

1 Ensembles, Applications

Exercice 1.1. — A toute partie A de E , on associe la fonction $\mathbb{1}_A$ de E dans $\{0, 1\}$ définie par : $\mathbb{1}_A(x) = 1$, si $x \in A$, $\mathbb{1}_A(x) = 0$, sinon. On appelle $\mathbb{1}_A$ la fonction caractéristique de A .

1. (a) Montrer que $\mathcal{P}(E)$ est en bijection avec $\{0, 1\}^E$, l'ensemble des applications de E vers $\{0, 1\}$.
 (b) Montrer que $|A| = \sum_{x \in E} \mathbb{1}_A(x)$.
2. (a) Montrer que $\mathbb{1}_A + \mathbb{1}_{\bar{A}} = 1$.
 (b) Montrer que $\mathbb{1}_{A \cap B} = \mathbb{1}_A \mathbb{1}_B$.
 (c) Montrer que $\mathbb{1}_{A \cup B} = \mathbb{1}_A + \mathbb{1}_B - \mathbb{1}_A \mathbb{1}_B$.
3. (a) Montrer que $\mathbb{1}_{\bigcup_{i=1}^n A_i} = 1 - \prod_{i=1}^n (1 - \mathbb{1}_{A_i})$.
 (b) En déduire la formule du crible : $\left| \bigcup_{i=1}^n A_i \right| = \sum_{k=1}^n (-1)^{k+1} \left(\sum_{i_1 < \dots < i_k} |A_{i_1}| \cdots |A_{i_k}| \right)$.

Exercice 1.2. — Compter le nombre d'entiers entre 1 et 1000, qui ne sont divisibles ni par 5, ni par 7, ni par 13.

Exercice 1.3. — Soit E un ensemble. Pour $A, B \in \mathcal{P}(E)$, on appelle différence symétrique $A \Delta B = (A \setminus B) \cup (B \setminus A)$.

1. (a) Montrer que $A \Delta B = (A \cup B) \setminus (A \cap B)$.
 (b) Montrer que $A \Delta B = B \Delta A$
 (c) $A \Delta \emptyset = A, A \Delta A = \emptyset$
2. (a) Montrer que $\mathbb{1}_{A \Delta B} = (\mathbb{1}_A - \mathbb{1}_B)^2 = |\mathbb{1}_A - \mathbb{1}_B|$.
 (b) $A \Delta (B \Delta C) = (A \Delta B) \Delta C$.
3. Lorsque E est fini non vide, trouver une bijection entre les parties de E de cardinal pair et les parties de E de cardinal impair.

Exercice 1.4. — Soit X et Y deux ensembles. Montrer que

$$X = Y \Leftrightarrow X \cup Y = X \cap Y.$$

Exercice 1.5. — Soit E en ensemble non vide et A et B deux parties non vides de E et f l'application de $\mathcal{P}(E)$ dans $\mathcal{P}(A) \times \mathcal{P}(B)$ définie par : $f(X) = (X \cap A, X \cap B)$.

- Montrer que f est injective si et seulement si $A \cup B = E$.
- Montrer que f est surjective si et seulement si $A \cap B = \emptyset$.
- Déterminer f^{-1} dans le cas où f est bijective.

Exercice 1.6. — Soit X, Y et Z trois ensembles. Soit $f : X \rightarrow Y$ et $G : Y \rightarrow Z$.

- Montrer que si $g \circ f$ est surjective alors g est surjective.
- Montrer que si $g \circ f$ est injective alors f est injective.
- Montrer que si f et g sont injectives alors $g \circ f$ est injective.
- Montrer que si f et g sont surjectives alors $g \circ f$ est surjective.

Exercice 1.7. — Soit E en ensemble non vide et A et B deux parties non vides de E et f l'application de $\mathcal{P}(E)$ dans $\mathcal{P}(A) \times \mathcal{P}(B)$ définie par : $f(X) = (X \cap A, X \cap B)$.

- Montrer que f est injective si et seulement si $A \cup B = E$.
- Montrer que f est surjective si et seulement si $A \cap B = \emptyset$.
- Déterminer f^{-1} dans le cas où f est bijective.

