Logique et Ensembles

Vincent Pilaud

Janvier 2004

1 Logique

1.1 Propositions

Définition 1 *Les propositions sont des affirmations dont on peut dire sans ambiguité si elles sont vraies ou fausses.*

Exemple 1
1. *"π est un nombre rationnel" est une proposition (fausse en l'occurence !).*
2. *"la nostalgie n'est plus ce qu'elle était" n'est pas une proposition.*

1.2 Les connecteurs logiques

Définition 2 *Les connecteurs logiques sont des opérations sur les propositions.*

Exemple 2
1. *les connecteurs $\vee$("ou"), $\wedge$ ("et"), $\neg$ ("non") :*
   Soient P et Q deux propositions,
   *$P \vee Q$ est vraie si P est vraie **ou** Q est vraie,*
   *$P \wedge Q$ est vraie si P est vraie **et** Q est vraie,*
   $\neg P$ est vraie si P est fausse.
2. *les connecteurs $\Rightarrow$ ("implique") et $\Leftrightarrow$ ("équivaut à") :*
   Soient P et Q deux propositions,
   *$P \Rightarrow Q$ est vraie si Q est vraie **si** P est vraie,*
   *$P \Leftrightarrow Q$ est vraie si P est vraie **si et seulement si** Q est vraie.*

Remarque 1 *Il est plus facile d'expliciter les opérations effectuées par les connecteurs logiques sur des tables de vérité :*

P	Q	$P \vee Q$	$P \wedge Q$	$\neg P$	$P \Rightarrow Q$	$P \Leftrightarrow Q$
v	v	v	v	f	v	v
v	f	v	f	f	f	f
f	v	v	f	v	v	f
f	f	f	f	v	v	v

Proposition 1 *On a les équivalences suivantes :*

$$(P \Rightarrow Q) \Leftrightarrow ((\neg P) \vee Q)$$

$$(P \Leftrightarrow Q) \Leftrightarrow ((P \Rightarrow Q) \wedge (Q \Rightarrow P))$$

Démonstration 1 *On écrit les tables de vérités des deux propositions :*

P	Q	$\neg P$	$(\neg P) \vee Q$	$P \Rightarrow Q$	$P \Rightarrow Q$	$Q \Rightarrow P$	$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$	$P \Leftrightarrow Q$
v	v	f	v	v	v	v	v	v
v	f	f	f	f	f	v	f	f
f	v	v	v	v	v	f	f	f
f	f	v	v	v	v	v	v	v

□

1.3 Etude d'un exemple : le théoreme de Pythagore

Théoreme 1 *Le théorème de Pythagore :*

1. *proposition de Pythagore :*
   Soit ABC un triangle.
   ABC est rectangle en $A \Rightarrow AB^2 + AC^2 = BC^2$

2. *réciproque de la proposition :*
   Soit ABC un triangle.
   $AB^2 + AC^2 = BC^2 \Rightarrow ABC$ est rectangle en A

On a donc : ABC est rectangle en $A \Leftrightarrow AB^2 + AC^2 = BC^2$

Démonstration 2 *On rappelle quelques notions sur le produit scalaire de deux vecteurs :*
Soient $\vec{AB}$ et $\vec{AC}$ deux vecteurs. On définit leur produit scalaire par :

$$\vec{AB}.\vec{AC} = \|\vec{AB}\|.\|\vec{AC}\|.\cos(\vec{AB}, \vec{AC})$$

On note les équivalences suivantes :

$$\begin{aligned} \vec{AB}.\vec{AC} = 0 &\Leftrightarrow (\|\vec{AB}\| = 0) \vee (\|\vec{AC}\| = 0) \vee (\cos(\vec{AB}, \vec{AC}) = 0) \\ &\Leftrightarrow (AB) \perp (AC) \end{aligned}$$

On a en outre : $\vec{AB}.\vec{AB} = \|\vec{AB}\|^2 = AB^2$
On peut alors faire la preuve :

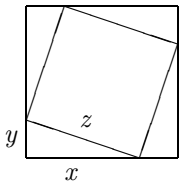
$$\begin{aligned} BC^2 &= \vec{BC}.\vec{BC} \\ &= (\vec{BA} + \vec{AC}).(\vec{BA} + \vec{AC}) \\ &= \vec{BA}.\vec{BA} + \vec{BA}.\vec{AC} + \vec{AC}.\vec{BA} + \vec{AC}.\vec{AC} \\ &= AB^2 + AC^2 + 2\vec{BA}.\vec{AC} \end{aligned}$$

Donc on a l'équivalence :

$$AB^2 + AC^2 = BC^2 \Leftrightarrow \vec{BA}.\vec{AC} = 0 \Leftrightarrow (AB) \perp (AC) \Leftrightarrow ABC \text{ est rectangle en } A$$

□

Remarque 2 *Signalons une autre méthode pour montrer la proposition de Pythagore :*
Soit ABC un triangle rectangle et $x = AB$, $y = AC$ et $z = BC$. On considère un carré de côté $x + y$:



Par comparaison des angles sur les triangles isométriques, on montre que la figure du centre est un carré de côté z. On calcule alors l'aire du carré par deux méthodes :

$$(x + y)^2 = Aire = z^2 + 4\frac{xy}{2}$$

$$x^2 + y^2 = z^2$$

□

Remarque 3 *On définit les triplets Pythagoriciens comme des triplets d'entiers (a, b, c) qui vérifient la relation de Pythagore $a^2 + b^2 = c^2$.*

Il est clair qu'il existe une infinité de triplets Pythagoriciens : il suffit de prendre $(3n, 4n, 5n)$ avec $n \in \mathbb{N}$. On dit que les triplets de la forme $(3n, 4n, 5n)$ sont colinéaires au triplet $(3, 4, 5)$.

Il est alors intéressant de se poser la question de l'existence d'une infinité de triplets Pythagoriciens non colinéairs deux à deux.

Euclide fait la preuve suivante :

le carré d'un nombre impair est toujours impair, donc $\forall m \in \mathbb{N}$, m impair, $\exists n \in \mathbb{N}$ tel que $m^2 = 2n+1 = (n+1)^2 - n^2$, donc $(n+1)^2 = m^2 + n^2$.

Il reste à montrer que les triplets ainsi obtenus sont non colinéaires . Soit donc $(m, n, n+1)$ et $(m', n', n'+1)$ deux triplets Pythagoriciens de cette forme. Si ils sont colinéaires, $\exists k \in \mathbb{N}$ tel que $kn' = n$ et $k(n'+1) = (n+1)$; mais alors $k = 1$.

□

1.4 Les raisonnements de base

Proposition 2

$$(P \Rightarrow Q) \Leftrightarrow (\neg P \Leftrightarrow \neg Q) \ : \ \textit{contraposée}$$

$$(\neg P \Rightarrow Q) \wedge (\neg P \Rightarrow \neg Q) \Rightarrow (P) \ : \ \textit{absurde}$$

$$(\neg P \Rightarrow Q) \wedge (P \Rightarrow Q) \Rightarrow (Q) \ : \ \textit{tiers exclu}$$

Remarque 4 *Ces formules sont bien sûr les points de départ de raisonnements mathématiques usuels : les raisonnements par contraposition, par l'absurde et par tiers exclu.*

Exemple 3 *Soit ABC un triangle de côtés de longueurs respectives $AB = 3$, $AC = 4$ et $BC = 6$. Alors ABC n'est pas rectangle.*

Preuve 1 *On utiluse la contraposée de la proposition de Pythagore :*
$AB^2 + AC^2 \neq BC^2 \Rightarrow ABC$ n'est pas rectangle en A.
$BA^2 + BC^2 \neq AC^2 \Rightarrow ABC$ n'est pas rectangle en B.
$CA^2 + CB^2 \neq AB^2 \Rightarrow ABC$ n'est pas rectangle en C.
Donc ABC n'est pas rectangle.

□

Exemple 4 *Le problème des trois prisonniers :*

Trois prisonniers très intelligents sont alignés de tel sorte que le premier ne voit aucun des deux autres, le second ne voit que le premier et le troisième voit les deux autres. Le geolier dispose de trois chapeaux noirs et de deux chapeaux blancs et place un chapeau sur la tête de chaque prisonnier. Il annonce alors que celui des trois qui donnera la couleur de son chapeau en étant sûr de ne pas se tromper pourra sortir. Seul le premier prisonnier sort.

Quelle était la couleur du chapeau du premier prisonnier ?

Réponse : noire.

Preuve 2 *Raisonnons par l'absurde : supposons que la couleur du chapeau du premier prisonnier soit blanche. Il y a alors deux cas :*

- *soit le deuxième a un chapeau blanc, et alors le troisième prisonnier se serait empressé de répondre qu'il avait un chapeau noir.*
- *soit le deuxième a un chapeau, mais alors, comme le troisième ne répond pas, le deuxième sait que son chapeau est noir.*

Les deux cas amènent donc une contradiction, donc le chapeau du premier est noir.

□

Proposition 3 *Le raisonnement par récurrence :*

Soit $P(n)$ une proposition qui dépend de n.

Si on parvient à montrer que $P(0)$ est vraie et que $(P(n) \Rightarrow P(n+1))$ pour tout entier n, alors on aura montré que $P(n)$ est vraie pour tout entier n.

Remarque 5 *Il faut penser à une échelle dont on pourrait atteindre la première marche et sur laquelle on saurait passer d'une marche à la suivante. Il est clair qu'on pourra atteindre toutes les marches.*

En revanche si la première marche est trop haute, ou que l'une des marches est cassée, on ne pourra pas atteindre toutes les marches.

