Chapitre I

Ensembles

1.⁻ C'est quoi ?

a) Ensembles, quantificateurs

Définition I.1. On appelle **ensemble** toute collection (non ordonnée) d'objets distincts, appelés éléments.

Notation. $a \in E$ signifie que l'objet a est un élément de l'ensemble E.

La question qui va nous occuper dans un premier temps est la suivante : **comment décrire un ensemble ?** De prime abord, deux choix s'offrent à nous.

1. **Lister les éléments de l'ensemble.**

$$E = \{\clubsuit, \nabla, 4\}\,.$$

2. **Caractériser l'ensemble par une propriété.**

$$E = \{\ \underbrace{x \in \mathbb{R}}_{\text{cas de base}}\ \mid \underbrace{x > 0}_{\text{prédicat}}\}\,.$$

3. **Comme image d'une application.**

$$E = \{x^2 + 1 \,|\, x \in [0, 1]\}\,.$$

Vocabulaire. Un ensemble ne contenant qu'un seul élément est appelé **singleton.**

◇ **Quantificateurs**

Définition I.2. On définit les deux **quantificateurs suivants** :

1. le **quantificateur universel**, noté "$\forall$"
2. le **quantificateur existentiel**, noté "$\exists$"

On appelle **phrase** (ou expression) **quantifiée** toute propriété faisant intervenir des quantificateurs.

Signification des quantificateurs :
Soit P une assertion portant sur les éléments d'un ensemble $\mathbb{E}$. On définit alors de nouvelles assertions :

1. $\forall x \in \mathbb{E}, P(x)$, qui signifie que tous les éléments de $\mathbb{E}$ vérifient la propriété P.
2. $\exists x \in \mathbb{E}, P(x)$, qui signifie qu'il existe un élément de $\mathbb{E}$ qui vérifie la propriété P.

De plus, si un **unique** élément de $\mathbb{E}$ vérifie P, on note : $\exists! x \in \mathbb{E}, P(x)$.

➠ **Exemple I.1.**

$$F = \{n \in \mathbb{N} \,|\, \exists p \in \mathbb{N},\ n = 2p\}$$

décrit l'ensemble des entiers naturels pairs.

◇ Échange de quantificateurs

Soit P une propriété dépendant de deux paramètres $x \in \mathbb{E}$ et $y \in \mathbb{F}$. Alors les deux propriétés suivantes sont équivalentes :

1. $\exists x \in \mathbb{E}, \exists y \in \mathbb{F}, P(x, y)$
2. $\exists y \in \mathbb{F}, \exists x \in \mathbb{E}, P(x, y)$

Il est ainsi possible au sein d'une phrase quantifiée d'intervertir deux quantificateurs existentiels sans en changer le sens. De la même façon, sont équivalents :

1. $\forall x \in \mathbb{E}, \forall y \in \mathbb{F}, P(x, y)$
2. $\forall y \in \mathbb{F}, \forall x \in \mathbb{E}, P(x, y)$

➠ **Exemple I.2.** Pour $x, y \in \mathbb{Z}$, on définit $P(x, y) = x|y$.

En revanche, il est **impossible** d'échanger la place d'un quantificateur universel et d'un quantificateur existentiel, comme nous le verrons ci-après. Les deux équivalences ci dessus donnent un sens aux notations "$\exists (x, y) \in \mathbb{E} \times \mathbb{F}, P(x, y)$" et "$\forall (x, y) \in \mathbb{E} \times \mathbb{F}, P(x, y)$".

◇ Dépendances

Le problème des dépendances dans les phrases quantifiées est très important en mathématiques. Par exemple, considérons les deux assertions suivantes, portant sur une fonction $f : \mathbb{R} \to \mathbb{R}$:

(1) $\forall x \in \mathbb{R}, \quad \exists y \in \mathbb{R}_+, \quad y = x^2$;

(2) $\exists y \in \mathbb{R}_+, \quad \forall x \in \mathbb{R}, \quad y = x^2$.

Ces deux assertions ne sont **absolument pas** équivalentes ! Pourtant, la seule différence entre ces deux assertions est la place occupée par le "$\forall x \in \mathbb{R}$"...

