

CORRECTION PARTIEL 2022-2023

Exercice 1.

1. Si E, F sont deux ensembles, on note E^F pour l'ensemble des fonctions de F dans E . On a une bijection $\mathcal{P}(E) \rightarrow \{0, 1\}^E$, envoyant une partie $A \subset E$ sur l'indicatrice 1_A de A . La bijection réciproque $\{0, 1\}^E \rightarrow \mathcal{P}(E)$ envoie $f : E \rightarrow \{0, 1\}$ sur $f^*(\{1\})$.

Comme les ensembles $\mathcal{P}(E)$ et $\{0, 1\}^E$ sont en bijection (et qu'ils sont finis), ils ont le même nombre d'éléments. Or, il y a 2^n éléments dans $\{0, 1\}^E$. En effet, le choix d'une fonction $E \rightarrow \{0, 1\}$ correspond à celui, pour chacun des n éléments de E , de son image dans $\{0, 1\}$. Il y a 2 choix possible pour chaque éléments, d'où un total de 2^n éléments dans $\{0, 1\}^E$.

2. L'ensemble $\{1, 2, 3\}$ contient 3 éléments, donc l'ensemble $\mathcal{P}(E)$ en contient $2^3 = 8$ d'après la question précédente.

- Il y a (comme toujours) une unique partie contenant 0 éléments : la partie vide \emptyset .
- Les parties à 1 élément sont $\{1\}, \{2\}, \{3\}$.
- Les parties à 2 éléments sont les complémentaires des parties à 1 élément. Ce sont donc $\{2, 3\}, \{1, 3\}, \{1, 2\}$.
- Les parties à 3 éléments sont les complémentaires des parties à 0 éléments. Il y a donc une unique partie à 3 éléments, qui est E lui-même.

On obtient donc

$$\mathcal{P}(\{1, 2, 3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{2, 3\}, \{1, 3\}, \{1, 2\}, \{1, 2, 3\}\}.$$

Exercice 2.

1. On doit supposer que $E \neq \emptyset$ (sinon le résultat est faux). On fixe $x_0 \in E$. Soit $y \in F$, on a deux possibilités :

- Si $y \in f_*(E)$, i.e. si il existe $x \in E$ tel que $f(x) = y$. Il existe alors par injectivité un unique $x \in E$ tel que $f(x) = y$, et on peut poser $g(y) = x$.
- Si $y \notin f_*(E)$, alors on pose (arbitrairement) $g(y) = x_0$.

Pour $x \in E$, on a $f(x) \in f_*(E)$ par définition, et x est l'unique antécédent de $f(x)$ par f . Par construction de g , on a alors $(g \circ f)(x) = g(f(x)) = x$. Comme ceci est vrai pour tout $x \in E$, on a bien $g \circ f = \text{Id}_E$.

2. La non-unicité de g repose notamment sur le choix de x_0 que nous avons fait dans la question précédente. Ici, pour $x_0 = 0$, on trouve

$$g_0(0) = 0, \quad g_0(1) = 1, \quad g_0(2) = x_0 = 0.$$

Pour $x_1 = 1$, on trouve

$$g_1(0) = 0, \quad g_1(1) = 1, \quad g_1(2) = x_1 = 1.$$

D'après la question précédente, on a $g_0 \circ f = g_1 \circ f = \text{Id}_E$, tout en ayant $g_0 \neq g_1$.

3. On a

$$\begin{aligned} f^*(\{0\}) &= \{x \in E \mid f(x) = 0\} = \{0\}, \\ f^*(\{2\}) &= \{x \in E \mid f(x) = 2\} = \emptyset, \\ f_*(\{0, 1\}) &= \{f(0), f(1)\} = \{0, 1\}. \end{aligned}$$

Exercice 3.

1. On procède par récurrence sur d . Premièrement pour $d = 1$, on pose $\varphi : \mathbb{N} \rightarrow \mathbb{Z}$ définie par

$$\begin{cases} \varphi(2n) = n, \\ \varphi(2n+1) = -n. \end{cases}$$

Cette fonction est surjective. Donc \mathbb{Z} est dénombrable (et clairement infini).

Supposons maintenant que \mathbb{Z}^d est dénombrable pour un certain $d \geq 1$. On a par hypothèse une surjection $\psi : \mathbb{N} \rightarrow \mathbb{Z}^d$. L'application $(n, m) \mapsto (\varphi(n), \psi(m)) \in \mathbb{Z}^d \times \mathbb{Z} = \mathbb{Z}^{d+1}$ est une surjection $\mathbb{N}^2 \rightarrow \mathbb{Z}^{d+1}$. Comme \mathbb{N}^2 et \mathbb{N} sont équipotents, on obtient qu'il existe une surjection $\mathbb{N} \rightarrow \mathbb{Z}^{d+1}$, et donc \mathbb{Z}^{d+1} est dénombrable.