Exemple 5

$$\text{pour tout entier } n,\ 1+2+3+\ldots+(n-1)+n=\sum_{k=1}^{n}k=\frac{n(n+1)}{2}$$

Preuve 3 *On raisonne par récurrence sur n :*

- *Initialisation : le résultat est clair pour $n=0$.*
- *Transmission : supposons le résultat vrai au rang n. On a alors :*

$$\sum_{k=1}^{n+1}k=\sum_{k=1}^{n}k+(n+1)=\frac{n(n+1)}{2}+(n+1)=\frac{n(n+1)+2(n+1)}{2}=\frac{(n+1)(n+2)}{2}$$

d'où le résultat.

□

Exemple 6

$$\text{pour tout entier } n,\ 1+4+9+\ldots+(n-1)^2+n^2=\sum_{k=1}^{n}k^2=\frac{n(n+1)(2n+1)}{6}$$

Preuve 4 *On raisonne par récurrence sur n :*

- *Initialisation : le résultat est clair pour $n=0$.*
- *Transmission : supposons le résultat vrai au rang n. On a alors :*

$$\begin{aligned}\sum_{k=1}^{n+1}k^2 &= \sum_{k=1}^{n}k^2+(n+1)^2\\ &= \frac{n(n+1)(2n+1)}{6}+(n+1)^2\\ &= \frac{n(n+1)(2n+1)+6(n+1)^2}{6}\\ &= \frac{(n+1)[n(2n+1)+6(n+1)]}{6}\\ &= \frac{(n+1)(2n^2+7n+6)}{6}\\ &= \frac{(n+1)(n+2)(2n+3)}{6}\end{aligned}$$

□

Remarque 6 *cf "Les Tours de Hanoi et la partition du cercle" pour d'autres preuves intéressantes.*

1.5 Les quantificateurs

Définition 3 *On définit les quantificateurs suivants :*

- *quantificateur universel : "pour tout x dans A, P(x) est vraie" se note $\forall x\in A, P(x)$*
- *quantificateur existentiel : "il existe x dans A tel que P(x) est vraie" se note $\exists x\in A, P(x)$*
- *quantificateur existentiel unique : "il existe un unique x dans A tel que P(x) est vraie" se note $\exists !x\in A, P(x)$*

Proposition 4 *Négation des quantificateurs :*

$$\neg(\forall x\in A, P(x))\Leftrightarrow(\exists x\in A, \neg P(x))$$

$$\neg(\exists x\in A, P(x))\Leftrightarrow(\forall x\in A, \neg P(x))$$

$$\neg(\exists !x\in A, P(x))\Leftrightarrow((\forall x\in A, \neg P(x))\vee(\exists x_1\in A, \exists x_2\in A, (x_1\neq x_2)\wedge(P(x_1))\wedge(P(x_2)))$$

2 Ensembles

2.1 la notion d'ensemble

Définition 4 *On dit d'un objet qu'il est un ensemble si l'on peut dire sans ambiguité quelle est la condition d'appartenance à cet objet.*

Si A est un ensemble, $x \in A$ signifie x appartient à A, ou encore x est élément de A.

Exemple 7 *1. L'ensemble des entiers naturels pairs est un ensemble,*

2. l'ensemble des "hommes importants" n'est pas un ensemble.

Exemple 8 *On connaît bien les ensembles de nombres :*

- $\mathbb{N}$ *est l'ensemble des entiers naturels,*
- $\mathbb{Z}$ *est l'ensemble des entiers relatifs,*
- $\mathbb{Q}$ *est l'ensemble des nombres rationnels,*
- $\mathbb{R}$ *est l'ensemble des nombres réels.*

Définition 5 *Soient A et B deux ensembles. On dit que A est inclus dans B, ou encore que A est une partie de B si tout élément de A est aussi élément de B :*

$$A \subset B \Leftrightarrow \forall x \in A, x \in B$$

On dit que A est égal à B si ils ont exactement les mêmes éléments :

$$A = B \Leftrightarrow (A \subset B) \wedge (B \subset A) \Leftrightarrow (\forall x, x \in A \Leftrightarrow x \in B)$$

Définition 6 *Il existe un seul ensemble qui n'a aucun élément. On le note $\emptyset$.*

2.2 Ecriture des ensembles

Il y a deux moyens d'écrire les ensembles :

1. En extension : On écrit tous les éléments de l'ensemble A entre $\{\ \}$: $A = \{x; y; z\}$.

   Exemple 9 - *Un singleton est un ensemble n'ayant qu'un seul élément :* $\{x\}$,
   - *une paire est un ensemble ayant deux éléments :* $\{x; y\}$.

2. En compréhension : On définit l'ensemble A comme étant constitué de tous les éléments d'un autre ensemble B qui vérifient une propriété P : $A = \{x \in B | P(x)\}$.

   Exemple 10 - $[1; 3] = \{x \in \mathbb{R} | 1 \leq x \leq 3\}$,
   - $\emptyset = \{x \in \mathbb{R} | x = x + 1\}$.

2.3 Ensemble des parties d'un ensemble

Définition 7 *Soit A un ensemble. Il existe un ensemble constitué de toutes les parties de A.On le note $\wp(A)$.*

Notons que $B \in \wp(A) \Leftrightarrow B \subset A$.

Exemple 11 - $\wp(\emptyset) = \emptyset$,
- $\wp(\{x; y\}) = \{\emptyset; \{x\}; \{y\}; \{x; y\}\}$.

Proposition 5 *Soient A et B deux ensembles. On a $A = B \Leftrightarrow \wp(A) = \wp(B)$.*

Démonstration 3 $\Rightarrow$ *) évident.*

$\Leftarrow$ *) Montrons la double inclusion :*

- $A \subset A \Rightarrow A \in \wp(A) = \wp(B) \Rightarrow A \subset B$,
- *de même,* $B \subset A$.

□

2.4 Produit cartésien

Définition 8 *Le couple (x, y) est l'ensemble$\{\{x\}; \{x; y\}\}$.*

Remarque 7 *Attention à ne pas confondre la paire $\{x; y\}$ avec le couple (x, y). En fait, si (x, y) et (x', y') sont deux couples, on a : $(x, y) = (x', y') \Leftrightarrow (x = x') \wedge (y = y')$.*

Définition 9 *Soient A et B deux ensembles. Le produit cartésien de A et B est l'ensemble des couples (x, y) avec $x \in A$ et $y \in B$: $A \times B = \{(x, y) | (x \in A) \wedge (y \in B)\}$*

Exemple 12 *Soit $A = \{x; y; z\}, B = \{1; 2\}$*
Le produit cartésien de A et B est : $A \times B = \{(x, 1); (x, 2); (y, 1); (y, 2); (z, 1); (z, 2)\}$.
On remarque que le nombre d'éléments de $A \times B$ est le produit du nombre d'éléments de A par celui de B. On peut aisément généraliser ce résultat à n'importe quels ensembles X et Y finis.

Exemple 13 *Soient A, B, C et D quatre ensembles non vides. Alors $A \times B = C \times D \Leftrightarrow (A = C) \wedge (B = D)$*

Preuve 5 *montrons que $A \subset C$ (l'autre inclusion étant symétrique et l'autre égalité se prouvant de la même manière) : soit $x \in A$.*
$B \neq \emptyset \Rightarrow \exists y \in B \Rightarrow (x, y) \in A \times B = C \times D \Rightarrow x \in C$.

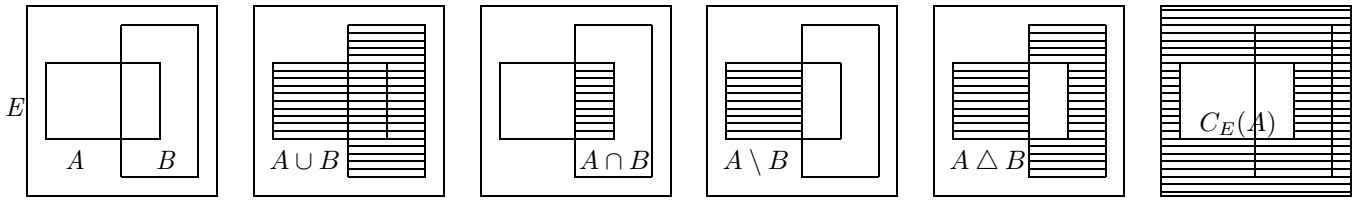
□

2.5 Opérations sur les ensembles

On définit de nombreuses opérations sur les ensembles :
soient A et B deux parties d'un ensemble E ; on définit :

1. Union : $A \cup B = \{x \in E | (x \in A) \vee (x \in B)\}$,
2. Intersection : $A \cap B = \{x \in E | (x \in A) \wedge (x \in B)\}$,
3. Différence : $A \setminus B = \{x \in E | (x \in A) \wedge (x \notin B)\}$,
4. Différence symétrique : $A \triangle B = (A \setminus B) \cup (B \setminus A)$
5. Complémentaire de A dans E : $C_E(A) = \{x \in E | (x \notin A)\} = E \setminus A$,

Remarque 8 *On peut voir ces opérations sur un dessin :*



Exemple 14 *Soient $A = \{1; 2; 3; 4; 5; 6\}$ et $B = \{1; 3; 5; 7; 9\}$ des sous ensembles de $E = \{1; 2; 3; 4; 5; 6; 7; 8; 9\}$. Alors :*
- $A \cup B = \{1; 2; 3; 4; 5; 6; 7; 9\}$,
- $A \cap B = \{1; 3; 5\}$,
- $A \setminus B = \{2; 4; 6\}$,
- $A \triangle B = \{2; 4; 6; 7; 9\}$
- $C_E(A) = \{7; 8; 9\}$,

Exercice 1

$$A \triangle B = C_{A \cup B}(A \cap B) = (C_E(A) \cap B) \cup (C_E(B) \cap A)$$
$$C_E(A \cup B) = (C_E(A)) \cap (C_E(B))$$