Exercice 1.8. — Soit E et F deux ensembles et f une application de E dans F .

- Démontrer que pour toute famille (A_i) de parties de E on a :

$$f\left(\bigcup_{i \in I} A_i\right) = \bigcup_{i \in I} f(A_i), \quad f\left(\bigcap_{i \in I} A_i\right) \subset \bigcap_{i \in I} f(A_i).$$

Donner un exemple d'inclusion stricte.

- Démontrer que pour toute famille (B_i) de parties de F on a :

$$f^-(\bigcup_{i \in I} A_i) = \bigcup_{i \in I} f^-(A_i), \quad f^-(\bigcap_{i \in I} A_i) = \bigcap_{i \in I} f^-(A_i), \quad f^-(F \setminus B) = E \setminus f^-(B).$$

- Montrer que l'on a pour tout $X \subset E$ et tout $Y \subset F$:

$$X \subset f^-(f(X)), \quad f(f^-(Y)) \subset Y.$$

- Montrer que f est injective si et seulement si pour tout $X, Y \in \mathcal{P}(E)$, on a $f(X \cap Y) = f(X) \cap f(Y)$.

Exercice 1.9. — Soit A et B deux ensembles finis.

- Montrer qu'il existe une injection de A dans B si et seulement si $|A| \leq |B|$.
- Montrer qu'il existe une surjection de B sur A si et seulement si $|A| \leq |B|$.

Exercice 1.10. — Soit E et F deux ensembles de même cardinal fini et $f : E \rightarrow F$. Montrer que les propositions suivantes sont équivalentes :

- i) f est injective. ii) f est surjective. iii) f est bijective.

Exercice 1.11. — Soit E un ensemble.

- Montrer qu'il existe une injection de E dans $\mathcal{P}(E)$.
- Montrer qu'il n'existe pas de surjection de E sur $\mathcal{P}(E)$. *On pourra raisonner par contradiction en considérant pour f surjective, l'ensemble $A = \{x \in E; x \notin f(x)\}$.*
- Montrer qu'il n'existe pas d'injection de $\mathcal{P}(E)$ dans E .
- Construire une bijection explicite entre \mathbb{N} et l'ensemble de ses parties finies (indication : on utilisera l'existence et l'unicité de l'écriture d'un entier naturel en base 2, qui est admise ici).

Exercice 1.12. — Soit φ une injection de \mathbb{N} dans \mathbb{N} . Montrer que $\lim_{n \rightarrow +\infty} \varphi(n) = +\infty$.

Exercice 1.13. — Montrer que les applications suivantes de \mathbb{N}^2 dans \mathbb{N} sont des bijections :

$$(x, y) \mapsto x + \frac{1}{2}(x+y)(x+y+1), \quad (x, y) \mapsto 2^y(2x+1)-1.$$

2 Algorithme d'Euclide. Pgcd

Exercice 2.1. — Soit $n \geq 2$ un entier. Trouver le pgcd et les coefficients de Bézout correspondants de $n - 1$ et $n + 1$ ainsi que ceux de $n^2 + 1$ et $n^3 - n$.

Exercice 2.2. — Résoudre l'équation $(2n + 8, 3n + 15) = 6$.

Exercice 2.3. — Résoudre dans \mathbf{Z}^2 les équations suivantes :

$$(a) 5x - 18y = 4, \quad (b) 12x + 7y = 15, \quad (c) 6x + 15y = 28, \quad (d) 1681x + 1271y = 99999$$

Exercice 2.4. — Soit a, b, c des éléments d'un anneau euclidien (\mathbf{Z} par exemple)

1. (a) Montrer que si $(a, c) = 1$ et $(b, c) = 1$, alors $(ab, c) = (a, c)(b, c) = 1$.
 (b) Montrer que $((a, c), (b, c)) | ((a, b), c)$.
2. On suppose à présent que $(a, b) = 1$.
 - (a) Montrer que $(a^n, b^m) = 1$ pour tous $n, m \in \mathbf{N}$.
 - (b) Montrer que si $k \in \mathbf{Z}$ divise b alors $(k, b) = 1$.
 - (c) En déduire que pour tout $c \in \mathbf{Z}$, on a $(a, bc) = (a, c)$.
 - (d) Montrer que $(ab, c) = (a, c)(b, c)$.

