Bric-à-brac II

Olivier Sellès, transcrit par Denis Merigoux

Table des matières

1 Relations d'ordre

1.1 Relation d'ordre

1.1.1 Définition

Soit E un ensemble et $\mathcal{R}$ une relation binaire sur E [a]. Pour $x, y \in E$, on note $x\mathcal{R}y$ (lire :« x est en relation avec y ») au lieu de $(x, y) \in \mathcal{R}$. On dit que $\mathcal{R}$ est une relation d'ordre si :

(1) $\mathcal{R}$ est réflexive : $\forall x \in E,\ x\mathcal{R}x$

(2) $\mathcal{R}$ est antisymétrique : $\forall x, y \in E,\ (x\mathcal{R}y) \wedge (y\mathcal{R}x) \Rightarrow x = y$

(3) $\mathcal{R}$ est transitive : $\forall x, y, z \in E,\ (x\mathcal{R}y) \wedge (y\mathcal{R}z) \Rightarrow x\mathcal{R}z$

a. $\mathcal{R}$ est donc une partie de $E \times E$

Très souvent, si $\mathcal{R}$ est une relation d'ordre sur E, on notera $x \leqslant y$ au lieu de $x\mathcal{R}y$.

1.1.2 Exemples

- $\leqslant$ sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ est l'ordre naturel.
- Sur $E = \mathbb{N}^*$, on définit $\mathcal{R}$ par $\forall m \in \mathbb{N}^*,\ m\mathcal{R}n \Leftrightarrow m \mid n$. $\mathcal{R}$ est une relation d'ordre car :
  - $m \mid m$;
  - $(m \mid n) \wedge (n \mid m) \Rightarrow m = n$;
  - $(m \mid n) \wedge (n \mid p) \Rightarrow m \mid p$.
- Soit X un ensemble non vide et $E \in \mathcal{P}(X)$. Alors $\mathcal{R}$ défini par $A\mathcal{R}B \Leftrightarrow A \subset B$ sur E est une relation d'ordre sur E.
- Soit X un ensemble non vide et $E = \mathcal{F}(X, \mathbb{R})$ [a]. Pour $f, g \in E$ on pose $f \leqslant g \Leftrightarrow \forall x \in X, f(x) \leqslant g(x)$. Alors $\leqslant$ est une relation d'ordre dans $\mathcal{F}(X, \mathbb{R})$.

1.1.3 Vocabulaire

Un ensemble ordonné ou ordre est un couple $(E, \leqslant)$ avec E un ensemble et $\leqslant$ une relation d'ordre . L'ordre $(E, \leqslant)$ est dit total (on dit aussi que $\leqslant$ est une relation d'ordre totale) si :

$$\forall x, y \in E, (x \leqslant y) \vee (y \leqslant x)$$

On dit que x et y sont toujours comparables.

Soit $(E, \leqslant)$ un ordre. Pour $x, y \in E$, on note :
- $x < y$ pour $x \leqslant y$ et $x \neq y$;
- $x \geqslant y$ pour $y \leqslant x$;
- $x > y$ pour $y < x$.

Piège ! Il y a des ordres qui ne sont pas totaux :
- $(\mathbb{N}^*, |)$ car 2 et 3 ne sont pas comparables.
- Si X est non vide, $(\mathcal{P}(X), \subset)$ n'est pas total dès que X possède au moins deux éléments distincts a et b [b].
- Soit X un ensemble non vide. Alors $(\mathcal{F}(X, \mathbb{R}), \leqslant)$ n'est pas total dès que X possède deux éléments distincts a et b. En effet,

$$f : \begin{array}{l} a \longrightarrow 1 \\ b \longrightarrow 0 \\ x \notin \{a, b\} \rightarrow 0 \end{array} \quad \text{et} \quad g : \begin{array}{l} a \longrightarrow 0 \\ b \longrightarrow 1 \\ x \notin \{a, b\} \rightarrow 0 \end{array}$$

a. E est l'ensemble des fonctions de X dans $\mathbb{R}$.

b. En effet, $\{a\}$ et $\{b\}$ ne sont pas comparables par l'inclusion.

1.2 Majorant, minorant, maximum, minimum

1.2.1 Définitions

Soit $(E, \leqslant)$ un ordre, $A \subset E$ tel que $A \neq \varnothing$ et $x \in E$.

(1) On dit que :
- x majore A si $\forall a \in A,\ x \geqslant a$: x est un majorant de A.
- x minore A si $\forall a \in A,\ x \leqslant a$: x est un minorant de A.

(2) On note les propriétés suivantes :
- A est majorée si elle admet au moins un majorant.
- A est minorée si elle admet au moins un minorant.

(3) Soit $a \in A$. On dira que :
- a est un plus grand élément de A si $\forall a' \in A,\ a' \leqslant a$.
- a est un plus petit élément de A si $\forall a' \in A,\ a' \geqslant a$.

Remarque Il ne peut exister qu'un seul plus grand élément d'un ensemble qui en admet. En effet, si a_2 et a_1 sont deux plus grands éléments, alors $a_1 \leqslant a_2$ et $a_1 \geqslant a_2$ donc $a_1 = a_2$.

1.2.2 Maximum et minimum

On appelle a le maximum de A si a est le plus grand élément de A. On note alors $a = \max A$.
De même, un éventuel plus petit élément de A est unique et est le minimum de A. On le note $\min A$.

Remarques
- Si A possède un maximum, elle est majorée. La réciproque est cependant fausse : si $E = \mathbb{R}$ et $A = [0, 1[$ est majorée mais ne possède pas de maximum.
- Si $(E, \leqslant)$ est total, toute partie finie non vide de E possède un maximum et un minimum.

1.3 Borne supérieure, borne inférieure

1.3.1 Définitions

- Soit $(E, \leqslant)$ un ordre et $A \subset E$ majorée. L'ensemble B des majorants de A est non vide. Si B a un minimum, alors celui-ci s'appelle la borne supérieure de A et se note $\sup A$.
- Soit $(E, \leqslant)$ un ordre et $A \subset E$ minorée. L'ensemble B car si orants de A est non vide. Si B a un maximum, alors celui-ci s'appelle la borne inférieure de A et se note $\inf A$.
- Soit $x \in E$ et $A \in \mathcal{P}(E)$. A est majorée et admet une borne supérieure si et seulement si :
  - $\forall a \in A,\ a \leqslant x$ (x majore A)
  - $\forall y \in E,\ y$ majore $A \Rightarrow x \leqslant y$.

Piège ! Il peut exister des parties non vides, majorées mais sans borne supérieure. Prenons un exemple : soit $E = \mathbb{Q}$ muni de l'ordre naturel $\leqslant$.S$A = \left\{r \in \mathbb{Q}_+ | r^2 \leqslant 2\right\}$, A est une partie non vide de $\mathbb{Q}$. On a $1 \in A$ et A est majorée par 2 : si $x \in Q$ avec $x > 2$, $x^2 > 4$ donc $x \notin A$.

Supposons que A admet une borne supérieure dans $\mathbb{Q}$, et soit $x = \sup A$. Prouvons que $x^2 = 2$.
- Si $x^2 < 2$, soit $\varepsilon \in \mathbb{Q}_+^*$ et $d = 2 - x^2 > 0$. Alors,

$$\begin{aligned} 2 - (x + \varepsilon)^2 &= 2 - x^2 - 2\varepsilon x - \varepsilon^2 \\ &= d - 2\varepsilon x - \varepsilon^2 \\ &= d - \varepsilon(2x + \varepsilon) \end{aligned}$$

Prenons $\varepsilon \leqslant 1$. Alors $2x + \varepsilon \leqslant 2x + 1$ donc

$$2 - (x+\varepsilon)^2 \geqslant d - \varepsilon(2x+1)$$

On choisit de plus $\varepsilon \in \left]0, \dfrac{d}{2x+1}\right[$, par exemple $\varepsilon = \min\left(1, \dfrac{d}{2(2x+1)}\right)$. A ce moment là, on note que

$$\begin{aligned} 2 - (x+\varepsilon)^2 > 0 &\Rightarrow x + \varepsilon \in A \\ &\Rightarrow x + \varepsilon \leqslant \sup A \\ &\Rightarrow \varepsilon \leqslant 0 \end{aligned}$$

Ce qui est impossible [a].

– Si $x^2 > 2$. Soit $\varepsilon \in \mathbb{Q}_+^*$ tel que $\varepsilon < x$ et $d = x^2 - 2 > 0$. Alors

$$(x-\varepsilon)^2 = x^2 - 2x\varepsilon + \varepsilon^2 > d - 2\varepsilon x$$

Prenons de plus $\varepsilon \in \left]0, \dfrac{d}{2x}\right[$, par exemple $\varepsilon = \min\left(\dfrac{x}{2}, \dfrac{d}{4x}\right)$. Alors $(x-\varepsilon)^2 > 2$ donc $y \in A \Rightarrow y < x - \varepsilon$ donc $x - \varepsilon$ majore A. Ainsi,

$$\begin{aligned} \sup A \leqslant x - \varepsilon &\Rightarrow x \leqslant x - \varepsilon \\ &\Leftrightarrow \varepsilon \leqslant 0 \end{aligned}$$

Ce qui est impossible [b].

– On déduit des deux cas précédents que $x^2 = 2$, ce qui est impossible vu que $x \in \mathbb{Q}$. A n'admet donc pas de borne supérieure.

1.3.2 Théorème fondamental de $\mathbb{R}$ (admis)

Toute partie non vide majorée de $\mathbb{R}$ admet une borne supérieure.

Corollaire Toute partie non vide minorée de $\mathbb{R}$ admet une borne inférieure.

Démonstration Soit A une partie non vide minorée de $\mathbb{R}$ et B l'ensemble des minorants de A. Alors $B \neq \varnothing$ et $\forall (a,b) \in A \times B$, $b \leqslant a$ donc B est non vide et majorée. Soit $\beta = \sup B$. Montrons que β minore A.
Soit $a \in A$, alors a majore B. β est le plus petit majorant de B donc $\beta \leqslant a$ donc β est un minorant de A.
Si x est un minorant de A, $x \in B$ donc $x \leqslant \sup B$ donc β est bien le plus grand minorant de A.

1.4 Description des sous-groupes de $(\mathbb{R}, +)$

1.4.1 Définitions

– Soit $H \in \mathcal{P}(\mathbb{R})$. Alors H est un sous-groupe de $(\mathbb{R}, +)$ si :
  ∘ $0 \in H$
  ∘ $\forall (x,y) \in H$, $-x \in H$ et $y + x \in H$
– Soit $A \subset \mathbb{R}$, on dit que A est dense dans $\mathbb{R}$ si $\forall x \in \mathbb{R}, \forall \varepsilon > 0$, $\exists a \in A / |a - x| < \varepsilon \Leftrightarrow a \in [x-\varepsilon, x+\varepsilon]$. On peut approcher x à ε près par un élément de A.

1.4.2 Propriété particulière

H est un sous-groupe de $\mathbb{R}$ si l'une ou l'autre des conditions suivantes est vérifiée :
– $\exists a \in \mathbb{R} / H = a\mathbb{Z}$;
– H est dense dans $\mathbb{R}$.

Les deux conditions s'excluant mutuellement.

a. Aaaaaaargh !
b. Aaaaaaargh !

Démonstration Soit H un sous-groupe de $(\mathbb{R},+)$.

- Si $H=\{0\}$, alors $H=0\mathbb{Z}$.
- Supposons que $H\neq\{0\}$. Il existe donc $h\in H/h\neq 0$ donc $-h\in H$. On a donc $H_+^*=H\cap\mathbb{R}_+^*\neq\varnothing$, qui est minoré (par 0 par exemple). Soit maintenant $a=\inf H_+^*$, donc $a\geqslant 0$ [a].

  1er cas : $a>0$

  ◦ Montrons que $a\in H$. Supposons pour cela que $a\notin H$. $2a>a$ donc $2a$ ne peut pas minorer H_+^*. Toujours car a est le plus grand minorant de H_+^* on sait que $\exists y\in H_+^*/y<2a$ et $a\leqslant y$, et même $a<y$ car on suppose que $a\notin H$. $a<y$ donc y ne minore pas non plus H_+^* donc $\exists x\in H_+^*/x<y$. On a donc
  $$a<x<y<2a$$
  Ainsi, $y-x\in\,]0,a[$. Or $y-x\in H$ car H est un sous-groupe donc $y-x\in H_+^*$ et $y-x<a=\inf H_+^*$, ce qui est impossible [b].

  ◦ Ainsi, $a\in H$ et H est un sous-groupe de $\mathbb{R}$ donc $a\mathbb{Z}\subset H$. Démontrons l'inclusion inverse. Soit $h\in H$, $n=\mathrm{E}\left(\dfrac{h}{a}\right)$ donc
  $$na\leqslant h<(n+1)\,a$$
  donc $h-na\in[0,a[$. Or $h-na\in H$:
  → Si $h-na\neq 0$ alors $h-na\in H_+^*$ et $h-na<a=\inf H_+^*$, ce qui est impossible [c].
  → Ainsi $h-na=0$ donc $h=na\in a\mathbb{Z}$.

  2ème cas : $a=0$ Montrons que H est dense dans $\mathbb{R}$.
  Soit $x\in\mathbb{R}$ et $\varepsilon>0$. $\varepsilon>\inf H_+^*$ donc ε n'est pas un minorant de H_+^*, donc $\exists h\in H_+^*/h<\varepsilon$. Soit maintenant $n=\mathrm{E}\left(\dfrac{x}{h}\right)$, donc
  $$nh\leqslant x<(n+1)\,h\Leftrightarrow 0\leqslant x-nh<h$$
  donc $|x-nh|<h<\varepsilon$ et $nh\in\mathbb{Z}h\subset H$ puisque $h\in H$. Ainsi, H est dense dans $\mathbb{R}$.

1.4.3 Corollaires

Corollaire n°1 Montrons que $\mathbb{Q}$ est dense dans $\mathbb{R}$.

$\mathbb{Q}$ est un sous-groupe de $(\mathbb{R},+)$ donc soit il est de la forme $a\mathbb{Z}$ avec $a\in\mathbb{R}_+^*$, soit il est dense dans $\mathbb{R}$.

Supposons qu'il existe $a>0/\mathbb{Q}=a\mathbb{Z}$. Alors $1\in\mathbb{Q}=a\mathbb{Z}$ donc $\exists m\in\mathbb{N}$ tels que $1=ma\Leftrightarrow a=\dfrac{1}{m}$. Or $\dfrac{1}{2m}\in\mathbb{Q}$ mais $\dfrac{1}{2m}\notin\dfrac{1}{m}\mathbb{Z}$ car $\dfrac{1}{2}\notin\mathbb{Z}$ donc $\mathbb{Q}$ n'est pas de la forme $a\mathbb{Z}$ donc $\mathbb{Q}$ est dense dans $\mathbb{R}$.

Corollaire n°2 $\mathbb{R}\backslash\mathbb{Q}$ est aussi dense dans $\mathbb{R}$.

Soient $a,b\in\mathbb{R}$ avec $a<b$. Montrons que $]a,b[\cap(\mathbb{R}\backslash\mathbb{Q})\neq\varnothing$. Or $\mathbb{Q}$ est dense dans $\mathbb{R}$ donc $\left]\dfrac{a}{\sqrt{2}},\dfrac{b}{\sqrt{2}}\right[\cap\mathbb{Q}\neq\varnothing$. Montrons que cet ensemble est infini.

