Devoir Surveillé n° 1 (3h)

Correction de l'exercice 1 –

- On montre que $\boxed{(i) \Longrightarrow (ii)}$. On suppose donc (i), et on se donne A et B dans $\mathcal{B}$.
  - $*$ L'appartenance $A \triangle B \in \mathcal{B}$ provient directement de (i)
  - $*$ On remarque que $A \cup B = (A \triangle B) \triangle (A \cap B)$. Or, d'après (i), $A \triangle B$ et $A \cap B$ sont dans $\mathcal{B}$, donc en appliquant encore (i), $(A \triangle B) \triangle (A \cap B) \in \mathcal{B}$. Ainsi $A \cup B \in \mathcal{B}$.

  On a bien obtenu (ii).
- On montre que $\boxed{(ii) \Longrightarrow (iii)}$. On suppose donc (ii), et on se donne A et B dans $\mathcal{B}$.
  - $*$ L'appartenance $A \cup B \in \mathcal{B}$ proviet directement de (ii).
  - $*$ On remarque que $A \setminus B = (A \cup B) \triangle B$, donc en appliquant deux fois les règles de stabilité de (ii), $A \setminus B \in \mathcal{B}$.

  On a bien obtenu (iii).
- On montre que $\boxed{(iii) \Longrightarrow (i)}$. On suppose donc (iii), et on se donne A et B dans $\mathcal{B}$.
  - $*$ On remarque que $A \triangle B = (A \setminus B) \cup (B \setminus A)$. Or, d'après (iii), $A \setminus B \in \mathcal{B}$, et $B \setminus A \in \mathcal{B}$, donc leur union aussi. Ainsi, $A \triangle B \in \mathcal{B}$.
  - $*$ On remarque que $A \cap B = A \setminus (A \setminus B)$. Ainsi, on obtient de même que $A \cap B \in \mathcal{B}$.

  On a bien obtenu (i).

Les trois implications $(i) \Longrightarrow (ii) \Longrightarrow (iii) \Longrightarrow (i)$ amènent l'$\boxed{\text{équivalence entre les propriétés } (i),\ (ii) \text{ et } (iii)}$.

Correction du problème 1 – (Définitions et démonstrations par induction structurelle)

1. **Existence de F, et description par le haut**

   Soit $\mathcal{M} = \{G \subset E \mid F_0 \subset G \text{ et } G \text{ stable par chacun des } f_i\}$.

   (a) De façon évidente, $\boxed{E \in \mathcal{M}}$.

   (b)
   - Puisque pour tout $G \in \mathcal{M}$, $F_0 \subset G$, on a : $\boxed{F_0 \subset \bigcap_{G \in \mathcal{M}} G = F}$.
   - Soit $i \in [\![1, m]\!]$ et $(x_1, \dots, x_{k_i}) \in F^{k_i}$. Soit $G \in \mathcal{M}$. Puisque $F \subset G$ on a : $(x_1, \dots, x_{k_1}) \in G^{k_i}$, et G étant dans $\mathcal{M}$, il est stable par f_i. On a donc :

     $$f(x_1, \dots, x_{k_i}) \in G.$$

     Cela étant vrai pour tout G de $\mathcal{M}$, $f(x_1, \dots, x_{k_i}) \in \bigcap_{G \in \mathcal{M}} G = F$. Ainsi, $\boxed{F \text{ est stable par } f_i}$, et ceci pour tout $i \in [\![1, m]\!]$.

   (c) F est un ensemble contenant F_0 et stable par les f_i. De plus, étant donné H un autre ensemble vérifiant ces propriétés, $H \in \mathcal{M}$, donc $\bigcap_{G \in \mathcal{M}} G \subset H$ (H étant un terme de cette intersection). Ainsi, $F \subset H$.

   On en déduit que $\boxed{F \text{ est bien l'ensemble défini par induction structurelle à partir de } F_0 \text{ et des } f_i.}$

2. **Description par le bas de F**

   Soit pour tout $n \in \mathbb{N}$,

   $$F_{n+1} = F_n \cup \bigcup_{i=1}^{m} f_i(F_n^{k_i}).$$

   Ainsi, F_{n+1} est obtenu en rajoutant à F_n l'ensemble des éléments pouvant s'obtenir des éléments de F_n en appliquant l'une des fonctions f_i.

   (a) Soit, pour tout n dans $\mathbb{N}$, la propriété $\mathcal{P}(n)$: F_n est bien défini, et $F_n \subset F$.

   L'ensemble F_0 est bien défini (par hypothèse) et $F_0 \subset F$ (par définition de F), d'où $\mathcal{P}(0)$.