2.6 Etude d'un exemple : constructibilité

Définition 10 *On se place dans le plan $\mathbb{R}^2$.*

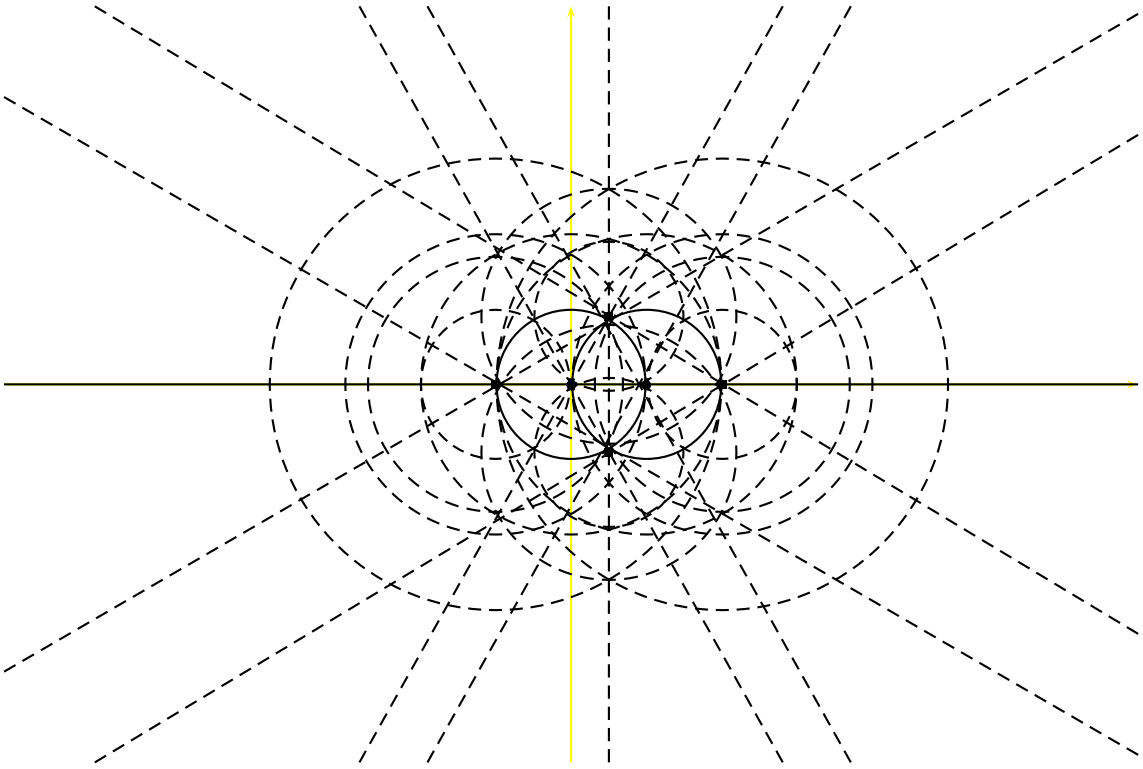
On définit l'ensemble $\mathcal{CONS}_n$ des points constructibles en n étapes par l'induction suivante :

- $\mathcal{CONS}_0 = \{(0,0);(1,0)\}$,
- *Supposons défini les ensembles $\mathcal{CONS}_k$ pour $k < n$.*
  On dit qu'une droite est constructible en n étapes si elle passe par deux points constructibles en strictement moins de n étapes,
  On dit qu'un cercle est constructible en n étapes si son centre est constructible en strictement moins de n étapes et qu'il passe par un point constructible en strictement moins de n étapes,
  On dit qu'un point est constructible en n étapes (donc qu'il est dans $\mathcal{CONS}_n$), si il est l'intersection de deux droites, ou d'une droite et d'un cercle, ou de deux cercles constructibles en n étapes.

On définit l'ensemble $\mathcal{CONS}$ des points constructibles par :

$$\mathcal{CONS} = \mathcal{CONS}_0 \cup \mathcal{CONS}_1 \cup \ldots = \bigcup_{n\in\mathbb{N}} \mathcal{CONS}_n$$

On dit qu'un réel x est constructible si $(x,0) \in \mathcal{CONS}$.



Proposition 6 *Quelques résultats importants :*

1. *Equation de droite :*
   On cherche l'équation de la droite Δ passant par deux points $A(x_A, y_A)$ et $B(x_B, y_B)$ distincts (avec par exemple $x_A \neq x_B$).

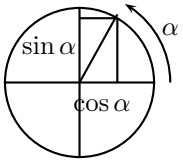
$$\begin{aligned}
P(x,y) \in \Delta &\Leftrightarrow \vec{AP} \text{ et } \vec{AB} \text{ sont colinéaires} \\
&\Leftrightarrow \exists \lambda \in \mathbb{R}, \vec{AP} = \lambda.\vec{AB} \\
&\Leftrightarrow \begin{cases} x - x_A = \lambda.(x_B - x_A) \\ y - y_A = \lambda.(y_B - y_A) \end{cases} \\
&\Leftrightarrow \begin{cases} \lambda = \frac{x-x_A}{x_B-x_A} \\ y - y_A = \frac{x-x_A}{x_B-x_A}.(y_B - y_A) \end{cases} \\
&\Leftrightarrow y = x.\frac{y_B - y_A}{x_B - x_A} + (y_A - x_A.\frac{y_B - y_A}{x_B - x_A})
\end{aligned}$$

Remarque 9 *On suppose ici que $x_A - x_B \neq 0$ pour pouvoir diviser par $x_A - x_B$. Si ce n'est pas le cas, on ne peut pas paramétrer y en fonction de x, mais comme A et B sont distincts, $x_A - x_B = 0 \Rightarrow y_A - y_B \neq 0$ et on peut donc paramétrer x par y.*

2. *Equation de cercle :*
On cherche l'équation du cercle Ω de centre $A(x_A, y_A)$ et de rayon R.

$$\begin{aligned} P(x,y) \in \Omega &\Leftrightarrow AP = R \Leftrightarrow AP^2 = R^2 \\ &\Leftrightarrow \vec{AP}.\vec{AP} = R^2 \\ &\Leftrightarrow \begin{pmatrix} x - x_A \\ y - y_A \end{pmatrix} . \begin{pmatrix} x - x_A \\ y - y_A \end{pmatrix} = R^2 \\ &\Leftrightarrow (x - x_A)^2 + (y - y_A)^2 = R^2 \end{aligned}$$

3. *Formules trigonométriques :*
On rappelle que le cosinus et le sinus d'un angle se lisent sur le cercle trigonométrique.



On en déduit immédiatement certaines formules simples (la première formule correspond à l'équation du cercle, les autres reviennent simplement à regarder sur la figure les angles correspondants) :

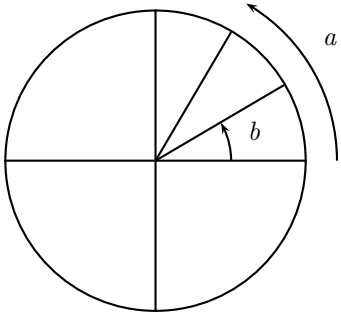
$$(\sin x)^2 + (\cos x)^2 = 1$$

$$\cos(-x) = \cos x \ et \ \sin(-x) = -\sin x$$

$$\cos(\pi - x) = -\cos x \ et \ \sin(\pi - x) = \sin x$$

$$\sin(\frac{\pi}{2} - x) = \cos x \ et \ \cos(\frac{\pi}{2} - x) = \sin x$$

On a d'autre part :



$$\begin{aligned} \cos(a-b) &= \|\vec{OP}\|.\|\vec{OQ}\|.\cos(\vec{OP},\vec{OQ}) \\ &= \vec{OP}.\vec{OQ} \\ &= \begin{pmatrix} \cos b \\ \sin b \end{pmatrix} . \begin{pmatrix} \cos a \\ \sin a \end{pmatrix} \\ &= \cos a.\cos b + \sin a.\sin b \end{aligned}$$

Par les formules précédentes, on peut alors en déduire :

$$\cos(a+b) = \cos a.\cos b - \sin a.\sin b$$

$$\sin(a+b) = \sin a.\cos b + \cos a.\sin b$$

$$\sin(a-b) = \sin a.\cos b - \cos a.\sin b$$

En sommant puis en soustrayant les deux premières entre elles et les deux suivantes entre elles, on obtient

$$\cos(a-b) + \cos(a+b) = 2\cos a\cos b$$

$$\cos(a-b) - \cos(a+b) = 2\sin a\sin b$$

$$\sin(a-b) + \sin(a+b) = 2\sin a\cos b$$

En remplaçant b par a, on obtient :

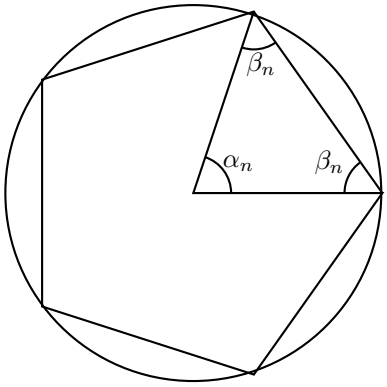
$$1 + \cos(2a) = 2(\cos a)^2$$

$$1 - \cos(2a) = 2(\sin a)^2$$

$$\sin(2a) = 2\sin a\cos a$$

Remarque 10 *Il n'est pas inutile de connaître ces formules et de savoir les retrouver.*

4. *Polygônes réguliers :*



On rappelle juste que l'angle au centre d'un polygône régulier à n côtés est donné par $\alpha_n = \frac{2\pi}{n}$ et qu'un angle extérieur est donné par $\beta_n = \pi(\frac{1}{2} - \frac{1}{n})$.

5. *Barycentres :*
Soit $n \in \mathbb{N} \setminus \{0\}$.
Soient $A_1, A_2, \ldots, A_n$ n points du plan et $\alpha_1, \alpha_2, \ldots, \alpha_n$ n réels tels que $\sum_{k=1}^n \alpha_k \neq 0$. Le barycentre G de $A_1, A_2, \ldots, A_n$ pour les coefficients $\alpha_1, \alpha_2, \ldots, \alpha_n$ est défini par $\sum_{k=1}^n \alpha_k.\vec{GA_k} = \vec{0}$.
On dit que G est l'isobarycentre des points $A_1, A_2, \ldots, A_n$ si G est le barycentre de $A_1, A_2, \ldots, A_n$ pour les coefficients $1, 1, \ldots, 1$.

