# Théorèmes d'isomorphismes et actions de groupes.

## 1 Exercice 1. *Groupes monogènes*

*Soit $G$ un groupe monogène. Montrer que soit $G \cong \mathbb{Z}$, soit $G \cong \mathbb{Z}/n\mathbb{Z}$ pour un entier strictement positif $n$.*

Soit $g \in G$ tel que $\langle g \rangle = G$. Considérons le morphisme

$$\begin{aligned} \phi : \mathbb{Z} &\longrightarrow G \\ k &\longmapsto g^k. \end{aligned}$$

On a $\operatorname{im}\phi = \langle g \rangle = G$. De plus, par le premier théorème d'isomorphisme

$$\mathbb{Z}/\ker\phi \cong \operatorname{im}\phi = G.$$

- ▷ Si $\ker\phi$ est le sous-groupe trivial $\{0\}$, on a donc $G \cong \mathbb{Z}$.
- ▷ Si $\ker\phi$ est un sous-groupe non trivial de $\mathbb{Z}$, alors $\ker\phi = n\mathbb{Z}$, et on a donc $G \cong \mathbb{Z}/n\mathbb{Z}$.

## 2 Exercice 2.

*Soit $n > 0$ un entier.*

1. *Montrer que $\mathbb{Z}/n\mathbb{Z}$ contient $\varphi(n)$ éléments d'ordre $n$, où $\varphi(n)$ désigne le nombre d'entiers $k \in [\![0, n-1]\!]$ premiers à $n$.*
2. *Montrer que pour tout $d > 0$ divisant $n$, $\mathbb{Z}/n\mathbb{Z}$ admet un unique sous-groupe d'ordre $d$ formé des multiples de $\overline{n/d}$.*
3. *En déduire que pour tout diviseur $d > 0$ de $n$, $\mathbb{Z}/n\mathbb{Z}$ contient $\varphi(d)$ éléments d'ordre $d$ et que $\sum_{0<d|n} \varphi(d) = n$.*

**1.** Soit $k \in [\![0, n-1]\!]$. Montrons que $\langle \bar{k} \rangle = \mathbb{Z}/n\mathbb{Z}$ si et seulement si $\operatorname{pgcd}(k, n) = 1$.

- ▷ Si $\langle \bar{k} \rangle = \mathbb{Z}/n\mathbb{Z}$ alors il existe $a \in \mathbb{Z}$ tel que
$$a\bar{k} = \underbrace{\bar{k} + \cdots + \bar{k}}_{a \text{ fois}} = \bar{1}.$$
Ainsi, il existe $b \in \mathbb{Z}$ tel que $ak - 1 = bn$, soit $ak + bn = 1$. On en conclut, par le théorème de Bézout, que $k$ et $n$ sont premiers entre-eux.
- ▷ Si $\operatorname{pgcd}(k, n) = 1$ alors il existe $a, b \in \mathbb{Z}$ tels que $ak+bn = 1$ et donc $ak \equiv 1 \pmod{n}$. Ainsi, $k + \cdots + k \equiv 1 \pmod{n}$. Or, $\langle \bar{1} \rangle = \mathbb{Z}/n\mathbb{Z}$ et donc, comme $\langle \bar{1} \rangle \subseteq \langle \bar{k} \rangle$ on a que
$$\langle \bar{k} \rangle = \mathbb{Z}/n\mathbb{Z}.$$

Par bijection, on a donc
$$\varphi(n) = \#\{k \in [\![0, n-1]\!] \mid \operatorname{pgcd}(k, n) = 1\}$$
éléments d'ordre $n$.