   Soit $n \in \mathbb{N}$. Supposons que $\mathcal{P}(n)$ est vrai. Alors

- Comme $F_n \subset F \subset E$, pour tout $i \in [\![1, m]\!]$, f_i est définie sur $F_n^{k_i}$, donc $f_i(F_n^{k_i})$ est bien défini, donc aussi leur union, puis F_{n+1}.
- Comme $F_n \subset F$, et comme F est stable par les f_i, $f_i(F_n^{k_i}) \subset f_i(F^{k_i}) \subset F$, puis $F_{n+1} \subset F$.

Ainsi, $\mathcal{P}(n+1)$ est vérifié.

Par conséquent, $\mathcal{P}(0)$ est vraie, et pour tout n dans $\mathbb{N}$, $\mathcal{P}(n)$ entraîne $\mathcal{P}(n+1)$. D'après le principe de récurrence, $\mathcal{P}(n)$ est vraie pour tout n dans $\mathbb{N}$.

(b) Soit $G = \bigcup_{n \in \mathbb{N}} F_n$. De ce qui précède, on déduit : $F_0 \subset G \subset F$.

Par ailleurs, étant donné $i \in [\![1, m]\!]$ et $(x_1, \ldots, x_{k_i}) \in G^{k_i}$, il existe $(n_1, \ldots, n_{k_i}) \in \mathbb{N}^{k_i}$ tel que pour tout $j \in [\![1, k_i]\!]$, $x_i \in F_{n_j}$. Comme $(F_n)_{n \in \mathbb{N}}$ est une suite croissante pour l'inclusion, en posant $n_0 = \max_{j \in [\![1, k_i]\!]} (n_j)$,

$$(x_1, \ldots, x_{k_i}) \in F_{n_0}^{k_i}, \qquad \text{donc:} \qquad f_i(x_1, \ldots, x_{k_i}) \in F_{n_0+1} \subset G.$$

Ainsi, G est stable par les f_i. Par minimalité de F, on en déduit que $G = F$, soit $\boxed{F = \bigcup_{n \in \mathbb{N}} F_n}$.

3. **Principe d'induction structurelle**

Soit $\mathcal{P}$ une propriété définie sur $G \subset E$ tel que $F \subset G$, telle que :

- $\forall x \in F_0, \quad \mathcal{P}(x)$
- $\forall i \in [\![1, m]\!], \ \forall (x_1, \ldots, x_{k_i}) \in F^{m_i}, \quad \mathcal{P}(x_1) \wedge \cdots \wedge \mathcal{P}(x_{k_i}) \Longrightarrow \mathcal{P}(f_i(x_1, \ldots, x_{k_i}))$.

(a) Soit $V = \{x \in F \mid \mathcal{P}(x) \text{ est vraie}\}$.

- D'après la première hypothèse sur $\mathcal{P}$, $F_0 \subset V$.
- D'après la seconde hypothèse et la définition de V, pour tout $i \in [\![1, m]\!]$ et tout $(x_1, \ldots, x_{k_i}) \in V^{k_i}$, on a $(x_1, \ldots, x_{k_i}) \in F^{k_i}$, et donc $f_i(x_1, \ldots, x_{k_i}) \in F$. Par ailleurs, puisque $\mathcal{P}(x_1), \ldots, \mathcal{P}(x_{k_i})$ sont vrais, il en est de même ; par la seconde hypothèse sur $\mathcal{P}$, de $f_i(x_1, \ldots, x_{k_i})$. Ainsi, $f_i(x_1, \ldots, x_{k_i}) \in V$.
- Ainsi, V contient F_0 et est stable par les f_i. Par minimalité de F, on a donc $F \subset V$.
- Par définition de V, $V \subset F$.
- Ainsi, d'après le principe de double-inclusion, $V = F$ c'est-à-dire que $\boxed{\mathcal{P}(x) \text{ est vraie pour tout } x \in F.}$

(b) Dans la question précédente, nous avons utilisé la description par le haut. Nous retrouvons le même résultat en utilisant la description par le bas :

Soit, pour tout n dans $\mathbb{N}$, la propriété $\mathcal{Q}(n)$: $\mathcal{P}(x)$ est vraie pour tout x de F_n.

La propriété $\mathcal{Q}(0)$ provient des hypothèses.

Soit donc $n \in \mathbb{N}$, et supposons $\mathcal{Q}(n)$ vraie. Alors $\mathcal{P}$ est vraie sur F_n, et d'après les hypothèses faites sur $\mathcal{P}$, elle est vraie aussi sur les $f_i(F_n^{k_i})$, donc sur F_{n+1}, d'où $\mathcal{Q}(n+1)$.