Le noeud du problème réside dans les **dépendances**. Dans l'assertion (1), le réel y dépend de x : en effet, ce que signifie cette phrase quantifiée, c'est que si on fixe x dans $\mathbb{R}$, **alors** on va pouvoir trouver un y tel que la propriété soit vérifiée. Tandis que (2) nous indique que l'on va pouvoir trouver y tel que la propriété soit vraie pour tous x.

Conséquence :
Lorsque l'on manipule des phrases quantifiées, il faut apporter une attention toute particulière aux dépendances des paramètres entre eux afin d'éviter de monumentales erreurs d'interprétation. Une règle efficace en pratique est la suivante : les "$\exists$" dépendent des "$\forall$" qui les précédent. Par exemple, dans $\exists z,\, \forall t,\, \exists q, P(z,t,q)$ le paramètre q dépend de t alors que z et t ne dépendent d'aucun des autres paramètres (et ne sont pas dépendant entre eux).

◇ Difficultés

Cette définition naïve n'est pas sans risques. L'une des complications rencontrées, appelée **paradoxe de Russel**, peut s'énoncer de la façon suivante : soit $\mathscr{E} = \{E \text{ ensemble} \,|\, E \notin E\}$; a–t–on $\mathscr{E} \in \mathscr{E}$? Peu importe que l'on suppose que ce soit vrai ou faux, on arrive à une contradiction.

Pour éviter ce type de difficulté, on prendra toujours gare à définir nos ensembles à partir d'un cas de base précis, clair et sans ambiguïté.

b) Concepts élémentaires de théorie des ensembles

◇ Égalité

Axiome A. Deux ensembles sont égaux si et seulement si ils ont les mêmes éléments.

➠ **Exemple I.3.**
- $\{0,1,2\} = \{2,0,1\}$;
- $\{1,2\} \neq \{2,12\}$.

Par conséquent, la **seule** méthode valable pour démontrer que deux ensembles A et B sont égaux est la suivante :
- se donner $x \in A$ et démontrer que $x \in B$;
- réciproquement, se donner $x \in B$ et montrer que $x \in A$.

◇ Inclusion

Définition I.3. On dit qu'un ensemble A est **inclus** dans un ensemble B si $\forall x \in A,\ x \in B$.

Notation. $A \subset B$

✖ **Attention :** ne pas confondre inclusion et appartenance : $1 \in \mathbb{R}$, $\{1\} \subset \mathbb{R}$.

Proposition I.1. Soient A, B, C des ensembles. Alors :
(i) $A \subset A$ **[reflexivité]** ;
(ii) $(A \subset B) \wedge (B \subset A) \Leftrightarrow (A = B)$ **[antisymétrie]** ;
(iii) $(A \subset B) \wedge (B \subset C) \Rightarrow (A \subset C)$ **[transitivité]**.

Démonstration. Immédiat. □

✌ **Remarque I.1.** Le point (ii) nous indique que pour démontrer une égalité d'ensembles, il faut démontrer deux inclusions. **À retenir.**

◇ Zoologie des ensembles classiques

Axiome B. Il existe un ensemble ne contenant aucun élément, appelé **ensemble vide** et noté $\emptyset$.

✌ **Remarque I.2.** Si P est un prédicat faux sur un ensemble E, alors $\{x \in E \,|\, P(x)\} = \emptyset$. Par exemple, $\emptyset = \{x \in \mathbb{R} \,|\, x^2 < 0\}$.

Profitons de ce paragraphe pour rappeler quelques définitions logiquement vues dans une vie antérieure.

— $\mathbb{N}$ est l'ensemble des entiers naturels.