Remarque 11 *La définition du barycentre est équivalente à : $\vec{OG} = \frac{\sum_{k=1}^n \alpha_k \vec{OA_k}}{\sum_{k=1}^n \alpha_k}$.*
En effet,

$$\begin{aligned}
\sum_{k=1}^n \alpha_k.\vec{GA_k} = \vec{0} &\Leftrightarrow \sum_{k=1}^n \alpha_k.(\vec{GO} + \vec{OA_k}) = \vec{0} \\
&\Leftrightarrow \sum_{k=1}^n \alpha_k \vec{OG} = \sum_{k=1}^n \alpha_k \vec{OA_k} \\
&\Leftrightarrow \vec{OG} = \frac{\sum_{k=1}^n \alpha_k \vec{OA_k}}{\sum_{k=1}^n \alpha_k}
\end{aligned}$$

Exemple 15
- $\mathcal{CONS}_0 = \{(0,0);(1,0)\}$,
- $\mathcal{CONS}_1 = \{(0,0);(1,0);(-1,0);(2,0);(\frac{1}{2},\frac{\sqrt{3}}{2});(\frac{1}{2},-\frac{\sqrt{3}}{2})\}$,
- $\mathcal{CONS}_2 = \ldots$

Exercice 2 *Retrouver $\mathcal{CONS}_1$ par les équations des cercles.*

Proposition 7 *1. Si A et B sont deux points constructibles, alors le milieu du segment $[A;B]$ est constructible.*

2. Si Δ est une droite constructible et P est un point constructible, la droite passant par P et perpendiculaire (resp. : parallèle) à Δ est constructible.

3. On en déduit que $x \in \mathbb{R}$ est constructible $\Leftrightarrow \exists y \in \mathbb{R}, (x,y) \in \mathcal{CONS}$.

Démonstration 4 *Constructions très classiques.*

□

Proposition 8 *1. Tout entier relatif est constructible.*

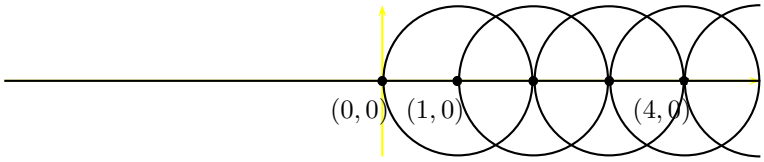
2. Tout rationnel est constructible.

3. Si $x \geq 0$ est constructible, $\sqrt{x}$ est constructible.

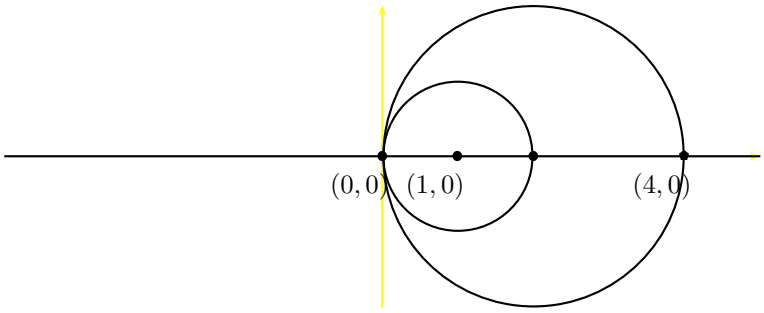
Démonstration 5 *Notons que l'axe des abscisses est constructible.*

1. *Montrons par récurrence que $\forall n \in \mathbb{N} \setminus \{0\}, n-1$ et n sont constructibles.*
   - *0 et 1 sont constructibles car $(0,0) \in \mathcal{CONS}$ et $(1,0) \in \mathcal{CONS}$,*
   - *supposons que $n-1$ et n soient constructibles. Alors on trace le cercle de centre $(n,0)$ et passant par $(n-1,0)$. Il est constructible et coupe l'axe des abscisses (constructible) en $(n+1,0)$. Donc $n+1$ est constructible.*

   Pour construire un entier négatif, on fait le même travail dans les négatifs.

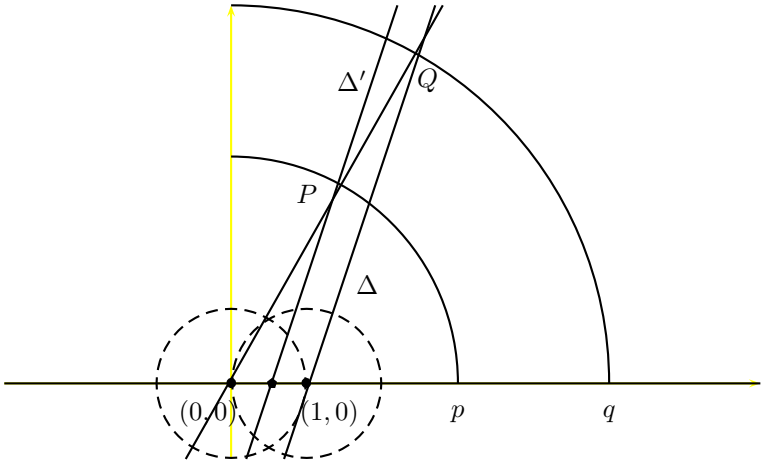


Remarque 12 *On voit ici que l'on a besoin de construire $n-1$ cercles pour obtenir le point $(n,0)$ par cette méthode. Elle n'est clairement pas optimale : par exemple, on n'a besoin que de 2 cercles pour construire le point $(4,0)$:*

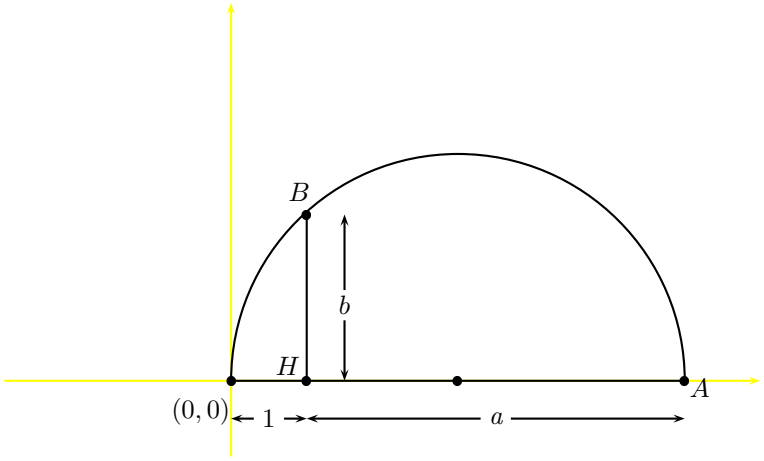


En fait si $n \in \mathbb{N}$ se décompose en base 2 sous la forme $n = 2^p + 2^{p-1}\alpha_{p-1} + \ldots + 4\alpha_2 + 2\alpha_1 + \alpha_0 = 2^p + \sum_{k=0}^{p-1} 2^k \alpha_k$, (avec $\forall k \in \{0;\ldots;p-1\}, \alpha_k \in \{0;1\}$) alors on a besoin de $p + \alpha_{p-1} + \ldots + \alpha_2 + \alpha_1 + \alpha_0 = p + \sum_{k=0}^{p-1} \alpha_k$ cercles pour construire n.

2. *On utilise le théorème de Thalès : Si $(p,q) \in \mathbb{N} \times (\mathbb{N} \setminus \{0\})$, on reporte p en P et q en Q sur une droite déjà construite passant par 0. On trace ensuite la droite Δ passant par Q et $(1,0)$, puis la droite Δ' passant P et parallèle à Δ. Δ' coupe l'axe des abscisses (constructible) en $\frac{p}{q}$.*



3. On utilise la construction suivante :



(a) Méthode 1 : On a l'équation :

$$(\frac{a-1}{2})^2 + b^2 = (\frac{a+1}{2})^2$$

$$b^2 = (\frac{a+1}{2})^2 - (\frac{a-1}{2})^2 = a$$

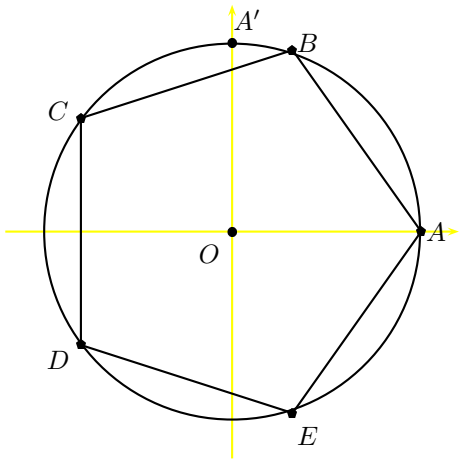
$$b = \sqrt{a}$$

(b) Méthode 2 : les triangles OHB et BHA sont semblables, donc on a égalité des rapports :

$$\frac{a}{b} = \frac{b}{1} \Rightarrow a = b^2$$

□

On va maintenant s'intéresser à la construction d'un pentagone régulier. Le but est de placer à la règle et au compas cinq points régulièrement espacés sur le cercle de centre O et de rayon 1, c'est-à-dire :



Pour cela, on va construire le réel $\cos(\frac{2\pi}{5})$ (car $\frac{2\pi}{5}$ est l'angle au centre d'un pentagone régulier).