Par conséquent, $\mathcal{Q}(0)$ est vraie, et pour tout n dans $\mathbb{N}$, $\mathcal{Q}(n)$ entraîne $\mathcal{Q}(n+1)$. D'après le principe de récurrence, $\mathcal{Q}(n)$ est vraie pour tout n dans $\mathbb{N}$.

4. **Exemple : les formules de la logique propositionnelle**

Soit $\mathcal{V}$ un ensemble fini (les variables propositionnelles P, Q, R...) et E l'ensemble de tous les mots (c'est-à-dire juxtaposition de lettres) que l'on peut former avec les variables propositionnelles et les symboles (,), $\wedge$, $\vee$, $\neg$, $\Longrightarrow$ et $\Longleftrightarrow$. On définit les fonctions suivantes, à une ou deux variables dans E :

$$f_1(F) = \neg F \quad f_2(F, G) = (F \vee G) \quad f_3(F, G) = (F \wedge G) \quad f_4(F, G) = (F \Longrightarrow G) \quad f_5(F, G) = (F \Longleftrightarrow G).$$

L'ensemble $\mathcal{F}$ des formules propositionnelles est l'ensemble défini par induction structurelle à partir de l'ensemble de base $\mathcal{V}$ et des fonctions f_1, f_2, f_3, f_4 et f_5.

(a) Nous utilisons le principe d'induction structurelle.

Soit, pour tout $F \in \mathcal{F}$, $\mathcal{P}(F)$: « la formule F a autant de parenthèses ouvrantes que de parenthèses fermantes »

- Soit $F \in \mathcal{V}$. Alors F n'a aucune parenthèse (ni ouvrante ni fermante), donc $\mathcal{P}(F)$ est vérifié.
- Soit $F \in \mathcal{F}$ tel que $\mathcal{P}(F)$ soit vérifié. Alors $\neg F$ a autant de parenthèse ouvrante et fermante que F, d'où $\mathcal{P}(\neg F)$.

- Soit $(F,G) \in \mathcal{F}^2$ tel que $\mathcal{P}(F)$ et $\mathcal{P}(G)$ soient vérifiés. Alors dans chacune des formules $f_2(F,G)$, $f_3(F,G)$, $f_4(F,G)$ et $f_5(F,G)$, on ajoute une parenthèse ouvrante et une parenthèse fermante à celles de F et G. Comme F et G avaient chacune autnat de parenthèses ouvrantes que de parenthèses fermantes, il en est de même de $f_2(F,G)$, $f_3(F,G)$, $f_4(F,G)$ et $f_5(F,G)$, d'où $\mathcal{P}(f_2(F,G))$, $\mathcal{P}(f_3(F,G))$, $\mathcal{P}(f_4(F,G))$ et $\mathcal{P}(f_5(F,G))$

Ainsi, d'après le principe d'induction structurelle, $\mathcal{P}(F)$ est vraie pour tout F de $\mathcal{F}$:

$\boxed{\text{Une formule de } \mathcal{F} \text{ a toujours autant de parenthèses ouvrantes que de parenthèses fermantes}}$.

(b) On appelle *segment initial* d'un mot $m = m_1m_2\dots m_k$ un mot $m_1m_2\dots m_i$, $i \in [\![1,k]\!]$ (il s'agit donc du début du mot m). Un segment initial de m est dit *propre* s'il est différent de m lui-même.

i. On montre une propriété plus forte, en utilisant une induction structurelle.

Soit pour tout $F \in \mathcal{F}$, $\mathcal{Q}(F)$: « tout segment initial F' de F vérifie $o(F') \geqslant f(F')$, et si F commence par une parenthèse (, et si F' est un segment propre, $o(F') > f(F')$ »

- Soit $F \in \mathcal{V}$. Le seul segment initial de F est F lui-même, qui vérifie $o(F) = v(F) = 0$. Par ailleurs, F ne commence pas par une parenthèse, donc n'est pas concerné par la seconde condition. D'où $\mathcal{Q}(F)$.
- Soit $F \in \mathcal{F}$ tel que $\mathcal{Q}(F)$ soit vraie. Soit G' un segment initial de $G = \neg F$.
  - Soit $G' = \neg$, et vérifie $o(G') = f(G') = 0$,
  - Soit $G' = \neg F'$, où F' est un segment initial de F, et $o(G') = o(F') \geqslant f(F') = f(G')$, l'inégalité du milieu provenant de $\mathcal{Q}(F)$.