— $\mathbb{Z}$ est l'ensemble des entiers relatifs, *i.e*

$$\mathbb{Z} = \{a - b \,|\, a, b \in \mathbb{N}\} \,.$$

— $\mathbb{D}$ est l'ensemble des nombres décimaux, soit :

$$\mathbb{D} = \left\{ \frac{m}{10^n} \;\middle|\; m \in \mathbb{Z},\, n \in \mathbb{N} \right\} \,.$$

— $\mathbb{Q}$ est l'ensemble des nombres rationnels, soit :

$$\mathbb{Q} = \left\{ \frac{p}{q} \;\middle|\; p \in \mathbb{Z},\, q \in \mathbb{N}^* \right\} \,.$$

— $\mathbb{R}$ est l'ensemble des nombres réels.

— $\mathbb{C}$ est l'ensemble des nombres complexes, soit :

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

où i est tel que $i^2 = -1$.

Rappelons au passage que l'on a la chaine d'inclusions suivante :

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{D} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \,.$$

◇ Parties d'un ensemble

Axiome C. Soit E un ensemble. Alors il existe un unique ensemble, noté $\mathscr{P}(E)$, tel que :

$$A \in \mathscr{P}(E) \Leftrightarrow A \subset E \,.$$

Cet ensemble est appelé **ensembles des parties de** E.

✌ **Remarque I.3.**

— Il s'agit donc d'un ensemble d'ensembles ...

— Quel que soit l'ensemble E, on a toujours $\emptyset \in \mathscr{P}(E)$ et $E \in \mathscr{P}(E)$.

➠ **Exemple I.4.**

— $\mathscr{P}(\emptyset) = \{\emptyset, \{\emptyset\}\}$.

— $\mathscr{P}(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

✌ **Remarque I.4.** La construction "moderne" de l'ensemble $\mathbb{N}$ des entiers naturels s'obtient via les "ensembles parties itérés" de l'ensemble vide, *i.e* les $\mathscr{P}(\mathscr{P}(\ldots \ldots \mathscr{P}(\emptyset)))$.

2.⁻ Opérations sur les ensembles

a) Réunion

Définition I.4. Soient A, B deux sous–ensembles d'un ensemble E ; on appelle **réunion** de A et B l'ensemble

$$\{x \in E \,|\, (x \in A) \vee (x \in B)\} .$$

Notation. $A \cup B$

➠ **Exemple I.5.** $\{1, 2\} \cup \{2, 7\} = \{1, 2, 7\}$.

✌ **Remarque I.5.** De façon plus générale, si $(A_i)_{i\in I}$ est une famille d'ensembles indexée par un ensemble I, ce qui signifie qu'à chaque élément i de I on associe un unique sous–ensemble A_i d'un ensemble E, on pose :

$$\bigcup_{i\in I} A_i = \{x \in E \,|\, \exists i \in I,\, x \in A_i\} .$$

Il s'agit du plus petit sous–ensemble de E contenant tous les A_i. Notons que I peut tout à fait être infini ; on peut par exemple montrer assez aisément (démontrer deux inclusions) que

$$\bigcup_{n\in\mathbb{N}^*} \left[0, 1 - \frac{1}{n}\right[= [0, 1[.$$

Notation. Si $I = \{1, \ldots, n\}$, on notera $\bigcup_{i=1}^{n} A_i$ la réunion $\bigcup_{i\in I} A_i$.

Proposition I.2. Soient A, B, C, D quatre ensembles. Alors :

(i) $A \cup B = B \cup A$ **[commutativité]** ;

(ii) $(A \cup B) \cup C = A \cup (B \cup C)$ **[associativité]** ;

(iii) $A \cup \emptyset = A$ **[$\emptyset$ est neutre]** ;

(iv) $A \cup A = A$ **[idempotence]** ;

(v) $(A \cup B = A) \Leftrightarrow (B \subset A)$;

(vi) $(A \subset B) \wedge (C \subset D) \Rightarrow (A \cup C \subset B \cup D)$.

Démonstration. Immédiat en utilisant les propriétés du connecteur $\vee$. Un dessin peut être utile pour (v) et (vi). □

b) Intersection

Définition I.5. Soient A, B deux sous–ensembles d'un ensemble E ; on appelle **instersection** de A et B l'ensemble

$$\{x \in E \,|\, (x \in A) \wedge (x \in B)\} .$$

Notation. $A \cap B$

Exemple I.6.
— $\{1,2\} \cap \{2,7\} = \{2\}$;
— $\{1,3\} \cap \{2,7\} = \emptyset$.