Pour cela supposons que $\left]\dfrac{a}{\sqrt{2}},\dfrac{b}{\sqrt{2}}\right[\cap\mathbb{Q}$ est fini donc on peut le noter $\{r_1,r_2,\ldots,r_n\}$ avec
$$\frac{a}{\sqrt{2}}<r_1<\cdots<r_n<\frac{b}{\sqrt{2}}$$
Or on sait que $\left]\dfrac{a}{\sqrt{2}},r_1\right[\cap\mathbb{Q}\neq\varnothing$ car $\mathbb{Q}$ est dense dans $\mathbb{R}$ donc on peut trouver $r_0\in\left]\dfrac{a}{\sqrt{2}},r_1\right[\cap\mathbb{Q}\subset\left]\dfrac{a}{\sqrt{2}},\dfrac{b}{\sqrt{2}}\right[\cap\mathbb{Q}$, ce qui est impossible [d]. Ainsi, on peut trouver un $r\in\mathbb{Q}^*$ tel que
$$\frac{a}{\sqrt{2}}<r<\frac{b}{\sqrt{2}}\Leftrightarrow a<\sqrt{2}r<b$$

a. **Piège !**
Si A est non vide et minorée, on a pas forcément $\inf A\in A$. Par exemple $A=\,]0,1]$, $\inf A=0\notin A$.
b. Aaaaaaargh !
c. Aaaaaaargh !
d. Aaaaaaargh !

De plus, $r\sqrt{2} \in \mathbb{R}\backslash\mathbb{Q}$ [a] donc $\mathbb{R}\backslash\mathbb{Q}$ est dense dans $\mathbb{R}$.

Corollaire n°3 On admet que $\pi \notin \mathbb{Q}$. Alors $\mathbb{Z} + 2\pi\mathbb{Z} = \{p + 2\pi q | p, q \in \mathbb{Z}\}$ est dense dans $\mathbb{R}$.

Montrons que $\mathbb{Z} + 2\pi\mathbb{Z}$ est un sous-groupe de $(\mathbb{R}, +)$. En effet :

- $0 = 0 + 2\pi 0 \in \mathbb{Z} + 2\pi\mathbb{Z}$
- $\forall m, n \in \mathbb{Z}$, $-m - 2\pi n = (-m) + 2\pi(-n) \in \mathbb{Z} + 2\pi\mathbb{Z}$
- $\forall m, n, p, q \in \mathbb{Z}$, $m + 2\pi n + p + 2\pi q = (m + n) + 2\pi(p + q) \in \mathbb{Z} + 2\pi\mathbb{Z}$

Ainsi, $\mathbb{Z} + 2\pi\mathbb{Z}$ est un sous-groupe de $(\mathbb{R}, +)$. Montrons qu'il n'est pas de la forme $a\mathbb{Z}$, $a \in \mathbb{R}$.

Supposons qu'il existe $a > 0/\mathbb{Z}+2\pi\mathbb{Z} = a\mathbb{Z}$. On a $1 = 1+2\pi 0 \in \mathbb{Z}+2\pi\mathbb{Z} = a\mathbb{Z}$ donc $\exists m \in \mathbb{Z}/1 = ma \Leftrightarrow a = \dfrac{1}{m}$.

Or $2\pi = 0 + 2\pi 1 \in \mathbb{Z} + 2\pi\mathbb{Z} = a\mathbb{Z}$ donc $\exists n \in \mathbb{Z}/2\pi = na \Leftrightarrow 2\pi = \dfrac{n}{m} \Leftrightarrow \pi = \dfrac{n}{2m} \in \mathbb{Q}$, ce qui est impossible [b].

Donc $\mathbb{Z} + 2\pi\mathbb{Z}$ est dense dans $\mathbb{R}$.

Corollaire n°4 $\cos\mathbb{N}$ est dense dans $[-1, 1]$, c'est-à-dire $\forall x \in [-1, 1], \forall \varepsilon > 0, \exists n \in \mathbb{N}/x - \cos n < \varepsilon$.

Soit $x \in [-1, 1]$ et $\varepsilon > 0$, on pose $\theta = \arccos x \in [0, \pi]$. $\mathbb{Z} + 2\pi\mathbb{Z}$ est dense dans $\mathbb{R}$ donc

$$\exists p, q \in \mathbb{Z}/\,|\theta - (p + 2\pi q)| < \varepsilon$$

On note que $\cos|p| = \cos p = \cos(p + 2\pi q)$. De plus [c] pour $u, v \in \mathbb{R}$,

$$|\cos u - \cos v| \leqslant |u - v| \quad \text{et} \quad |\sin u - \sin v| \leqslant |u - v|$$

Ainsi,

$$\begin{aligned} |\cos\theta - \cos|p|| &= |\cos\theta - \cos(p + 2\pi q)| \\ &\leqslant |\theta - p - 2\pi q| \\ &< \varepsilon \end{aligned}$$

Donc $\cos\mathbb{N}$ est dense dans $[-1, 1]$.

2 est génératricealence

2.1 Généralités

2.1.1 Définition

Soit E un ensemble, $\mathcal{R}$ une relation binaire sur E. On dit que R est une relation d'équivalence si :

(1) $\mathcal{R}$ est réflexive : $\forall x \in E$, xRx

(2) $\mathcal{R}$ est symétrique : $\forall x, y \in E$, $xRy \Rightarrow y\mathcal{R}x$

(3) R est transitive : $\forall x, y, z \in E$, $((x\mathcal{R}y) \wedge (yRz)) \Rightarrow x\mathcal{R}z$

2.1.2 Exemple principal

$E = \mathbb{Z}$, soit $n \in \mathbb{N}^*$. On note $\mathcal{R}_n$ la relation binaire définie sur $\mathbb{Z}$ par $\forall a, b \in \mathbb{Z}$,

$$a\mathcal{R}_n b \Leftrightarrow n \mid b - a$$

a. En effet, si $r\sqrt{2} \in \mathbb{Q}$, alors $\sqrt{2} = \dfrac{r\sqrt{2}}{r} \in \mathbb{Q}$: Aaaaaaargh !

b. Aaaaaaargh !

c. En effet, soient $u, v \in \mathbb{R}$ avec $u \leqslant v$ par exemple. Alors

$$\begin{aligned} \left|e^{iv} - e^{iu}\right| &= \left|\int_u^v ie^{it}\,dt\right| \\ &< \int_u^v \left|ie^{it}\right| dt \\ &< |v - u| \end{aligned}$$

En prenant les parties réelles et imaginaires on obtient le résultat escompté.

Remarques $\forall x, y, a, b \in \mathbb{Z}$:
- $1 \mid x$, $x \mid 0$ et $x \mid x$.
- $x \mid y$ (dans $\mathbb{Z}$) revient à dire $|x| \mid |y|$ (dans $\mathbb{N}$).
- Si $(x, y) \neq (0, 0)$, $x \mid y \Rightarrow |x| < |y|$.
- Si $x \mid y$ et $y \mid z$ alors $x \mid z$
- Si $x \mid a$ et $x \mid b$ alors $x \mid au + bv$

Montrons que $\mathcal{R}_n$ est une relation d'équivalence sur $\mathbb{Z}$:

(1) Si $a \in \mathbb{Z}$, $n \mid 0 = a - a$ donc $a\mathcal{R}_n a$

(2) Soient $a, b \in \mathbb{Z}$ tels que $a\mathcal{R}_n b$. Alors $n \mid b - a$ donc $\exists m \in \mathbb{Z}$ tel que $b - a = mn$ donc $a - b = -mn$ donc $n \mid a - b$, d'où le résultat.

(3) Soient $a, b, c \in \mathbb{Z}$ tels que $a\mathcal{R}_n b$ et $b\mathcal{R}_n c$. Alors

$$n \mid b - a \quad \text{et} \quad n \mid c - b \Rightarrow n \mid b - a + c - b = c - a$$

donc $a\mathcal{R}_n c$.

2.2 Propriétés des relations d'équivalence

2.2.1 Propriétés générales

Soit $\mathcal{R}$ une relation d'équivalence sur E (non-vide).
- Pour $x \in E$, on note $\mathrm{cl}_{\mathcal{R}}(x)$ l'ensemble des éléments y en relation avec x, c'est-à-dire $\mathrm{cl}_{\mathcal{R}}(x) = \{y \in E | x\mathcal{R}y\}$.
- Soit $C \in \mathcal{P}(E)$, C est une classe d'équivalence s'il existe $x \in E$ tel que $C = \mathrm{cl}_{\mathcal{R}}(x)$.
- Si $x \in E$, $\mathrm{cl}_{\mathcal{R}}(x) \neq \varnothing$ car $x \in \mathrm{cl}_{\mathcal{R}}(x)$. Aucune classe d'équivalence n'est vide.
- Soient C, D deux classes d'équivalence et supposons que $C \cap D \neq \varnothing$. Soient $x, y \in E$ tels que $C = \mathrm{cl}_{\mathcal{R}}(x)$ et $D = \mathrm{cl}_{\mathcal{R}}(y)$ et $a \in C \cap D$. On a $x\mathcal{R}a$ et $y\mathcal{R}a$ donc $a\mathcal{R}y$ donc $x\mathcal{R}y$ donc $y \in \mathrm{cl}_{\mathcal{R}}(x)$. Si $z \in D$, $y\mathcal{R}z$ et on sait que $x\mathcal{R}y$ donc $x\mathcal{R}z$ donc $z \in C$. Ainsi $D \subset C$ et par symétrie $C \subset D$ donc $D = C$.

On déduit de la remarque précédente que

$$C \cap D \neq 0 \Rightarrow C = D$$

Par contraposée,

$$C \neq D \Rightarrow C \cap D = \varnothing$$

- $x \in \mathrm{cl}_{\mathcal{R}}(x)$ si $x \in E$ donc x appartient toujours à une classe d'équivalence. On note ${}^{E}/_{\mathcal{R}}$ l'ensemble des classes d'équivalence. Alors ${}^{E}/_{\mathcal{R}}$ est une partie de $\mathcal{P}(E)$.

Soit Ω une partie de $\mathcal{P}(E)$. Ω est une partition de E si :

(1) $\forall A \in \Omega$, $A \neq \varnothing$

(2) $\forall A, B \in \Omega$, $A \neq B \Rightarrow A \cap B = \varnothing$

(3) $\bigcup_{A \in \Omega} A = E$

2.2.2 Retour à l'exemple

$E = \mathbb{Z}$, $n \in \mathbb{N}^*$. L'ensemble ${}^{E}/_{\mathcal{R}_n}$ des classes d'équivalences pour $\mathcal{R}_n$ se note ${}^{\mathbb{Z}}/_{n\mathbb{Z}}$. Pour $x \in \mathbb{Z}$, on note $\overline{x} = \mathrm{cl}_{\mathcal{R}_n}(x)$.

Pour $y \in \mathbb{Z}$,

$$\begin{aligned} y \in \overline{x} &\Leftrightarrow y \equiv x \ [n] \\ &\Leftrightarrow n \mid y - x \\ &\Leftrightarrow \exists k \in \mathbb{Z} / y = x + nk \\ &\Leftrightarrow y \in x + n\mathbb{Z} \end{aligned}$$

Ainsi, $\overline{x} = x + n\mathbb{Z} = \{x + kn | k \in \mathbb{Z}\}$.

Montrons que $\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}$

$\Rightarrow$ Il est clair que $\left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\} \subset \mathbb{Z}/n\mathbb{Z}$.

$\Leftarrow$ Soit $C \in \mathbb{Z}/n\mathbb{Z}$, alors $\exists x \in \mathbb{Z}/C = \overline{x}$. On écrit ensuite [a] $x = nq + r$ avec $q \in \mathbb{Z}$ et $r \in [[0, n-1]]$. Ainsi $x - r = nq$ donc $n \mid x - r$ donc $r \in \overline{x}$. Or $r \in \overline{r}$ donc $r \in \overline{x} \cap \overline{r} \neq \varnothing$ donc $\overline{x} = \overline{r}$ donc $\overline{x} \in \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}$.

De plus, les classes $\overline{0}$, $\overline{1}$, ..., $\overline{n-1}$ sont deux à deux distinctes. En effet, soit $0 \leqslant k < l \leqslant n-1$ avec $\overline{k} = \overline{l}$. Alors $l \in \overline{l} = \overline{k}$ donc $k \equiv l \ [n]$ et $n \mid l - k$, ce qui est impossible [b] car $1 \leqslant l - k \leqslant n - 1$.

$\mathbb{Z}/n\mathbb{Z}$ est donc un ensemble fini et de cardinal n. Pour $n = 2$, les classes $\overline{0}$ et $\overline{1}$ désignent les nombres pairs et impairs et forment bien une partition de $\mathbb{Z}$.

2.3 Lois sur $\mathbb{Z}/n\mathbb{Z}$

2.3.1 Opérations dans $\mathbb{Z}/n\mathbb{Z}$

La congruence modulo n est compatible avec les opérations sur $\mathbb{Z}$:

$$a \equiv a' \ [n] \quad \text{et} \quad b \equiv b' \ [n] \Rightarrow a + b \equiv a' + b' \ [n] \quad \text{et} \quad ab \equiv a'b' \ [n]$$

Démonstration

- Montrons que $n \mid (a' + b') - (a + b)$. On sait que $n \mid a' - a$ et $n \mid b' - b$ donc $n \mid a' + b' - a - b$.
- Montrons que $n \mid a'b' - ab$. On a :

$$\begin{aligned} a'b' - ab &= a'b' + a'b - a'b - ab \\ &= \left(a' - a\right) b + a' \left(b' - b\right) \end{aligned}$$

Or $n \mid a' - a$ et $n \mid b' - b$ d'où le résultat.

Remarque $a \equiv a' \ [n] \Rightarrow \forall k \in \mathbb{N}, \ a^k \equiv a'^k \ [n]$

2.3.2 Lois de compositions internes de $\mathbb{Z}/n\mathbb{Z}$

Définitions longu $A, B \in \mathbb{Z}/n\mathbb{Z}$. Si $a, a' \in A$ et $b, b' \in B$, alors $a \equiv a' \ [n]$ et $b \equiv b' \ [n]$. Donc $a + b \equiv a' + b' \ [n]$ et $ab \equiv a'b' \ [n]$.

Ainsi, $\overline{a + b} = \overline{a' + b'}$ et $\overline{ab} = \overline{a'b'}$. Il est donc cohérent de poser $\forall a \in A$ et $\forall b \in B$:

- $A \dot{+} B = \overline{a + b}$
- $A \dot{\times} B = \overline{ab}$

On définit ainsi deux lois de composition interne sur $\mathbb{Z}/n\mathbb{Z}$. Ainsi, par définition, $\forall x, y \in \mathbb{Z}$:
- $\overline{x} \dot{+} \overline{y} = \overline{x + y}$
- $\overline{x} \dot{\times} \overline{y} = \overline{xy}$

Propriétés Prenons un exemple pour $n = 4$, alors $\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \overline{1}, \overline{2}, \overline{3}\right\}$. On a donc

$\dot{+}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\dot{\times}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

On voit que :

a. En effectuant la division euclidienne de x par n dans $\mathbb{Z}$.

b. Aaaaaaargh !

– $\dot{+}$ est commutative, associative, admet un neutre ($\overline{0}$).
– $\dot{\times}$ est commutative, associative, admet un neutre ($\overline{1}$) et est distributive par rapport à $\dot{+}$.
Ainsi, $\left(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times}\right)$ est un anneau commutatif [a].

Quels sont les éléments inversibles par $\dot{\times}$? Soit $k \in [\![0, n-1]\!]$. Alors :

$$\begin{aligned} k \text{ est inversible par } \dot{\times} &\Leftrightarrow \exists C \in \mathbb{Z}/n\mathbb{Z} / \overline{k} \dot{\times} C = \overline{1} \\ &\Leftrightarrow \exists l \in \mathbb{Z} / \overline{k} \dot{\times} \overline{l} = \overline{1} \\ &\Leftrightarrow \exists l \in \mathbb{Z} / \overline{kl-1} = \overline{0} \\ &\Leftrightarrow \exists l \in \mathbb{Z} / n \mid kl - 1 \\ &\Leftrightarrow \exists l, m \in \mathbb{Z} / kl - 1 = mn \\ &\Leftrightarrow \exists l, m \in \mathbb{Z} / kl - mn = 1 \\ &\Leftrightarrow k \wedge n = 1 \end{aligned}$$

La dernière équivalence est obtenue grâce à la relation de Bézout [b]. Notons $\mathcal{U}$ l'ensemble des inversibles de $\mathbb{Z}/n\mathbb{Z}$ par $\dot{\times}$. Alors $\mathcal{U} = \left\{\overline{k} | k \in [\![0, n-1]\!], k \wedge n = 1\right\}$.