  Par ailleurs, $\neg F$ ne commence pas par une parenthèse, d'où $\mathcal{Q}(\neg F)$.
- Soit $F, G \in \mathcal{F}$ tels que $\mathcal{Q}(F)$ et $\mathcal{Q}(G)$ soient vérifiés. Soit H' un segment initial de $(F \vee G)$.
  - Soit $H' =$ (donc $1 = o(H') > f(H') = 0$;
  - Soit $H' = (F'$ où F' est un segment initial de F, donc
$$o(H') = o(F') + 1 \geqslant f(F') + 1 = f(H') + 1 > f(H');$$
  - Soit $H' = (F\vee$, et on conclut de même ;
  - Soit $H' = (F \vee G'$ où G' est un segment initial de G, et
$$o(H') = o(F) + o(G') + 1 \geqslant f(F) + f(G') + 1 = f(H') + 1 > f(H');$$
  - Soit $H' = (F \vee G)$, et H' est un formule donc vérifie d'après la question précédente $o(H') = f(H')$.

  Ainsi, on a dans tous les cas $o(F') \geqslant f(F')$, et l'inégalité est stricte si F' est un segment initial propre. D'où $\mathcal{P}(F)$.
- Les cas de $F \wedge G$, $F \implies G$ et $F \iff G$ se traitent de la même façon.

Ainsi, d'après le principe d'induction structurelle, pour toute formule F commençant par une parenthèse, et pour tout segment inital propre F', $\boxed{o(F') > f(F')}$.

ii. On raisonne encore par induction structurelle, pour montrer pour tout $F \in \mathcal{F}$, $\mathcal{R}(F)$: « un segment initial propre de F ne peut pas être une formule. »

- Un élément de $\mathcal{V}$ n'a pas de segment propre, donc $\mathcal{R}$ est vraie par défaut sur $\mathcal{V}$.
- Soit F une formule telle que $\mathcal{R}(F)$ soit vraie. Soit G' un segment initial propre de $\neg F$. Supposons que G' est une formule. Comme G' commence par $\neg$, il s'écrit nécessairement sous la forme $\neg F'$, où F' est aussi une formule (G' est obtenu par stabilité, en considérant la description par le bas, et nécessairement en appliquant pour terminer la règle f_1). Ainsi, F' est une formule, et un segment initial de F, ce qui contredit l'hypothèse $\mathcal{R}(F)$. Par conséquent, $\mathcal{R}(G)$ est vraie.
- Soit F et G des formules telles que $\mathcal{R}(F)$ et $\mathcal{R}(G)$ soient vraies. Alors $(F \vee G)$, $(F \wedge G)$, $(F \implies G)$ et $(F \iff G)$ commencent par une parenthèse (. Tout segment initial H' d'une de ces formules vérifie donc $o(H') > f(H')$ d'après 4(b)i, et ne peut donc pas être une formule d'après 4(a) (remarquez qu'on n'utilise pas l'hypothèse de l'induction ici).

D'après le principe d'induction structurelle,

$\boxed{\text{un segment initial propre d'une formule ne peut pas être une formule.}}$

(c) (Théorème de lecture unique d'une formule)

L'examen du premier caractère montre que ces trois cas s'excluent les uns des autres. Les formules construites par les règles f_1 à f_5 font débuter les nouvelles formules par le symbole $\neg$ ou (. Les seules formules ne commençant pas par $\neg$ et (sont donc les formules initiales à savoir les formules de $\mathcal{V}$, donc les variables (on a utilisé ici la description par le bas). Ainsi, toute formule F n'étant pas dans $\mathcal{V}$ commence par $\neg$ ou (:

- Si F commence par $\neg$, il existe G tel que $F = \neg G$. Si G et G' sont tels que $F = \neg G = \neg G'$, la suppression du premier caractère conserve l'égalité, donc $G = G'$. D'où l'unicité de cette écriture.
- Si F commence par (, il existe G et H, et un connecteur γ tels que $F = (G\gamma H)$. Si (G', β, H') sont tels que $F = (G\gamma H) = (G'\beta H')$, alors on peut supprimer les parenthésages, et on a l'égalité suivante des mots : $G\gamma H = G'\beta H'$.

  Suivant que G est plus long ou non que G', soit G est un segment initial de G', soit G' est un segment initial de G. Or, G et G' étant des formules, la question précédente implique alors $G = G'$, puis $\gamma = \beta$, puis $H = H'$.

  Ainsi, la décomposition $F = (G\gamma H)$ est unique.