Vocabulaire. Deux ensembles A, B tels que $A \cap B = \emptyset$ sont dits **disjoints**.

Remarque I.6. De façon plus générale, si $(A_i)_{i\in I}$ est une famille de sous–ensembles d'un ensemble E indexée par un ensemble I, on pose :

$$\bigcap_{i\in I} A_i = \{x \in E \,|\, \forall i \in I,\, x \in A_i\} \ .$$

Il s'agit du plus grand sous–ensemble de E contenu dans tous les A_i. Notons que I peut tout à fait être infini ; on peut par exemple montrer assez aisément (démontrer deux inclusions) que

$$\bigcap_{n\in\mathbb{N}^*} \left[0, 1 + \frac{1}{n}\right] = [0,1] \ .$$

Proposition I.3. Soient A, B, C, D quatre ensembles. Alors :
(i) $A \cap B = B \cap A$ **[commutativité]** ;
(ii) $(A \cap B) \cap C = A \cap (B \cap C)$ **[associativité]** ;
(iii) $A \cap \emptyset = \emptyset$ **[$\emptyset$ est absorbant]** ;
(iv) $A \cap A = A$ **[idempotence]** ;
(v) $(A \cap B = A) \Leftrightarrow (A \subset B)$;
(vi) $(A \subset B) \wedge (C \subset D) \Rightarrow (A \cap C \subset B \cap D)$.

Démonstration. Immédiat en utilisant les propriétés du connecteur $\wedge$. Un dessin peut une fois encore être utile pour (v) et (vi). □

Proposition I.4. Soient A, B, C trois ensembles. Alors :
(i) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
(ii) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Démonstration. Faisons le premier :

$$\begin{aligned} x \in A \cap (B \cup C) &\Leftrightarrow (x \in A) \wedge (x \in B \cup C) \\ &\Leftrightarrow (x \in A) \wedge ((x \in B) \vee (x \in C)) \\ &\Leftrightarrow ((x \in A) \wedge (x \in B)) \vee ((x \in A) \wedge (x \in C)) \quad \text{par distributivité} \\ &\Leftrightarrow (x \in A \cap B) \vee (x \in A \cap C) \\ &\Leftrightarrow (x \in A \cap B) \cup (A \cap C) \ . \end{aligned}$$

□

c) Différence, complémentaire

Définition I.6. Soient A, B deux parties d'un ensemble E. On appelle :
— **différence de A et B** l'ensemble $A \setminus B = \{x \in A \,|\, x \notin B\}$;
— **complémentaire de A** l'ensemble $\overline{A} = \{x \in E \,|\, x \notin A\}$.

Notation. Le complémentaire de A pourra aussi être noté A^c.

✌ **Remarque I.7.** Si A est une partie de E on a :
— $\overline{A} = E \setminus A.$;
— $A \setminus A = \emptyset$;
— $A \setminus \emptyset = A.$

➠ **Exemple I.7.** $\{1, 2, 3\} \setminus \{1, 4, 5\} = \{2, 3\}$.

Nous disposons d'une version ensembliste des lois de de Morgan via la proposition suivante.

Proposition I.5. Soient A, B, C trois parties d'un ensemble E. Alors :
(i) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$;
(ii) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$

Démonstration. Utiliser les lois de de Morgan logique en traduisant l'appartenance aux ensembles étudiants en termes de connecteurs. □

◇ Négation de phrases quantifiées

Pour exprimer proprement le complémentaire d'un ensemble, il est excessivement utile de savoir nier une phrase quantifiée. Nous donnons ici les règles à suivre.

