel que

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

Si $r' = 0$, on pose $q = -q'$ et $r = 0$ et on obtient le couple recherché.

Si $r' \neq 0$, $r' \in \llbracket 1, b-1 \rrbracket$ 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 $a = bq + r$, ($0 \leq r < |b|$) et $a = bq' + r'$, ($0 \leq r' < |b|$). Comme $0 \leq r < b$ et $0 \leq r' < b$, 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 $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ tel que $ab \neq 0$

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

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

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

On a : $d \mid a, b \Rightarrow |d| \leq m \min(|a|, |b|)$ et $\text{Card}(\mathcal{D}) < \infty$ 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 $\text{ppcm}(a, b) \mid m$

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

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

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

□

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 $d \mid \text{pgcd}(a, b)$

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

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

Soit $\ell = \text{ppcm}(m, d)$, $\ell \geq m$, a et b sont multiples de m et d

D'après le théorème précédent :

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

Sachant qu'on a $\ell \geq m$ et $\ell \leq m$, on en conclut que $\ell = m$

□

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

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

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

5.3 Algorithme d'Euclide

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

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

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

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

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

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

Si $r_1 \neq 0 \implies \exists!(q_2, r_2), r = q_2 r_1 + r_2, 0 \leq r_2 < r_1$

\vdots

Si $r_{n-2} \neq 0 \implies \exists!(q_{n-1}, r_{n-1}), r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}, 0 \leq r_{n-1} < r_{n-2}$

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

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

Exemple 5.3.1.

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

$$72 = 58 \times 1 + 14$$

$$58 = 14 \times 4 + 2$$

$$14 = 2 \times 7 + 0$$

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

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

$$625 = 216 \times 2 + 193$$

$$216 = 193 \times 1 + 23$$

$$193 = 23 \times 8 + 9$$

$$23 = 9 \times 2 + 5$$

$$9 = 5 \times 1 + 4$$

$$5 = 4 \times 1 + 1$$

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