Correction du problème 2 – Théorème de Howie

1. (a)
   - L'application Φ est $\boxed{\text{bien définie}}$, puisqu'il n'y a d'ambiguïté de définition : par hypothèse, un élément $x \in A \sqcup B$ appartient toujours soit à A, soit à B, et à un et un seul de ces deux ensembles.
   - Soit $y \in A' \sqcup B'$. Alors :
     * soit $y \in A'$ et par surjectivité de φ, il existe $x \in A$ tel que $\varphi(x) = y$, donc $\Phi(x) = y$
     * soit $y \in B'$ et par surjectivité de φ, il existe $x \in B$ tel que $\psi(x) = y$, donc $\Phi(x) = y$

     Ainsi Φ est $\boxed{\text{surjective}}$.
   - Soit x et y distincts dans $A \sqcup B$.
     * Si x et y sont tous deux dans A, alors $\Phi(x) = \varphi(x)$ et $\Phi(x) = \varphi(x)$; de plus, φ étant injective, $\varphi(x) \neq \varphi(y)$, donc $\Phi(x) \neq \Phi(y)$.
     * De même si x et y sont tous deux dans B.
     * Si $x \in A$ et $y \in B$ (de même dans le cas inverse), $\Phi(x) \in A'$ et $\Phi(y) \in B'$. Comme $A' \cap B' = \varnothing$, cela entraîne $\Phi(x) \neq \Phi(y)$.

     D'où l'$\boxed{\text{injectivité}}$ de Φ.
   - De la surjectivité et l'injectivité de Φ découle la $\boxed{\text{bijectivité de } \Phi}$.

   On aurait aussi pu construire une réciproque de Φ, en la construisant de la même manière que Φ, à partir des réciproques de φ et ψ.

   (b) On montre par récurrence sur $n \in \mathbb{N}$ que si A et B sont deux ensembles finis de même cardinal n, alors il existe une bijection de A à B.
   - Initialisation : Soit A et B deux ensembles de cardinal 0. Ainsi, $A = \varnothing$ et $B = \varnothing$. Il y a une unique application de A vers B, qui est l'application vide. Cette application est bien injective (par défaut : on ne peut pas trouver 2 éléments distincts dans A, donc pas de défaut d'injectivité) et surjective (aussi par défaut : il n'y a pas d'élément à atteindre dans B)
   - Soit $n \in \mathbb{N}$. On suppose que la propriété est vrai pour des ensembles de cardinal n. Soit A et B de cardinal $n+1$. Soit a un élément de A et b un élément de B. On pose $A' = A \setminus \{a\}$ et $B' = B \setminus \{b\}$. Puisque le cardinal de A' et de B' est n, par hypothèse de récurrence, il existe une bijection $\varphi : A' \to B'$. Il existe aussi une bijection de $\{a\}$ dans $\{b\}$ (l'application qui à l'unique élément a associe b). D'après la question 1(a), on en déduit qu'il existe une bijection de $A = A' \sqcup \{a\}$ dans $B = B' \sqcup \{b\}$.
   - Ainsi, d'après le principe de récurrence, pour tous ensembles A et B de même cardinal, $\boxed{\text{il existe une bijection } \varphi : A \to B}$.

   On verra plus tard qu'en fait, cette propriété est à la base de la définition générale des cardinaux quelconques (ou plutôt des comparaisons de cardinaux).

2. (a)
   - Soit $\pi : X \to X$ idempotente. Soit $x \in \operatorname{Im}(\pi)$. Il existe donc $y \in X$ tel que $x = \pi(y)$. On a alors :

     $$\pi(x) = \pi \circ \pi(y) = \pi(y),$$

     par la propriété d'idempotence de π. De la définition de π, il vient alors que $\boxed{\pi(x) = x}$.

- Réciproquement, si pour tout $x \in \mathrm{Im}(\pi)$, $\pi(x) = x$, soit $y \in X$. En appliquant l'hypothèse à $\pi(y) \in \mathrm{Im}(\pi)$, on obtient : $\pi(\pi(y)) = \pi(y)$. Ceci étant vrai pour tout y de X, $\pi \circ \pi = \pi$. Ainsi, $\boxed{\pi \text{ est idempotente}}$.

(b) Par définition de $p_{a,b}$, $a \notin \mathrm{Im}(p_{a,b})$. Or, a est le seul élément qui ne soit pas point fixe de $p_{a,b}$. Ainsi, pour tout $y \in \mathrm{Im}(p_{a,b})$, $p_{a,b}(y) = y$. D'après la caractérisation de la question précédente, $\boxed{p_{a,b} \text{ est idempotente}}$.
On aurait aussi pu facilement faire une vérification directe.