Proposition I.6. Soit P un prédicat dépendant d'un paramètre x. Alors :
1. $\overline{(\forall x, P(x))} \Leftrightarrow (\exists x, \overline{P(x)})$
2. $\overline{(\exists x, P(x))} \Leftrightarrow (\forall x, \overline{P(x)})$

➠ **Exemple I.8.**

$$\begin{aligned}
&\overline{\forall \varepsilon > 0, \quad \forall x \in \mathbb{R}, \quad \exists \delta > 0, \quad \forall y \in \mathbb{R}, \quad (|x-y| \leq \delta) \Rightarrow (|f(x)-f(y)| \leq \varepsilon)} \\
&\Leftrightarrow \exists \varepsilon > 0, \quad \forall x \in \mathbb{R}, \quad \overline{\exists \delta > 0, \quad \forall y \in \mathbb{R}, \quad (|x-y| \leq \delta) \Rightarrow (|f(x)-f(y)| \leq \varepsilon)} \\
&\Leftrightarrow \exists \varepsilon > 0, \quad \exists x \in \mathbb{R}, \quad \overline{\exists \delta > 0, \quad \forall y \in \mathbb{R}, \quad (|x-y| \leq \delta) \Rightarrow (|f(x)-f(y)| \leq \varepsilon)} \\
&\vdots \\
&\Leftrightarrow \exists \varepsilon > 0, \quad \exists x \in \mathbb{R}, \quad \forall \delta > 0, \quad \exists y \in \mathbb{R} \quad (|x-y| \leq \delta) \wedge (|f(x)-f(y)| > \varepsilon)
\end{aligned}$$

d) Produit cartésien

Définition I.7. On appelle **couple** toute paire ordonnée d'objets. On dira que deux couples (a, b) et (c, d) sont égaux si et seulement si $(a = c) \wedge (b = d)$.

➠ **Exemple I.9.** $(\spadesuit, \hbar) \neq (\hbar, \spadesuit)$.

Définition I.8. Soient A, B deux ensembles. On appelle **produit cartésien de** A **et** B l'ensemble

$$\{(a,b) \,|\, a \in A,\, b \in B\}\ .$$

Notation. $A \times B$

➠ **Exemple I.10.** Vous connaissez sans doute déjà $\mathbb{R}^2$. Notons que l'on peut généraliser : $\mathbb{R}^3$ est par exemple le produit cartésien (associatif !) de $\mathbb{R}^2$ par $\mathbb{R}$.

3.⁻ Ensemble des entiers naturels, récurrence(s)

L'ensemble $\mathbb{N}$ des entiers naturels est un ensemble **infini**, muni d'une **addition** et d'une **multiplication**. Il s'agit de lois de composition internes : la somme et le produit de deux entiers naturels restent des entiers naturels. On peut également le munir de deux relations d'ordre (*cf.* chapitre V), à savoir :

- l'**ordre naturel** : on notera $a \leq b$ (pour $a, b \in \mathbb{N}$) si $\exists c \in \mathbb{N},\ b = a + c$; c est alors **noté** $b - a$ (la soustraction n'est pas une opération admissible sur $\mathbb{N}$). Il s'agit d'un ordre total : si $a, b \in \mathbb{N}$ alors $(a \leq b) \vee (b \leq a)$;
- la **divisibilité** : on notera $a|b$ ("a divise b") si $\exists c \in \mathbb{N},\ b = ac$; c est alors **noté**, lorsque $a \neq 0$, $\frac{b}{a}$. Il ne s'agit pas d'un ordre total : $2 \not| 3$ et $3 \not| 2$.

Notation. Dans toute la suite, pour $n \leq m$, on posera $[\![n, m]\!] = \{n, n+1, \ldots, m\}$.

a) Principe de récurrence

Axiome D. Toute partie non vide de $\mathbb{N}$ possède un plus petit élément (minimum).

Vocabulaire. Pour une partie A de $\mathbb{N}$ on appellera plus petit élément (resp. plus grand élément) ou minimum (resp. maximum) tout élément n vérifiant :

$$\forall a \in A, \quad a \geq n \ \text{ (resp. } a \leq n \text{).}$$

Cet axiome, bien qu'utile en lui-même comme nous le verons par la suite, nous amène la conséquence suivante, moins "évidente".

Proposition I.7. Toute partie de $\mathbb{N}$ non vide et majorée admet un plus grand élément (maximum).

