

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

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

- ▷ 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 $k \in \llbracket 0, n-1 \rrbracket$ 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 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 $k \in \llbracket 0, n-1 \rrbracket$. Montrons que $\langle \bar{k} \rangle = \mathbb{Z}/n\mathbb{Z}$ si et seulement si $\text{pgcd}(k, n) = 1$.

▷ Si $\langle \bar{k} \rangle = \mathbb{Z}/n\mathbb{Z}$ alors il existe $a \in \mathbb{Z}$ tel que

$$a\bar{k} = \underbrace{\bar{k} + \dots + \bar{k}}_{a \text{ fois}} = \bar{1}.$$

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 $\text{pgcd}(k, n) = 1$ alors il existe $a, b \in \mathbb{Z}$ tels que $ak + bn = 1$ et donc $ak \equiv 1 \pmod{n}$. Ainsi, $k + \dots + k \equiv 1 \pmod{n}$. 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

$$\varphi(n) = \#\{k \in \llbracket 0, n-1 \rrbracket \mid \text{pgcd}(k, n) = 1\}$$

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 $d\bar{a} = \bar{0}$. Ainsi, il existe $b \in \mathbb{Z}$ tel que $da = nb$, d'où $a = nb/d$ et donc $\bar{a} = \overline{bn/d}$. 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,

$$\mathbb{Z}/n\mathbb{Z} = \bigsqcup_{d \mid n} A_d,$$

d'où

$$n = \sum_{d \mid n} \#A_d = \sum_{d \mid n} \varphi(d).$$

– 2/12 –

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 $H := \{\text{id}, (1\ 2)\}$ 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 $k \in \llbracket 0, n \rrbracket$.
1. Soit G un p -groupe non trivial. On fait agir G sur G par conjugaison. Ainsi, par la formule des classes, on a

$$p^n = \#G = \#Z(G) + \sum_{g \in \mathcal{R}} \underbrace{[G : C_G(g)]}_{p^{x_i} > 1},$$

où \mathcal{R} est un système de représentants des classes de conjugaisons de G contenant plus d'un élément.

On sait donc que $p \mid \sum_{g \in \mathcal{R}} [G : C_G(g)]$ et $p \mid \#G$, ce qui permet d'en déduire que $p \mid \#Z(G)$. D'où, $Z(G)$ n'est pas trivial.

2. Le centre de G est un sous-groupe, d'où par le théorème de LAGRANGE et par la question 1, on sait que l'ordre de $Z(G)$ est p ou p^2 .
 - ▷ Dans le cas où $Z(G)$ est d'ordre p^2 , on a $Z(G) = G$, d'où G abélien.
 - ▷ Supposons $\#Z(G) = p$. Soit $x \in G \setminus Z(G)$, et considérons le sous-groupe

$$Z(x) := \{g \in G \mid gx = xg\} \leq G.$$

En deux temps, montrons que $Z(G) \subsetneq Z(x) \subsetneq G$.

- On a l'inclusion $Z(G) \subseteq Z(x)$ mais cette inclusion est stricte car $x \in Z(x) \setminus Z(G)$.

- Montrons que $Z(x) \neq G$. Par l'absurde, si $Z(x) = G$, alors x commute avec tout élément de G , et donc $x \in Z(G)$, **absurde**.

Quel est l'ordre de $Z(x)$? C'est nécessairement p ou p^2 , mais dans chacun des cas, on arrive à une contradiction avec les inclusions strictes plus-haut. C'est **absurde**.

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 $\pi_H : G \rightarrow G/H$.

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 $\pi_K : G \rightarrow G/K$ la projection canonique.
 - a) Montrer que π_K induit un unique morphisme de groupes $\bar{\pi}_K : G/H \rightarrow G/K$ 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. On procède en deux temps.

Dans un premier temps, supposons que $K \triangleleft G$ et montrons que l'on a $\pi_H(K) \triangleleft G/H$. Soit $\bar{g} \in G/H$ et soit $g \in G$ un élément tel que $\pi_H(g) = \bar{g}$ qui existe par surjectivité de π_H . Alors,

$$\pi_H(K) = \pi_H(gHg^{-1}) = \bar{g} \pi_H(K) \bar{g}^{-1},$$

d'où $\pi_H(K) \triangleleft G/H$.

Dans un second temps, supposons

$$\forall \bar{g} \in G/H, \quad \bar{g} \pi_H(K) \bar{g}^{-1} = \pi_H(K).$$

Soit $g \in G$ et $k \in K$, et montrons que $gkg^{-1} \in K$. On sait que l'on a $\bar{g} = gH$ et $\pi_H(k) = kH$. Alors,

$$gkg^{-1}H \subseteq (gH)(kH)(g^{-1}H) = k'H \subseteq K,$$

pour un certain $k' \in K$ (on applique ici l'hypothèse). Ainsi, comme $e \in H$, on a en particulier $gkg^{-1} \in K$. On en déduit ainsi que $K \triangleleft G$.