L'ensemble $\mathbb{Z}^{\mathbb{N}}$ n'est pas dénombrable car il contient en particulier $\{0, 1\}^{\mathbb{N}}$, qui est en bijection avec $\mathcal{P}(\mathbb{N})$, et donc indénombrable.

2. Par définition, $\mathbb{Z}_d[X]$ est inclus dans l'ensemble des polynômes de degré au plus d , que nous notons $\mathbb{Z}_{\leq d}[X]$. On a une bijection $\mathbb{Z}^{d+1} \rightarrow \mathbb{Z}_{\leq d}[X]$, envoyant (a_0, \dots, a_d) sur $a_0 + a_1X + \dots + a_dX^d$. Comme \mathbb{Z}^{d+1} est dénombrable d'après la question précédente, on déduit que $\mathbb{Z}_{\leq d}[X]$ est dénombrable. L'ensemble $\mathbb{Z}_d[X]$ est alors dénombrable comme sous-ensemble d'un ensemble dénombrable.

3. Par définition, on a

$$\mathbb{Z}[X] = \bigcup_{d \geq 0} \mathbb{Z}_d[X].$$

L'ensemble $\mathbb{Z}[X]$ est alors une union dénombrable (indexée par \mathbb{N}) d'ensembles qui sont dénombrables d'après la question précédente. Il s'agit alors d'un ensemble dénombrable.

4. Pour $P \in \mathbb{Z}[X] \setminus \{0\}$, on pose $\rho(P)$ l'ensemble des racines de P dans \mathbb{C} . Si P est de degré d , on sait que $\text{Card}(\rho(P)) \leq d$. En particulier, $\rho(P)$ est fini (donc dénombrable). Par définition, $\overline{\mathbb{Q}}$ est formé des nombres qui appartiennent à un certain $\rho(P)$ pour (au moins) un $P \in \mathbb{Z}[X] \setminus \{0\}$. On a donc

$$\overline{\mathbb{Q}} = \bigcup_{P \in \mathbb{Z}[X] \setminus \{0\}} \rho(P).$$

L'ensemble $\overline{\mathbb{Q}}$ est alors une union dénombrable (indexée par $\mathbb{Z}[X] \setminus \{0\} \subset \mathbb{Z}[X]$) d'ensembles finis, donc dénombrables. Il s'agit alors d'un ensemble dénombrable. De même, $\overline{\mathbb{Q}} \cap \mathbb{R}$ est dénombrable comme sous-ensemble d'un ensemble dénombrable.

5. On sait que \mathbb{R} est indénombrable, donc $\overline{\mathbb{Q}} \cap \mathbb{R}$, qui est dénombrable, ne peut pas être égal à \mathbb{R} . Il existe donc des éléments dans $\mathbb{R} \setminus (\overline{\mathbb{Q}} \cap \mathbb{R})$, c'est à dire des nombres réels qui ne sont pas dans $\overline{\mathbb{Q}}$, autrement dit qui ne sont pas racines d'un polynôme non nul à coefficients dans $\mathbb{Z}[X]$.

Exercice 4.

1. Les deux ensembles sont égaux, en effet pour $z \in \mathbb{C}$, on a

$$\begin{aligned} |z - z_0| = r &\Leftrightarrow \left| \frac{z}{r} - \frac{z_0}{r} \right| = 1 \\ &\Leftrightarrow \exists \theta \in [0, 2\pi] \mid \frac{z}{r} - \frac{z_0}{r} = e^{i\theta} \\ &\Leftrightarrow \exists \theta \in [0, 2\pi] \mid z - z_0 = re^{i\theta} \\ &\Leftrightarrow \exists \theta \in [0, 2\pi] \mid z = z_0 + re^{i\theta} \end{aligned}$$

Ensuite, le premier ensemble (égal au second) est par définition constitué des nombres complexes dont la distance avec z_0 est égale à r : Il s'agit du cercle de centre z_0 et de rayon r .

2. Soient $z_0 \in \mathbb{C}$ et $r > 0$. Le cercle de centre z_0 et de rayon r passe par les trois points z_1, z_2, z_3 si et seulement si

$$r = |z_0 - z_1| = |z_0 - z_2| = |z_0 - z_3|.$$

En particulier, la distance entre z_0 et z_1 est égale à la distance entre z_0 et z_2 . Autrement dit, z_0 est sur la médiatrice de z_1, z_2 , qui est une droite perpendiculaire à la droite (z_1z_2) . De même, on obtient que z_0 est sur la médiatrice de z_2, z_3 . Comme z_1, z_2, z_3 ne sont pas alignés, les droites (z_1z_2) et (z_2z_3) ne sont pas parallèles, et les médiatrices respectives de z_1, z_2 et z_2, z_3 ne sont pas parallèles. Ces deux médiatrices ont donc un unique point d'intersection, qui doit être égal au point z_0 . Il y a donc au plus un cercle qui passe par z_1, z_2, z_3 .