**2.** On sait que $\langle \overline{n/d} \rangle$ est un groupe, et $d\,\overline{n/d} = \bar{n} = \bar{0}$. Ainsi, on a que $\#\langle \overline{n/d} \rangle = d$. Il ne reste qu'à montrer l'unicité. Soit un sous-groupe $H \leq \mathbb{Z}/n\mathbb{Z}$ d'ordre $d$. Soit $\bar{a} \in H$ tel que $d\bar{a} = 0$. Ainsi, il existe $b \in \mathbb{Z}$ tel que $da = nb$, d'où $a = nb/d$ et donc $\bar{a} = b\,\overline{n/d}$. On en déduit que $\bar{a} \in \langle \overline{n/d} \rangle$. On conclut que $H = \langle \overline{n/d} \rangle$ par inclusion et égalité des cardinaux.

**3.** Soit $\bar{a}$ un élément d'ordre $d$, et donc $\#\langle \bar{a} \rangle = d$. Par la question 2 et l'exercice 1, on a $\langle \bar{a} \rangle = \langle \overline{n/d} \rangle \cong \mathbb{Z}/d\mathbb{Z}$. Or, par la question 1, il y a $\varphi(d)$ éléments d'ordre $d$ dans $\mathbb{Z}/d\mathbb{Z}$. Ainsi, il y a $\varphi(d)$ éléments d'ordre $d$ dans $\mathbb{Z}/n\mathbb{Z}$.

Posons $A_d := \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \#\langle \bar{a} \rangle = d\}$. Si $d \nmid n$ alors $A_d = \emptyset$ car l'ordre d'un élément divise $n$ (théorème de LAGRANGE). Si $d \mid n$ alors $\#A_d = \varphi(d)$ (question 2). De plus,
$$\mathbb{Z}/n\mathbb{Z} = \bigsqcup_{d|n} A_d,$$
d'où
$$n = \sum_{d|n} \#A_d = \sum_{d|n} \varphi(d).$$

# 3 Exercice 3.

1. *Montrer que le groupe $\mathbb{Z}/n\mathbb{Z}$ est simple si, et seulement si, $n$ est premier.*
2. *Soit $G$ un groupe fini abélien. Montrer que $G$ est simple si et seulement si $G \cong \mathbb{Z}/p\mathbb{Z}$ avec $p$ un nombre premier.*

1. Le groupe $\mathbb{Z}/n\mathbb{Z}$ est commutatif. Ainsi, tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est distingué. On a donc que $\mathbb{Z}/n\mathbb{Z}$ est simple si, et seulement si, $\mathbb{Z}/n\mathbb{Z}$ ne possède pas de sous-groupes non triviaux. De plus, un entier $n$ n'a que des diviseurs triviaux (1 ou $n$) si et seulement si $n$ est premier. Et, avec le théorème de Lagrange, on sait que l'ordre de tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ divise $n$. D'où l'équivalence.
2. Le groupe $G$ est commutatif. Ainsi, tout sous-groupe de $G$ est distingué. On a donc que $G$ est simple si, et seulement si, $G$ ne possède pas de sous-groupes non triviaux. Ainsi, par le théorème de Lagrange, l'ordre du groupe $G$ est premier.

# 4 Exercice 4.

*Soit $G$ un groupe et $H$ un sous-groupe de $G$ d'indice 2. Montrer que $H$ est distingué dans $G$. Montrer que le résultat n'est pas vrai si on remplace 2 par 3.*

Soit $g \in G \setminus H$. On a la partition $G = H \sqcup gH$. Ainsi $gH$ est le complément de $H$ dans $G$. Similairement, $Hg$ est le complément de $H$ dans $G$. Ainsi, on a $gH = Hg$.

Si $h \in H$, alors $hH = H = Hh$ car $H$ est un sous-groupe contenant les éléments $h$ et $h^{-1}$.

On en conclut, dans les deux cas, que $H \triangleleft G$.