2. Pour tout $k \in K$, on a que $kHk^{-1} = H$ car $k \in G$, on en déduit $H \triangleleft K$. Montrons que $\pi_H(K) \cong K/H$. On a même égalité de ces deux ensembles si l'on voit K/H comme l'ensemble des classes à gauches de H . En effet,

$$\pi_H(k) = kH \quad \text{d'où} \quad \pi_H(K) = \{kH \mid k \in K\},$$

et

$$K/H = \{kH \mid k \in K\}.$$

On a donc l'égalité.

3. a) On factorise par le quotient :

$$\begin{array}{ccc} G & \xrightarrow{\pi_K} & G/K \\ & \searrow \pi_H & \nearrow \bar{\pi}_K \\ & & G/H \end{array},$$

qui est possible car $K = \ker \pi_K \supseteq H$. Le morphisme $\bar{\pi}_K : G/H \rightarrow G/K$ est l'unique morphisme faisant commuter le diagramme ci-dessus.

- b) Par construction,

$$\begin{aligned} \ker \bar{\pi}_K &= \{\bar{g} \in G/H \mid \pi_K(g) = K\} \\ &= \{\pi_H(g) \mid g \in \ker \pi_K\} \\ &= \pi_H(\ker \pi_K) = \pi_H(K) \underset{Q_2}{\cong} K/H. \end{aligned}$$

- c) Appliquons le premier théorème d'isomorphisme à $\bar{\pi}_K$, qui est surjectif :

$$(G/H)/(\ker \bar{\pi}_K) = (G/H)/\ker \bar{\pi}_K \cong \text{im } \bar{\pi}_K = G/K,$$

c'est le troisième théorème d'isomorphisme.

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 $\pi_H : G \rightarrow G/H$.

1. a) Soit K un sous-groupe de G . Montrer $\pi_H^{-1}(\pi_H(K)) = KH$.
 b) En déduire que π_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 $[G : K] = [G/H, \pi_H(K)]$.

1. a) On a

$$\begin{aligned}
 \pi_H^{-1}(\pi_H(K)) &= \{g \in G \mid \pi_H(g) \in \pi_H(K)\} \\
 &= \{g \in H \mid gH = kH \text{ avec } k \in K\} \\
 &= \bigcup_{k \in K} kH \\
 &= \{kh \mid k \in K, h \in H\} \\
 &= KH.
 \end{aligned}$$

- b) L'image directe par π_H envoie un sous-groupe de G contenant H sur sous-groupe de G/H . De plus, l'image réciproque par π_H envoie un sous-groupe de G/H sur un sous-groupe de G contenant H . Montrons la bijection puis la croissance.

- ▷ Si $\pi_H(K_1) = \pi_H(K_2)$ où K_1, K_2 sont deux sous-groupes de G contenant H alors

$$K_1 = K_1H = \pi_H^{-1}(\pi_H(K_1)) = \pi_H^{-1}(\pi_H(K_2)) = K_2H = K_2.$$

D'où l'injectivité.

- ▷ On sait déjà que $\pi_H : G \rightarrow G/H$ est surjective, alors l'image directe $\tilde{\pi}_H : S_G \rightarrow S_{G/H}$ où S_G est l'ensemble des sous-groupes de G .

▷ L'image directe et l'image réciproque par π_H est une application croissante.

2. On procède en deux temps.

▷ Soit $L \triangleleft G/H$. Pour tout $g \in G$ et tout $x \in \pi_H^{-1}(L)$, on a

$$\pi_H(gxg^{-1}) = (gxg^{-1})H = (gH)(xH)(gH)^{-1} \in L,$$

car L est distingué dans G/H . Ainsi $xgx^{-1} \in \pi_H^{-1}(L)$ et donc $\pi_H^{-1}(L)$ est distingué dans G .

▷ Soit $K \triangleleft G$ un sous-groupe distingué contenant H . Pour tout $xH \in G/H$ et tout $kH \in \pi_H(K)$ avec $k \in K$, on a

$$(xH)(kH)(xH)^{-1} = (xkx^{-1})H.$$

Comme $K \triangleleft G$, on a $xkx^{-1} \in K$ d'où $(xkx^{-1})H \in \pi_H(K)$. On en déduit que $\pi_H(K)$ est distingué dans le groupe quotient G/H .

3.