Proposition 9

$$\cos(\frac{\pi}{5}) = \frac{\sqrt{5}+1}{4} \text{ et } \cos(\frac{2\pi}{5}) = \frac{\sqrt{5}-1}{4}$$

Démonstration 6 *1. On calcule la somme de vecteurs :*

$$\begin{aligned}
\vec{OA}+\vec{OB}+\vec{OC}+\vec{OD}+\vec{OE} &= \vec{OA}+(\cos(\frac{2\pi}{5})\vec{OA}+\sin(\frac{2\pi}{5})\vec{OA'})+(\cos(\frac{4\pi}{5})\vec{OA}+\sin(\frac{4\pi}{5})\vec{OA'}) \\
&\quad +(\cos(\frac{6\pi}{5})\vec{OA}+\sin(\frac{6\pi}{5})\vec{OA'})+(\cos(\frac{8\pi}{5})\vec{OA}+\sin(\frac{8\pi}{5})\vec{OA'}) \\
&= (1+\cos(\frac{2\pi}{5})+\cos(\frac{4\pi}{5})+\cos(\frac{6\pi}{5})+\cos(\frac{8\pi}{5}))\vec{OA} \\
&\quad +(\sin(\frac{2\pi}{5})+\sin(\frac{4\pi}{5})+\sin(\frac{6\pi}{5})+\sin(\frac{8\pi}{5}))\vec{OA'} \\
&= (1-2\cos(\frac{\pi}{5})+2\cos(\frac{2\pi}{5}))\vec{OA}
\end{aligned}$$

On peut faire le même calcul avec le point B et on trouve :

$$(1-2\cos(\frac{\pi}{5})+2\cos(\frac{2\pi}{5}))\vec{OA} = (1-2\cos(\frac{\pi}{5})+2\cos(\frac{2\pi}{5}))\vec{OB}$$

Comme $\vec{OA}$ et $\vec{OB}$ ne sont pas colinéaires, on en déduit :

$$1-2\cos(\frac{\pi}{5})+2\cos(\frac{2\pi}{5}) = 0$$

Remarque 13 *O est donc l'isobarycentre des points A, B, C, D, E.*

2. On a donc :

$$2\cos(\frac{2\pi}{5}) = 4(\cos(\frac{\pi}{5}))^2-2 = 2\cos(\frac{\pi}{5})-1$$

$$4(\cos(\frac{\pi}{5}))^2-2\cos(\frac{\pi}{5})-1 = 0$$

$$\Delta = 4+16 = 20 = (2\sqrt{5})^2$$

$$\cos(\frac{\pi}{5}) = \frac{2\pm 2\sqrt{5}}{8} = \frac{1\pm\sqrt{5}}{4}$$

Comme $\cos(\frac{\pi}{5})$ est positif, on trouve le résultat :

$$\cos(\frac{\pi}{5}) = \frac{1+\sqrt{5}}{4}$$

D'autre part,

$$\cos(\frac{2\pi}{5}) = 2(\cos(\frac{\pi}{5}))^2-1 = \frac{\sqrt{5}-1}{4}$$

□

Par conséquent, on sait construire $\cos(\frac{2\pi}{5})$ et il ne reste plus qu'à reconstruire le pentagone.

□

Exercice 3 *Construire le triangle équilatéral et l'hexagone régulier de la même façon.*

Remarque 14 *On peut prouver que l'on ne peut pas construire l'heptagone régulier à la règle et au compas, mais cette preuve fait appel à des notions de théorie des corps que l'on voit en deuxième année de classe préparatoire.*

3 Les applications

3.1 Définition

Définition 11 *Soient A et B deux ensembles. Une application f de A dans B est un sous ensemble de $A \times B$ tel que $\forall x \in A, \exists! y \in B, (x, y) \in f$.*

On définit donc l'ensemble des applications de A dans B par :

$$\mathcal{F}(A, B) = \{f \in \wp(A \times B) | \forall x \in A, \exists! y \in B, (x, y) \in f\}$$

Remarque 15 *Cette définition est une manière formelle de dire qu'une application f de A dans B associe une et une seule image $y = f(x)$ dans B à tout élément x de A.*

*On dit que y est l'image de x par f et que x est **un** antécédent de y.*

On note souvent :

$$\begin{array}{rcl} f : A & \longrightarrow & B \\ x & \longmapsto & f(x) \end{array}$$

3.2 Propriétés

Définition 12 *Soient A et B deux ensembles et $f \in \mathcal{F}(A, B)$. On dit que :*

1. *f est injective si $\forall (x, x') \in A^2, ((f(x) = f(x')) \Rightarrow (x = x'))$,*
2. *f est surjective si $\forall y \in B, \exists x \in A, f(x) = y$,*
3. *f est bijective si $\forall y \in B, \exists! x \in A, f(x) = y$.*

Remarque 16 *il faut bien comprendre ce que veulent dire ces définitions :*

1. *f est injective si tout élément de B a au plus un antécédent,*
2. *f est surjective si tout élément de B a au moins un antécédent,*
3. *f est bijective si tout élément de B a exactement un antécédent.*

Exercice 4 *Comment choisir les ensembles A et B pour que l'application $f : A \longrightarrow B$ définie par $f(x) = x^2$ soit injective (resp. : surjective) ?*

3.3 Les applications associées

Définition 13 *Soient A et B deux ensembles et $f \in \mathcal{F}(A, B)$. On associe à f deux applications :*

1. *Image directe :*

$$\begin{array}{rcl} IDf : \wp(A) & \longrightarrow & \wp(B) \\ X & \longmapsto & \{y \in B | \exists x \in X, f(x) = y\} \end{array}$$

2. *Image réciproque :*

$$\begin{array}{rcl} IRf : \wp(B) & \longrightarrow & \wp(A) \\ Y & \longmapsto & \{x \in A | f(x) \in B\} \end{array}$$

Proposition 10 *Soient A et B deux ensembles et $f \in \mathcal{F}(A, B)$. Alors $\forall (Y_1, Y_2) \in \wp(B)^2$*

$$IRf(Y_1 \cup Y_2) = IRf(Y_1) \cup IRf(Y_2)$$

$$IRf(Y_1 \cap Y_2) = IRf(Y_1) \cap IRf(Y_2)$$

$$IRf(Y_1 \triangle Y_2) = IRf(Y_1) \triangle IRf(Y_2)$$

$$IRf(C_B(Y_1)) = C_A(IRf(Y_1))$$

Démonstration 7 *On ne démontre ici que la première assertion, les autres étant laissées en exercice :*

$$\begin{array}{rcl} x \in IRf(Y_1 \cup Y_2) & \Leftrightarrow & f(x) \in Y_1 \cup Y_2 \\ & \Leftrightarrow & (f(x) \in Y_1) \vee (f(x) \in Y_2) \\ & \Leftrightarrow & (x \in IRf(Y_1)) \vee (x \in IRf(Y_2)) \\ & \Leftrightarrow & x \in IRf(Y_1) \cup IRf(Y_2) \end{array}$$

□

Remarque 17 *Pour l'image directe, les formules ne sont pas aussi simples :*
Soient A et B deux ensembles et $f \in \mathcal{F}(A,B)$. Alors $\forall (X_1, X_2) \in \wp(A)^2$

$$IDf(X_1 \cup X_2) = IDf(X_1) \cup IDf(X_2)$$

$$IDf(X_1 \cap X_2) \subsetneq IDf(X_1) \cap IDf(X_2)$$

Démonstration 8 - *Union :*

$$\begin{aligned} y \in IDf(X_1 \cup X_2) &\Leftrightarrow \exists x \in X_1 \cup X_2, f(x) = y \\ &\Leftrightarrow (\exists x \in X_1, f(x) = y) \vee (\exists x \in X_2, f(x) = y) \\ &\Leftrightarrow (y \in IDf(X_1)) \vee (y \in IDf(X_2)) \\ &\Leftrightarrow y \in IDf(X_1) \cup IDf(X_2) \end{aligned}$$

- *Intersection :*

$$\begin{aligned} y \in IDf(X_1 \cap X_2) &\Rightarrow \exists x \in X_1 \cap X_2, f(x) = y \\ &\Rightarrow (y \in IDf(X_1)) \wedge (y \in IDf(X_2)) \\ &\Rightarrow y \in IDf(X_1) \cap IDf(X_2) \end{aligned}$$

En revanche, l'autre inclusion est fausse.
Contre-exemple : posons $A = \{1;2;3\}$, $B = \{x;y\}$ et f définie par : $f(1) = f(2) = x, f(3) = y$. Posons ensuite $X_1 = \{1;3\}$ et $X_2 = \{2;3\}$. Alors,

$$IDf(X_1 \cap X_2) = IDf(\{3\}) = \{y\} \neq \{x;y\} = \{x;y\} \cap \{x;y\} = IDf(X_1) \cap IDf(X_2)$$

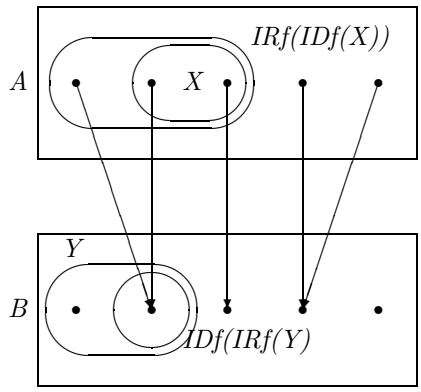
□

Proposition 11 *Soient A et B deux ensembles et $f \in \mathcal{F}(A,B)$. Alors $\forall X \in \wp(A), \forall Y \in \wp(B)$*

$$Y \supset IDf(IRf(Y))$$

$$X \subset IRf(IDf(X))$$

Démonstration 9 - $y \in IDf(IRf(Y)) \Rightarrow \exists x \in IRf(Y), f(x) = y \Rightarrow y \in Y$
- $x \in X \Rightarrow f(x) \in IDf(X) \Rightarrow x \in IRf(IDf(X))$
- *En revanche, l'autre inclusion est fausse dans les deux cas.*
Contre-exemple sur un dessin :



□

Proposition 12 *on a les équivalences suivantes :*

$$f \text{ injective} \Leftrightarrow \forall X \in \wp(A), IRf(IDf(X)) = X$$

$$f \text{ surjective} \Leftrightarrow \forall Y \in \wp(B), IDf(IRf(Y)) = Y$$

Démonstration 10 *On ne prouve ici que la première équivalence, la seconde étant laissée en exercice.*

$\Leftarrow$ *On considère le singleton* $\{x\} = IRf(IDf(\{x\}))$.
Soit $x' \in A$ *tel que* $f(x) = f(x')$. *Alors* $f(x') \in IDf(\{x\})$, *donc* $x' \in IRf(IDf(\{x\}) = \{x\}$, *donc* $x' = x$.
Donc f *est bien injective.*

$\Rightarrow$ *Soit* $X \in \wp(A)$. *On a déjà vu que* $X \subset IRf(IDf(X))$. *Il ne reste donc qu'à prouver l'autre inclusion.*
Soit $x \in IRf(IDf(X))$. *Alors* $f(x) \in IDf(X)$, *donc* $\exists x' \in X tel\ que f(x) = f(x')$. *Mais comme* f *est injective,* $x = x' \in X$.