Pour montrer que le résultat est faux en remplaçant 2 par 3, on considère $G := \mathfrak{S}_3$ et $H := \{\mathrm{id}, (1\ 2)\}$ un sous-groupe de $G$. Le sous-groupe $H$ a pour indice $[G : H] = |\mathfrak{S}_3|/|H| = 3$. Cependant, $H$ n'est

pas un sous-groupe distingué de $G$ :

$$(1\ 2\ 3)(1\ 2)(1\ 2\ 3)^{-1} = (2\ 3) \notin H.$$

# 5 Exercice 5.

*Soit $p$ un nombre premier.*

1. *Rappeler pourquoi le centre d'un $p$-groupe est non trivial.*
2. *Montrer que tout groupe d'ordre $p^2$ est abélien, classifier ces groupes.*
3. *Soit $G$ un groupe d'ordre $p^n$. Montrer que $G$ admet un sous-groupe distingué d'ordre $p^k$ pour tout $k \in [\![0, n]\!]$.*

# 6 Exercice 6. *Troisième théorème d'isomorphisme*

*Soit $H$ un groupe et soient $H$ et $K$ des sous-groupes tels que $H \triangleleft G$ et $H \leq K$. On notera $\pi_H : G \to G/H$.*

1. *Montrer que le groupe $\pi_H(K)$ est distingué dans $G/H$ si et seulement si $K$ est distingué dans $G$.*
2. *Justifier que $H$ est distingué dans $K$ et que l'on a un isomorphisme $\pi_H(K) \cong K/H$.*
3. *On suppose $K$ distingué dans $G$. On note $\pi_K : G \to G/K$ la projection canonique.*
   a) *Montrer que $\pi_K$ induit un unique morphisme de groupes $\bar{\pi}_K : G/H \to G/K$ tel que $\pi_K = \bar{\pi_K} \circ \pi_H$.*
   b) *Montrer que le noyau de $\bar{\pi}_K$ est $\pi_H(K) \cong K/H$.*
   c) *En déduire le troisième théorème d'isomorphisme.*

1. Supposons $K$ distingué dans $G$. Alors, $\pi_H(K)$ est distingué dans $G/H$ car $\pi_H$ est surjective (exercice 6 du TD 1). Réciproquement, si $\pi_H(K)$ est distingué dans $G/H$, alors

# 7 Exercice 7. *Sous-groupe d'un quotient*

*Soit $G$ un groupe, et $H$ un sous-groupe distingué de $G$. On note la projection canonique $\pi_H : G \to G/H$.*

1. **a)** *Soit $K$ un sous-groupe de $G$. Montrer $\pi_H^{-1}(\pi_H(K)) = KH$.*
   **b)** *En déduire que $\pi_H$ induit une bijection croissante entre les sous-groupes de $G/H$ et les sous-groupes de $G$ contenant $H$.*
2. *Montrer que les sous-groupes distingués de $G/H$ sont en correspondance avec les sous-groupes distingués de $G$ contenant $H$.*
3. *Montrer que la correspondance précédente préserve l'indice : si $K$ est un sous-groupe de $G$ d'indice fini contenant $H$, alors on a $[G : K] = [G/H, \pi_H(K)]$.*

# 8 Exercice 8. *Combinatoire algébrique*

*Soit $\Bbbk$ un corps fini à $q$ éléments et $n \in \mathbb{N}^*$. On définit $\mathrm{PGL}_n(\Bbbk)$ comme le quotient $\mathrm{GL}_n(\Bbbk)/\Bbbk^\times$, où $\Bbbk^\times$ correspond au sous-groupe distingué formé de la forme $\lambda \mathrm{I}_n$ avec $\lambda \in \Bbbk \setminus \{0\}$. On considère l'action de $\mathrm{GL}_n(\Bbbk)$ sur l'ensemble des droites vectorielles de $\Bbbk^n$.*