✌ **Remarque I.8.**

- Une partie A de $\mathbb{N}$ est dite **majorée** (resp. **minorée**) si $\exists M \in \mathbb{N}$ tel que $\forall x \in \mathbb{N},\ x \leq M$ (resp. $x \geq M$). Nous reviendrons sur cette notion dans le chapitre V.
- Remarquons que toute partie non vide de $\mathbb{N}$ est minorée.

Démonstration. Soit $A \subset \mathbb{N}$ non vide et majorée. Posons :

$$B = \{x \in \mathbb{N} \,|\, \forall a \in A,\, a \leq x\}$$

l'ensemble des majorants de A. Alors :
- $B \neq \emptyset$ car A est majorée ;
- $B \subset \mathbb{N}$.

Ainsi, d'après l'axiome D, il existe $b \in B$ tel que $\forall x \in B,\, b \leq x$ ($b = \min B$). Remarquons de plus que b majore A par construction.

Cas 1 : $b = 0$. Alors $A = \{0\}$ car A est majorée par 0. La démonstration est terminée.

Cas 2 : $b \neq 0$. Alors $b - 1 \in \mathbb{N}$ et, comme $b = \min B$, ne majore pas A. Ainsi, il existe $a \in A$ tel que $a > b - 1$; ce qui signifie que $b - 1 < a \leq b$. La seule possibilité est alors que $a = b$; b est alors un majorant de A appartenant à l'ensemble : $b = \max A$.

□

Nous pouvons désormais énoncer le **principe de succession**, propriété fondamentale de l'ensemble des entiers naturels.

Proposition I.8. Soit $A \subset \mathbb{N}$ telle que :
- $0 \in A$;
- $\forall n \in \mathbb{N},\, (n \in A) \Rightarrow (n + 1 \in A)$.

Alors $A = \mathbb{N}$.

Démonstration. Supposons $A \neq \mathbb{N}$, *i.e* il existe $n \in \mathbb{N} \setminus A$. Posons $B = \mathbb{N} \setminus A$; alors :
- $B \neq \emptyset$;
- $B \subset \mathbb{N}$.

De fait, par axiome D, il existe $n_0 = \min B$. Par définition, $n_0 - 1 \in A$ et donc $n_0 = (n_0 - 1) + 1 \in A$, ce qui est absurde. □

Corollaire I.8.a (Principe de récurrence)**.**
Soit $\mathscr{P}$ un prédicat dépendant d'une variable $n \in \mathbb{N}$ tel que :
- $\mathscr{P}(0)$ est vraie **[initialisation]** ;
- $\forall n \in \mathbb{N},\, \mathscr{P}(n) \Rightarrow \mathscr{P}(n+1)$ **[hérédité]**.

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

Démonstration. Appliquer la proposition précédente à l'ensemble $A = \{n \in \mathbb{N} \,|\, \mathscr{P}(n)\}$. □

✌ **Remarque I.9.**
- Si $n_0 > 0$ est entier naturel que $\mathscr{P}(n_0)$ est vérifiée, alors l'hérédité entraîne que $\forall n \geq n_0$, $\mathscr{P}(n)$ est vraie. Ceci permet de faire des démonstrations par récurrence initialisées à $n = 1, 2, 3$ ou 42.
- Toute rédaction de récurrence doit faire apparaître clairement initialisation et hérédité.

— Il est absolument **proscrit** de faire débuter une hérédité par "Supposons la propriété vraie pour tout n" ...

✍ **Exercice I.1.** Soit $n \geq 2$; démontrer que 10 divise $2^{2^n} - 6$.