On remarque que $\overline{1} \in \mathcal{U}$. Si $a, b \in \mathcal{U}$, alors $a^{-1} \in \mathcal{U}$ (car a est bien inversible) et $a \dot{\times} b \in \mathcal{U}$ (pour la même raison appliquée à $a \dot{\times} b$).

Démonstration du théorème de Fermat On remarque que si $x, y \in \mathbb{Z}$, alors $x \equiv y \ [n] \Leftrightarrow y \in \overline{x} \Leftrightarrow \overline{y} = \overline{x}$.

Soit $n \in \mathbb{N}^*$,$a \in \mathbb{Z}$ tel que $a \wedge n = 1$ et $g = \overline{a} \in G = \mathcal{U}\left(\mathbb{Z}/n\mathbb{Z}\right)$ [c]. Soit

$$\begin{aligned} \sigma : \ G &\longrightarrow G \\ z &\longmapsto g \dot{\times} z \end{aligned}$$

Alors σ est bien définie car G est stable par $\dot{\times}$. Notons g^{-1} l'inverse de g par $\dot{\times}$ et soit

$$\begin{aligned} \tau : \ G &\longrightarrow G \\ z &\longmapsto g^{-1} \dot{\times} z \end{aligned}$$

Pour $z \in G$,

$$\begin{aligned} \sigma \circ \tau &= g \dot{\times} \left(g^{-1} \dot{\times} z\right) \\ &= \overline{1} \dot{\times} z \\ &= z \end{aligned}$$

De plus,

$$\begin{aligned} \tau \circ \sigma &= g^{-1} \dot{\times} \left(g \dot{\times} z\right) \\ &= z \end{aligned}$$

Donc σ et τ sont deux bijections réciproques l'une de l'autre. Notons $G = \{z_1, z_2, \ldots, z_N\}$ et $N = \varphi(n)$. On a aussi puisque σ est bijective, $G = \left\{g \dot{\times} z_1, g \dot{\times} z_2, \ldots, g \dot{\times} z_N\right\}$.

a. Il est clair que pour $x \in [\![0, n-1]\!]$, $\overline{n-x}$ est l'opposé de $\overline{x}$ par rapport à $+$.
b. Définissons la fonction indicatrice d'Euler.
Pour $n \in \mathbb{N}^*$, $\varphi(n) = \text{Card}\left\{k \in [\![0, n-1]\!] | k \wedge n = 1\right\}$. On a alors $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$,...
Si p est un nombre premier alors $\varphi(p) = p - 1$.
c. Ensemble des éléments de $\mathbb{Z}/n\mathbb{Z}$ inversibles par $\dot{\times}$.

Soit $P = \prod_{k=1}^{N} z_k \in G$. $\dot{\times}$ est commutative donc

$$\begin{aligned} P &= \prod_{k=1}^{N} g \dot{\times} z \\ &= \prod_{k=1}^{N} g \dot{\times} \prod_{k=1}^{N} z_k \\ &= \prod_{k=1}^{N} g \dot{\times} P \\ &= g^N \dot{\times} P \end{aligned}$$

D'où :

$$\begin{aligned} \overline{1} &= P^{-1} \dot{\times} P \\ &= g^N \dot{\times} P \dot{\times} P^{-1} \\ &= g^N \\ &= \overline{a}^N \\ &= \overline{a^N} \end{aligned}$$

Donc $a^N \equiv 1\ [n]$. Si $a \wedge n = 1$, alors $a^{\varphi(n)} \equiv 1\ [n]$. En particulier, si p est un nombre premier alors, pour tout $a \in \mathbb{Z}$ tel que p ne divise pas a [a], $a^{p-1} \equiv 1\ [p]$. D'où $a^p \equiv 0\ [p]$, relation valable même si $p \mid a$.

3 Entiers naturels

3.1 Construction de $\mathbb{N}$ grâce aux axiomes de Péano

3.1.1 Axiomes de Péano

Il existe un ensemble non vide noté $\mathbb{N}$, muni d'une relation d'ordre totale $\leqslant$ vérifiant :

(1) Toute partie non vide de $\mathbb{N}$ admet un plus petit élément (ou minimum).

(2) Toute partie non vide majorée de $\mathbb{N}$ admet un maximum.

(3) $\mathbb{N}$ n'est pas majoré.

On notera 0 le plus petit élément de $\mathbb{N}$ et $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$. $\mathbb{N}^*$ n'est pas vide car sinon $\mathbb{N}$ serait majorée par 0.

3.1.2 Successeur, prédécesseur

- Soit $m \in \mathbb{N}$. $\mathbb{N}$ n'étant pas majorée, alors $A = \{x \in \mathbb{N} | x > m\} \neq \varnothing$. On note $s = \min A$ le successeur de m. On a donc $m < s(m)$ et $\forall n \in \mathbb{N}$, $n > m \Rightarrow n \geqslant s(m)$.
- Soit $m \in \mathbb{N}^*$. Alors $B = \{x \in \mathbb{N} | x < m\} \neq \varnothing$ et admet un maximum. On note $p = \max A$ le prédécesseur de m. On a donc $m > p(m)$ et $\forall n \in \mathbb{N}$, $n < m \Rightarrow n \leqslant p(m)$.

On note $1 = s(0)$, $2 = s(1)$,..., $9 = s(8)$.

Remarque

- Pour $m \in \mathbb{N}$, $s(m) \in \mathbb{N}^*$ et $p(s(m)) = m$.
  En effet, $m < s(m)$ donc $m \leqslant p(s(m))$. Si $m < p(s(m))$, alors $p(s(m)) \geqslant s(m)$, ce qui n'est pas possible [b].

a. C'est à dire $a \not\equiv 0\ [p]$

b. Aaaaaaargh !

– De même, pour $n \in \mathbb{N}^*$, $p(m) \in \mathbb{N}$ et $s(p(m)) = m$.

Ainsi $s : \mathbb{N} \longrightarrow \mathbb{N}^*$ et $p : \mathbb{N}^* \longrightarrow \mathbb{N}$ donc $p \circ s = \mathrm{Id}_{\mathbb{N}}$ et $s \circ p = \mathrm{Id}_{\mathbb{N}^*}$. p et s sont des bijections réciproques l'une de l'autre.

3.1.3 Principe de récurrence

Soit P un prédicat sur $\mathbb{N}$. On suppose que :
– $P(0)$ est vrai.
– $\forall n \in \mathbb{N}$, $P(n)$ vrai $\Rightarrow P(s(n))$ vrai.
Alors, $\forall n \in \mathbb{N}$, $P(n)$ est vraie.

Démonstration Supposons que $A = \{n \in \mathbb{N} | P(n) \text{ est faux}\} \neq \varnothing$. Alors on peut considérer $a = \min A$. Or $0 \notin A$ donc $0 < a$ et $p(a) < a$ donc $p(a) \notin A$ donc $P(p(a))$ est vrai donc $P(s(p(a))) = P(a)$ est vrai, ce qui est impossible [a].

3.1.4 Opérations

Addition

On définit une addition + par récurrence en posant :
(1) $\forall n \in \mathbb{N}$, $n + 0 = n$
(2) $\forall n, m \in \mathbb{N}$, $n + s(m) = s(m + n)$

Ainsi,

$$\begin{aligned} 2 + 1 &= 2 + s(0) \\ &= s(0 + 2) \\ &= s(2) \\ &= 3 \end{aligned}$$

On vérifie que + est :
– commutative, associative, admet 0 comme neutre.
– $\forall n \in \mathbb{N}$, $s(n) = n + 1$.
– + est compatible avec l'ordre : $\forall a, b \in \mathbb{N}$, $a \leqslant b \Rightarrow a + c \leqslant b + c$.

Pour tous entiers naturels a et b, si $a \leqslant b$ alors il existe un unique entier naturel c tel que $a + c = b$. c se note $b - a$. On vérifie alors que $\forall n \in \mathbb{N}$, $p(n) = n - 1$.

Multiplication

On définit une multiplication $\times$ par récurrence en posant :
(1) $\forall n \in \mathbb{N}$, $n \times 0 = 0$.
(2) $\forall n, m \in \mathbb{N}$, $n \times s(m) = n \times m + n$.

On a $\forall \in \mathbb{N}$, $n \times 1 = n \times s(0) = n \times 0 + n = n$. On vérifie que :
– $\times$ est commutative, associative, admet 1 comme neutre.
– $\times$ est compatible avec l'ordre : $\forall a, b, c \in \mathbb{N}$, $a \leqslant b \Rightarrow a \times c \leqslant b \times c$.

3.1.5 Reformulation du principe de récurrence

Récurrence simple Soit P un prédicat sur $\mathbb{N}$. On suppose que :
(1) $P(0)$ est vrai.
(2) $\forall n \in \mathbb{N}$, $(P(n) \Rightarrow P(n + 1))$.
Alors, $\forall n \in \mathbb{N}$, $P(n)$ est vrai.

a. Aaaaaaargh !

Récurrence simple à partir de l'entier n_0 Soit [a] P un prédicat sur $\mathbb{N}$, $n_0 \in \mathbb{N}$. On suppose que :

(1) $P(n_0)$ est vrai.

(2) $\forall n \in \mathbb{N}$, $(P(n) \Rightarrow P(n+1))$.

Alors, $\forall n \geqslant n_0$, $P(n)$ est vrai.

La démonstration se fait en appliquant une récurrence simple à $Q(n) = P(n+n_0)$.

Récurrence double Soit P un prédicat sur $\mathbb{N}$. On suppose que :

(1) $P(0)$ et $P(1)$ est vrai.

(2) $\forall n \in \mathbb{N}$, $(P(n)$ et $P(n+1) \Rightarrow P(n+2))$.

Alors, $\forall n \in \mathbb{N}$, $P(n)$ est vrai.

La démonstration se fait en appliquant une récurrence simple à $Q(n) = P(n)$ et $P(n+1)$.

Récurrence forte Soit P un prédicat sur $\mathbb{N}$. On suppose que :

(1) $P(0)$ est vrai.

(2) $\forall n \in \mathbb{N}$, $(\forall k \in [\![0,n]\!], P(k) \Rightarrow P(n+1))$.

Alors, $\forall n \in \mathbb{N}$, $P(n)$ est vrai.

La démonstration se fait en appliquant une récurrence simple à $Q(n) = \forall k \in [\![0,n]\!], P(k)$.

Exemple Tout entier relatif $n \geqslant 2$ s'écrit comme un produit de nombres premiers [b].

Soit H_n : « n est le produit de nombres premiers ».

- H_2 est vrai car 2 est premier.
- Soit $n \in \mathbb{N}$, $n \geqslant 2$. Supposons que $\forall k \in [\![2,n]\!]$, H_k est vrai et prouvons que H_{n+1} est vrai.
  - Si $n+1$ est premier, alors H_{n+1} est vrai.
  - Si $n+1$ n'est pas premier, $n+1$ possède un diviseur non-trivial $u \in [\![2,n]\!]$ donc $n+1 = uv$ avec $v \in [\![2,n]\!]$. Or H_u et H_v sont vrais donc u et v s'écrivent comme un produit de nombres premiers donc $n+1$ aussi donc H_{n+1} est vrai.

3.2 Division euclidienne

3.2.1 Généralités

Soit $a \in \mathbb{N}$, $b \in \mathbb{N}^*$. Alors il existe un unique couple $(q,r) \in \mathbb{N}^2$ appelé division euclidienne de a par b tel que :

(1) $a = bq + r$

(2) $r < b$

Démonstration Soit $A = \{k \in \mathbb{N} | kb \leqslant a\}$.

- Supposons que (q,r) existe et vérifie 1. et 2. Alors $a = bq + r \geqslant bq$ donc $q \in A$. Si $l > q$, alors $bl \geqslant b(q+1) = bq + b \geqslant bq + r = a$ donc $l \notin A$. Ainsi, pour $l \in \mathbb{N}$, $l \in A \Rightarrow l < q$ donc nécessairement $q = \max A$ donc $r = a - bq$.
- A est non vide car $0 \in A$. A est majorée par a [c] donc on peut considérer $q = \max A$ donc $bq \leqslant a$. Soit $r = a - bq$ donc $a = bq + r$ et $r < b$ [d].

a. Résultat aussi appelée théorème de Nigel, ou théorème d'Aménofis.

b. On rappelle que :
- $p \in \mathbb{N}$ est premier si $p \geqslant 2$ et si les deux seuls diviseurs de p dans $\mathbb{N}$ sont 1 et p.
- $b \mid a$ dans $\mathbb{N}$ signifie qu'il existe un entier naturel c tel que $a = bc$.
- $\forall a \in \mathbb{N}$, $a \mid a$, $1 \mid a$ et $a \mid 0$.
- $\forall a, b \in \mathbb{N}$, $b \mid a \Rightarrow b \in [\![1,a]\!]$

c. En effet si $k \geqslant a+1$ alors $kb \geqslant ab + b \geqslant a$ or $b \geqslant 1$ donc $k \notin A$ donc $k \in A \Rightarrow k < a+1$ donc a majore A.

d. En effet si $r \geqslant b$, $r = b + l$ avec $l \in \mathbb{N}$ d'où $a = b(q+1) + l$ donc $b(q+1) \leqslant a$ donc $q+1 \in A$, ce qui n'est pas possible car q est le maximum de A. Aaaaaargh !

Vocabulaire

- Si (q, r) est la division euclidienne de a par b dans $\mathbb{N}$:
  - q est le quotient de la division euclidienne de a par b.
  - r est le reste de la division euclidienne de a par b.
- $b \mid a \Leftrightarrow r = 0$. En effet :

  $\Leftarrow$ Évident [a] !

  $\Rightarrow$ Si $b \mid a$, $a = bc = bc + 0$ et $0 < b$ donc $(c, 0)$ est la division euclidienne de a par b et $r = 0$.

3.2.2 Applications

Division euclidienne dans $\mathbb{Z}$

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. Alors il existe un unique couple d'entiers naturels (q, r) tel que :
(1) $a = bq + r$
(2) $0 \leqslant r < |b|$

Démonstration

Unicité Soient (q_1, r_1) et (q_2, r_2) dans $\mathbb{Z}^2$ deux couples vérifiant les deux conditions énoncées ci-dessus. Alors,

$$\begin{aligned} bq_1 + r_1 = bq_2 + r_2 &\Leftrightarrow r_1 - r_2 = b(q_2 - q_1) \\ &\Leftrightarrow |r_1 - r_2| = |b|\,|q_2 - q_1| \end{aligned}$$

Donc $|r_2 - r_1| \in [\![0, |b| - 1]\!]$. Si $q_1 \neq q_2$, alors $|b|\,|q_1 - q_2| > |b|$, ce qui est impossible [b]. Donc $q_1 = q_2$ puis $r_1 = r_2$.

Existence Soit (q', r') la division euclidienne de $|a|$ par $|b|$ dans $\mathbb{N}$. Alors $|a| = q'|b| + r'$ avec $r' \in [\![0, |b| - 1]\!]$. On écrit $|a| = \alpha a$ où $\alpha \in \{\pm 1\}$ et $|b| = \beta b$ où $\beta \in \{\pm 1\}$, donc

$$\alpha a = q'\beta b + r' \Leftrightarrow a = \alpha\beta b q' + \alpha r' \quad \text{car } \alpha^2 = 1$$

- Si $\alpha = 1$, $q = \beta q'$ et $r = r'$.
- Si $\alpha = -1$, $a = -\beta q' b - r'$:
  - Si $r' = 0$, on prend $q = -\beta q'$ et $r = 0$.
  - Si $r' \in [\![1, |b| - 1]\!]$, $a = (-\beta' q - 1)\,b + b - r'$ car $b - r \in [\![0, |b| - 1]\!]$ donc on prend $q = -\beta q' - 1$ et $r = b - r'$.

