Feuille de TD n° 5

Morphismes de groupes, permutations

29 mars 2022

Pour commencer . . .

Exercice 1.
Dire si les groupes suivants sont isomorphes ou non. Le prouver.

1. $(\mathbb{Z}, +)$ et $(\mathbb{Q}, +)$
2. $(\mathbb{Q}, +)$ et $(\mathbb{R}, +)$
3. $\mathbb{Z}/13\mathbb{Z}$ et $\mathbb{Z}/15\mathbb{Z}$
4. $(\mathbb{Z}/2Z) \times (\mathbb{Z}/4\mathbb{Z})$ et U_8 (racines 8èmes de l'unité)
5. $\mathbb{Z}/n!\mathbb{Z}$ et $\mathcal{S}_n$, $n \geq 2$.
6. $\mathbb{Z}/8\mathbb{Z}$ et le groupe $\mathfrak{Q} = \{1, -1, i, -i, j, -j, k, -k\}$ des quaternions ($i^2 = -1$, $j^2 = -1$,$ij = k = -ij$) (voir TD précédent)
   Pour aller plus loin . . .
7. $(\mathbb{Z}, +)$ et $(\mathbb{Z}^2, +)$
8. $(\mathbb{Z}^n, +)$ et $(\mathbb{Z}^m, +)$, $n < m$
   On pourra utiliser la base canonique de $\mathbb{Q}^m$ et chercher une contradiction.
9. $(\mathbb{Q}, +)$ et $(\mathbb{Q}^2, +)$
10. $(\mathbb{R}, +)$ et $(\mathbb{R}^2, +)$. (Pas de preuve demandée.)
11. $(\mathbb{R}, +)$ et $(\mathbb{R}^n, +)$, $n > 0$.