➥ **Correction :** *Par récurrence ...*
— *Pour $n = 2$, $2^{2^n} - 6 = 10$.*
— *Si la propriété est vraie au rang n, on remarque que $2^{2^{n+1}} - 6 = \left(2^{2^n}\right)^2 - 6$. Or, par hypothèse de récurrence, il existe $c \in \mathbb{N}$ tel que $2^{2^n} = 10c + 6$. En réinjectant, on tombe sur*

$$\begin{aligned} 2^{2^{n+1}} - 6 &= (10c+6)^2 - 6 \\ &= 100c^2 + 120c + 36 - 6 \\ &= 10(10c^2 + 12c + 3) \end{aligned}$$

d'où le résultat.

b) Récurrence double

Proposition I.9. Soit $\mathscr{P}$ un prédicat dépendant d'une variable $n \in \mathbb{N}$ tel que :
— $\mathscr{P}(0)$ et $\mathscr{P}(1)$ sont vraies **[initialisation double]** ;
— $\forall n \in \mathbb{N}$, $(\mathscr{P}(n) \wedge \mathscr{P}(n+1)) \Rightarrow \mathscr{P}(n+2)$ **[hérédité à deux rangs]**.
Alors $\forall n \in \mathbb{N}$, $\mathscr{P}(n)$ est vraie.

✍ **Exercice I.2.** On définit la **suite de Fibonacci** (Leonardo, 1175—1250) $(F_n)_n$ de la façon suivante :

$$F_0 = 0, \quad F_1 = 1 \quad \text{et} \quad \forall n \geq 0,\ F_{n+2} = F_n + F_{n+1}\ .$$

On note ϕ et $\overline{\phi}$ les racines du polynôme $X^2 - X - 1$. Démontrer que :

$$\forall n \geq 0, \quad F_n = \frac{\phi^n - \overline{\phi}^n}{\phi - \overline{\phi}}\ .$$

➥ **Correction :** *L'initialisation double est immédiate. Si on suppose la propriété vraies aux rangs n et $n+1$ pour un certain $n \geq 0$ alors*

$$\begin{aligned} F_{n+2} &= F_n + F_{n+1} \\ &= \frac{\phi^n - \overline{\phi}^n}{\phi - \overline{\phi}} + \frac{\phi^{n+1} - \overline{\phi}^{n+1}}{\phi - \overline{\phi}} \text{ par hypothèse de récurrence} \\ &= \frac{1}{\phi - \overline{\phi}} \left(\left(\phi^n + \phi^{n+1}\right) - \left(\overline{\phi}^n + \overline{\phi}^{n+1}\right) \right)\ . \end{aligned}$$

Il nous suffit pour conclure de remarquer que

$$\phi^n + \phi^{n+1} = \phi^n(1+\phi) = \phi^n \phi^2 = \phi^{n+2}$$

et que l'on a un résultat analogue pour $\overline{\phi}$.

c) Récurrence forte

Proposition I.10. Soit $\mathscr{P}$ un prédicat dépendant d'une variable $n \in \mathbb{N}$ tel que :
— $\mathscr{P}(0)$ est vraie **[initialisation]** ;
— $\forall n \in \mathbb{N}$, $(\forall k \in [\![0, n]\!],\ \mathscr{P}(k)) \Rightarrow \mathscr{P}(n+1)$ **[hérédité forte]**.
Alors $\forall n \in \mathbb{N}$, $\mathscr{P}(n)$ est vraie.

Démonstration. Appliquer le principe de récurrence au prédicat $\mathscr{Q}(n) : \forall k \leq n,\ \mathscr{P}(n)$. □

➠ **Exemple I.11.** Démontrons par récurrence forte sur $n \in \mathbb{N}$ que :

$$\forall n \in \mathbb{N} \setminus \{0, 1\},\ \mathscr{P}(n)\ :\ n \text{ admet un diviseur premier.}$$

— $n = 2$ est divisible par 2, qui est premier.
— Soit $n \in \mathbb{N}$; supposons que $\mathscr{P}(k)$ soit vérifiée pour tout $k \in [\![2, n]\!]$. Si $n+1$ est premier, c'est terminé ; dans le cas contraire, il existe $a, b \in [\![2, n]\!]$ tels que $n + 1 = ab$. Or, par hypothèse de récurrence, a (par exemple) admet un diviseur premier, d'où le résultat.

✍ **Exercice I.3.** Démontrer que :

$$\forall n \in \mathbb{N}^*, \quad \exists\, (p, q) \in \mathbb{N}^2,\ n = 2^p(2q + 1)\,.$$