Petite histoire : écriture en base b Pour la suite, $b \in \mathbb{N}$ et $b \geqslant 2$, on appellera b la base d'écriture. Soit $a \in \mathbb{N}$. On définit deux suites d'entiers (q_k) et (r_k) avec $k \geqslant 0$ par récurrence en posant :

(1) (q_0, r_0) est la division euclidienne de a par b.
(2) Pour $k \in \mathbb{N}$, (q_{k+1}, r_{k+1}) est la division euclidienne de q_k par b.

On a :

$$\begin{aligned} a &= bq_0 + r_0 \\ &= b^2 q_1 + b r_1 + r_0 \\ &= b^3 q_2 + b^2 r_2 + b r_1 + r_0 \\ &= b^4 q_3 + b^3 r^3 + b^2 r_2 + b r_1 + r_0 \end{aligned}$$

On pose P_n : « $a = b^{n+1} q_n + \sum_{l=0}^{n} r_l b^l$ »

- P est vrai pour $n = \{0, 1, 2\}$.

a. *Obvious !*
b. Aaaaaaargh !

– Supposons que P_n est vrai pour $k \in \mathbb{N}$. On a alors :

$$\begin{aligned} a &= b^{n+1}q_n + \sum_{l=0}^{n} r_l b^l \\ &= b^{n+1}\left(bq_{n+1} + r_{n+1}\right) + \sum_{l=0}^{n} r_l b^l \\ &= b^{n+2}q_{n+1} + \sum_{l=0}^{n+1} r_l b^l \end{aligned}$$

Lemme Il n'existe pas de suite d'entiers naturels strictement décroissante.

En effet, si $(p_n)_{n\in\mathbb{N}}$ est une telle suite, $A = \{p_n | n \in \mathbb{N}\}$ est une partie non vide de $\mathbb{N}$ qui n'admet pas de minimum, ce qui est impossible [a].

Revenons au problème principal et supposons que $\forall n \in \mathbb{N}$, $q_n \neq 0$. Alors pour $n \in \mathbb{N}$, $q_n = bq_{n+1} + r_{n+1}$ avec $0 \leqslant r_{n+1} < b$ donc

$$q_n \geqslant bq_{n+1} \geqslant 2q_{n+1} > q_{n+1} \quad \text{car } q_{n+1} \neq 0$$

Donc (q_n) est une suite d'entiers naturels strictement décroissante, ce qui est impossible [b].

Ainsi, $\exists l \in \mathbb{N}$ tel que $q_j = 0$. Soit alors $m = \min\{j \in \mathbb{N} | q_j = 0\}$ donc $q_m = 0$. La division euclidienne de 0 par b est $(0,0)$ donc $q_{m+1} = 0 = r_{m+1}$ puis, par récurrence, $\forall l > m$, $q_l = r_l = 0$.

Remarque Si $a \neq 0$, $r_m \neq 0$.

En effet :

– Si $m = 0$, $q_0 = 0$ et $r_0 = a \neq 0$.

– Si $m \geqslant 1$, $q_{m-1} = bq_m + r_m = r_m$ et $q_{m-1} \neq 0$ par hypothèse.

On a donc :

$$a = \underbrace{b^{m+1}q_m}_{0} + \sum_{l=0}^{m} b^l r_l = \sum_{l=0}^{m} b^l r_l$$

Bilan (provisoire) Si $a \in \mathbb{N}^*$, $\exists m \in \mathbb{N}$ et une liste $(r_0, \ldots, r_m)$ d'entiers compris entre 0 et $b-1$ alors :

(1) $r_m \geqslant 1$

(2) $a = \sum_{l=0}^{m} r_l b^l$

Supposons qu'il existe $n \in \mathbb{N}$ et $(s_0, \ldots, s_n)$ une liste d'entiers naturels appartenant à $[\![0, b-1]\!]$ tels que $s_n \geqslant 1$ et $a = \sum_{k=0}^{n} s_k b^k$.

– Supposons que $n > m$. Alors

$$a = \sum_{l=0}^{n} s_l b^l = \sum_{l=0}^{n} r'_l b^l \text{ avec } \begin{cases} r'_l = r_l & \text{si } l \leqslant m \\ r'_l = 0 & \text{si } l > m \end{cases} = \sum_{l=0}^{m} r_l b^l$$

Ainsi,

$$s_n b^n = \sum_{l=0}^{n-1} \left(r'_l - s_l\right) b^l$$

a. En effet, $\forall n \in \mathbb{N}$, $p_{n+1} < p_n$ or toute partie non vide de $\mathbb{N}$ admet un plus petit élément donc aaaaaaargh !

b. Aaaaaaargh !

On a $s_n b^n \geqslant b^n$ et

$$\begin{aligned}\left|\sum_{l=0}^{n-1}\left(r'_l - s_l\right)b^l\right| &\leqslant \sum_{l=0}^{n-1}\underbrace{\left|r'_l - s_l\right|}_{\leqslant b-1}b^l \\ &\leqslant (b-1)\sum_{l=0}^{n-1} b^l \\ &\leqslant (b-1)\frac{b^n-1}{b-1} \quad \text{car } b \neq 1 \\ &\leqslant b^n\end{aligned}$$

Ce qui est impossible [a] car ceci reviendrait à dire que $s_n b^n \leqslant b^n$.

– De même, on ne peut pas avoir $m < n$ donc $m = n$.

Montrons maintenant que $\forall k \in [\![0, n]\!]$, $r_k = s_k$.

Supposons qu'il existe au moins un $k \in [\![0, n]\!]$ tel que $r_k \neq s_k$, alors on peut considérer

$$j = \min\left\{p \in [\![0, n]\!] \,|\, r_p \neq s_p\right\}$$

Alors

$$\begin{aligned}\sum_{l=0}^{m}\left(r_l - s_l\right)b^l &= 0 \\ &= \left(r_j - s_j\right)b^j + \underbrace{\sum_{l=0}^{j-1}\left(r_l - s_l\right)b^l}_{0}\end{aligned}$$

D'où :

$$\underbrace{\left|r_j - s_j\right|b^j}_{\geqslant b^j} = \underbrace{\left|\sum_{l=0}^{j-1}\left(r_l - s_l\right)b^l\right|}_{< b^j}$$

Ce qui est impossible [b].

Conclusion Si $a \in \mathbb{N}^*$ et $b \in \mathbb{N}$, $n \geqslant 2$, alors il existe un unique entier naturel n et une unique liste $(r_0, \ldots, r_n)$ d'entiers compris entre 0 et $b-1$ tels que $r_n \geqslant 1$ et

$$a = \sum_{k=0}^{n} r_k b^k$$

On note alors $a = \overline{r_m \cdots r_0}^b$, et $(r_0, \ldots, r_n)$ est la liste de chiffres de a en base b.

Pour écrire a sans ambiguïté il faut disposer d'un symbole par chiffre disponible, soit b symboles. Si $b \leqslant 10$ on prendra les symboles usuels (0, 1, etc). Si $b > 10$ il faut ajouter d'autres symboles pour représenter les autres entiers de $[\![10, b-1]\!]$.

En base hexadécimale, $A = 10$, $B = 11$, $C = 12$, …, $F = 14$.

Je note ici un programme Maple qui donne l'écriture en base b d'un nombre a :

```
base := proc (a::posint, b::posint)
local q, r, i, q0, k, S;
if 1 < b then
   q := iquo(a, b);
   array(0 .. 1000, []);
```

a. Aaaaaaargh !

b. Aaaaaaargh !

```
    r[0] := irem(a, b);
    i := 1;
    while q <> 0 do
       q0 := q;
       q := iquo(q, b);
       r[i] := irem(q0, b);
       i := i+1;
       end do;
    if b <= 10 then
       S := sum(10^k*r[k], k = 0 .. i-1);
       print(S[b]);
    else for k from 0 to i-1 do
       print(r[k]);
       end do;
       print("Le chiffre du bas du résultat correspond au chiffre le plus à gauche dans
       une écriture plus conventionnelle, les chiffres supérieurs ou égaux à 10 sont
       remplacés par des symboles ordinairement : pour une base hexadécimale,
       A=10,etc");
    end if;
    else
       print("La base doit être supérieure ou égale à 2 !");
end if;
end proc;
```

3.3 Plus Grand Commun Diviseur et éléments d'arithmétique

3.3.1 PGCD

Définitions

- Pour $n \in \mathbb{N}$, on note $\mathcal{D}(n)$ l'ensemble des diviseurs de n dans $\mathbb{N}$. Si $n \neq 0$, alors $\mathcal{D}(n) \subset [\![1, n]\!]$.
- Soient $a, b \in \mathbb{N}$ tels que $(a, b) \neq (0, 0)$. Alors l'ensemble $\mathcal{D}(a) \cap \mathcal{D}(b)$ est une partie de $\mathbb{N}$ non vide ($1 \mid a$ et $1 \mid b$) et majorée (par $\max(a, b)$). On appelle $\mathrm{PGCD}(a, b)$ ou $a \wedge b$ l'entier $\max(\mathcal{D}(a) \cap \mathcal{D}(b))$.
- On dit que a et b sont premiers entre eux si $a \wedge b = 1$. Ceci signifie que $\mathcal{D}(a) \cap \mathcal{D}(b) = \{1\}$, c'est-à-dire que 1 est le seul diviseur commun à a et à b.

Propriétés

- Soit $a, b \in \mathbb{N}^*$. Alors $a \mid b \Leftrightarrow \mathrm{PGCD}(a, b) = a$. En effet :
  - $\Rightarrow$ On a $\mathcal{D}(a) \subset \mathcal{D}(b)$ donc $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a)$ et $\max(\mathcal{D}(a)) = a$.
  - $\Leftarrow$ On sait que $a \wedge b \in \mathcal{D}(b)$ donc $a \wedge b \mid b$.
- Soit p un nombre premier et $a \in \mathbb{N}^*$. Alors

$$p \mid a \quad \text{ou} \quad p \wedge a = 1$$

  Ces deux possibilités s'excluent mutuellement.
- On p et q sont deux nombres premiers distincts, alors $p \wedge q = 1$.

Algorithme d'Euclide

Soit $b \in \mathbb{N}^*$ et $q, r \in \mathbb{N}$ tels que $a = bq + r$. Alors $a \wedge b = b \wedge r$.

En effet, $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(r)$:
- Si $k \mid a$ et $k \mid b$, alors $k \mid b$ et $k \mid a - bq = r$.
- Si $k \mid b$ et $k \mid r$, alors $k \mid b$ et $k \mid bq + r = a$.

Application On dispose de l'algorithme d'Euclide pour déterminer le PGCD de deux entiers non nuls. Soient $a, b \in \mathbb{N}^*$. On considère le processus suivant :

$$\begin{array}{rl} a = bq_0 + r_0 & 0 < r_0 < b \\ b = q_1 r_0 + r_1 & 0 < r_1 < r_0 \\ r_0 = q_2 r_1 + r_2 & 0 < r_2 < r_1 \\ \vdots & \\ r_{k-1} = q_{k+1} r_k + r_{k+1} & 0 < r_{k+1} < r_k \\ \vdots & \\ r_{N-1} = q_{N+1} r_N + 0 & 0 < r_N < r_{N-1} \end{array}$$

On finit par parvenir à 0. Sinon la suite d'entiers des restes $(r_k)_{k\in\mathbb{N}}$ serait strictement décroissante et infinie, ce qui est impossible [a]. Le processus se termine donc nécessairement.

On a alors :

$$a \wedge b = b \wedge r_0 = r_0 \wedge r_1 = \cdots = r_{N-1} \wedge r_N = r_N \wedge 0 = r_N$$

$a \wedge b$ est ainsi le dernier reste non nul dans la suite des opérations de l'algorithme d'Euclide.

3.3.2 Éléments d'arithmétique

Théorème de Bézout Considérons la suite des opérations de l'algorithme d'Euclide appliquée à a et à b :

$$\begin{array}{rl} a = bq_0 + r_0 & 0 < r_0 < b \\ b = q_1 r_0 + r_1 & 0 < r_1 < r_0 \\ r_0 = q_2 r_1 + r_2 & 0 < r_2 < r_1 \\ \vdots & \\ r_{k-1} = q_{k+1} r_k + r_{k+1} & 0 < r_{k+1} < r_k \\ \vdots & \\ r_{N-1} = q_{N+1} r_N + 0 & 0 < r_N < r_{N-1} \end{array}$$

Démontrons par récurrence que $\forall k \in [\![-1, N-1]\!]$,

$$r_k = au_k + bv_k$$

– Notons $r_{-1} = b$, $u_{-1} = 0$ et $v_{-1} = 1$. Ainsi

$$r_{-1} = u_{-1}a + v_{-1}b$$

De même, posons $u_0 = 1$ et $v_0 = -q_0$ alors

$$r_0 = u_0 a + v_0 b$$

– Soit $k \in [\![0, N-1]\!]$. Supposons avoir trouvé les relatifs u_{k-1}, v_{k-1}, u_k et v_k tels que que $r_{k-1} = au_{k-1} + bv_{k-1}$ et $r_k = u_k a + v_k b$. On a d'après l'algorithme d'Euclide :

$$\begin{array}{rcl} r_{k-1} = q_{k+1} r_k + r_{k+1} & \Leftrightarrow & u_{k-1}a + v_{k-1}b = q_{k+1}\left(u_k a + v_k b\right) + r_{k+0} \\ & \Leftrightarrow & r_{k+1} = a\underbrace{(u_{k-1} - q_{k+1}u_k)}_{\in\mathbb{Z}} + b\underbrace{(v_{k-1} - q_{k+1}v_k)}_{\in\mathbb{Z}} \end{array}$$

– Ainsi, $\forall k \in [\![-1, N]\!]$, $\exists u_k, v_k \in \mathbb{Z}$ tels que

$$r_k = au_k + bv_k$$

En particulier pour $k = N$, $r_N = a \wedge b$.

On en déduit un énoncé du théorème de Bézout : soient $a, b \in \mathbb{N}^*$, alors il existe un couple de relatifs (u, v) tel que

$$a \wedge b = au + bv$$

a. Aaaaaaargh !

Corollaire L'ens$d$ un diviseur commun à a et à b. Alors $d \leqslant a \wedge b$ et même $d \mid a \wedge b$.

En effet, soient $u, v \in \mathbb{Z}$ tels que $a \wedge b = au + bv$. $d \mid b$ et $d \mid a$ dans $\mathbb{N}$ donc dans $\mathbb{Z}$ donc $d \mid au + bv = a \wedge b$ dans $\mathbb{Z}$. Or $d, a \wedge b \in \mathbb{N}^*$ donc $d \mid a \wedge b$ dans $\mathbb{N}$.

Théorème de Bézout : le retour

Soient $a, b \in \mathbb{N}$ tels que $(a, b) \neq (0, 0)$. Alors

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

Démonstration

$\Rightarrow$ Déjà fait [a] (application directe du précédent énoncé de ce même théorème).

$\Leftarrow$ Soit d est un diviseur de a et b dans $\mathbb{N}$. Alors $d \mid au + bv$ donc $d \in \{\pm 1\}$ or $d \in \mathbb{N}$ donc $d = 1$ donc

$$\max\left(\mathcal{D}(a) \cap \mathcal{D}(b)\right) = 1$$

Théorème de Carl Friedrich Gauss

Soient $a, b \in \mathbb{N}$. On suppose $a \wedge b = 1$ et $a \mid bc$. Alors $a \mid c$.

Démonstration $a \wedge b = 1$ donc $\exists u, v \in \mathbb{Z} / au + bv = 1$. Donc $c = acu + bcv$ or $a \mid acu$ et $a \mid bc$ donc $a \mid bcv$ donc $a \mid c$.

Application Soit p un nombre premier, $a, b \in \mathbb{N}^*$. Alors

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

En effet :

$\Rightarrow$ Évident [b] !

$\Leftarrow$ Si $p \nmid a$, alors $p \wedge a = 1$ car p est premier d'où $p \mid b$ d'après le théorème de [c] Gauss.

Plus globalement, si $p \mid a_1 a_2 \cdots a_n$, alors p divise au moins l'un des a_i.