---

1. Non. Pour $f : \mathbb{Z} \to \mathbb{Q}$ morphisme de groupe, posons $r = f(1)$.
   Pour tout $n \in \mathbb{Z}$, on a $f(n) = f(n.1) = n.f(1) = n.r$ (car f est un morphisme de groupes pour la loi $+$).
   Alors, on a $Im(f) = r.\mathbb{Z}$, l'ensemble des multiples du rationnel r.
   Ainsi, le rationnel $\frac{r}{2}$ (ou 1 si $r = 0$) n'est pas dans $Im(f)$. Donc le morphisme f n'est pas bijectif.
2. Non. $\mathbb{Q}$ est dénombrable et $\mathbb{R}$ est infini non-dénombrable, donc ces ensembles ne sont pas en bijection. Un isomorphisme est une bijection, donc il n'en existe pas entre $\mathbb{Q}$ et $\mathbb{R}$.
3. Non. Ces groupes n'ont pas le même cardinal. Ils ne peuvent pas être isomorphes.
4. Non. L'ordre des éléments de $\mathbb{Z}/2\mathbb{Z}$ est 1 ou 2. L'ordre des éléments de $\mathbb{Z}/4\mathbb{Z}$ est $1, 2$ ou 4. Les éléments de $(\mathbb{Z}/2Z) \times (\mathbb{Z}/4\mathbb{Z})$ sont de la forme $(\bar{a}, \bar{b})$. Leur ordre est alors $1, 2$ ou 4.
   Or, U_8 possède des éléments d'ordre 8 (comme $\exp(\frac{2i\pi}{8})$). Ces groupes ne sont donc pas isomorphes.
5. Non si $n \geq 3$.
   Ces groupes ont le même cardinal. Mais $\mathbb{Z}/n!\mathbb{Z}$ est un groupe commutatif, tandis que $\mathcal{S}_n$ n'est pas un groupe commutatif. En effet, on a $(1\,2) \circ (2\,3) = (1\,2\,3) \neq (1\,3\,2) = (2\,3) \circ (1\,2)$.
   Si $n = 2$, ces deux groupes sont des groupes à 2 éléments qui sont isomorphes.
6. Non.
   Ces groupes ont le même cardinal. Mais $\mathbb{Z}/8\mathbb{Z}$ est un groupe commutatif, tandis que $\mathfrak{Q}$ n'est pas un groupe commutatif.
   En effet, on a $1 \neq -1$, donc $ji \neq -ji = ij$.
7. Non.
   Soit $f : \mathbb{Z} \to \mathbb{Z}^2$ un morphisme de groupes. On pose $(a, b) = f(1)$.
   Si $(a, b) = 0$, alors f n'est pas injectif, donc pas un isomorphisme.
   Si $(a, b) \neq 0$, alors on a $f(n) = f(n.1) = n.f(1) = n(a, b)$.
   Donc $Im(f) = (a, b)\mathbb{Z}$.
   Comme $(a, b) \neq (0, 0)$, on a donc $(-b, a) \notin Im(f)$. Donc f n'est pas surjectif, donc pas un isomorphisme.
8. Non.
   Supposons par l'absurde avoir $f : \mathbb{Z}^n \to \mathbb{Z}^m$ un isomorphisme de groupes.
   On va utiliser les propriétés des $\mathbb{Q}$-espaces vectoriels de dimension finie, en faisant attention à se ramener à des coefficients entiers.
   Posons $e_1, \ldots, e_m$ la base canonique de $\mathbb{Q}^m$ (elle est dans $\mathbb{Z}^m$.
   Alors, il existe $x_1, \ldots, x_m \in \mathbb{Z}^n$ tels que $f(x_i) = e_i$ par surjectivité.
   La famille $(x_1, \ldots, x_m)$ est une famille à $m > n$ éléments dans $\mathbb{Q}^n$, qui est un $\mathbb{Q}$-ev de dimension n. Donc cette famille est liée.
   On a donc des rationnels non-tous nuls $r_1, \ldots, r_m \in \mathbb{Q}$ tels que $r_1x_1 + \ldots + r_mx_m = 0$.
   En multipliant ces rationnels $r_1, \ldots, r_m$ par leur dénominateur commun, on a ainsi des nombres entiers $k_1, \ldots, k_m$, non tous nuls, tels que $k_1x_1 + \ldots + k_mx_m = 0$.
   Mais alors, on a $0 = f(0) = f(k_1x_1 + \ldots + k_mx_m) = f(k_1x_1) + \ldots + f(k_mx_m)$, $0 = k_1f(x_1) + \ldots + k_mf(x_m) = k_1e_1 + \ldots + k_me_m$.
   Comme les k_i sont non tous nuls et que la famille $(e_1, \ldots, e_m)$ est libre dans $\mathbb{Q}^m$, le vecteur $k_1e_1 + \ldots + k_me_m$ est donc non-nul, ce qui est impossible.
9. Non.
   Soit $f : \mathbb{Q} \to \mathbb{Q}^2$ un morphisme de groupes. On pose $(a, b) = f(1)$.
   Si $(a, b) = 0$, alors f n'est pas injectif, donc pas un isomorphisme.
   Si $(a, b) \neq 0$, alors on a $f(n) = f(n.1) = n.f(1) = n(a, b)$.

Pour tout $r \in \mathbb{Q}$, on a $r = \frac{p}{q}$, d'où $f(qr) = f(q.r) = q.f(r)$ et $f(qr) = f(p) = p.f(1) = p(a,b)$.
On en déduit que $f(r) = \frac{p}{q}(a,b)$.
Ainsi, on a $Im(f) = (a,b)\mathbb{Q}$. Comme $(a,b) \neq (0,0)$, on a donc $(-b,a) \notin Im(f)$. Donc f n'est pas surjectif, donc pas un isomorphisme.

10. Oui.
La preuve est difficile.
Les ensembles $\mathbb{R}$ et $\mathbb{R}^2$ sont des $\mathbb{Q}$-ev.
Ils possèdent des bases B et B' comme $\mathbb{Q}$-ev (des bases infinies).
Comme ces ensembles sont infinis non-dénombrables, B est en bijection avec $\mathbb{R}$ et B' en bijection avec $\mathbb{R}^2$.
Or, $\mathbb{R}$ est en bijection avec $\mathbb{R}^2$, donc B est en bijection avec B'.
Avec cette bijection entre bases, on peut construire un isomorphisme de $\mathbb{Q}$-ev entre $\mathbb{R}$ et $\mathbb{R}^2$.
Un isomorphisme de $\mathbb{Q}$-ev est entre autres un morphisme de groupes, ce qui donne le résultat.

