Feuille de TD n° 4

Ensembles dénombrables, Permutations, Groupes

22 mars 2022

■ *Pour commencer . . .*

Exercice 1.
Dire si les ensembles suivants sont dénombrables :

1. $\{2^n \mid n \geq 0\}$;
2. $\mathbb{N} \times \mathbb{R}$;
3. $\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$;
4. L'ensemble des nombres premiers ;
5. L'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$.

---

1) et 4) sont des parties infinies de $\mathbb{N}$, donc elles sont dénombrables.
2) Cet ensemble contient l'ensemble $\{0\} \times \mathbb{R}$ qui est en bijection avec $\mathbb{R}$ et est donc indénombrable. Donc $\mathbb{N} \times \mathbb{R}$ est indénombrable.
3) $\sqrt{2}$ est irrationnel donc si $a + b\sqrt{2} = c + d\sqrt{2}$ avec $a, b, c, d \in \mathbb{Q}$, alors $a = c$ et $b = d$. Donc on peut définir

$$\varphi : \begin{array}{ccc} \mathbb{Q}[\sqrt{2}] & \longrightarrow & \mathbb{Q}^2 \\ a + b\sqrt{2} & \longmapsto & (a, b) \end{array}.$$

φ est alors injective. Or $\mathbb{Q}^2$ est dénombrable donc $\mathbb{Q}[\sqrt{2}]$ est au plus dénombrable. Or $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}]$ donc $\mathbb{Q}[\sqrt{2}]$ est infini. Finalement $\mathbb{Q}[\sqrt{2}]$ est dénombrable.
5) La fonction ψ de $\mathbb{R}$ dans $\mathcal{F}(\mathbb{R}, \mathbb{R})$, qui à $c \in \mathbb{R}$ associe la fonction constante à c, est injective. Or $\mathbb{R}$ n'est pas dénombrable donc $\mathcal{F}(\mathbb{R}, \mathbb{R})$ n'est pas dénombrable.

Exercice 2.

1. $\mathcal{S}_2$ est-il un groupe abélien ?
2. On considère $\sigma_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}$ et $\sigma_2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{bmatrix}$ deux éléments de $\mathcal{S}_4$.
   (a) Calculer $\sigma_1 \circ \sigma_2$ et $\sigma_2 \circ \sigma_1$.
   (b) Écrire ces deux composées comme des transpositions.
   (c) $\mathcal{S}_4$ est-il un groupe abélien ?
   (d) Que valent σ_1^{-1} et σ_2^{-1} ?

---

1. $\mathcal{S}_2$ contient deux éléments : l'identité et la transposition $\begin{pmatrix} 1 & 2 \end{pmatrix}$. $\mathcal{S}_2$ est donc clairement commutatif.
2. (a) On utilise la méthode du cours. On obtient
$$\sigma_1 \circ \sigma_2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{bmatrix} \quad \text{et} \quad \sigma_2 \circ \sigma_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{bmatrix}.$$
   (b) On remarque que $\sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 4 \end{pmatrix}$ et $\sigma_2 \circ \sigma_1 = \begin{pmatrix} 3 & 4 \end{pmatrix}$.
   (c) On a $\sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1$ donc $\mathcal{S}_4$ n'est pas abélien.
   (d) σ_1 et σ_2 sont des transpositions donc sont leurs propres inverses.

Exercice 3.
Soit $n \in \mathbb{N}^*$. Soient i, j, $k \in [\![1, n]\!]$.

1. Calculer $\begin{pmatrix} i & j \end{pmatrix} \begin{pmatrix} i & k \end{pmatrix}$.
2. Calculer $\begin{pmatrix} i & j \end{pmatrix} \begin{pmatrix} i & k \end{pmatrix} \begin{pmatrix} i & j \end{pmatrix}$.
3. Soit $\sigma \in \mathcal{S}_n$, que vaut $\sigma \begin{pmatrix} i & j \end{pmatrix} \sigma^{-1}$?