Variante du théorème de Gauss Soient $a, b \in \mathbb{N}^*$. Alors

$$(a \wedge b = 1 \quad \text{et} \quad a \wedge c = 1) \Leftrightarrow a \wedge (bc) = 1$$

Démonstration

$\Leftarrow$ Évident [d] ! Si $d \mid a$ et $d \mid b$ alors $d \mid a$ et $d \mid bc$ donc $d \mid a \wedge (bc) = 1$ donc $a \wedge b = 1$. De même, $a \wedge c = 1$.

$\Rightarrow$ Il existe $u, v, s, t \in \mathbb{Z}$ tels que $au + bv = 1$ et $as + ct = 1$. Or :

$$\begin{aligned} 1 &= 1 \cdot 1 \\ &= (au + bv)(as + ct) \\ &= a\underbrace{(uas + utc + bvs)}_{\in \mathbb{Z}} + b\underbrace{ctv}_{\in \mathbb{Z}} \end{aligned}$$

Donc $a \wedge (bc) = 1$.

a. Ou, pour rester fidèle à ce cher M. Sellès, « *djafé !* »
b. « *Obvious !* »
c. Carl Friedrich !
d. « *Obvious !* »

Généralisation Si $a \wedge b_1 = a \wedge b_2 = \cdots = a \wedge b_n$, alors $a \wedge \left(\prod_{k=1}^{n} b_k \right) = 1$.

Corollaire Supposons que $a \wedge b = 1$. Alors $\forall \beta \in \mathbb{N}$, $a \wedge b^\beta = 1$. De plus, $\forall \beta, \alpha \in \mathbb{N}$, $a^\alpha \wedge b^\beta = 1$.

Petite histoire sur l'unicité de l'écriture en produit de facteurs premiers d'un entier naturel Soient $r, s \in \mathbb{N}^*$Form$p_1, p_2, \ldots, p_r$ et $q_1, q_2, \ldots, q_s$ des nombres premiers. Supposons que :

$$\prod_{k=1}^{r} p_k = \prod_{i=1}^{s} q_i$$

Alors $p_1 \mid \prod_{i=1}^{s} q_i$ donc p_1 divise au moins l'un des q_i.

Supposons, (quitte à renuméroter les q_i) que $p_1 \mid q_1$. Or q_1 est premier donc $p_1 \in \{1, q_1\}$ or p_1 est premier donc $p_1 = q_1$. Il reste alors

$$\prod_{k=2}^{r} p_k = \prod_{i=2}^{s} q_i$$

En réitérant ceci (récurrence), on prouve que $r = s$ et, aux permutations près, $q_i = p_i$, c'est-à-dire qu'il existe une application $\sigma : [\![1, r]\!] \longrightarrow [\![1, s]\!]$ bijective telle que $\forall 1 \leqslant i \leqslant r$, $p_i = q_{\sigma(i)}$.

Théorème Tout entier naturel $n \geqslant 2$ s'écrit

$$n = \prod_{k=1}^{r} p_k$$

avec $r \in \mathbb{N}^*$ et $p_1, p_2, \ldots, p_r$ des nombres premiers.

Cette écriture est unique à l'ordre près des termes du produit.

4 Ensembles finis

4.1 Définitions, faits de base

4.1.1 Définitions

Soit E un ensemble. E est fini s'il existe un $n \in \mathbb{N}$ et une bijection de E dans $[\![1, n]\!] = \{k \in \mathbb{N} | 1 \leqslant k \leqslant n\}$.
Avec cette définition, si $E = \varnothing$, E est en bijection avec lui même : $\varnothing = [\![1, 0]\!]$.
Si $n \in \mathbb{N}^*$, $\varnothing$ n'est pas en bijection avec $[\![1, n]\!] \neq \varnothing$ [a] donc $n = 0$ est l'unique entier naturel tel que $\varnothing$ est en bijection avec $[\![1, n]\!]$.

a. C'est à dire qu'il n'existe aucune application bijective de $[[1, n]]$ dans $\varnothing$.

Lemme Soit $n, p \in \mathbb{N}^*$. Alors :

(1) Il existe une injection de $[\![1, n]\!]$ dans $[\![1, p]\!]$ si et seulement si $n \leqslant p$.

(2) Il existe une surjection de $[\![1, n]\!]$ dans $[\![1, p]\!]$ si et seulement si $n \geqslant p$.

(3) Il existe une bijection de $[\![1, n]\!]$ dans $[\![1, p]\!]$ si et seulement si $n = p$.

Démonstration

(1) $\Leftarrow$ Évident [a] ! $\begin{array}{l}[\![1,n]\!] \longrightarrow [\![1,p]\!] \\ x \longmapsto x\end{array}$ fait l'affaire [b] So

$\Rightarrow$ Soit H_n : « Pour $p \in \mathbb{N}^*$, s'il existe une injection de $[\![1,n]\!]$ dans $[\![1,p]\!]$, alors $n \leqslant p$ ».

- H_1 est trivial.
- Soit $n \in \mathbb{N}^*$. Supposons, que H_n, st vrai et prouvons H_{n+1}. Soit $p \in \mathbb{N}^*$, supposons qu'il existe $f : [\![1,n+1]\!] \longrightarrow [\![1,p]\!]$ injective et montrons que $n+1 \leqslant p$.
  - Supposons que $f(n+1) = p$. On a $\forall k \in [\![1,n]\!]$, $f(k) \neq f(n+1) = p$ donc $f(k) \in [\![1,p-1]\!]$, ce qui implique que $p-1 \geqslant 1$. Posons $g : \begin{array}{l}[\![1,n]\!] \longrightarrow [\![1,p-1]\!] \\ k \longmapsto f(k)\end{array}$. g est injective car f est injective donc $n \leqslant p-1 \Leftrightarrow n+1 \leqslant p$.
  - Supposons que $l = f(n+1) \neq p$. Soit

$$\begin{array}{rl}\tau : & [\![1,p]\!] \longrightarrow [\![1,p]\!] \\ & l \longmapsto p \\ & p \longmapsto l \\ & x \notin \{l,p\} \longmapsto x\end{array}$$

Alors τ est bijective donc $\tau \circ \tau = \mathrm{Id}_{[\![1,p]\!]}$ [c]. Alors $\tilde{f} = \tau \circ f$ est injective de $[\![1,n]\!]$ dans $[\![1,p]\!]$ par composition d'applications injectives et $\tilde{f}(n+1) = \tau(l) = p$. On est là ramené au premier cas.

4.1.2 Théorème et définition

Soit E un ensemble fini. Alors il existe $n \in \mathbb{N}$ tel que E est en bijection avec $[\![1,n]\!]$. n s'appelle le cardinal de E et se note Card$E$ ou $|E|$ ou $\#E$.

Démonstration Si $E = \varnothing$, on a vu que 0 est l'unique $n \in \mathbb{N}$ tel que E est en bijection avec $[\![1,n]\!]$ donc Card$\varnothing = 0$ [d].

Supposons que $E \neq \varnothing$, alors E n'est pas en bijection avec $\varnothing = [\![1,0]\!]$. Soit $n,p \in \mathbb{N}^*$ tels que E est en bijection avec $[\![1,n]\!]$ et $[\![1,p]\!]$ et soit $f : [\![1,n]\!] \longrightarrow E$ bijective et $g : [\![1,p]\!] \longrightarrow E$ bijective. Alors $g^{-1} \circ f$ est bijective et va bien de $[\![1,n]\!]$ dans $[\![1,p]\!]$ donc $n = p$.

Application Soient $p,q \in \mathbb{N}$ tels que $p \leqslant q$. Alors $\begin{array}{l}[\![1,q-p+1]\!] \longrightarrow [\![p,q]\!] \\ x \longmapsto p-x+1\end{array}$ est une bijection donc $[\![p,q]\!]$ est fini [e] donc Card $[\![p,q]\!] = q-p+1$.

Proposition

Soit E un ensemble fini et X un ensemble. Si X est en bijection avec E, alors X est fini et Card$X$ = Card$E$.

Démonstration Soit $f : E \longrightarrow X$ bijective et $\varphi : [\![1,n]\!] \longrightarrow E$ une bijection avec $n = \mathrm{Card}E$. Alors $f \circ \varphi$ est une bijection de $[\![1,n]\!]$ dans X.

Exemple Soit $n \in \mathbb{N}^*$. $[\![0,n-1]\!] \longrightarrow \mathbb{Z}/n\mathbb{Z}$ est bijective donc $\mathbb{Z}/n\mathbb{Z}$ est fini et Card$\mathbb{Z}/n\mathbb{Z}$ = Card $[\![0,n-1]\!] = n$.

a. « *Obvious !* »
b. « *does the job !* »
c. « *Une petite dédicace à nos amis les canadiens... Évidemment si on sait pas que Toronto c'est au Canada...* »
d. « *Ouf !* »
e. Je n'oserai pas reporter ici le jeu de mot douteux de M. Sellès portant sur ces derniers mots.

Propriétés Soient E, F deux ensembles finis non vides :

(1) S'il existe une injection de E dans F, alors $\text{Card}E \leqslant \text{Card}F$.

(2) S'il existe une surjection de E dans F, alors $\text{Card}E \geqslant \text{Card}F$.

Démonstration

(1) Soit $n = \text{Card}E$, $p = \text{Card}F$, $\varphi : [\![1, n]\!] \longrightarrow E$ bijective et $\psi : [\![1, p]\!]$ bijective. Si $f : E \longrightarrow F$ est injective, alors $\psi^{-1} \circ f \circ \varphi$ est injective dans $[\![1, n]\!]$ dans $[\![1, p]\!]$ donc $n \leqslant p$.

4.1.3 Principe des tiroirs

Si $\text{Card}E \geqslant \text{Card}F$, il n'existe pas d'applications injective de E dans F. Ainsi si $f : E \longrightarrow F$, f ne peut être injective donc $\exists a \neq b / f(a) = f(b)$.

Ceci est connu sous le nom de principe des tiroirs [a].

Applications

– Soit $N \in \mathbb{N}^*$. Montrons qu'il existe un multiple de N dont l'écriture décimale ne comporte que des 0 et des 1. Considérons les entiers $0, 1, 11, 111, \ldots, \underbrace{111\cdots111}_{N}$ distincts. L'application

$$\begin{aligned} \{0, 1, 11, 111, \ldots, 111\cdots111\} &\longrightarrow \mathbb{Z}/N\mathbb{Z} \\ x &\longmapsto \overline{x} \end{aligned}$$

ne peut pas être injective car $\text{Card}\{0, 1, 11, 111, \ldots, 111\cdots111\} = N + 1 > N = \text{Card}\mathbb{Z}/NZ$ donc

$$\begin{aligned} \exists 0 \leqslant k < l \leqslant N / \overline{x_k} = \overline{x_l} &\Leftrightarrow N \mid x_k - x_l \\ &\Leftrightarrow N \mid \underbrace{1\cdots1}_{l} - \underbrace{1\cdots1}_{k} \\ &\Leftrightarrow N \mid \underbrace{1\cdots1}_{l}\underbrace{0\cdots0}_{k} \end{aligned}$$

– Soit $n \in \mathbb{N}^*$ et $1 \leqslant a_1 < a_2 < \cdots < a_n \leqslant 2n$ avec $a_i \in \mathbb{N}$. Alors $\exists i < j$ tel que $a_i \mid a_j$.
En effet, pour $1 \leqslant k \leqslant n + 1$, $a_k = 2^{\alpha_k} m_k$ avec m_k impair et $m_k \in [\![1, 2n]\!]$. Or

$$(2\mathbb{N} + 1) \cap [\![1, 2n]\!] = \{1, 3, 5, \ldots, 2n - 1\}$$

donc $\text{Card}\,(2\mathbb{N} + 1) \cap [\![1, 2n]\!] = n$. D'après le principe des tiroirs, $\exists k < l / m_k = m_l = m$ donc $a_k = 2^{\alpha_k} m$ et $a_l = 2^{\alpha_l} m$ or $\alpha_k < \alpha_l$ car $a_k < a_l$ donc $a_k \mid a_l$.

Théorème

Soit E un ensemble fini non vide et $F \subset E$. Alors F est fini et $\text{Card}F \leqslant \text{Card}E$. De plus, $F = E \Leftrightarrow \text{Card}F = \text{Card}E$ [a].

a. Ce théorème évite de montrer une inclusion inverse, par exemple.

Démonstration Soit H_n : « Si E est fini et de cardinal n et si $F \subset E$, alors F est fini et $\text{Card}F \leqslant \text{Card}E$. De plus, $\text{Card}F = \text{Card}E \Leftrightarrow E = F$ ».

– H_0 est trivial : $\varnothing$ est l'unique ensemble fini de cardinal 0.

– Soit $n \in \mathbb{N}$, E un ensemble fini de cardinal $n + 1$ et $F \subset E$.

  ◦ Si $F = E$, alors F est bien de cardinal $n + 1$.

  ◦ Si $F \neq E$, alors $\exists a \in E / a \notin F$ donc $F \subset E \setminus \{a\}$. Si l'on admet que $E \setminus \{a\}$ est fini et de cardinal n, d'après l'hypothèse de récurrence, F est fini et de cardinal $\text{Card}F \leqslant n < \text{Card}E$.

a. « *Si on range n paires de chaussettes dans p tiroirs avec n > p, deux paires vont se retrouver dans le même tiroir. Quand même j'ai réussi à caser le mot chaussette dans mon cours....* »

Lemme Soit E un ensemble fini non vide et $a \in E$. Alors $E \setminus \{a\}$ est fini et $\text{Card}E \setminus \{a\} = \text{Card}E - 1$.

Démonstration Soit $n = \text{Card}E$ et $\varphi : [\![1, n]\!] \longrightarrow E$ bijective.
- Si $\varphi(n) = a$, $\forall k \in [\![1, n-1]\!]$, $\varphi(k) \in E \setminus \{a\}$. Alors $\tilde{\varphi} : \begin{array}{l} [\![1, n-1]\!] \longrightarrow E \\ k \longmapsto \varphi(k) \end{array}$ est bijective donc $E \setminus \{a\}$ est fini et de cardinal $n - 1$.
- Si $\varphi(n) \neq a$, soit $k = \varphi^{-1}(a) \in [\![1, n-1]\!]$ et

$$\begin{array}{rl} \tau : & [\![1, n]\!] \longrightarrow [\![1, n]\!] \\ & k \longmapsto n \\ & n \longmapsto k \\ & l \notin \{k, n\} \longmapsto l \end{array}$$

est bijective car $\tau \circ \tau = \text{Id}_{[\![1,n]\!]}$. Alors $\varphi \circ \tau : [\![1, n]\!] \longrightarrow E$ est bijective et $\varphi \circ \tau(n) = \varphi(k) = a$. On est donc ramené au cas précédent.

Propositions Soit E un ensemble fini et X un ensemble.

(1) S'il existe une injection de X dans E, X est fini de cardinal plus petit que $\text{Card}E$.

(2) S'il existe une surjection de E dans X, X est fini de cardinal plus petit que $\text{Card}E$.

Démonstration

(1) Soit $f : X \longrightarrow E$ injective et $F = f(X)$. Alors $\tilde{f} : \begin{array}{l} X \longrightarrow f(X) \\ t \longmapsto f(t) \end{array}$ est bijective. Or F est fini donc X est fini et $\text{Card}X = \text{Card}f(X) \leqslant \text{Card}E$.