Exercice 2.5. —

1. Si $t > 1$ est un entier et $t^m - 1 \mid t^n - 1$ alors $m \mid n$.
2. Montrer que si $(a, b) = 1$ alors $(a^m - b^m, a^n - b^n) = a^{(m,n)} - b^{(m,n)}$.

Exercice 2.6. — Suite de Fibonacci.

On considère la *suite de Fibonacci* $(F_n)_{n \geq 0}$ d'éléments de \mathbf{N} , définie par $F_0 = 0$, $F_1 = 1$, $F_{n+1} = F_n + F_{n-1}$.
 On pose $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$.

1. Montrer que pour tout entier $n \geq 1$, on a l'identité $A^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$.
2. En déduire la relation $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$.
3. Montrer que $F_{n+m} = F_{n+1}F_m + F_nF_{m-1}$.
4. Montrer que $(F_n, F_{m+n}) = (F_n, F_m)$, puis que $(F_n, F_m) = F_{(n,m)}$.

Exercice 2.7. — Écriture matricielle dans l'algorithme d'Euclide

Soit $a, b \in \mathbf{Z}$. Posons $r_0 = a$, $r_1 = b$, $u_0 = 1$, $v_0 = 1$, $u_1 = 1$, $v_1 = 1$ et définissons par récurrence pour $i \geq 1$,

$$r_{i+1} = r_{i-1} - q_i r_i, \quad u_{i+1} = u_{i-1} - q_i u_i, \quad v_{i+1} = v_{i-1} - q_i v_i,$$

où q_i est un entier relatif quelconque.

1. Montrer que pour tout $i \geq 0$, on a $\text{pgcd}(r_i, r_{i+1}) = \text{pgcd}(a, b)$ et $u_i a + v_i b = r_i$.
2. (a) Montrer qu'on a pour tout $i \geq 1$, $\begin{pmatrix} r_i & u_i & v_i \\ r_{i+1} & u_{i+1} & v_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \cdot \begin{pmatrix} r_{i-1} & u_{i-1} & v_{i-1} \\ r_i & u_i & v_i \end{pmatrix}$
 (b) Montrer que pour tout $i \geq 0$, on a $\begin{vmatrix} u_i & v_i \\ u_{i+1} & v_{i+1} \end{vmatrix} = (-1)^i$.
3. A présent, on définit q_i et $r_{i+1}, u_{i+1}, v_{i+1}$ de la façon suivante, pour $i \geq 1$:
 Si $r_i = 0$ alors $r_{i+1} = r_i$, $u_{i+1} = u_i$, $v_{i+1} = v_i$, sinon $q_i = u_{i-1} \div u_i$ (le quotient de u_{i-1} par u_i , tel que $0 \leq u_{i-1} - q_i u_i < |u_i|$) et $r_{i+1} = r_{i-1} - q_i r_i$, $u_{i+1} = u_{i-1} - q_i u_i$, $v_{i+1} = v_{i-1} - q_i v_i$.
 - (a) Montrer que la suite r_i est décroissante pour $i \geq 1$.
 - (b) Montrer que il existe un rang n tel que $r_n = d \neq 0$ et $r_{n+1} = 0$. Montrer que d est le pgcd de a et b .
 - (c) $u_{n+1} = \frac{b}{d}(-1)^{n+1}$, $v_{n+1} = \frac{a}{d}(-1)^n$.
4. On suppose ici que $0 < b < a$.
 - (a) Montrer que les suites u_i et v_i sont de signes alternés et croissantes en valeur absolue.
 - (b) Montrer que $|u_n| \leq \frac{b}{2d}$, $|v_n| \leq \frac{a}{2d}$ (on notera que $q_n \geq 2$).