□

3.4 Composition des applications

Définition 14 *Soient* A, B *et* C *trois ensembles. Soient* $f \in \mathcal{F}(A, B)$ *et* $g \in \mathcal{F}(B, C)$.
On définit $g \circ f \in \mathcal{F}(A, C)$, *appelée composée de* f *par* g *par :* $\forall x \in A, g \circ f(x) = g(f(x))$.

Proposition 13 *Soient* A, B *et* C *trois ensembles. Soient* $f \in \mathcal{F}(A, B)$ *et* $g \in \mathcal{F}(B, C)$.
On a les implications suivantes :

$$f \text{ et } g \text{ injectives} \Rightarrow g \circ f \text{ injective}$$

$$f \text{ et } g \text{ surjectives} \Rightarrow g \circ f \text{ surjective}$$

$$g \circ f \text{ injective} \Rightarrow f \text{ injective}$$

$$g \circ f \text{ surjective} \Rightarrow g \text{ surjective}$$

Démonstration 11

1. *Soit* $(x_1, x_2) \in A^2$ *tel que* $g \circ f(x_1) = g \circ f(x_2)$,
   $(g \text{ injective}) \wedge (g \circ f(x_1) = g \circ f(x_2)) \Rightarrow f(x_1) = f(x_2)$
   $(f \text{ injective}) \wedge (f(x_1) = f(x_2)) \Rightarrow x_1 = x_2$, *donc* $g \circ f$ *est injective.*
2. *Soit* $z \in C$,
   $g \text{ surjective} \Rightarrow \exists y \in B, g(y) = z$
   $f \text{ surjective} \Rightarrow \exists x \in A, f(x) = y$
   Donc $\exists x \in A, g \circ f(x) = z$, *donc* $g \circ f$ *est surjective.*
3. *Soit* $(x_1, x_2) \in A^2$ *tel que* $f(x_1) = f(x_2)$, *alors* $g \circ f(x_1) = g \circ f(x_2)$ *et comme* $g \circ f$ *est injective,* $x_1 = x_2$, *donc* f *est injective.*
4. *Soit* $z \in C$; *comme* $g \circ f$ *est surjective,* $\exists x \in A, g \circ f(x) = z$. *Pour cet* x, $f(x) \in B$ *et* $g(f(x)) = z$, *donc* g *est surjective.*

□

Remarque 18 *Notons que* $g \circ f$ *peut être injective sans que* g *ne le soit :*
Contre-exemple : soient $A = \{x\}$,$B = \{y; z\}$ *et* $C = \{t\}$; $f \in \mathcal{F}(A, B)$ *définie par* $f(x) = y$ *et* $g \in \mathcal{F}(B, C)$ *définie par* $g(y) = t$ *et* $g(z) = t$. *Alors* $g \circ f$ *est injective et* g *ne l'est pas.*

3.5 Application réciproque

Définition 15 *Soit* A *un ensemble.*
L'application identité est l'application $Id_A \in \mathcal{F}(A, A)$ *définie par :* $\forall x \in A, Id_A(x) = x$.

Définition 16 *Soient* A *et* B *deux ensembles et* $f \in \mathcal{F}(A, B)$ *bijective. Il existe une unique application de* $\mathcal{F}(B, A)$, *notée* f^{-1} *et appelée inverse de* f, *qui vérifie :* $f \circ f^{-1} = Id_B$ *et* $f^{-1} \circ f = Id_A$.
Bien entendu, f^{-1} *est aussi bijective et* $(f^{-1})^{-1} = f$.

Remarque 19 *L'application* f^{-1} *associe à chaque élément* y *de* B *son unique antécédent par* f. *Il faut donc voir l'action de* f^{-1} *comme l'action inverse de celle de* f.

Proposition 14 *Soient* A, B *et* C *trois ensembles. Soient* $f \in \mathcal{F}(A, B)$ *et* $g \in \mathcal{F}(B, C)$ *deux applications bijectives.*
Alors $g \circ f$ *est bijective et son inverse est :* $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Démonstration 12 *Il est clair que tout* z *dans* C *a un unique antécédent par* $g \circ f$ *: c'est l'unique antécédent par* f *de l'unique antécédent de* z *par* g.
De plus, $(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ f \circ f^{-1} \circ g^{-1} = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ g^{-1} = Id_C$ *et* $(f^{-1} \circ g^{-1}) \circ (g \circ f) = Id_A$.

□

3.6 Restriction et prolongement d'une application

Soient A et B deux ensembles et $f : A \longrightarrow B$.
Il s'agit ici de modifier l'ensemble de départ A de l'application f.

Définition 17 *Si E est une partie de A, on note $f_{|E}$ l'application de E dans B définie par $\forall x \in E, f_{|E}(x) = f(x)$. Cette application s'appelle restriction de f à E.*
Si A est une partie de E', une application ϕ de E' dans B telle que $\phi_{|A} = f$ sera appelée prolongement de f à E'.

Proposition 15 *Soient A et B deux ensembles et $f : A \longrightarrow B$.*
f injective $\Rightarrow$ toute restriction de f est injective,
f surjective $\Rightarrow$ tout prolongement de f est surjectif.

Démonstration 13 *On ne démontre que la première assertion, l'autre étant laissée en exercice. Soient $x_1, x_2 \in E$ tels que $f_{|E}(x_1) = f_{|E}(x_2)$. Alors $f(x_1) = f(x_2)$, donc par injectivité de f, $x_1 = x_2$. Donc $f_{|E}$ est injective.*

□

3.7 Etude d'un exemple : la partie entière

Définition 18 *On définit l'application partie entière par :*

$$\begin{array}{rcl} E : \mathbb{R} & \longrightarrow & \mathbb{Z} \\ x & \longmapsto & E[x] \text{ où } E[x] \text{ est le seul entier relatif tel que } E[x] \leq x < E[x] + 1 \end{array}$$

Remarque 20 *$E[x]$ est aussi le seul entier relatif tel que $x - 1 < E[x] \leq x$.*

Exemple 16
1. $\forall p \in \mathbb{Z}, \forall x \in \mathbb{R}, E[x + p] = E[x] + p$.
2. $\forall x \in \mathbb{Z}, E[-x] = -E[x]$,
   $\forall x \in \mathbb{R} \setminus \mathbb{Z}, E[-x] = -E[x] - 1$.
3. *etc...*

Preuve 6
1. *Il suffit d'écrire que : $E[x] \leq x < E[x] + 1 \Rightarrow E[x] + p \leq x + p < E[x] + p + 1$ et $E[x] + p \in \mathbb{Z} \Rightarrow E[x + p] = E[x] + p$.*
2. *si $x \in \mathbb{Z}, E[x] = x$ et $E[-x] = -x \Rightarrow E[-x] = -E[x]$,*
   sinon, $E[x] < x < E[x]+1 \Rightarrow -E[x]-1 < -x < -E[x] = -E[x]-1+1$ et $-E[x]-1 \in \mathbb{Z} \Rightarrow E[-x] = -E[x]-1$.

□

Exemple 17
1. $\forall n \in \mathbb{N} \setminus \{0\}, \forall x \in \mathbb{R}, E[nx] - n < nE[x] \leq E[nx]$,
2. $\forall n \in \mathbb{N} \setminus \{0\}, \forall x \in \mathbb{R}, E[\frac{1}{n}E[nx]] = E[x]$.

Preuve 7
1. *Il suffit d'écrire que : $x - 1 < E[x] \leq x \Rightarrow nx - n < nE[x] \leq nx$.*
   mais $E[nx] \leq nx$, donc $E[nx] - n \leq nx - n < nE[x]$,
   et $nE[x] \in \mathbb{Z}$ et $nE[x] \leq nx \Rightarrow nE[x] \leq E[nx]$.
   d'où le résultat.
2. *par conséquent, $\frac{1}{n}E[x] - 1 < E[x] \leq \frac{1}{n}E[nx]$, donc $E[\frac{1}{n}E[nx]] = E[x]$.*

□

Exercice 5 *Le but de l'exercice est de montrer que*

$$\forall n \in \mathbb{N}, \forall x \in \mathbb{R}, \sum_{k=0}^{n-1} E[x + \frac{k}{n}] = E[nx]$$

On définit la fonction f par :

$$\begin{array}{rcl} f : \mathbb{R} & \longrightarrow & \mathbb{N} \\ x & \longmapsto & \displaystyle\sum_{k=0}^{n-1} E[\frac{x+k}{n}] \end{array}$$

1. *montrer que* $\forall x \in \mathbb{R}, f(x+1) = f(x) + 1$.
2. *En déduire que* $\forall p \in \mathbb{N}, \forall x \in \mathbb{R}, f(x+p) = f(x) + p$.
3. *Montrer que* $\forall x \in [0;1[, f(x) = 0$.
4. *En déduire que* $E = f$.
5. *Conclure.*

Définition 19 *On définit la fonction partie fractionnaire par :*

$$\begin{array}{rcl} F : \mathbb{R} & \longrightarrow & [0;1[\\ x & \longmapsto & x - E[x] \end{array}$$

Exemple 18 1. $\forall p \in \mathbb{Z}, \forall x \in \mathbb{R}, F[x+p] = F[x]$

2. *Si* $x \in \mathbb{Z}, F[x] + F[-x] = 0$,
   sinon $F[x] + F[-x] = 1$.