4.2 Cardinaux classiques

4.2.1 Réunion

Soit E et F deux ensembles finis tels que $E \cap F = \varnothing$. Alors

$$\text{Card}(E \cup F) = \text{Card}E + \text{Card}F$$

Démonstration Si $E = \varnothing$ ou $F = \varnothing$, c'est trivial. Supposons que $(E, F) \neq (\varnothing, \varnothing)$, soit $n = \text{Card}E$, $p = \text{Card}F$, $\varphi : [\![1, n]\!] \longrightarrow E$ bijective et $\psi : [\![1, p]\!] \longrightarrow F$ bijective. Alors :

$$\begin{array}{rl} f : & [\![1, n+p]\!] \longrightarrow E \cup F \\ & k \longmapsto \begin{cases} \varphi(k) & \text{si } 1 \leqslant k \leqslant n \\ \psi(k-n) & \text{si } n+1 \leqslant k \leqslant n+p \end{cases} \end{array}$$

- f est bien définie.
- f est surjective : soit $x \in E \cup F$.
  - Si $x \in E$, $\exists k \in [\![1, n]\!] / x = \varphi(k) = f(k)$.
  - Si $x \in F$, $\exists l \in [\![1, p]\!] / x = \psi(l) = f(n + l)$.
- f est injective : soient $k, l \in [\![1, n+p]\!]$ avec $k < l$. Montrons que $f(k) \neq f(l)$.
  - Si $1 \leqslant k < l \leqslant n$, on a $f(k) = \varphi(k) \neq \varphi(l) = f(l)$ car φ est injective.
  - Si $n+1 \leqslant k < l \leqslant n$, $f(k) = \psi(k-n) \neq \psi(l+n) = f(l)$ car ψ est injective.
  - Si $k < n < l$, on ne peut pas avoir $\varphi(k) = \psi(l)$ car $\varphi(k) \in E$ et $\psi(l) \in F$ et $E \cap F = \varnothing$.

Corollaires

(1) Soit $n \in \mathbb{N}^*$ et $E_1, E_2, \ldots, E_n$ des ensembles finis tels que $E_i \cap E_j = \varnothing$ pour $i \neq j$. Alors $\bigcup_{i=1}^{n} E_i$ est fini et

$$\mathrm{Card} \bigcup_{i=1}^{n} E_i = \sum_{i=i}^{n} \mathrm{Card} E_i$$

(2) Soit E un ensemble fini et $A \subset E$. Alors on a

$$\mathrm{Card}\,(E \backslash A) = \mathrm{Card} E - \mathrm{Card} A$$

En effet, A et $E\backslash A$ sont des parties de E donc sont finies et on a $E = E \cup (E\backslash A)$ et $A \cap (E\backslash A) = \varnothing$ d'où $\mathrm{Card} E = \mathrm{Card} A + \mathrm{Card} E\backslash A$.

(3) Soit E un ensemble fini. Si Ω est une partition de E, alors

$$\mathrm{Card} E = \sum_{A \in \Omega} \mathrm{Card} A$$

En effet, A et $E\backslash A$ sont des parties de E donc on Plus généralement, si $A_1, A_2, \ldots, A_n$ sont des parties de E telles que $A_i \cap A_j = \varnothing$ pour $i \neq j$ et $E = \bigcup_{i=1}^{n} A_i$, alors

$$\mathrm{Card} E = \sum_{k=1}^{n} \mathrm{Card} A_k$$

Généralisation

Soient E et F deux ensembles finis. Alors $E \cup F$ est fini et

$$\mathrm{Card} E \cup F = \mathrm{Card} E + \mathrm{Card} F - \mathrm{Card} E \cap F$$

Démonstration $E \cap F$ est nécessairement fini : c'est une partie de l'ensemble fini E. Soit $G = E \backslash (E \cup F)$, on a $F \cap G = \varnothing$ [a] et $E \cup F = G \cup F$.

- Il est clair que $(G \cup F) \subset (E \cup F)$ puisque $G \subset E$.
- Si $x \in E \cup F$, si $x \in F$, alors $x \in G \cup F$ sinon on a nécessairement $x \in E$ et $x \notin F$ donc $x \in G$. G est fini (c'est aussi une partie de E), F et G sont finis disjoints donc $F \cup G$ est fini et

$$\begin{aligned} \mathrm{Card} F \cup G &= \mathrm{Card} F + \mathrm{Card} G \\ &= \mathrm{Card} F + \mathrm{Card} E - \mathrm{Card}\,(E \cap F) \end{aligned}$$

Corollaire Si $n \in \mathbb{N}^*$, $E_1, E_2, \ldots, E_n$ sont des ensembles finis, alors $\bigcup_{i=1}^{n} E_i$ est fini et

$$\mathrm{Card} \bigcup_{i=1}^{n} E_i \leqslant \sum_{i=1}^{n} E_i$$

4.2.2 Produit cartésien

Soient E et F des ensembles finis, alors $E \times F$ est fini et $\mathrm{Card} E \times F = \mathrm{Card} E \cdot \mathrm{Card} F$.

a. Si jamais $x \in F \cup G$, $x \in F$ et $x \in G \subset E$ donc $x \in E$ donc $x \in (E \cup F)$, ce qui n'est pas possible : Aaaaaaargh !

Démonstration
- Si E ou F est vide, la preuve est triviale.
- Supposons E et F non vides. Pour $x \in E$, $A_x = \{(x,y)\,|y \in F\}$. A_x est non vide et $A_x \subset (E \times F)$. $\Omega = \{A_x | x \in E\}$ forme une partition de $E \times F$. Si $x \in E$ est fixé donc A_x est en bijection avec F via $y \in F \longrightarrow (x,y) \in A_x$. Donc A_x est fini et $\mathrm{Card}A_x = \mathrm{Card}F$ donc $E \times F$ est une réunion finie d'ensembles deux à deux disjoints donc $E \times F$ est fini et

$$\begin{aligned}\mathrm{Card}E \times F &= \mathrm{Card}\bigcup_{x\in E} A_x \\ &= \sum_{x\in E} \mathrm{Card}A_x \\ &= \sum_{x\in E} \mathrm{Card}F \\ &= \mathrm{Card}F \cdot \sum_{x\in E} 1 \\ &= \mathrm{Card}E \cdot \mathrm{Card}F\end{aligned}$$

Corollaire Soient $E_1, E_2, \ldots, E_n$ des ensembles finis, alors $E_1 \times E_2 \times \cdots \times E_n$ et

$$\mathrm{Card}E_1 \times E_2 \times \cdots \times E_n = \prod_{i=1}^{n} \mathrm{Card}E_i$$

4.2.3 Ensemble de parties d'un ensemble fini

Soit E un ensemble fini. Alors $\mathcal{P}(E)$ est fini et

$$\mathrm{Card}\mathcal{P}(E) = 2^{\mathrm{Card}E}$$

Démonstration H_n : « Si E est un ensemble fini de cardinal n, alors $\mathcal{P}(E)$ est fini de cardinal 2^n ».
- H_0 est vrai : $\varnothing$ est le seul ensemble de cardinal 0 et on a $\mathcal{P}(\varnothing) = \{\varnothing\}$. Donc $\mathcal{P}(\varnothing)$ est fini de cardinal $1 = 2^0$.
- Soit $n \in \mathbb{N}$, supposons que H_n est vrai et soit E un ensemble fini de cardinal $n+1$. Soit $a \in E$, $\Lambda = \{A \in \mathcal{P}(E)\,|a \notin A\}$ et $\Gamma = \{A \in \mathcal{P}(E)\,|a \in A\}$. Il est clair que $\Lambda \cap \Gamma = \varnothing$, on a $\Lambda = \mathcal{P}(E \backslash \{a\})$ or $E \backslash \{a\}$ est fini de cardinal n donc, d'après H_n, Λ est fini de cardinal 2^n.
  De plus, Λ et Γ sont en bijection : $X \in \Lambda \longrightarrow X \cup \{a\} \in \Gamma$ est bijective de réciproque $Y \in \Gamma \longrightarrow Y \backslash \{a\} \in \Lambda$. Donc Γ est aussi fini de cardinal 2^n. Or $\mathcal{P}(E) = \Lambda \cup \Gamma$ et $\Lambda \cap \Gamma = \varnothing$ donc $\mathcal{P}(E)$ est fini et

$$\begin{aligned}\mathrm{Card}\mathcal{P}(E) &= \mathrm{Card}\Lambda + \mathrm{Card}\Gamma \\ &= 2^n + 2^n \\ &= 2^{n+1}\end{aligned}$$

4.2.4 Petite histoire sur la définition ensembliste des coefficients du binôme

Soit $n \in \mathbb{N}^*$ et E un ensemble fini de cardinal n : on a vu que si $A \subset E$, alors A est fini et $\mathrm{Card}A \in [[0,n]]$ donc pour $p \in [\![0,n]\!]$, on note $\mathcal{P}_p(E)$ l'ensemble des parties de E à p éléments. $\mathcal{P}_p(E) \subset \mathcal{P}(E)$ donc $\mathcal{P}_p(E)$ est un ensemble fini. Notons γ_n^p le cardinal de $\mathcal{P}_p(E)$ [a]. Il est clair que les ensembles $\mathcal{P}_p(E)$ tels que $0 \leqslant p \leqslant n$ sont

a. Il est clair que si F est fini et de cardinal n, $\mathcal{P}_p(F)$ est en bijection avec $\mathcal{P}_p(E)$

deux à deux disjoints [a] et $\bigcup_{p=0}^{n} \mathcal{P}_p(E) = \mathcal{P}(E)$ donc :

$$\begin{aligned} 2^n &= \text{Card}\mathcal{P}(E) \\ &= \sum_{p=0}^{n} \gamma_n^p \end{aligned}$$

- $\mathcal{P}_0(E) = \{\varnothing\}$ donc $\gamma_n^0 = 1$. De même, $\mathcal{P}_n(E) = \{E\}$ donc $\gamma_n^n = 1$.
- Soit $p \in [\![0, n]\!] \setminus \{0, n\}$. Si $A \in \mathcal{P}_p(E)$, alors $E \backslash A \in \mathcal{P}_{n-p}(E)$ donc

$$\varphi : \begin{array}{l} \mathcal{P}_p(E) \longrightarrow \mathcal{P}_{n-p}(E) \\ A \longmapsto E \backslash A \end{array} \quad \text{et} \quad \psi : \begin{array}{l} \mathcal{P}_{n-p}(E) \longrightarrow \mathcal{P}_p(E) \\ A \longmapsto E \backslash A \end{array}$$

  sont deux bijections réciproques l'une de l'autre car $\psi \circ \varphi = \text{Id}_{\mathcal{P}_{n-p}(E)}$ et $\varphi \circ \psi = \text{Id}_{\mathcal{P}_p(E)}$. Ainsi $\mathcal{P}_{n-p}(E)$ et $\mathcal{P}_p(E)$ sont en bijection donc ils ont le même cardinal donc

$$\gamma_n^p = \gamma_n^{n-p}$$

Proposition Pour $n, p \in \mathbb{N}$ tel que $0 \leqslant p \leqslant n$,

$$\gamma_{n+1}^{p+1} = \gamma_n^p + \gamma_n^{p+1}$$

Pour $p > n$, $\mathcal{P}_p(E) = \varnothing$ donc $\gamma_n^p = 0$.

Prouvons cette assertion. Soit $n \in \mathbb{N}$ et $p \in \mathbb{N}$ tel que $0 \leqslant p \leqslant n$. Soit E un ensemble fini de cardinal $n+1$ et $a \in E$. Posons $\Gamma = \{A \in \mathcal{P}_{p+1}(E) \,|\, a \in A\}$ et $\Lambda = \{A \in \mathcal{P}_{p+1}(E) \,|\, a \notin A\}$. Il est clair que $\mathcal{P}_{p+1}(E) = \Gamma \cup \Lambda$ et que $\Gamma \cap \Lambda = \varnothing$. Or $\Lambda = \mathcal{P}_{p+1}(E \setminus \{a\})$ donc $\text{Card}\Lambda = \gamma_n^{p+1}$ et Γ est en bijection avec $\mathcal{P}_p(E \setminus \{a\})$ [b] donc $\text{Card}\Gamma = \gamma_n^p$. Par conséquent,

$$\begin{aligned} \text{Card}\mathcal{P}_{p+1}(E) &= \text{Card}\Gamma + \text{Card}\Lambda \\ &= \gamma_n^{p+1} + \gamma_n^p \\ &= \gamma_{n+1}^{p+1} \end{aligned}$$

Théorème

Pour $n \in \mathbb{N}$ et $0 \leqslant p \leqslant n$,

$$\gamma_n^p = \frac{n!}{p!\,(n-p)!}$$

Démonstration Soit H_n : « $\forall p \in [\![0, n]\!]$, $\gamma_n^p = \binom{n}{p}$ ».

- H_0 est vrai car $\gamma_0^0 = 1 = \binom{0}{0}$.
- Soit $n \in \mathbb{N}$. Supposons que H_n est vrai. Soit $p \in [\![0, n+1]\!]$.
  - Si $p = 0$, $\gamma_0^{n+1} = 1 = \binom{n+1}{0}$.
  - Si $p = n+1$, $\gamma_{n+1}^{n+1} = 1 = \binom{n+1}{n+1}$.
  - Si $p \in [\![0, n+1]\!] \setminus \{0, n+1\}$, alors

$$\begin{aligned} \gamma_{n+1}^p &= \gamma_{n+1}^{(p-1)+1} \\ &= \gamma_{n+1}^{p-1} + \gamma_n^p \\ &= \binom{n}{p-1} + \binom{n}{p} \\ &= \binom{n+1}{p} \end{aligned}$$

a. Une partie ne peut être de cardinal p et q avec $p \neq q$.

b. Via l'application $X \in \mathcal{P}_p(E \setminus \{a\}) \longrightarrow X \cup \{a\} \in \Gamma$ de réciproque $Y \in \Gamma \longrightarrow Y \setminus \{a\} \in \mathcal{P}_p(E \setminus \{a\})$.

Exercice Calculer

$$S = \sum_{A \in P} \sum_{k \in A} k$$

avec $P = \mathcal{P}([\![1, n]\!])$.

1ère méthode Pour $A \in \mathcal{P}([\![1, n]\!])$, on note $\overline{A} = \mathcal{P}([\![1, n]\!]) \setminus A$. L'application $A \xrightarrow{\psi} \overline{A}$ est une bijection de $\mathcal{P}([\![1, n]\!])$ car $\psi \circ \psi = \mathrm{Id}_{\mathcal{P}([\![1,n]\!])}$. Ainsi,

$$\begin{aligned}
S &= \sum_{A \in P} \left(\sum_{k \in \overline{A}} k \right) \\
2S &= \sum_{A \in P} \sum_{k \in \overline{A}} k + \sum_{A \in P} \sum_{k \in A} k \\
&= \sum_{A \in P} \left(\sum_{k \in \overline{A}} k + \sum_{k \in A} k \right) \\
&= \sum_{A \in P} \sum_{A \cup \overline{A}} k \quad \text{car } A \cap \overline{A} = \varnothing \\
&= \sum_{A \in P} \sum_{k \in [[1,n]]} k \\
&= \sum_{A \in P} \frac{n(n+1)}{2} \\
&= \frac{n(n+1)}{2} \sum_{A \in P} 1 \\
&= 2^n \frac{n(n+1)}{2}
\end{aligned}$$

Ainsi, $S = 2^{n-2} n(n+1)$.

2ème méthode Soit $k \in [[1, n]]$. k apparaît dans S autant de fois qu'il existe de parties A de $[[1, n]]$ qui contient k. Donc k apparaît dans S 2^{n-1} fois car $\{A \in P | k \in A\}$ est en bijection avec $\mathcal{P}([[1, n]]) \setminus \{k\}$ donc

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

4.2.5 Ensemble des applications entre deux ensembles finis

Soient E et F deux ensembles finis. Alors $\mathcal{F}(E, F)$ est fini et $\mathrm{Card}\mathcal{F}(E, F) = (\mathrm{Card}F)^{\mathrm{Card}E}$. Ainsi on note $\mathcal{F}(E, F) = F^E$.

Démonstration Soit H_n : « Si E est fini de cardinal n, et si F est fini, alors $\mathcal{F}(E, F)$ est fini et $\mathrm{Card}\mathcal{F}(E, F) = (\mathrm{Card}F)^n$ ».