11. Oui.
On montre cela par récurrence sur $n \geq 2$.
En effet, cela est vrai pour $n = 2$. Et si cette proposition est vraie pour un $n \geq 2$, alors on a $\mathbb{R}^{n+1} = \mathbb{R}^n \times \mathbb{R} \simeq \mathbb{R} \times \mathbb{R} \simeq \mathbb{R}$.

Exercice 2.
Soient $(G, \star)$ et (H, Δ) des groupes, et $f : G \to H$ un morphisme de groupes.

1. Soit G_1 un sous-groupe de G. Montrer que $f(G_1)$ est un sous-groupe de H.
2. Soit H_1 un sous-groupe de H. Montrer que $f^{-1}(H_1)$ est un sous-groupe de G.
3. Soit $x \in G$. Montrer que $f(\langle x \rangle) = \langle f(x) \rangle$.
4. Soit $S \subset G$ une partie de G.
Montrer que $f(\langle S \langle) = \langle f(S) \rangle$.
5. Soit $S' \subset H$. Montrer qu'en général on a $f^{-1}(\langle S' \rangle) \neq \langle f^{-1}(S) \rangle$.

---

1. On montre que $f(G_1)$ contient e_H, et que pour $x, y \in f(G_1)$ on a $xy \in f(G_1)$ et $x^{-1} \in f(G_1)$.
2. On montre que $f^{-1}(H_1)$ contient e_G, et que pour $x, y \in f^{-1}(H_1)$ on a $xy \in f^{-1}(H_1)$ et $x^{-1} \in f^{-1}(H_1)$.
3. On a $\langle y \rangle = \{y^n,\ n \in \mathbb{Z}\}$. Or, on a vu en cours que $f(x^n) = f(x)^n$.
Donc, $f(\langle x \rangle) = \{f(x^n),\ n \in \mathbb{Z}\} = \{f(x)^n,\ n \in \mathbb{Z}\} = \langle f(x) \rangle$.
4. Le sous-groupe $\langle S \rangle$ est formé de tous les éléments de G de la forme $a_1 \star \ldots \star a_m$, avec $m \geq 1$, et ($a_i \in S$ ou $a_i^{-1} \in S$).
Or, on a $f(a_1 \star \ldots \star a_m) = f(a_1)\Delta \ldots \Delta f(a_m)$.
On obtient donc l'égalité : $f(\langle S \langle) = \langle f(S) \rangle$.
5. On prend $G = H = \mathbb{Z}$ et $f(n) = 2n$. On prend $S' = \{3\}$.
Alors, on a $\langle S' \rangle = 3\mathbb{Z}$. On a $\langle S' \rangle \cap Im(f) = 6\mathbb{Z}$.
Cela donne : $f^{-1}(\langle S' \rangle) = 3\mathbb{Z}$, et $\langle f^{-1}(S) \rangle = \langle \emptyset \rangle = \{0\}$.

Exercice 3. Soit G un groupe fini.
Pour tout $a \in G$, on pose $\Phi_a : x \in G \mapsto axa^{-1} \in G$.

1. Vérifier que Φ_a est un automorphisme de G (un isomorphisme de G dans G.
2. Montrer que pour $Aut(G) = \{f : G \to G, f \text{ automorphisme }\}$, $(Aut(G), \circ)$ est un groupe.
3. On pose $I = \{\Phi_a \mid a \in G\}$. Montrer que I est un sous-groupe de $Aut(G)$.
4. Montrer que $h : a \in G \mapsto \Phi_a \in I$ est un morphisme de groupes.
Déterminer $Ker(h)$.
5. On suppose que G est un groupe commutatif.
Déterminer I.
6. On suppose que I est un groupe cyclique (engendré par un seul élément, $I = \langle x \rangle =$.
Montrer que G est un groupe commutatif.
7. En déduire que les ensembles I et $Aut(G)$ ne sont en général pas égaux.