---

1. On note $\gamma = \begin{pmatrix} i & j \end{pmatrix} \begin{pmatrix} i & k \end{pmatrix}$. Pour tout $x \in [\![1, n]\!] \setminus \{i, j, k\}$, $\gamma(x) = x$. De plus, $\gamma(i) = k$, $\gamma(k) = j$ et $\gamma(j) = i$. On dit que γ est un 3-cycle et on note $\gamma = \begin{pmatrix} i & j & k \end{pmatrix}$.
2. On note $\delta = \begin{pmatrix} i & j \end{pmatrix} \begin{pmatrix} i & k \end{pmatrix} \begin{pmatrix} i & j \end{pmatrix}$, on a $\delta(i) = i$, $\delta(j) = k$ et $\delta(k) = j$. Tous les autres points sont fixes donc $\delta = \begin{pmatrix} j & k \end{pmatrix}$.
3. Soit $\theta = \sigma \begin{pmatrix} i & j \end{pmatrix} \sigma^{-1}$. Si $x \in [\![1, n]\!]$ avec $\sigma^{-1}(x) \notin \{i, j\}$, on a $\theta(x) = \sigma(\sigma^{-1}(x)) = x$. Maintenant, $\theta(\sigma(i)) = \sigma(j)$ et $\theta(\sigma(j)) = \sigma(i)$. Finalement, $\sigma \begin{pmatrix} i & j \end{pmatrix} \sigma^{-1} = \begin{pmatrix} \sigma(i) & \sigma(j) \end{pmatrix}$.

■ *Pour aller plus loin . . .*

Exercice 4. *Dans cet exercice, on admet qu'une union dénombrable d'ensembles finis est au plus dénombrable : si pour tout $n \in \mathbb{N}$, A_n est un ensemble fini, alors $\cup_{n\in\mathbb{N}} A_n$ est au plus dénombrable.*

Soit $f : [a,b] \longrightarrow \mathbb{R}$ une fonction croissante. Pour tout $x \in]a,b[$, on définit

$$\delta(x) = \lim_{y\to x^+} f(y) - \lim_{y\to x^-} f(y).$$

Pour tout $n \in \mathbb{N}^*$, on définit

$$E_n = \left\{ x \in]a,b[\mid \delta(x) > \frac{1}{n} \right\}.$$

1. Montrer que pour tout $n \in \mathbb{N}^*$, E_n est fini.
2. En déduire que l'ensemble des points de discontinuité de f est au plus dénombrable.

---

1. Soit $n \in \mathbb{N}^*$. Soit $N \in \mathbb{N}$, on suppose qu'il existe $x_1 < \ldots < x_N \in E_n$. Alors pour tout $x_1 < x \leq b$, comme f est croissante,

   $$f(x) \geq \lim_{y\to x_1^+} f(y) = \delta(x_1) + \lim_{y\to x_1^-} f(y) > \frac{1}{n} + f(a).$$

   Par récurrence, on peut montrer que pour tout $x > x_N$, $f(x) > \frac{N}{n} + f(a)$, et donc $n\big(f(b)-f(a)\big) > N$. Ainsi le cardinal de E_n est plus petit que $n\big(f(b)-f(a)\big)$, c'est-à-dire E_n est fini.
2. Soit E l'ensemble des points de discontinuité de f :

   $$E = \{x \in]a,b[\mid \delta(x) \neq 0\} = \{x \in]a,b[\mid \delta(x) > 0\},$$

   car f est croissante. On a donc

   $$E = \cup_{n\in\mathbb{N}^*} E_n,$$

   et E est donc au plus dénombrable.

Un peu d'Algèbre . . .

Exercice 5.
Soient $(G,\star)$ et H un sous-groupe avec $H \neq G$.
Le complémentaire de H est-il un sous-groupe ? Dire pourquoi.
Déterminer le sous-groupe engendré par le complémentaire de H.