- H_0 est vrai : si $E = \varnothing$, il y a une seule application de E dans F qui est $(\varnothing, F, \varnothing)$ donc $\mathcal{F}(\varnothing, F)$ est fini et

$$\mathrm{Card}\mathcal{F}(\varnothing, F) = 1 = (\mathrm{Card}F)^0$$

- Soit $n \in \mathbb{N}$, supposons que H_n est vrai et montrons H_{n+1}. Soit E un ensemble de cardinal $n + 1$, donc $E \neq \varnothing$ et soit F est ensemble fini.

- Si $F=\varnothing$, il n'y a pas d'applications de E dans $\varnothing$ donc $\mathcal{F}(E,\varnothing)=\varnothing$ est fini et de cardinal $0=0^{n+1}$.
- Si $F\neq\varnothing$, soit $a\in E$. Pour $b\in F$, $\Omega=\{f\in\mathcal{F}(E,F)\,|\,f(a)=b\}$. Il est clair que $\mathcal{F}(E,F)$ est réunion de divers Ω_b lorsque b décrit F et que ces ensembles sont deux à deux disjoints :

$$b\neq c\Leftrightarrow\Omega_b\neq\Omega_c$$

Pour $b\in F$, Ω_b est en bijection avec $\mathcal{F}(E\backslash\{a\},F)$ [a] donc $E\backslash\{a\}$ est fini de cardinal n donc, d'après l'hypothèse de récurrence, $\mathcal{F}(E\backslash\{a\},F)$ est fini et $\mathrm{Card}\mathcal{F}(E\backslash\{a\},F)=(\mathrm{Card}F)^n$ donc

$$\mathrm{Card}\Omega_b=\mathrm{Card}\mathcal{F}(E\backslash\{a\},F)=(\mathrm{Card}F)^n$$

Par conséquent et par réunion d'ensembles finis, $\mathcal{F}(E,F)$ est fini et

$$\begin{aligned}\mathrm{Card}\mathcal{F}(E,F) &= \sum_{b\in F}\mathrm{Card}\Omega_b\\ &= \sum_{b\in F}(\mathrm{Card}F)^n\\ &= (\mathrm{Card}F)^n\sum_{b\in F}1\\ &= (\mathrm{Card}F)^n\cdot\mathrm{Card}F\\ &= (\mathrm{Card}F)^{n+1}\end{aligned}$$

Autre méthode Prenons $E=[\![1,n]\!]$ et $F=[\![1,p]\!]$ avec $n,p\in\mathbb{N}^*$. Se donner une application f de $[\![1,n]\!]$ dans $[\![1,p]\!]$ revient à se donner le n-uple [b] $(f(1),f(2),\ldots,f(n))$ qui est élément de $[\![1,p]\!]^n$. $\mathcal{F}([\![1,n]\!],[\![1,p]\!])$ est en bijection avec $[\![1,p]\!]^n$ [c] donc $\mathcal{F}([\![1,n]\!],[\![1,p]\!])$ est fini et de cardinal $(\mathrm{Card}\,[\![1,p]\!])^n=p^n$.

4.2.6 Injections entre deux ensembles finis

Définition ensembliste des arrangements probabilistes Si E et F sont deux ensembles finis, notons $\mathcal{I}(E,F)$ l'ensemble des application injectives de E dans F. $\mathcal{I}(E,F)\subset\mathcal{F}(E,F)$ donc $\mathcal{I}(E,F)$ est fini et de cardinal plus petit que p^n (où $p=\mathrm{Card}F$ et $n=\mathrm{Card}E$). Ainsi on notera $A_p^n=\mathrm{Card}\mathcal{I}(E,F)$. Ce cardinal ne dépend que de n et de p, et non de la nature des éléments de E ou de F.

- Si $n>p$, il n'y a pas d'injections de E dans F donc $A_p^n=0$.
- Supposons que E et F sont deux ensembles non vides, c'est-à-dire que $n\geqslant 1$ et $p\geqslant 1$ et $n\leqslant p$. Soit $a\in E$, alors $\forall b\in F$, on appelle $\Omega_b=\{f\in\mathcal{I}(E,F)\,|\,f(a)=b\}$. $\mathcal{I}(E,F)$ est réunion disjointe des divers Ω_b lorsque b décrit F. De plus à b fixé, Ω_b est en bijection avec l'ensemble des applications de $E\backslash\{a\}$ dans $F\backslash\{b\}$. Ainsi, $\mathrm{Card}\Omega_b=A_{n-1}^{p-1}$. Or

$$\begin{aligned}A_p^n &= \sum_{b\in F}\mathrm{Card}\Omega_b\\ &= \sum_{b\in F}A_{p-1}^{n-1}\\ &= A_{p-1}^{n-1}\sum_{b\in F}1\\ &= pA_{p-1}^{n-1}\end{aligned}$$

Or pour $p\in\mathbb{N}^*$, $A_p^1=p$ donc

$$A_p^n=pA_{p-1}^{n-1}=p(p-1)A_{p-2}^{n-2}=\cdots=p(p-1)(p-2)\cdots(p-(n-2))A_{p-(n-1)}^{n-(n-1)}=\frac{p!}{(p-n)!}$$

a. Via $g\in F\longrightarrow\begin{pmatrix}E\longrightarrow F\\ a\longmapsto b\\ x\neq a\longmapsto g(x)\end{pmatrix}\in\Omega_b$.

b. Pour comprendre ce terme barbare, souvenons nous qu'on 2-uple est un couple et qu'un 3-uple est un triplet, par exemple.

c. Via $f\in\mathcal{F}([[1,n]],[[1,p]])\longrightarrow(f(1),f(2),\ldots,f(n))\in[[1,p]]^n$.

Montrons ce résultat de manière rigoureuse. Soit H_p : « $\forall n \in [\![0,p]\!]$, $A_p^n = \dfrac{p!}{(n-p)!}$ ».

- H_0 est vrai : il y a une seule application de $\varnothing$ dans $\varnothing$, injective de surcroît. Ainsi

$$A_0^0 = 1 = \frac{0!}{(0-0)!}$$

- Soit $p \in \mathbb{N}$. Supposons que H_p est vrai et montrons H_{p+1}. Soit $n \in [\![0,p+1]\!]$.
  - Si $n = 0$, $A_{p+1}^0 = 1$ et $\frac{(p+1)!}{(p+1-0)!} = 1$.
  - Si $n \geqslant 1$,

$$\begin{aligned} A_{p+1}^n &= (p+1)\, A_p^{n-1} \\ &= (p+1)\, \frac{p!}{(p-(n-1))!} \\ &= \frac{(p+1)!}{(p+1-n)!} \end{aligned}$$

Autre démonstration (à ressortir en colle) Soit $1 \leqslant n \leqslant p$. Pour fabriquer une injection de $[\![1,n]\!]$ dans $[\![1,p]\!]$, il y a :

- p façons de choisir $f(1)$;
- $p-1$ façons de choisir $f(2)$;
- $\ldots$;
- $p-n+1$ façons de choisir $f(n)$.

Soit au total $p(p-1)(p-2)\cdots(p-n+1)$ façons de définir f.

On a donc :

$$A_p^n = \frac{p!}{(p-n)!}$$

Cas particulier Si E est fini de cardinal n, il y a $A_n^n = n!$ injections de E dans E.

Remarque La lettre A vient du mot arrangement : si X est un ensemble fini de cardinal p et si $n \in [\![1,p]\!]$, on appelle n-arrangement d'éléments de X toute liste $(x_1, x_2, \ldots, x_n)$ d'éléments de X tous distincts. Se donner une telle liste, c'est se donner une injection de $[\![1,n]\!]$ dans X, il y a donc A_p^n tels arrangements.

4.3 Applications et ensembles finis

4.3.1 Petite histoire

Soit E un ensemble fini non vide.

Soit F un ensemble quelconque et soit $f : E \longrightarrow F$ et $\tilde{f} : \begin{array}{c} E \longrightarrow f(E) \\ x \longrightarrow f(x) \end{array}$. Cette dernière application est surjective donc $f(E)$ est fini et $\mathrm{Card} f(E) \leqslant \mathrm{Card} E$.

- Si f est injective, $\tilde{f}$ est bijective donc $\mathrm{Card} f(E) = \mathrm{Card} E$.
- Si f n'est pas injective, $\exists a, b \in E$ tels que $f(a) = f(b)$ et $a \neq b$. Soit $g : \begin{array}{c} E \backslash \{a\} \longrightarrow f(E) \\ x \longmapsto f(x) \end{array}$, g reste surjective donc $\mathrm{Card} f(E) \leqslant \mathrm{Card}(E \backslash \{a\}) < \mathrm{Card} E$.

Ainsi, on a les résultats suivants :

- $f(E)$ est fini et $\mathrm{Card} f(E) \leqslant \mathrm{Card} E$.
- $\mathrm{Card} f(E) = \mathrm{Card} E$ si et seulement si f est injective.

Supposons que F est finie et soit $f : E \longrightarrow F$, $f(E) \subset F$ donc $\text{Card} f(E) \leqslant \text{Card} F$ donc $\text{Card} f(E) \leqslant \min(\text{Card} E, \text{Card} F)$ en toute généralité.

De plus,

$$\begin{aligned} f \text{ est surjective} &\Leftrightarrow f(E) = F \\ &\Leftrightarrow \text{Card} f(E) = \text{Card} F \end{aligned}$$

Si $\text{Card} E < \text{Card} F$, f ne peut pas être injective car $\text{Card} f(E) \leqslant \text{Card} E < \text{Card} F$. De même, si $\text{Card} F < \text{Card} E$, f ne peut pas être injective car $\text{Card} f(E) \leqslant \text{Card} F < \text{Card} E$.

Supposons de plus que $\text{Card} E = \text{Card} F$ ce qui est vrai en particulier lorsque $E = F$.

- Soit $f : E \longrightarrow F$ injective. Alors f est bijective car $\text{Card} f(E) = \text{Card} E = \text{Card} F$ donc f est surjective.
- Soit $f : E \longrightarrow F$ surjective. Alors $\text{Card} f(E) = \text{Card} F = \text{Card} E$ donc f est injective donc bijective.

4.3.2 Théorème

Soient E, F deux ensembles finis de même cardinal et $f : E \longrightarrow E$. Les assertions suivantes sont équivalentes [a] :

(1) f est injective.

(2) f est surjective.

(3) f est bijective.

a. Ou LASSE pour les intimes.

En particulier [d], si E est un ensemble fini et $f : E \longrightarrow E$, alors

$$f \text{ est injective} \Leftrightarrow f \text{ est surjective} \Leftrightarrow f \text{ est bijective}$$

4.3.3 Permutations d'un ensemble fini

Vocabulaire

- Une bijection de E dans E s'appelle une permutation. On note $\mathfrak{S}(E)$ ou $S(E)$ l'ensemble des permutation de E.
- Si E est un ensemble fini de cardinal $n \in \mathbb{N}^*$. On a $\mathfrak{S}(E) = \mathcal{I}(E, E)$ donc $\text{Card}\mathfrak{S}(E) = n!$. Il y a $n!$ permutation si E est fini de cardinal n.
- Pour $n \in \mathbb{N}^*$, on note $S_n = \mathfrak{S}(\llbracket 1, n \rrbracket)$.

Exemples

- $S_2 = \left\{\text{Id}_{\llbracket 1,2 \rrbracket}, \tau_{12}\right\}$ où $\tau_{12} : \begin{array}{l} 1 \longmapsto 2 \\ 2 \longmapsto 1 \end{array}$.
- $S_3 = \left\{\text{Id}_{\llbracket 1,3 \rrbracket}, \tau_{12}, \tau_{13}, \tau_{23}, \gamma, \sigma\right\}$ avec :

$$\tau_{12} : \begin{array}{l} 1 \longmapsto 2 \\ 2 \longmapsto 1 \\ 3 \longmapsto 3 \end{array} \quad \tau_{13} : \begin{array}{l} 1 \longmapsto 3 \\ 2 \longmapsto 2 \\ 3 \longmapsto 1 \end{array} \quad \tau_{23} : \begin{array}{l} 1 \longmapsto 1 \\ 2 \longmapsto 3 \\ 3 \longmapsto 2 \end{array} \quad \gamma : \begin{array}{l} 1 \longmapsto 2 \\ 2 \longmapsto 3 \\ 3 \longmapsto 1 \end{array} \quad \sigma = \gamma \circ \gamma : \begin{array}{l} 1 \longmapsto 3 \\ 2 \longmapsto 1 \\ 3 \longmapsto 2 \end{array}$$

Propriétés de la composition $\circ$ est une loi de composition interne dans S_n, associative, admettant un neutre $\text{Id}_{\llbracket 1,n \rrbracket}$ et tout élément de S_n admet un inverse (application réciproque). Ainsi, $(S_n, \circ)$ est un groupe.

Voici la table de composition pour $n = 3$:

d. Ce théorème est aussi appelé « *principe de fainéantise. Bah oui si vous démontrez l'une vous les avez tous !* »

$\circ$	Id	τ_{12}	τ_{13}	τ_{23}	γ	σ
Id	Id	τ_{12}	τ_{13}	τ_{23}	γ	σ
τ_{12}	τ_{12}	Id	σ	γ	τ_{23}	τ_{13}
τ_{13}	τ_{13}	γ	Id	σ	τ_{12}	τ_{23}
τ_{23}	τ_{23}	σ	γ	Id	τ_{13}	τ_{12}
γ	γ	τ_{13}	τ_{23}	τ_{13}	σ	Id
σ	σ	τ_{23}	τ_{12}	τ_{13}	Id	γ

Transpositions Soit E un ensemble et $a, b \in E$, $a \neq b$. On note τ_{ab} la transposition qui échange a en b et laisse les autres points invariants.

$$\begin{array}{rl} \tau_{ab}: & E \longrightarrow E \\ & a \longmapsto b \\ & b \longmapsto a \\ & x \notin \{a,b\} \longmapsto x \end{array}$$

On remarque que $\tau_{ab} \in \mathfrak{S}(E)$ car $\tau_{ab} \circ \tau_{ab} = \mathrm{Id}_E$.

Soit $f : E \longrightarrow E$. Un point fixe de f est par définition un $x \in E$ tel que $f(x) = x$.

Théorème : écriture en composition

Soit E un ensemble fini de cardinal supérieur ou égal à 2 et $f \in \mathfrak{S}(E)$. Alors f peut s'écrire comme une composée de transpositions.

Démonstration Soit X l'ensemble des points fixes de f.

- Si $X = E$, $f = \mathrm{Id}_E$. On note que X est stable par $f : x \in X \longrightarrow f(x) \in X$. En effet, si $x \in X$, $f(x) = x \in X$. $E \backslash X$ est aussi stable par $f : f(E \backslash X) \subset E \backslash X$. Soit $x \in E \backslash X$, si $f(x) \in X$, alors $f(f(x)) = f(x)$. Or f est injective donc $f(x) = x$ donc $x \in X$, ce qui est impossible.
- Supposons que $X \neq E$. Soit $x \in E \backslash X$, $x \neq f(x)$ et $g = \tau_{xf(x)} \circ f$. $g(x) = x$ et g est bijective par composition. Si y est un point fixe de f, alors $y \neq x$ et $y \neq f(x)$ puisque x et $f(x)$ appartiennent à $E \backslash X$. Ainsi, $g(y) = \tau_{xf(x)} \circ f(y) = y$ donc les points fixes de f sont inclus dans les points fixes de g donc g a au moins un point fixe de plus que f.

En réitérant ce procédé, on parvient à obtenir un ensemble de points fixes égal à E : on fabrique l'identité en composant f avec des transpositions. On peut donc écrire f sous la forme :

$$\tau_1 \circ \tau_2 \circ \cdots \circ \tau_R \circ f = \mathrm{Id}_E \Leftrightarrow f = \tau_R \circ \tau_{R-1} \circ \cdots \circ \tau_1$$

où $\tau_1, \tau_2, \ldots, \tau_R$ sont des transpositions. En effet $\tau_1^{-1} = \tau_1$, $\tau_2^{-1} = \tau_2$,... du fait de la nature des transpositions.