---

1. Pour $a, b \in G$, on vérifique que $\Phi_a \circ \Phi_b = \Phi_{ab}$. On a de plus $\Phi_e = id_G$.
On en déduit que la fonction Φ_a est bijective, et que $\Phi_a^{-1} = \Phi_{a^{-1}}$.
Il reste à montrer que $\Phi_a : G \to G$ est un morphisme :
$$\forall x, y \in G,\ \Phi_a(xy) = axya^{-1} = (axa^{-1}aya^{-1} = \Phi_a(x)\Phi_a(y).$$
Cela est donc vrai.
2. La fonction Id_G est un automorphisme de G. Pour f, g deux automorphismes de G, on a vu en cours que f^{-1} est aussi un automorphisme.
On montre alors que $f \circ g$ est aussi un automorphisme. (fonction bijective, et morphisme de groupes). Cela montre que $(Aut(G), \circ)$ est un sous-groupe de $(Bij(G), \circ)$. Donc, $(Aut(G), \circ)$ est un groupe.

3. A la première question, on a montré que I est stable par multiplication, contient Id_G, et que tout élément possède un inverse dans I. C'est bien un sous-groupe de $Aut(G)$.
4. A la première question on a montré que $\Phi_a \circ \Phi_b = \Phi_{ab}$.
   Cela démontre que $h : a \mapsto \Phi_a$ est un morphisme de groupes.
   Son noyau est l'ensemble des $a \in G$ tels que $\Phi_a = Id_G$.
   Soit $b \in G$. On a $\Phi_a(b) = b$ ssi $aba^{-1} = b$, ssi $ab = ba$, ssi a et b commutent.
   Donc, on a $\Phi_a = Id_G$ ssi a commute avec tous les éléments de G.
   Ainsi, $Ker(h) = \{a \in G \text{ t.q. } ab = ba \, \forall b \in G\}$.
5. On a $I = \langle x \rangle$. Soit $a \in G$ tel que $\Phi_a = x$.
   Soit $b \in G$. Alors il existe n tel que $\Phi_b = \Phi_a^n = \Phi_{a^n}$.
   Alors, on a $a = \Phi_{a^n}(a) = \Phi_b(a)$, donc $a = bab^{-1}$, donc $ab = ba$.
   Ainsi a commute avec tous les éléments de G, donc $\Phi_a = id_G$, donc $I = \{id_G\}$, donc G est commutatif.
6. Prenons un contre-exemple. Pour $(G, \star) = (\mathbb{Z}, +)$, on a $I = \{Id_{\mathbb{Z}}\}$ car ce groupe est commutatif.
   Pourtant, $f : n \in \mathbb{Z} \mapsto -n \in \mathbb{Z}$ est un automorphisme de $\mathbb{Z}$.
   Ainsi, on a $Aut(\mathbb{Z}) \neq I$.

Un peu de Géométrie . . .

Exercice 4.
Décomposer les permutations suivantes en produit de cycles à supports disjoints, ainsi qu'en produit de transpositions, calculer leur ordre. Calculer enfin σ_1^{1000} et σ_2^{1000}.

$$\sigma_1 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 6 & 2 & 1 \end{bmatrix} \quad \text{et} \quad \sigma_2 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 6 & 9 & 7 & 2 & 5 & 8 & 1 & 3 \end{bmatrix}.$$

On a

$$\sigma_1 = \begin{pmatrix} 1 & 3 & 4 & 6 \end{pmatrix} \begin{pmatrix} 2 & 5 \end{pmatrix},$$

donc σ_1 est d'ordre 4. En effet, le 4-cycle $\begin{pmatrix} 1 & 3 & 4 & 6 \end{pmatrix}$ est d'ordre 4 donc l'ordre de σ_1 est plus grand que 4, et on peut vérifier que $\sigma_1^4 = \mathrm{Id}$. Ainsi $\sigma_1^{1000} = \mathrm{Id}$. Une décomposition de σ_1 en produit de transpositions est

$$\sigma_1 = \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 3 & 4 \end{pmatrix} \begin{pmatrix} 4 & 6 \end{pmatrix} \begin{pmatrix} 2 & 5 \end{pmatrix}.$$