Le complémentaire de H n'est pas un sous-groupe car il ne contient pas l'élément neutre e.
Soit K le sous-groupe engendré par le complémentaire de H. Alors $H \cup K = G$ est un groupe. On a donc d'après le cours que $H \subset K$. Comme K contient aussi $\bar{H}$, on a $K = G$.

Exercice 6.

1. Soit $(G,\star)$ un groupe commutatif. Soient $x \in G$ un élément d'ordre p et $y \in G$ un élément d'ordre q. Montrer que xy est d'ordre au plus pq.
2. xy est-il nécessairement d'ordre pq ? (donnez des exemples)
3. On pose $H = \mathrm{Bij}\,(\mathbb{Z}\times\mathbb{Z})$.
   Montrer que $f : (m,n) \mapsto (-n,m)$ et $g : (m,n) \mapsto (n,-m-n)$ sont des éléments de $(H,\circ)$ d'ordres 4 et 3.
   Quel est l'ordre de $f \circ g$?

---

1. Le groupe G étant commutatif, on a : $(xy)^{pq} = (x^p)^q (y^q)^p = 1^q 1^p = 1$. Donc xy est d'ordre au plus pq.
2. Non. Par exemple $-I_n$ est d'ordre 2 dans $Gl_n(\mathbb{K})$, et $(-I_n)(-I_n) = iI_n$ n'est pas d'ordre 4 mais d'ordre 1.
   Par contre, dans $\mathbb{C}^*$, $a = \exp(i\pi)$ est d'ordre 2, $b = \exp(2i\pi/3)$ est d'ordre 3 et $ab = \exp(5i\pi/6)$ est d'ordre 6.
3. On trouve $f^4 = id$ et $g^3 = id$, ce qui prouve que f et g sont des bijections de $\mathbb{Z}\times\mathbb{Z}$ d'ordre respectif 4 et 3. Enfin, $f \circ g(m,n) = (m+n,n)$ et $(f\circ g)^k(1,0) = (k,0)$, donc $(f\circ g)^k \neq Id$ pour $k > 0$. On en déduit que $f \circ g$ est d'ordre infini et pas d'ordre au plus 6. Cela ne contredit pas la première question, car l''hypothèse G commutatif n'est pas vérifiée.

Exercice 7.
1. Pour $(G,\star)$ un groupe, quels sont les éléments de G d'ordre 1 ?
2. Combien vaut $ord(x^{-1})$ en fonction de $ord(x)$?
3. Trouver des matrices de $Gl_3(\mathbb{R})$ d'ordres 2 et 3.
4. Soient $n \geq 2$ et $M \in Gl_n(\mathbb{R})$ une matrice diagonale. On suppose que M est d'ordre fini.
   Déterminer $ord(M)$.

5. Soit $n \geq 2$. On pose $G = Bij(\{1, \ldots, n\})$. On prend $f \in G$ avec $f(i) = i+1$ pour $1 \leq i \leq n-1$ et $f(n) = 1$.
   Calculer l'ordre de f dans $(G, \circ)$.

---

1. Si x est d'ordre 1, alors il vérifie $x^1 = e$, donc $x = e$.
2. On a $x^k = e$ si et seulement si on a $e = x^{-k} = (x^{-1})^k$. Donc, $ord(x^{-1}) = ord(x)$.
3. La matrice $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ est d'ordre 3.
   La matrice $-I_3$ est d'ordre 2.
4. On a $M = Diag(\lambda_1, \ldots, \lambda_n)$, avec $\lambda_i \neq 0$. M est d'ordre fini, donc il existe $k > 0$ tel que $M^k = I_n$.
   Cela veut dire que l'on a $\lambda_i^k = 1$, pour tout $1 \leq i \leq n$. Comme les λ_i sont réels, cela implique que $\lambda_i = 1$ ou -1.
   Ainsi, la diagonale de la matrice M est à valeurs dans $\{-1, 1\}$.
   On obtient que si $M = I_n$, alors M est d'ordre 1, et sinon M est d'ordre 2 (on a $M^2 = I_n$).
5. La fonction f est d'ordre n dans $(G, \circ)$.
   Montrons que $f^n = Id$ et que $f^k \neq Id$ pour $1 \leq k \leq n-1$.
   Pour $0 \leq k \leq n-1$, on a $f^k(1) = f \circ \ldots \circ f(1) = k+1$.
   Cela montre déjà que l'ordre de f est infini ou strictement supérieur à n.
   Ensuite, pour tout $1 \leq i \leq n$, on a $f^{n-i}(i) = f^{n-i}(f^i(1)) = f^n(1) = n$.
   Ainsi, on a $f^n(i) = f^i(f^{n-i}(i)) = f^i(n) = f^{i-1}(f(n)) = f^{i-1}(1) = i$.
   Cela montre que $f^n = f \circ \ldots \circ f = Id$.
   Donc, f est un élément d'ordre n dans $(G, \circ)$.