3. Pour faire un échange de contenu variables en informatique, on déplace d'abord y vers z puis x vers y et enfin z (avec son nouveau contenu) vers y. On fait la même chose ici, les déplacements étant représentés par les applications $p_{a,b}$ définies plus haut. On considère donc $\tilde{\tau} = p_{z,x} \circ p_{x,y} \circ p_{y,z}$.
En suivant les éléments au cours des compositions, on voit facilement que $\tilde{\tau}(x) = y$, $\tilde{\tau}(y) = x$, et pour tout $t \notin \{x, y, z\}$, $\tilde{\tau}(t) = t$. Ainsi, $\boxed{\tau_{x,y} \text{ et } \tilde{\tau} \text{ coïncident sur } X \setminus \{z\}}$.
En revanche, elles diffèrent sur z, puisque $\tau_{x,y}(z) = z$ alors que $\tilde{\tau}(z) = x$

4. On suppose que (φ, D') vérifie $\mathcal{P}$. Soit $d_0 \in D'$. On suppose que $\varphi(d_0) \neq d_0$, et on considère $\psi = \tau_{\varphi(d_0),d_0} \circ \varphi$, et $D'' = D' \setminus \{d_0\}$.

   (i) Soit x et y dans D'' tels que $\psi(x) = \psi(y)$. On a donc $\tau_{\varphi(d_0),d_0}(\varphi(x)) = \tau_{\varphi(d_0),d_0}(\varphi(y))$. Puisque $\tau_{\varphi(d_0),d_0} \circ \tau_{\varphi(d_0),d_0} = \mathrm{id}_X$, on obtient, en composant par $\tau_{\varphi(d_0),d_0}$, $\varphi(x) = \varphi(y)$. L'injectivité de φ sur D' (dont x et y son éléments) amène alors $x = y$.
   Ainsi, $\boxed{\psi_{|D''} \text{ est injective}}$.

   (ii) Soit $d \in D''$. Alors $\varphi(d) \in D'$ (par stabilité de D' par φ). De plus, $\varphi(d) \neq \varphi(d_0)$, car φ est injective. Ainsi :
   - si $\varphi(d) \neq d_0$, alors $\tau_{\varphi(d_0),d_0}(\varphi(d)) = \varphi(d) \neq d_0$. Puisque $\varphi(D') \subset D'$, on en déduit que $\psi(d) \in D''$;
   - si $\varphi(d) = d_0$, alors $\tau_{\varphi(d_0),d_0}(\varphi(d)) = \varphi(d_0) \neq d_0$ par hypothèse, et de même, $\psi(d) \in D''$.

   On a donc bien $\boxed{\psi(D'') \subset D''}$.

   (iii) Enfin, pour tout $x \in D \setminus D'' = (D \setminus D') \cup \{d_0\}$:
   - si $x \in D \setminus D'$, alors x est point fixe de φ ainsi que de $\tau_{d_0,\varphi(d_0)}$, donc $\psi(x) = x$;
   - si $x = d_0$,
   $$\psi(x) = \tau_{d_0,\varphi(d_0)}(\varphi(d_0)) = d_0 = x.$$

   Ainsi, $\boxed{\text{pour tout } x \in D \setminus D'', \psi(x) = x}$.

   Donc $\boxed{(\psi, D'') \text{ vérifie } \mathcal{P}}$.

5. On montre par récurrence sur le cardinal de D' que si (φ, D') vérifie $\mathcal{P}$, alors φ coïncide sur D avec une composée d'applications idempotentes.
   - Si $|D'| = \varnothing$, alors c'est trivialement vrai puisque par l'hypothèse (ii), φ coïncident sur D avec id_X qui est bien idempotente.
   - Soit $D' \subset D$ tel que (φ, D'') vérifie la propriété $\mathcal{P}$ pour tout $D'' \subset D$ tel que $|D''| < |D'|$.
     * S'il existe $d_0 \in D'$ tel que $\varphi(d_0) = d_0$, alors, en posant $D'' = D' \setminus \{d_0\}$, (φ, D'') vérifie encore $\mathcal{P}$. D'après l'hypothèse de récurrence, φ coïncide sur D avec une composée d'applications idempotentes.
     * Sinon, puisque D' est non vide, on peut poser $d_0 \in D'$ quelconque. On a alors $\varphi(d_0) \neq d_0$. On construit alors ψ et D'' comme dans la question précédente. Par hypothèse de récurrence, puisque (ψ, D'') vérifie $\mathcal{P}$, ψ coïncide sur D avec une composée d'applications idempotentes. De plus, puisque $\tau^2_{d_0,\varphi(d_0)} = \mathrm{id}_X$ (le carré étant à prendre au sens de la composition),
     $$\varphi = \tau_{d_0,\varphi(d_0)} \circ \psi.$$
     D'après la question 3, $\tau_{d_0,\varphi(d_0)}$ coïncide sur D avec une composée d'applications idempotentes. Comme $\psi(D) \subset D$, en composant ces applications avec celles décomposant ψ, on obtient bien une composée d'applications idempotentes coïncidant avec φ sur D.