Preuve 8 1. $F[x+p] = x + p - E[x+p] = x + p - (E[x] + p) = x - E[x] = F[x]$

2. *Si* $x \in \mathbb{Z}, F[x] = F[-x] = 0$,
   sinon $F[x] + F[-x] = x - E[x] - x - E[-x] = -E[x] - (-E[x] - 1) = 1$.

□

Exercice 6 *Montrer que*

$$\forall (p,q) \in (\mathbb{N} \setminus \{0\})^2, pgcd(p,q) = 1, \sum_{k=1}^{q-1} F[\frac{k.p}{q}] = \frac{q-1}{2}$$

Définition 20 *Soit* $A \subset \mathbb{R}$ *une partie de* $\mathbb{R}$.
On dit que A *est une partie dense de* $\mathbb{R}$ *si :* $\forall \epsilon > 0, \forall x \in \mathbb{R}, \exists a \in A$ *tel que* $|x - a| < \epsilon$.
On dit que A *est une partie discrète de* $\mathbb{R}$ *si :* $\forall x \in \mathbb{R}, \exists \epsilon > 0$ *tel que* $\forall y \in \mathbb{R}, |x - y| < \epsilon \Rightarrow (x = y) \vee (x \notin A)$.

Proposition 16 – $\mathbb{Q}$ *et* $\mathbb{R} \setminus \mathbb{Q}$ *sont denses dans* $\mathbb{R}$.
– $\mathbb{Z}$ *est discret.*

Démonstration 14 *Soit* $x \in \mathbb{R}$ *et* $\epsilon > 0$.
Soit $n \in \mathbb{N}$ *tel que* $\frac{1}{n} < \epsilon$.
On pose $y_1 = \frac{E[nx]}{n}$ *et* $y_2 = \frac{E[nx\sqrt{2}]}{n\sqrt{2}}$.
On vérifie que $y_1 \in \mathbb{Q}$, $y_2 \in \mathbb{R} \setminus \mathbb{Q}$ *et* $|x - y_1| < \epsilon$, $|x - y_1| < \epsilon$.

□

4 Relation binaire sur un ensemble

4.1 Définition et propriétés

Définition 21 *Une relation binaire sur un ensemble A est un sous-ensemble $R \subset A \times A$.*

Remarque 21 *On note souvent xRy pour $(x, y) \in R$.*
Une relation binaire sur un ensemble doit bien sûr être vue comme une relation entre les éléments de cet ensemble.

Exemple 19 *On définit la relation binaire sur $\mathbb{N}$ par : $\leq = \{(n, m) \in \mathbb{N}^2 | (n = m) \vee (\exists p \in \mathbb{N} \setminus \{0\}, succ^p(n) = m)\}$ (où $succ(n) = n + 1$) et on note $n \leq m$ pour $(n, m) \in \leq$.*

Définition 22 *Soit A un ensemble et R une relation binaire sur A. On dit que R est :*
- *réflexive si $\forall x \in A, xRx$,*
- *symétrique si $\forall (x, y) \in A^2, xRy \Rightarrow yRx$,*
- *antisymétrique si $\forall (x, y) \in A^2, (xRy) \wedge (yRx) \Rightarrow x = y$,*
- *transitive si $\forall (x, y, z) \in A^3, (xRy) \wedge (yRz) \Rightarrow xRz$,*

4.2 Relation d'ordre

Définition 23 *Soit A un ensemble et R une relation binaire sur A. On dit que R est une relation d'ordre si R est réflexive, antisymétrique et transitive.*
On dit que l'ordre R est total si on a de plus : $\forall (x, y) \in A^2, (xRy) \vee (yRx)$.

Exemple 20 *La relation $\leq$ définie par $\forall (n, m) \in \mathbb{N}^2, n \leq m \Leftrightarrow (n = m) \vee (\exists p \in \mathbb{N} \setminus \{0\}, succ^p(n) = m)$ (où $succ(n) = n + 1$) est une relation d'ordre sur $\mathbb{N}$.*
En effet, elle est clairement réflexive, antisymétrique ($\forall (m, n) \in \mathbb{N}^2, (m \leq n) \wedge (n \leq m) \Rightarrow (m = n)$) et transitive ($\forall (m, n, p) \in \mathbb{N}^3, (m \leq n) \wedge (n \leq p) \Rightarrow (\exists a \in \mathbb{N}, succ^a(m) = n) \wedge (\exists b \in \mathbb{N}, succ^b(n) = p) \Rightarrow (succ^{a+b}(m) = p) \Rightarrow (m \leq p)$).

Définition 24 *Si R est une relation d'ordre sur un ensemble A et A' est un sous-ensemble de A, on définit les notions de :*
- *majorant (resp. : minorant) : $m \in A$ est un majorant (resp. : minorant) de A' dans A si $\forall x \in A', xRm$ (resp. : mRx),*
- *plus grand élément (resp. : plus petit élément) : $n \in A'$ est le plus grand élément (resp. : plus petit élément) de A' si $\forall x \in A', xRn$ (resp. : nRx),*
- *borne supérieure (resp. : borne inférieure) : $b \in A$ est la borne supérieure (resp. : borne inférieure) de A' si b est un majorant (resp. : un minorant) de A' et $\forall m \in A, m$ majorant (resp. : minorant) de $A' \Rightarrow bRm$ (resp. : mRb).*

Remarque 22
- *Le plus grand élément de A est un majorant de A dans A.*
  La borne supérieure est le plus petit des majorants.
- *Pour certains ensembles, il n'y a pas de majorant, de plus grand élément ou de borne supérieure :*
  contre-exemple : $\mathbb{N}$ n'a pas de majorant, de plus grand élément ni de borne supérieure dans $\mathbb{N}$.
- *En général, il existe plusieurs majorants. En revanche le plus grand élément et la borne supérieure (s'ils existent) sont uniques.*
  preuve : antisymétrie de la relation d'ordre R.

Exemple 21
1. *$A = \mathbb{N}, A' = \{4, 5, 7, 9, 11, 15\}, R = \leq$. On a alors par exemple 19 majorant de A', $\max(A') = \sup(A') = 15$.*
2. *$A = \mathbb{Q}, B = \mathbb{R}, A' = \{x \in A | x^2 < 2\}, R = \leq$. Tout rationnel (resp. : réel) plus grand que $\sqrt{2}$ est majorant de A' dans $A = \mathbb{Q}$ (resp. : $B = \mathbb{R}$). A' n'a pas de plus grand élément. A' n'a pas de borne supérieure dans $A = \mathbb{Q}$ mais $\sqrt{2}$ est la borne supérieure de A' dans $B = \mathbb{R}$.*

4.3 Relation d'équivalence

Définition 25 *Soit A un ensemble et R une relation binaire sur A. On dit que R est une relation d'équivalence si R est réflexive, symétrique et transitive.*

Exemple 22 *Soit $n \in \mathbb{N}$.*

La relation $\equiv_{[n]}$ définie par $\forall (p,q) \in \mathbb{N}^2, p \equiv_{[n]} q \Leftrightarrow \exists k \in \mathbb{Z}, p-q = kn$ est une relation d'équivalence sur $\mathbb{N}$, appelée relation de congruence modulo n.

En effet, elle est clairement réflexive(prendre $k=0$), symétrique ($\forall (p,q) \in \mathbb{N}^2, (p \equiv_{[n]} q) \Rightarrow (\exists k \in \mathbb{Z}, p-q = kn) \Rightarrow (q-p = (-k)n)$ et transitive ($\forall (p,q,r) \in \mathbb{N}^3, (p \equiv_{[n]} q) \wedge (q \equiv_{[n]} r) \Rightarrow (\exists k \in \mathbb{Z}, p-q = kn) \wedge (\exists k' \in \mathbb{Z}, q-r = k'n) \Rightarrow (p-r = (k+k')n) \Rightarrow (p \equiv_{[n]} r)$).

Définition 26 *Soit A un ensemble et R une relation d'équivalence sur A. Pour $x \in A$, on appelle classe d'équivalence de x pour R l'ensemble : $cl_R(x) = \{y \in A | xRy\}$.*

Proposition 17 *Soit A un ensemble et R une relation d'équivalence sur A. Alors $\forall (x,y) \in A^2$,*

$$xRy \Leftrightarrow cl_R(x) = cl_R(y)$$

$$\neg(xRy) \Leftrightarrow cl_R(x) \cap cl_R(y) = \emptyset$$

Ainsi, les classes d'équivalence pour R forment une partition de A, c'est-à-dire : $\forall (x,y) \in A^2, (cl_R(x) = cl_R(y)) \vee (cl_R(x) \cap cl_R(y) = \emptyset)$.