On a

$$\sigma_2 = \begin{pmatrix} 1 & 4 & 7 & 8 \end{pmatrix} \begin{pmatrix} 2 & 6 & 5 \end{pmatrix} \begin{pmatrix} 3 & 9 \end{pmatrix},$$

donc σ_2 est d'ordre 12. En effet, $\sigma_2^k = \begin{pmatrix} 1 & 4 & 7 & 8 \end{pmatrix}^k \begin{pmatrix} 2 & 6 & 5 \end{pmatrix}^k \begin{pmatrix} 3 & 9 \end{pmatrix}^k$. Si $\sigma_2^k = \mathrm{Id}$ alors $\begin{pmatrix} 1 & 4 & 7 & 8 \end{pmatrix}^k = \mathrm{Id}$ donc k est un multiple de 4, $\begin{pmatrix} 2 & 6 & 5 \end{pmatrix}^k = \mathrm{Id}$ donc k est un multiple de 3, et $\begin{pmatrix} 3 & 9 \end{pmatrix}^k = \mathrm{Id}$ donc k est un multiple de 2. Ainsi, k est un multiple de 12.

On peut vérifier que $\sigma_2^{12} = \mathrm{Id}$. Ainsi, $\sigma_2^{1000} = \sigma_2^{12 \times 83 + 4} = \sigma_2^4 = \begin{pmatrix} 2 & 6 & 5 \end{pmatrix}^4 = \begin{pmatrix} 2 & 6 & 5 \end{pmatrix}$.
Une décomposition de σ_2 en produit de transpositions est

$$\sigma_2 = \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 4 & 7 \end{pmatrix} \begin{pmatrix} 7 & 8 \end{pmatrix} \begin{pmatrix} 2 & 6 \end{pmatrix} \begin{pmatrix} 6 & 5 \end{pmatrix} \begin{pmatrix} 3 & 9 \end{pmatrix}.$$

Exercice 5.
Soit $n \in \mathbb{N}^*$, soit $A \subset \mathcal{S}_n$. On dit que $\mathcal{S}_n$ est engendré (ou généré) par A si tout $\sigma \in \mathcal{S}_n$ s'écrit comme un produit d'éléments de A. On a déjà montré dans le cours que $\mathcal{S}_n$ est engendré par les transpositions.

1. Montrer que $\mathcal{S}_n$ est engendré par les transpositions $\begin{pmatrix} 1 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 3 \end{pmatrix}$, …, $\begin{pmatrix} 1 & n \end{pmatrix}$.
2. Montrer que $\mathcal{S}_n$ est engendré par les transpositions $\begin{pmatrix} 1 & 2 \end{pmatrix}$, $\begin{pmatrix} 2 & 3 \end{pmatrix}$, …, $\begin{pmatrix} n-1 & n \end{pmatrix}$.
3. On considère $t = \begin{pmatrix} 1 & 2 \end{pmatrix}$ et $c = \begin{pmatrix} 1 & 2 & \dots & n \end{pmatrix}$. En calculant $c^k t c^{-k}$, montrer que $\mathcal{S}_n$ est engendré par t et c.

---

1. On a $\begin{pmatrix} i & j \end{pmatrix} = \begin{pmatrix} 1 & i \end{pmatrix} \begin{pmatrix} 1 & j \end{pmatrix} \begin{pmatrix} 1 & i \end{pmatrix}$, donc toute transposition s'écrit comme produit de ces transpositions. Puisque les transpositions engendrent $\mathcal{S}_n$, les $\begin{pmatrix} 1 & i \end{pmatrix}$ engendrent $\mathcal{S}_n$.
2. D'après la question précédente, il suffit de montrer que toute transposition $\begin{pmatrix} 1 & i \end{pmatrix}$ est un produit des transpositions $\begin{pmatrix} k & k+1 \end{pmatrix}$. Or on a
   $$\begin{pmatrix} 1 & i \end{pmatrix} = \begin{pmatrix} 1 & i-1 \end{pmatrix} \begin{pmatrix} i-1 & i \end{pmatrix} \begin{pmatrix} 1 & i-1 \end{pmatrix}.$$
   Donc par récurrence, on obtient le résultat.
3. On a
   $$ctc^{-1} = \begin{pmatrix} 2 & 3 \end{pmatrix},$$
   et par récurrence
   $$c^k t c^{-k} = \begin{pmatrix} k+1 & k+2 \end{pmatrix}.$$
   Ainsi, d'après la question précédente, t et c engendrent $\mathcal{S}_n$.