   D'après le principe de récurrence, pour tout couple (φ, D') vérifiant $\mathcal{P}$, on peut en déduire que φ coïncide sur D avec un produit d'applications idempotentes.
   En particulier, en considérant $D' = D$, $\boxed{\text{si } (\varphi, D) \text{ vérifie } \mathcal{P}}$, alors il existe un entier n et des applications idempotentes $p_1, \dots, p_n$ tels que $\boxed{\varphi \text{ et } p_n \circ \cdots \circ p_1 \text{ coïncident sur } D}$.

6. *Soit $\varphi : X \to X$ une application et D un sous-ensemble strict de X. On suppose que $\varphi_{|D}$ est injective, mais on ne suppose plus que $\varphi(D) \subset D$.*

   (a) Comme φ est injective, sa corestriction à son image $\varphi(D)$ est à la fois injective et surjective, donc bijective. Les résultats admis en préambule de devoir amènent alors $|D| \leqslant |\varphi(D)|$ et $|\varphi(D)| \leqslant |D|$, donc $|D| = |\varphi(D)|$. Or,
   $$|D \setminus \varphi(D)| = |D \setminus (D \cap \varphi(D))| = |D| - |D \cap \varphi(D)|,$$
   et de même
   $$|\varphi(D) \setminus D| = |\varphi(D) \setminus (D \cap \varphi(D))| = |\varphi(D)| - |D \cap \varphi(D)| = |D| - |D \cap \varphi(D)|.$$
   L'égalité de ces cardinaux et la question 1(b) amènent l'existence d'une $\boxed{\text{bijection de } \varphi(D) \setminus D \text{ vers } D \setminus \varphi(D)}$.

   (b) Soit $\alpha : D \setminus \varphi(D) \to \varphi(D) \setminus D$ une bijection (l'existence étant prouvée das la question précédente), et $\beta = \mathrm{id}_{D \cap \varphi(D)}$, également bijective. On peut construire alors d'après la question 1(a) une application bijective
   $$\theta \ : \ (D \setminus \varphi(D)) \cup (D \cap \varphi(D)) \longrightarrow (\varphi(D) \setminus D) \cup (D \cap \varphi(D),$$
   c'est-à-dire $\boxed{\theta : D \to \varphi(D), \text{ bijective}}$. De plus, par construction, $\boxed{\theta \text{ coïncide avec } \beta}$ sur $D \cap \varphi(D)$, donc avec l'identité.

   (c) On prolonge θ à X, en une application $\tilde{\theta}$ obtenue en définissant $\tilde{\theta}(x) = x$ pour tout $x \notin D$. Alors, l'image de $\tilde{\theta}$ vérifie :
   $$\mathrm{Im}(\tilde{\theta}) = \tilde{\theta}(D) \cup \tilde{\theta}(X \setminus D) = \varphi(D) \cup (X \setminus D) = X \setminus (D \setminus \varphi(D)).$$
   Par construction, $\tilde{\theta}$ coïncide donc avec l'identité sur son image. On déduit alors de 2(a) que $\boxed{\tilde{\theta} \text{ est idempotente}}$. De plus elle $\boxed{\text{prolonge } \theta \text{ à } X}$.

   (d) Soit $\tilde{\varphi} = \varphi_{|D}^{|\varphi(D)}$ la restriction à D et corestriction à $\varphi(D)$ de φ. Comme $\varphi_{|D}$ est injective par hypothèse, et surjective sur son image par définition de l'image, $\tilde{\varphi}$ est bijective ;
   De plus, l'application θ est bijective de D dans $\varphi(D)$, donc θ^{-1} est bijective de $\varphi(D)$ dans D. Par conséquent,
   $$\theta^{-1} \circ \tilde{\varphi}(D) = \theta^{-1} \circ \varphi(D) = D.$$
   De plus, en tant que composée de deux bijections, $\theta^{-1} \circ \tilde{\varphi}$ est bijective, donc $(\theta^{-1} \circ \varphi)_{|D}$ est injective. On peut co-prolonger cette application à X (c'est-à-dire agrandir son ensemble d'arrivée, sans changer la définition de la fonction). La fonction obtenue, qu'on appelera α, est encore injective, et vérifie $\alpha(D) = \theta^{-1}(\varphi(D)) \subset D$, par définition de θ. Ainsi, le couple (α, D) vérifie $\mathcal{P}$ (le point (iii) étant vide das ce cas).
   On déduit de la question 5 que α coïncide sur D avec une composée d'applications idempotentes $p_n \circ \cdots \circ p_1$. Considérons alors
   $$\beta = \tilde{\theta} \circ p_n \cdots \circ p_1.$$
   D'après la question 6(c), il s'agit d'une composée d'applications idempotentes. De plus, pour tout $x \in D$, puisque
   $$p_n \circ \cdots \circ p_1(x) = \alpha(x) \in D,$$
   et comme $\tilde{\theta}$ coïncide avec θ sur D,
   $$\beta(x) = \theta(\alpha(x)) = \theta(\theta^{-1}(\varphi(x))) = \varphi(x).$$
   Ainsi, β et φ coïncident sur D
   On en déduit que $\boxed{\varphi \text{ coïncide sur } D \text{ avec une composée d'applications idempotentes}}$.