8 Exercice 8. Combinatoire algébrique

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

1. Déterminer le cardinal des groupes finis $\text{GL}_n(\mathbb{k})$, $\text{SL}_n(\mathbb{k})$ et $\text{PGL}_n(\mathbb{k})$.
Indication : compter les bases de \mathbb{k}^n .

2. On prend désormais $n = 2$.

a) Montrer que le nombre de droites vectorielles de \mathbb{k}^2 est égal à $q + 1$.

b) En déduire qu'il existe un morphisme de groupes injectif

$$\text{PGL}_2(\mathbb{k}) \hookrightarrow \mathfrak{S}_{q+1}.$$

3. Montrer que $\text{GL}_2(\mathbb{F}_2) = \text{SL}_2(\mathbb{F}_2) = \text{PGL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3$.

4. Montrer que $\text{PGL}_2(\mathbb{F}_3) \cong \mathfrak{S}_4$.

1. L'application

$$\begin{aligned} \mathrm{GL}_n(\mathbb{k}) &\longrightarrow \{\text{bases de } \mathbb{k}^n\} \\ (C_1 \ C_2 \ \cdots \ C_n) &\longmapsto (C_1, \dots, C_n) \end{aligned}$$

est une bijection. Construisons une base de \mathbb{k}^n :

- (1) On choisit le premier vecteur C_1 dans $\mathbb{k}^n \setminus \{0\}$, on a donc $q^n - 1$ choix.
- (2) On choisit le second vecteur C_2 dans $\mathbb{k}^n \setminus \mathrm{vect}(C_1)$, on a donc $q^n - q$ choix.
- (3) On choisit le troisième vecteur C_3 dans $\mathbb{k}^n \setminus \mathrm{vect}(C_1, C_2)$, on a donc $q^n - q^2$ choix.
- (4) *Et cetera.*

D'où,

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

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

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

Ainsi,

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

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

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

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 :

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

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

10 Exercice 10. Automorphismes intérieurs.

Soit G un groupe. Pour $g \in G$, on note $\phi_g : G \rightarrow G$ la fonction définie par $h \mapsto ghg^{-1}$. On note $\text{Int}(G)$ l'ensemble des ϕ_g pour $g \in G$.

1. Soit $g \in G$, montrer que ϕ_g est un automorphisme de groupes.
2. Montrer que la fonction $\phi : G \rightarrow \text{Int}(G)$ qui à g associe ϕ_g est un morphisme de groupes.
3. Montrer l'isomorphisme $G/Z(G) \cong \text{Int}(G)$ où $Z(G)$ est le centre du groupe G .
4. (Plus difficile) Montrer que si le groupe des automorphismes $\text{Aut}(G)$ de G est cyclique alors G est abélien.
5. (Aussi difficile) Supposons que $\text{Aut}(G)$ est trivial. Démontrer que tous les éléments de G sont d'ordre au plus 2, puis que G est soit trivial, soit isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

11 Exercice 11.

Soit $n \in \mathbb{N}$ et $k \in \llbracket 0, n \rrbracket$. On note $\wp_k(\llbracket 1, n \rrbracket)$ l'ensemble des parties à k éléments de $\llbracket 1, n \rrbracket$.

1. Montrer que \mathfrak{S}_n agit naturellement sur $\wp_k(\llbracket 1, n \rrbracket)$.
2. Justifier que cette action est transitive.
3. Calculer le stabilisateur de $\llbracket 1, k \rrbracket \in \wp_k(\llbracket 1, n \rrbracket)$.
4. En appliquant la formule orbite-stabilisateur, retrouver la valeur de $\binom{n}{k}$.

1. Posons l'action de groupes :

$$\forall \sigma \in \mathfrak{S}_n, \forall i \in \wp_k(\llbracket 1, n \rrbracket), \quad \sigma \cdot I = \sigma(I) = \{\sigma(i) \mid i \in I\}.$$

La partie $\sigma(I)$ contient k éléments de $\llbracket 1, n \rrbracket$. Et, de plus, l'application $\sigma \mapsto (I \mapsto \sigma(I))$ est

Table des matières

	Théorèmes d'isomorphismes et actions de groupes.	1
1	Exercice 1. <i>Groupes monogènes</i>	1
2	Exercice 2.	1
3	Exercice 3.	3
4	Exercice 4.	3
5	Exercice 5.	4
6	Exercice 6. <i>Troisième théorème d'isomorphisme</i>	5
7	Exercice 7. <i>Sous-groupe d'un quotient</i>	7
8	Exercice 8. <i>Combinatoire algébrique</i>	8
9	Exercice 9. <i>Formule de BURNSIDE</i>	10
10	Exercice 10. <i>Automorphismes intérieurs</i>	10
11	Exercice 11.	11