Réciproquement, le point z_0 , défini comme intersection des deux médiatrices précédentes, est à égale distance de z_1 et de z_2 , et à égale distance de z_2, z_3 . Par transitivité, il est à égale distance de z_1, z_2, z_3 , et donc le cercle de centre z_0 et de rayon $|z - z_0|$ passe bien par les trois points z_1, z_2, z_3 .

3. On note d la médiatrice de z_1, z_2 . Soit $C \in \mathcal{C}_{z_1, z_2}$, on pose $f(C)$ comme étant le centre du cercle C (ce centre est unique). Par définition, on a $z_1, z_2 \in C$, et donc $|z_1 - f(C)| = |z_2 - f(C)|$, autrement dit $f(C)$ se trouve sur la droite d . L'application f induit donc une application $\mathcal{C}_{z_1, z_2} \rightarrow d$.

Prouvons que f est une bijection. Premièrement, soit $z_0 \in d$. Par définition, on a $|z_1 - z_0| = |z_2 - z_0|$, et donc le cercle C de centre z_0 et de rayon $|z_1 - z_0|$ est un élément de \mathcal{C}_{z_1, z_2} , avec $f(C) = z_0$. L'application f est donc surjective. Ensuite, soient $C_1, C_2 \in \mathcal{C}_{z_1, z_2}$ tels que $f(C_1) = f(C_2)$. On a que C_2 est le cercle de centre $f(C_2) = f(C_1)$ et de rayon $|f(C_2) - z_1| = |f(C_1) - z_1|$. Les cercles C_1, C_2 ont donc le même centre et le même rayon : ils sont égaux, et f est injective. Comme f est injective et surjective, c'est une bijection.

4. On sait que la droite d est en bijection avec \mathbb{R} (c'est un sous-espace affine de dimension 1 de $\mathbb{C} \simeq \mathbb{R}^2$). On a donc une bijection entre \mathcal{C}_{z_1, z_2} et \mathbb{R} , qui est indénombrable.

5. Comme \mathbb{Q} est dénombrable, on sait que \mathbb{Q}^2 est lui aussi dénombrable. On a une surjection $\mathbb{Q}^2 \rightarrow \mathbb{Q} + i\mathbb{Q}$, qui envoie $(a, b) \rightarrow a + ib$. L'ensemble $\mathbb{Q} + i\mathbb{Q}$ est alors dénombrable.

6. On pose $E := (\mathbb{Q} + i\mathbb{Q}) \setminus ((z_1 z_2) \cap \mathbb{Q} + i\mathbb{Q})$ l'ensemble des points à coordonnées rationnelles qui ne sont pas alignés avec z_1, z_2 . Pour $z \in E$, il existe d'après la question 1 un unique cercle qui passe par z_1, z_2 et z . On pose $g(z)$ pour ce cercle, et on obtient une application g de E vers l'ensemble des cercles de \mathcal{C}_{z_1, z_2} qui passent par un point de $\mathbb{Q} + i\mathbb{Q}$.

Montrons que g est une surjection. Soit $C \in \mathcal{C}_{z_1, z_2}$ qui contient un point $z \in \mathbb{Q} + i\mathbb{Q}$. Comme l'intersection $(z_1 z_2) \cap C$ est réduite à $\{z_1, z_2\}$, le point z n'est pas aligné avec z_1, z_2 et donc $z \in E$. On a alors $g(z) = C$, et donc g est surjective. Comme E est dénombrable (comme sous-ensemble de $\mathbb{Q} + i\mathbb{Q}$), on déduit que l'ensemble des cercles de \mathcal{C}_{z_1, z_2} qui passent par un point de $\mathbb{Q} + i\mathbb{Q}$ est dénombrable.

7. Comme l'ensemble \mathcal{C}_{z_1, z_2} est indénombrable, il ne peut pas être égal au sous-ensemble des cercles de \mathcal{C}_{z_1, z_2} qui passent par un point de $\mathbb{Q} + i\mathbb{Q}$. Il existe donc un élément de \mathcal{C}_{z_1, z_2} qui ne passe par aucun point de $\mathbb{Q} + i\mathbb{Q}$, à part peut-être z_1, z_2 .