7. Soit f une application non bijective de X dans lui-même. On considère la partition $\{X_1, \dots, X_k\}$ de X associé à f (obtenue du partage en enlevant les parts éventuellement vides). Ainsi, pour tout $i \in [\![1, k]\!]$, et tout $(x, y) \in X_i^2$, $f(x) = f(y)$. On choisit, pour chaque part X_i, un élément $x_i \in X_i$ (appelé représentant de la part X_i), et on définit une application $p : X \mapsto X$ par :
   $$p(x) = x_i \text{ si } x \in X_i.$$

Ainsi, tout x est envoyé sur le représentant de la part de la partition dans laquelle il se trouve. En particulier, $p(x_i) = x_i$. Ceci implique que $p \circ p = p$, donc que $\boxed{p \text{ est idempotente}}$.

On a alors, pour tout $x \in X$, si $x \in X_i$, $f(x) = f(x_i) = f(p(x))$. Ainsi, $\boxed{f = f \circ p}$.

On note $D = \{x_i, i \in [\![1, k]\!]\}$ l'ensemble des représentants des parts de la partition. L'hypothèse de non bijectivité de f amène l'inclusion stricte $D \subsetneq X$. En effet, sinon, tous les éléments de x seraient des représentants de parts 2 à 2 distincts, donc auraient des images 2 à 2 distincts, ce qui impliquerait que f est injective, donc sa corestriction à son image serait bijective, d'où $|f(X)| = |X|$. Mais comme de plus $f(X) \subset X$ et comme X est fini, on en déduit que $f(X) = X$, donc que f est surjective. Cela contredit la non bijectivité de f.

Ainsi, $\boxed{D \subsetneq X}$.

Par définition de la partition $\{X_i,\ i \in [\![1, k]\!]\}$, pour tous $i, j \in [\![1, k]\!]$ tels que $i \neq j$, $f(x_i) \neq f(x_j)$. Ainsi, $f_{|D}$ est injective. On peut donc appliquer la question 5 : il existe des applications idempotentes $p_1, \dots, p_n$ telles que $p_n \circ \cdots \circ p_1$ coïncide avec f sur D.

Soit maintenant $x \in X$ quelconque. On a

$$f(x) = f(p(x)) = p_n \circ \cdots \circ p_1 \circ p(x),$$

puisque $p(x) \in D$. Ainsi, $\boxed{f = p_n \circ \cdots \circ p_1 \circ p}$.

On a bien exprimé f comme composée d'applications idempotentes.

8. On étudie la réciproque. On commence par caractériser les applications idempotentes bijectives. Soit $p : X \to X$ une application idempotente bijective. Alors $\mathrm{Im}(p) = X$ par surjectivité. Il vient alors par la question 3(a) que $p = \mathrm{id}_X$. Ainsi, la seule application idempotente bijective est id_X.

   Soit maintenant une application f, distincte de id_X, s'exprimant comme composée $f = p_n \circ \cdots \circ p_1$ d'applications idempotentes. Quitte à enlever les p_i égaux à id_X, on peut supposer que les p_i sont tous distincts de id_X, donc ne sont pas bijectifs. L'argument donné dans la question précédente (valable pour toute application d'un ensemble fini vers un ensemble de même cardinal) montre que les p_i ne sont pas injectifs. En particulier, il existe $x \neq y$ dans X tels que $p_1(x) = p_1(y)$. On a alors

   $$f(x) = p_n \circ \cdots \circ p_1(x) = p_n \circ \cdots \circ p_1(y) = f(y),$$

   donc f n'est pas injective, donc $\boxed{\text{pas bijective}}$.

   La seule application pour laquelle ce raisonnement ne tient pas est l'application id_X s'écrivant bien comme composée d'applications idempotentes (composée de facteurs id_X, autant qu'on veut).