1. *Déterminer le cardinal des groupes finis $\mathrm{GL}_n(\Bbbk)$, $\mathrm{SL}_n(\Bbbk)$ et $\mathrm{PGL}_n(\Bbbk)$. Indication : compter les bases de $\Bbbk^n$.*
2. *On prend désormais $n = 2$.*
   **a)** *Montrer que le nombre de droites vectorielles de $\Bbbk^2$ est égal à $q + 1$.*
   **b)** *En déduire qu'il existe un morphisme de groupes injectif*
   $$\mathrm{PGL}_2(\Bbbk) \hookrightarrow \mathfrak{S}_{q+1}.$$
3. *Montrer que $\mathrm{GL}_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2) = \mathrm{PGL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3$.*
4. *Montrer que $\mathrm{PGL}_2(\mathbb{F}_3) \cong \mathfrak{S}_4$.*

1. L'application
$$\begin{aligned} \mathrm{GL}_n(\Bbbk) &\longrightarrow \{\text{bases de } \Bbbk^n\} \\ \begin{pmatrix} C_1 & C_2 & \cdots & C_n \end{pmatrix} &\longmapsto (C_1, \dots, C_n) \end{aligned}$$
est une bijection. Construisions une base de $\Bbbk^n$ :

**(1)** On choisit le premier vecteur $C_1$ dans $\Bbbk^n \setminus \{0\}$, on a donc $q^n - 1$ choix.

**(2)** On choisit le second vecteur $C_2$ dans $\Bbbk^n \setminus \mathrm{vect}(C_1)$, on a donc $q^n - q$ choix.

**(3)** On choisit le troisième vecteur $C_3$ dans $\Bbbk^n \setminus \mathrm{vect}(C_1, C_2)$, on a donc $q^n - q^2$ choix.

**(4)** *Et cetera.*

D'où,

$$\#\mathrm{GL}_n(\Bbbk) = \prod_{i=0}^{n-1}(q^n - q^i).$$

L'application $\det : \mathrm{GL}_n(\Bbbk) \to \Bbbk^\times$ est un morphisme de groupes surjectif. De plus, $\ker \det = \mathrm{SL}_n(\Bbbk)$. On a ainsi, par le premier théorème d'isomorphisme,

$$\mathrm{GL}_n(\Bbbk)/\mathrm{SL}_n(\Bbbk) \cong \Bbbk^\times.$$

Ainsi,

$$\#\mathrm{SL}_n(\Bbbk) = \frac{\#\mathrm{GL}_n(\Bbbk)}{\#\Bbbk^\times} = \frac{\prod_{i=0}^{n-1}(q^n - q^i)}{q-1}.$$

Finalement, on a $\mathrm{PGL}_n(\Bbbk) := \mathrm{GL}_n(\Bbbk)/\Bbbk^\times$ d'où

$$\#\mathrm{PGL}_n(\Bbbk) = \frac{\prod_{i=0}^{n-1}(q^n - q^i)}{q-1}.$$

**2. a)**

# 9 Exercice 9. *Formule de Burnside*

*Soit $G$ un groupe fini agissant sur un ensemble fini $X$. On note $N$ le nombre d'orbites de l'action.*

***1.*** *Soit $Y := \{(g, x) \in G \times X \mid g \cdot x = x\}$. Interpréter le cardinal de $Y$ comme somme sur les éléments de $X$ d'une part, et de $G$ d'autre part.*

**2.** *En décomposant $X$ en union d'orbites, montrer la formule de Burnside :*

$$N = \frac{1}{\#G} \sum_{g \in G} \#\mathrm{Fix}(G).$$

**3.** *Soit $n$ un entier. Quel est le nombre moyen de points fixes des éléments de $\mathfrak{S}_n$ pour l'action naturelle sur $[\![1, n]\!]$.*

**4.** *On suppose que $G$ agit transitivement sur $X$ et que $X$ contient au moins deux éléments. Montrer qu'il existe un $g \in G$ agissant sans point fixe.*

**5.** *En déduire qu'un groupe fini n'est jamais l'union des conjugués d'un sous-groupe strict.*

# Table des matières