Démonstration 15
- *si xRy, alors $z \in cl_R(y) \Rightarrow yRz \Rightarrow xRz$ (par transitivité) $\Rightarrow z \in cl_R(x)$ donc $cl_R(y) \subset cl_R(x)$. Par symétrie, on a aussi yRx donc $cl_R(x) \subset cl_R(y)$, donc $cl_R(y) = cl_R(x)$.*
  Réciproquement, si $cl_R(y) = cl_R(x)$, $x \in cl_R(x)$ (par réflexivité), donc $x \in cl_R(y)$, donc xRy.
- *si $cl_R(x) \cap cl_R(y) \neq \emptyset$, soit $z \in cl_R(x) \cap cl_R(y)$. Alors $(xRz) \wedge (yRz)$, donc par symétrie et transitivité, xRy. Donc par contraposée, $\neg(xRy) \Rightarrow cl_R(x) \cap cl_R(y) = \emptyset$.*
  Réciproquement, si xRy, $x \in cl_R(x) \cap cl_R(y)$, donc $cl_R(x) \cap cl_R(y) \neq \emptyset$. D'où le résultat par contraposée.
- *$\forall (x,y) \in A^2$, soit xRy, et alors $cl_R(x) = cl_R(y)$, soit $\neg(xRy)$, et alors $cl_R(x) \cap cl_R(y) = \emptyset$.*

□

Définition 27 *Soit A un ensemble et R une relation d'équivalence sur A. L'ensemble des classes d'équivalence pour R est appelé ensemble quotient de A par R et est noté : $A/R = \{cl_R(x) | x \in A\}$.*

Exemple 23 *L'ensemble quotient de $\mathbb{N}$ par $\equiv_{[n]}$ est : $\mathbb{N}/\equiv_{[n]} = \{cl_{\equiv_{[n]}}(0); cl_{\equiv_{[n]}}(1); \ldots; cl_{\equiv_{[n]}}(n-1)\} = \{\{0; n; 2n; 3n; \ldots\}; \{1; n+1; 2n+1; \ldots\}; \ldots; \{n-1; 2n-1; 3n-1; \ldots\}\}$.*

5 Loi de composition interne sur un ensemble

5.1 Définitions

Définition 28 *Soit A un ensemble.*

Une loi de composition interne sur A est une application de A^2 dans A.

Si elle est notée $\star$, l'image de (x,y) sera notée $x \star y$ plutôt que $\star(x,y)$.

Définition 29 *Soit A un ensemble et $\star$ une loi de composition interne sur A.*

1. *On dit que $\star$ est :*
   - *associative si $\forall (x,y,z) \in A^3, (x \star y) \star z = x \star (y \star z)$,*
   - *commutative si $\forall (x,y) \in A^2, x \star y = y \star x$.*
2. *On dit que A possède un élément neutre pour $\star$ si $\exists e \in A$ tel que $\forall x \in A, x \star e = e \star x = x$.*
3. *Si un tel élément existe, on dit qu'un élément x de A est symétrisable dans A si $\exists x' \in A$ tel que $x \star x' = x' \star x = e$. x' est appelé symétrique de x pour $\star$.*
4. *On dit qu'un élément x de A est régulier à gauche (resp. : à droite) sur A si $\forall (y,z) \in A^2, x \star y = x \star z \Rightarrow y = z$ (resp. : $y \star x = z \star x \Rightarrow y = z$)*

Proposition 18 *Soit A un ensemble et $\star$ une loi de composition interne sur A.*

1. *Si il existe un élément neutre, alors il est unique,*
2. *Si il existe un élément neutre et que $\star$ est associative, alors pour tout x dans A, si il existe un symétrique de x, alors il est unique.*
3. *Si $\star$ est commutative, les éléments réguliers à gauche sont exactement les éléments réguliers à droite.*

Exemple 24 *Dans $\mathbb{N}$, muni de la loi $\times$, 0 n'est pas régulier car $x.0 = y.0 \not\Rightarrow x = y$.*

Démonstration 16 *1. Soient deux éléments neutres e, e' pour $\star$ dans A. Alors $e = e \star e' = e'$. D'où l'unicité.*

2. Soient x'_1, x'_2 deux symétriques de x pour $\star$. Alors $x'_1 = x'_1 \star e = x'_1 \star x \star x'_2 = e \star x'_2 = x'_2$.

3. Si la loi est commutative, $x \star y = y \star x = z \star x = x \star z$. D'où le résultat.

□

5.2 Etude d'un exemple : sous-groupes de $\mathbb{R}$

Définition 30 *Soit A un ensemble muni d'une loi de composition interne $\star$.*
On dit que $(A, \star)$ est un groupe si :

1. *$\star$ est associative sur A ,*
2. *A possède un élément neutre pour $\star$,*
3. *tout élément de A est symétrisable pour $\star$.*

On dit que $(A, \star)$ est un groupe commutatif (ou abélien) si de plus $\star$ est commutative sur A.

Définition 31 *Soit $(A, \star)$ un groupe.*
On dit que ensemble $(B, \star)$ est un sous-groupe de $(A, \star)$ si $B \subset A$ et $(B, \star)$ est un groupe.

Proposition 19 *Soit $(A, \star)$ un groupe (où le neutre est noté e et l'inverse de x est noté x^{-1}) et $B \subset A$.*

$$\text{Alors } (B, \star) \text{ sous-groupe de } (A, \star) \Leftrightarrow \begin{cases} e \in B \\ \forall (x, y) \in B^2, x \star y \in B \\ \forall x \in B, x^{-1} \in B \end{cases}$$

Exemple 25
- *$(\mathbb{R}, +)$ est un groupe ($+$ est l'addition usuelle sur $\mathbb{R}$).*
- *$(\mathbb{Z}, +)$ est un sous groupe de $(\mathbb{R}, +)$.*

Proposition 20 *Soit $(G, +)$ un sous groupe de $(\mathbb{R}, +)$.*
Alors G est dense ou $G = a\mathbb{Z} = \{a.z | z \in \mathbb{Z}\}$ avec $a \in \mathbb{R}$.

Les sous-groupes de $(\mathbb{R}, +)$ sont donc soit denses, soit discrets.

Démonstration 17 *Si $G = \{0\}$, pas de problème, G est discret.*
Sinon, $\exists x \in G \setminus \{0\}$. Si $x < 0, -x > 0$ et $-x \in G$ car $(G, +)$ est un groupe.
Donc $G \cap \mathbb{R}^+ \neq \emptyset \Rightarrow$ soit $\delta = \inf(G \cap \mathbb{R}^+)$

1. ***Lemme 1*** *Si $\delta \neq 0$, $G = \delta\mathbb{Z}$.*

   Preuve 9 *– Supposons que $\delta \notin G$. Alors $\exists (x, y) \in G \cap \mathbb{R}^+, x - \delta < \delta$ et $y - \delta < x - \delta$. Alors $0 < x - y < \delta$ et $x - y \in G$ ce qui contredit la définition de δ. Donc $\delta \in G$.*
   – Par conséquent, puisque $(G, +)$ est un groupe, $\delta\mathbb{Z} \subset G$
   – Supposons que $G \not\subset \delta\mathbb{Z}$, alors $\exists x \in G \setminus \delta\mathbb{Z}$. Alors $\exists z \in \mathbb{Z}$ tel que $z.\delta < x < (z+1).\delta$ (notons que $z = [\frac{x}{\delta}]$). Mais alors $z.\delta \in G$ et $x \in G \Rightarrow x - z.\delta \in G$ ce qui est absurde car $0 < x - z.\delta < \delta$.

2. ***Lemme 2*** *Si $\delta = 0$, alors G est dense.*

   Preuve 10 *Soit $x \in \mathbb{R}$ et $\epsilon > 0$. Il faut trouver $y \in G$ tel que $|x - y| < \epsilon$.*
   $\delta = 0$, donc $\exists y' \in G \cap \mathbb{R}^+, y' < \epsilon$.
   Alors $\frac{x}{y'} \leq [\frac{x}{y'}] < \frac{x}{y'} + 1$, donc $x \leq y'[\frac{x}{y'}] < x + y' < x + \epsilon$ et $y'[\frac{x}{y'}] \in G$ car $(G, +)$ est un groupe.
   $y'[\frac{x}{y'}]$ convient.

□

6 Les ensembles finis

6.1 La notion d'ensemble fini

Définition 32 *Un ensemble A est fini si il existe $n \in \mathbb{N}$ tel que A soit en bijection avec $\{1; 2; \ldots; n\}$.*
Si cet entier existe, il est unique. On dit que le cardinal de A est n, noté : $n = card(A) = \#(A)$.

Remarque 23 *Bien sûr, ce cardinal est le nombre d'éléments dans l'ensemble A. Les entiers $1, 2, \ldots, n$ permettent de compter les éléments de A.*

Proposition 21 *- Si A est une partie d'un ensemble B fini, alors A est fini et $card(A) \leq card(B)$.*
- Si A et B sont deux ensembles finis et f est une application de A dans B, alors

$$f \text{ injective} \Rightarrow card(A) \leq card(B)$$

$$f \text{ surjective} \Rightarrow card(A) \geq card(B)$$

$$f \text{ bijective} \Rightarrow card(A) = card(B)$$

6.2 Calcul du cardinal de certains ensembles

Proposition 22 *Si A et B sont deux ensembles finis,*

1. *$A \cap B$ et $A \cup B$ sont finis et $card(A \cap B) + card(A \cup B) = card(A) + card(B)$.*
2. *$A \times B$ est fini et $card(A \times B) = card(A).card(B)$.*

Démonstration 18 *Il suffit de faire un dessin.*

□

Proposition 23 *(théorème des bergers)*
Si A et B sont deux ensembles, avec B fini, et f est une application de A dans B telle qu'il existe $p \in \mathbb{N}$ tel que $\forall y \in B, card(IRf(\{y\})) = p$, alors A est également fini et $card(A) = p.card(B)$.

6.3 Les cardinaux connus

Proposition 24 *Si E et F sont deux ensembles de cardinaux respectifs p et n,*

1. $card(\wp(E))) = 2^p$
2. $card(\mathcal{F}(E, F)) = n^p$
3. $card(\{f \in \mathcal{F}(E, F) | f \text{ injective}\}) = \begin{cases} 0 \text{ si } n < p \\ \frac{n!}{(n-p)!} \text{ sinon} \end{cases}$
4. $card(\{f \in \mathcal{F}(E, F) | f \text{ bijective}\}) = \begin{cases} 0 \text{ si } n \neq p \\ n! \text{ sinon} \end{cases}$
5. $card(\{F \subset E | card(F) = p\}) = C_n^p = \frac{n!}{p!(n-p)!}$