Exercice 8. On pose $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2};\ a, b \in \mathbb{Z}\}$.

1. Montrer que $(\mathbb{Z}[\sqrt{2}], +)$ est un sous-groupe de $(\mathbb{R}, +)$.
2. Montrer que $\mathbb{Z}[\sqrt{2}] \setminus \{0\}$ est stable pour $\times$, mais que $(\mathbb{Z}[\sqrt{2}] \setminus \{0\}, \times)$ n'est pas un groupe.
3. On note $N(a + b\sqrt{2}) = a^2 - 2b^2$.
   Montrer que, pour tous x, y de $\mathbb{Z}[\sqrt{2}]$, on a $N(xy) = N(x)N(y)$.
4. En déduire que les éléments inversibles de $\mathbb{Z}[\sqrt{2}]$ sont ceux s'écrivant $a + b\sqrt{2}$ avec $a^2 - 2b^2 = \pm 1$.

— non-vide.
— stable par la loi + : $(a + b\sqrt{2}) + (a' + b'\sqrt{2}) = (a + a') + (b + b')\sqrt{2}$.
— stable par la loi $\times$:

$$(a + b\sqrt{2}) \times (a' + b'\sqrt{2}) = (aa' + 2bb') + (ab' + a'b)\sqrt{2}$$

.
— stable par passage à l'opposé $-(a + b\sqrt{2}) = -a + (-b)\sqrt{2}$.

Cela montre que $\mathbb{Z}[\sqrt{2}]$ est un sous-groupe de $(\mathbb{R}, +)$.
De plus, 2 n'est pas inversible dans $\mathbb{Z}[\sqrt{2}]$, car sinon on aurait $\frac{1}{2} = a + b\sqrt{2}$, ce qui contredirait le fait que $\sqrt{2}$ est irrationnel.

1. Posons $x = a + b\sqrt{2}$ et $y = a' + b'\sqrt{2}$. On a :

$$\begin{aligned} N(xy) &= (aa' + 2bb')^2 - 2(ab' + a'b)^2 \\ &= (aa')^2 - 2(ab')^2 - 2(a'b)^2 + (4bb')^2. \end{aligned}$$

   D'autre part,

$$\begin{aligned} N(x) \times N(y) &= (a^2 - 2b^2)(a'^2 - 2b'^2) \\ &= (aa')^2 - 2(ab')^2 - 2(a'b)^2 + (4bb')^2. \end{aligned}$$

2. Soit $x = a + b\sqrt{2}$. Supposons d'abord que x est inversible, d'inverse y. Alors $N(xy) = N(1) = 1$, et donc $N(x)N(y) = 1$.
   Or, $N(x)$ et $N(y)$ sont tous les deux des entiers.
   On a donc $N(x) = \pm 1$.
   Réciproquement, si $N(x) = \pm 1$, alors, en utilisant la quantité conjuguée :

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \pm(a - b\sqrt{2})$$

   ce qui montre que $a + b\sqrt{2}$ est inversible, d'inverse $\pm(a - b\sqrt{2})$.