Exercice 6. Soit $n \geq 2$. Montrer que les permutations d'ordre 2 ($\sigma^2 = \mathrm{Id}$) dans $\mathcal{S}_n$ sont exactement les produits de transpositions à supports disjoints.

Tout d'abord, si $\sigma \in \mathcal{S}_n$ est un produit de transpositions à supports disjoints, on a $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_r$. Toutes ces transpositions commutent deux à deux donc $\sigma^2 = \tau_1^2 \circ \cdots \circ \tau_r^2 = \mathrm{Id}$.

Réciproquement, soit $\sigma \in \mathcal{S}_n$ (avec $n \geq 3$, sinon le résultat est évident). On peut décomposer σ en un produit de cycles à supports disjoints : $\sigma = \gamma_1 \circ \cdots \circ \gamma_r$. Supposons qu'il existe $i \in [\![1, r]\!]$ tel que γ_i n'est pas une transposition. Soit A le support de γ_i, soit $x \in A$: $\sigma^2(x) = \gamma_i^2(x) \neq x$, donc $\sigma^2 \neq \mathrm{Id}$.

Exercice 7. Soit $n \geq 2$.

1. Soit $\sigma \in \mathcal{S}_n$ et $i \neq j \in [\![1, n]\!]$. Que vaut $\sigma \begin{pmatrix} i & j \end{pmatrix} \sigma^{-1}$?
2. On appelle *centre d'un groupe* $(G, \star)$ l'ensemble $Z(G)$ des éléments de G qui commutent avec tous les autres :

$$Z(G) = \{x \in G \mid \forall y \in G,\, x \star y = y \star x\}.$$

   Déterminer $Z(\mathcal{S}_n)$, le centre de $\mathcal{S}_n$.

---

1. Puisque σ est une bijection, on a $[\![1, n]\!] = \{\sigma(k) \mid k \in [\![1, n]\!]\}$. Soit $k \in [\![1, n]\!] \setminus \{i, j\}$, on a
$$\sigma \begin{pmatrix} i & j \end{pmatrix} \sigma^{-1}(\sigma(k)) = \sigma \begin{pmatrix} i & j \end{pmatrix}(k) = \sigma(k).$$
Donc le support de $\sigma \begin{pmatrix} i & j \end{pmatrix} \sigma^{-1}$ est inclus dans $\{\sigma(i), \sigma(j)\}$. Maintenant :
$$\sigma \begin{pmatrix} i & j \end{pmatrix} \sigma^{-1}(\sigma(i)) = \sigma(j) \quad \text{et} \quad \sigma \begin{pmatrix} i & j \end{pmatrix} \sigma^{-1}(\sigma(j)) = \sigma(i).$$
Finalement :
$$\sigma \begin{pmatrix} i & j \end{pmatrix} \sigma^{-1} = \begin{pmatrix} \sigma(i) & \sigma(j) \end{pmatrix}.$$
2. Soit $\sigma \in Z(\mathcal{S}_n)$, on a en particulier $\sigma \begin{pmatrix} i & j \end{pmatrix} = \begin{pmatrix} i & j \end{pmatrix} \sigma$, c'est-à-dire $\sigma \begin{pmatrix} i & j \end{pmatrix} \sigma^{-1} = \begin{pmatrix} i & j \end{pmatrix}$, pour tous $i \neq j$. D'après la question précédente, on en déduit que $\begin{pmatrix} i & j \end{pmatrix} = \begin{pmatrix} \sigma(i) & \sigma(j) \end{pmatrix}$, pour tous $i \neq j$. Donc pour tous $i \neq j$, on a $\{i, j\} = \{\sigma(i), \sigma(j)\}$. Si $n \geq 3$, on obtient que pour tout triplet (i, j, k), $\{i, j\} = \{\sigma(i), \sigma(j)\}$ et $\{i, k\} = \{\sigma(i), \sigma(k)\}$, donc $\sigma(i) = i$. Ainsi
$$Z(\mathcal{S}_n) = \begin{cases} \mathcal{S}_2 & \text{si } n = 2 \\ \{\mathrm{Id}\} & \text{si } n \geq 3 \end{cases}.$$