Exemple Soit $f \in S_7$ définie par

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 7 & 1 & 2 & 6 & 4 \end{pmatrix}$$

Alors :

$$\begin{aligned} \tau_{15} \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 7 & 5 & 2 & 6 & 4 \end{pmatrix} &\Rightarrow \tau_{23} \circ \tau_{15} \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 7 & 5 & 3 & 6 & 4 \end{pmatrix} \\ &\Rightarrow \tau_{37} \circ \tau_{23} \circ \tau_{15} \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 5 & 7 & 6 & 4 \end{pmatrix} \\ &\Rightarrow \tau_{45} \circ \tau_{37} \circ \tau_{23} \circ \tau_{15} \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 7 & 6 & 5 \end{pmatrix} \\ &\Rightarrow \tau_{57} \circ \tau_{45} \circ \tau_{37} \circ \tau_{23} \circ \tau_{15} \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} = \mathrm{Id}_{S_7} \end{aligned}$$

Donc $f = \tau_{15} \circ \tau_{23} \circ \tau_{37} \circ \tau_{45} \circ \tau_{57}$.

4.3.4 Cycles

Soit E un ensemble fini et $f \in \mathfrak{S}(E)$, $X = \{x \in E | x = f(x)\}$ et $A = E \backslash X$.
f est une permutation circulaire si $A \neq \varnothing$ et si les seules parties de A stables par f sont $\varnothing$ et A.

Exemples de cycles

- Toute transposition est un cycle. Soient $a \neq b$, $a, b \in E$ et $f = \tau_{ab}$. Alors $X = E \backslash \{a, b\}$ et $A = \{a, b\}$. Alors $f(\{a\}) = \{b\} \neq \{a\}$ et $f(\{b\}) = \{a\} \neq \{b\}$.
- Plus généralement, soit $p \geqslant 2$ et $a_1, a_2, \ldots, a_n$ des éléments distincts de E. On définit f par :

$$\begin{aligned} a_1 &\longmapsto a_2 \\ a_2 &\longmapsto a_3 \\ &\vdots \\ a_{p-1} &\longmapsto a_p \\ a_p &\longmapsto a_1 \end{aligned}$$

  et pour $x \notin \{a_1, a_2, \ldots, a_n\}$, $f(x) = x$. Ici $X = E \backslash \{a_1, a_2, \ldots, a_n\}$ et $A = \{a_1, a_2, \ldots, a_n\}$. Alors f est un cycle de support $\{a_1, a_2, \ldots, a_n\}$.

Propriétés

- Si B est une partie non vide de A stable par f, alors $A = B$.
- Pour $k \in \mathbb{N}^*$, $f^k = \underbrace{f \circ f \circ \cdots \circ f}_{k \text{ fois}}$, $f^0 = \mathrm{Id}_E$ et $f^{-k} = \left(f^{-1}\right)^k$.

Une meilleure expression de la partie A d'un cycle On a supposé que $A \neq \varnothing$, alors $\mathrm{Card} A \geqslant 2$. Si $a \in A$, $f(a) \in A$ et $a \neq f(a)$.

Soit $a \in A$ et soit $B = \left\{f^k(a) \,|\, k \in \mathbb{N}^*\right\}$. Alors $B \subset A$:

- Si $f^0(a) = a$, $a \in A$.
- Supposons que $f^k(a) \in A$ pour un k. Alors $f(k+1) = f \circ f^k(a) \in A$ par A est stable par f.

Ainsi $B \neq \varnothing$ car $a \in B$ et B est stable par f car $\forall k \in \mathbb{N}$, $f\left(f^k(a)\right) = f^{k+1}(a) \in B$. Ainsi, $A = B$ d'après la propriété énoncée un peu plus haut.

L'application $k \in \mathbb{N} \longrightarrow f^k(a) \in A$ ne peut pas être injective car $\mathbb{N}$ est infini et A est fini. Ainsi, il existe $k, l \in \mathbb{N}$ tels que $k < l$ et

$$\begin{aligned} f^k(a) = f^l(a) &\Leftrightarrow f^{-k}\left(f^k(a)\right) = f^{-k}\left(f^l(a)\right) \\ &\Leftrightarrow f^{k-l}(a) = a \end{aligned}$$

On peut donc poser $d(a) = \min\{m \in \mathbb{N}^* | f^m(a) = a\}$.

- Il est clair que $\left\{a, f(a), \ldots, f^{d(a)}(a)\right\} \subset B$.
- Réciproquement, si $k \in \mathbb{N}$, $k = qd(a) + r$ avec $q \in \mathbb{N}$ et $0 \leqslant r \leqslant d(a)$. Alors

$$\begin{aligned} f^k(a) &= f^{qd(a)+r}(a) \\ &= f^r \circ f^{qd(a)}(a) \\ &= f^r(a) \end{aligned}$$

  En effet, on montre par récurrence que $\forall l \in \mathbb{N}$, $f^{ld(a)}(a) = a$. On en déduit que

$$f^k(a) = f^r(a) \in \left\{a, f(a), \ldots, f^{d(a)-1}(a)\right\}$$

  Finalement, $A = B = \left\{a, f(a), \ldots, f^{d(a)-1}(a)\right\}$. Enfin, si pour $0 \leqslant l \leqslant k \leqslant d(a) - 1$:

$$f^l(a) = f^k(a) \Leftrightarrow f^{l-k}(a) = a$$

Mais $1 \leqslant l-k \leqslant d(a)$, ce qui est absurde au regard de la définition de $d(a)$. Les éléments de $\left\{a, f(a), \ldots, f^{d(a)-1}(a\right.$ sont donc tous distincts et

$$\text{Card}\left\{a, f(a), \ldots, f^{d(a)-1}(a)\right\} = d(a) = \text{Card}A$$

Finalement, $d(a) = \text{Card}A$ ne dépend pas de l'élément a choisi.

Expression de f sous la forme d'une permutation circulaire Soit $p = \text{Card}A$. Alors $\forall a \in A$, $f^p(a) = a$ et $A = \left\{a, f(a), \ldots, f^{d(a)-1}(a)\right\}$. Fixons alors $a \in A$ et notons $x_k = f^{k-1}(a)$ avec $1 \leqslant k \leqslant p$. Soit le cycle :

$$\begin{array}{rl} \gamma : & x_k \longmapsto x_{k+1} \quad (1 \leqslant k \leqslant p-1) \\ & x_p \longmapsto x_1 \\ & y \notin A \longmapsto y \end{array}$$

Vérifions que $f = \gamma$. Soit $y \in E$:
- Si $y \notin A$, alors y est point fixe de f donc $f(y) = y = \gamma(y)$.
- Si $y \in A$, il existe $k \in \mathbb{N}$ tel que $1 \leqslant k \leqslant p$ et $y = x_k$. $f(x_p) = x_1 = \gamma(x_p)$ et pour tout $k < p$, $f(x_k) = x_{k+1} = \gamma(x_k)$.

Vocabulaire

Soit f un cycle, $A = E\backslash X$ où X est l'ensemble des points fixes par f. Alors :
- A est le support du cycle.
- $\text{Card}A$ est la longueur du cycle.

Dénombrement

(1) Combien y a-t-il de cycles de support $A \subset E$? Notons $A = \{a, x_1, x_2, \ldots, x_R\}$, $R \in \mathbb{N}^*$. Un cycle de support A s'écrit toujours $\gamma = \begin{pmatrix} a & y_1 & \ldots & y_R \end{pmatrix}$ où $\{y_{1,y_2,} \ldots y_R\} = \{x_1, x_2, \ldots, x_R\}$. On peut aussi écrire $\gamma = \left\{a, x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(R)}\right\}$ où σ est une permutation de $[\![1, R]\!]$. L'ensemble des cycles de support A est en bijection avec S_R : il y en a donc

$$n! = (\text{Card}A - 1)!$$

(2) Combien y a-t-il de cycles de longueur p, avec $p \in [\![2, \text{Card}E]\!]$? Il y a $\binom{\text{Card}E}{p}$ façons de choisir le support du cycle, autant qu'il existe de parties de E à p éléments. Le support A du cycle étant choisi, il y a $(p-1)!$ cycles de support A donc il y a au total

$$(p-1)!\binom{\text{Card}E}{p}$$

cycles de longueur p. En particulier, il y a $(n-1)!$ cycles de longueur n (ou n-cycles).

Expression d'une permutation comme une composition de cycles

Petite histoire Soient α, β deux cycles de supports A et B avec $A \cap B = \varnothing$. Alors

$$\alpha \circ \beta = \beta \circ \alpha$$

En effet, soit $x \in E$:
- Si $x \notin A \cup B$, alors $\alpha(x) = x$ et $\beta(x) = x$ donc $\alpha \circ \beta(x) = x$ et $\beta \circ \alpha(x) = x$.
- Si $x \in A$, alors $x \notin B$ donc $\beta(x) = x$ donc $\alpha \circ \beta(x) = \alpha(x)$. De plus A est stable par α donc $\alpha(x) \in A$ donc $\alpha(x) \notin B$ donc $\beta \circ \alpha(x) = \alpha(x)$.
- Même argument pour $x \in B$.

Et on termine en beauté !

Montrons que $\forall f \in \mathfrak{S}(E)$, f s'écrit comme un produit (au sens de la composition) de cycles dont les supports sont 2 à 2 disjoints. Un tel produit est commutatif donc unique à l'ordre des termes près.

Démonstration Soit $f \in \mathfrak{S}(E)$. Si $f = \mathrm{Id}_E$, on convient que f est un produit vide de cycles.
Supposons que $f \neq \mathrm{Id}_E$. On définit la relation $\mathcal{R}_f$ sur E en posant $\forall x, y \in E$,

$$xR_f y \Leftrightarrow \exists k \in \mathbb{Z} / y = f^k(x)$$

$\mathcal{R}_f$ est une relation d'équivalence sur E :

(1) Soit $x \in E$. $x = f^0(x)$.

(2) Soient $x, y \in E$ tels que $x\mathcal{R}_f y$. Alors $\exists k \in \mathbb{Z}$ tel que

$$\begin{aligned} y = f^k(x) &\Leftrightarrow x = f^{-k}(y) \\ &\Leftrightarrow y\mathcal{R}_f x \end{aligned}$$

(3) Soient $x, y, z \in E$ tels que $x\mathcal{R}_f y$ et $y\mathcal{R}_f z$. Alors $\exists k, l \in \mathbb{Z}$ tels que

$$y = f^k(x) \quad \text{et} \quad y = f^l(z) \Rightarrow z = f^{k+l}(x)$$

Donc $x\mathcal{R}_f z$.

Pour $x \in E$, on note $O_f(x)$ la classe d'équivalence de x pour $\mathcal{R}_f$. Alors $O_f(x) = \left\{y \in E | \exists k \in \mathbb{Z}, y = f^k(x)\right\}$.

- Si x est un point fixe par f, alors $f(x) = x$ donc $\forall n \in \mathbb{N}$, $f^n(x) = x$. De plus $f^{-1}(x) = x$ donc $\forall k \in \mathbb{N}$, $f^{-k}(x) = x$ donc $O_f(x) = \{x\}$.
- Réciproquement, si pour $x \in E$, $O_f(x) = x$, alors $f(x) \in O_f(x) = \{x\}$ donc $f(x) = x$ donc x est un point fixe par f.

Soit $\Omega = {}^{E}/_{\mathcal{R}_f}$ l'ensemble des classes d'équivalences de $\mathcal{R}_f$.Soit s Ω est fini car $\mathrm{Card}\Omega \leqslant \mathrm{Card}E$ (une classe d'équivalence correspond toujours à un élément). Comme $f \neq \mathrm{Id}_E$, au moins un point de E n'est pas fixe par f, donc au moins l'une des classes d'équivalence n'est pas réduite à un singleton.

Notons $C_1, C_2, \ldots, C_R$ avec $R \in \mathbb{N}^*$ les diverse classes d'équivalence non réduits à un singleton. Ainsi $C_i = O_f(x_i)$ où $x_i \in E$ et $f(x_i) \neq x_i$. Soit $a \in E$ tel que $f(a) \neq a$. $O_f(a) \subset E$ donc $O_f(a)$ est fini et $\mathrm{Card}O_f(a) \leqslant \mathrm{Card}E$ donc

$$k \in [\![1, n+1]\!] \longrightarrow f^k(a) \in O_f(a)$$

n'est pas injective, d'après le principe des tiroirs [a]. Ainsi, il existe $k, l \in \mathbb{N}$ tels que $1 \leqslant k \leqslant l \leqslant n+1$ et

$$f^k(a) = f^l(a) \Leftrightarrow f^{l-k}(a) = a$$

donc $\exists m \in [\![1, n]\!]$ tel que $f^m(a) = a$, et en notant $d = \min\{m \in \mathbb{N}^* | f^m(a) = a\}$, on a que l'ensemble $\left\{a, f(a), \ldots, f^{d-1}(a)\right\}$ est constitué d'éléments tous distincts et $O_f(a) = \left\{a, f(a), \ldots, f^{d-1}(a)\right\}$.

Ici, pour $1 \leqslant i \leqslant R$, il existe $d_i \in \mathbb{N}^*$ tel que

$$C_i = \left\{x_i, f(x_i), \ldots, f^{d_i - 1}(x_i)\right\}$$

et les éléments de C_i sont tous distincts. Posons le cycle $\gamma_i = \begin{pmatrix} x_i & f(x_i) & \cdots & f^{d_i-1}(x_i) \end{pmatrix}$, montrons que $f = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_R$.

Le support de γ_i est C_i pour $1 \leqslant i \leqslant R$ et $C_i \cap C_j = \varnothing$ pour $i \neq j$ donc les γ_i commutent entre eux deux à deux. Soit $x \in E$.

- Si $x \notin C_1 \cup C_2 \cup \cdots \cup C_R$, alors $O_f(x)$ est un singleton donc x est point fixe de f donc $f(x) = x$ et $\gamma_i(x) = x$ car $x \notin C_i$ pour tout $1 \leqslant i \leqslant R$. Alors

$$\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_R(x) = x$$

a. En effet $n + 1 \geqslant \mathrm{Card}E = n$.

– Si $x \in C_1 \cup C_2 \cup \cdots \cup C_R$, soit $i \in [\![1, R]\!]$ tel que $x \in C_i$. Pour $i \neq j$, $x \notin C_j$ donc

$$\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_{i-1} \circ \gamma_{i+1} \circ \cdots \circ \gamma_R (x) = x$$

Donc

$$\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_{i-1} \circ \gamma_i \circ \gamma_{i+1} \circ \cdots \circ \gamma_R (x) = \gamma_i (x)$$

Soit $k \in [\![0, d_i - 1]\!]$ tel que $x = f^k (x_i)$. Alors

$$\gamma_i (x) = \begin{cases} f^{k+1} (x_i) & \text{si } k < d_i - 1 \\ f (x_i) & \text{si } k = d_i \end{cases}$$

et $f (x) = f^{k+1} (x_i)$ donc on a bien, pour $k = d_i - 1$, $f^{d_i} (x_i) = x_i$ donc

$$\gamma_i (x) = f (x)$$

Exemples

– Prenons $E = [[1, 9]]$ et $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 9 & 7 & 5 & 2 & 6 & 1 & 4 & 8 \end{pmatrix}$. Alors $O_f (1) = \{1, 3, 7\}$ donc et $O_f (2) = \{2, 9, 8, 4, 5\}$ donc

$$f = \begin{pmatrix} 1 & 3 & 7 \end{pmatrix} \circ \begin{pmatrix} 2 & 9 & 8 & 4 & 5 \end{pmatrix}$$

– Pour $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 5 & 6 & 7 & 2 & 4 & 3 & 9 & 1 \end{pmatrix}$, $O_f (1) = \{1, 8, 9\}$, $O_f (2) = \{2, 5\}$ et $O_f (3) = \{3, 6, 4, 7\}$ donc

$$g = \begin{pmatrix} 1 & 8 & 9 \end{pmatrix} \circ \begin{pmatrix} 2 & 5 \end{pmatrix} \circ \begin{pmatrix} 3 & 6 & 4 & 7 \end{pmatrix}$$