Théorie des groupes

Table des matières

1 informations utiles

Slavyana GENINSKA Jean RAIMBAUT
cours sur : http ://www.math.univ-toulouse.fr/ jraimbau/Enseignement/theorie_des_groupes.html

Première partie

Théories des groupes

Exemple. *Isométries préservant un triangle équilateral*

Rappel 1. *Isométrie du plan :*

$$f : \mathbb{R}^2 \to \mathbb{R}^2$$
$$\forall x, y \in \mathbb{R}^2,\ d(x,y) = d(f(x), f(y))$$

Exemple. *Isométries*
- *symétrie*
- *rotation*
- *translation*
- *symétrie glissée*

Remarque 1. *L'identité, notée Id, peut être vue comme une rotation (d'angle 0) ou comme une translation (par le vecteur nul).*

Soit T, un triangle équilatéral.

$$Isom(T) = \{f : \mathbb{R}^2 \to \mathbb{R}^2,\ \textit{isométrie} \parallel f(T) = T\}$$

est l'ensemble des isométries du plan sui préservent T.
Une telle application f a forcement au moins un point fixe :

$$Isom(T) = \{Id, r_{\frac{2\pi}{3}}, r_{-\frac{2\pi}{3}}, S_A, S_B, S_C\}$$

On peut alors faire les deux remarques suivantes :

Remarque 2.
- *$Isom(T)$ est stable par composition :*
  $S_A \circ S_B = r_{\frac{2\pi}{3}}$
  $S_B \circ S_A = r_{-\frac{2\pi}{3}}$
- *Toute application $f \in Isom(T)$ admet une transformation inverse $f^{-1} \in Isom(T)$*

Exemple. *Le groupe symétrique :*
Soit E, un ensemble de n objets, S_n est l'ensemble des bijection de E, appelé groupe symétrique.
Par exemple, le groupe symétrique S_3 avec $E = \{1,2,3\}$

Remarque 3.
- *S_3 est stable par composition*
- *Toute bijection admet un inverse qui est encore dans S_3*

Remarque 4. *Les deux exemples sont les mêmes d'un certain point de vue, il s'agit de la même structure algébrique (nous verrons plus tard qu'il s'agit d'un isomorphisme)*

Définition 1. *Un groupe est un ensemble G muni d'une application (appelée loi de groupe) :*

$$* : \begin{array}{l} G \times G \to G \\ (g,h) \mapsto g * h \end{array}$$

Cette loi vérifie les propriétés suivantes :

— *associativité :*

$$\forall g,h,k \in G,\ (g*h)*k = g*(h*k)$$

— *présence d'un élément neutre :*

$$\exists e \in G \ / \ \forall g \in G,\ g*e = e*g = g$$

— *existance de l'inverse (ou symétrique) :*

$$\forall g \in G,\ \exists h \in G \ / \ g*h = h*g = e$$

Exemple.

1. *$\mathbb{R}$ avec la loi $+$, l'élément neutre est alors 0 et le symétrique est l'opposé.*
2. *$\mathbb{R}^*$ avec la loi $\cdot$, l'élément neutre est alors 1 et le symétrique est l'inverse.*
3. *Soit $P \subset \mathbb{R}^2$, un polygone régulier à n cotés.*
   On note alors $Isom(P)$, l'ensemble des isométries le concervant :

   $$Isom(P) = \{f : \mathbb{R}^2 \to \mathbb{R}^2,\ \textit{isométrie} \parallel f(P) = P\}$$

   $Isom(P)$ est alors un groupe si on le muni de la loi de composition $\circ$.
   L'élément neutre est alors l'identité : $\forall f \in Isom(P),\ f \circ Id = Id \circ f = f$.
   Le symétrique est la transformation réciproque f^{-1}
   Ce groupe est alors appelé groupe diédral, on le note D_n (ou D_{2n} étant donné que ce groupe possède $2n$ éléments).

   Exemple.
   — *$D_3 = Isom(T)$ est le groupe présenté dans l'exemple 1,*
   D_3 possède six éléments
   — *D_4 est l'ensemble des isométries préservant le carré.*
   $D_4 = Isom(C) = \{Id, r_{\frac{\pi}{2}}, r_\pi, r_{-\frac{\pi}{2}}, S_{AC}, S_{MP}, S_{BD}, S_{NQ}\}$
   D_4 possède donc 8 éléments
4. *Si E est un ensemble, l'ensemble des bijections de E dans E est un groupe pour la loi $\cdot$ comme précédemment.*
   Si $E = \{1,\dots,n\}$, $Bij(E) S_n$
   Si $E = \mathbb{R}$, $Bij(\mathbb{R})$ est un groupe
5. *$\mathbb{R}^n$ muni de l'addition vectorielle est un groupe. Plus généralement, tout espace vectoriel E est un groupe pour l'addition*
6. *$GL_n(\mathbb{R}) = \{A \in M_{n,n}(\mathbb{R}) \parallel detA \neq 0\}$ Pour la multiplication matricielle, voir l'exercice 1.*

Contre-exemple.
1. $(\mathbb{N}, +)$ *n'est pas un groupe car aucun élément n'admet de symétrique*
2. $(\mathbb{R}, \cdot)$ *n'est pas un groupe car* 0 *n'admet pas de symétrique*
3. $(\mathbb{Z}^*, \cdot)$ *n'est pas un groupe car* 1 *et* -1 *sont les seuls éléments admettant un symétrique*
4. $(\{-1, 0, 1\}, +)$ *n'est pas un groupe car* $1 + 1 = 2 \notin \{-1, 0, 1\}$

Remarque 5. *Le groupe* $\mathbb{Z}$ *est* $(\mathbb{Z}, +)$.
Le groupe $\mathbb{R}^*$ *est* $(\mathbb{R}^*, \cdot)$.
Le groupe $\mathbb{R}^n$ *est* $(\mathbb{R}^n, +)$.

Définition 2. *On dit qu'un groupe G est commutatif (ou abélien) si :*

$$\forall g, h \in G, \Rightarrow g * h = h * g$$

Exemple. $(\mathbb{Z}, +)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$, $(\mathbb{R}^n, +)$ *sont des groupes abéliens.*

Contre-exemple. S_n *pour* $n \geq 3$, $GL_n(\mathbb{R})$ *pour* $n \geq 2$ *ne sont pas des groupes abléliens*

Exemple. *Soit* $n > 0$*, un entier fixé.*
$\mathbb{Z}/n\mathbb{Z}$*, l'ensemble des entiers* $a \in \mathbb{Z}$ *considéré modulo n :*

$$\bar{a} = \{a + kn \mid k \in \mathbb{R}^n\} \in \mathbb{Z}/n\mathbb{Z}$$

Pour $a, b \in \mathbb{Z}$, $\bar{a} = \bar{b}$ *si et seulement si, pour* $k \in \mathbb{Z}$, $a - b = kn$

Exemple. *Dans* $\mathbb{Z}/3\mathbb{Z}$,
$\bar{1} = \bar{4} = \bar{10} = \bar{-2}$ *mais* $\bar{1} \neq \bar{2}$

$$\mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$$

$$\bar{0} = \{3k \mid k \in \mathbb{Z}\}$$

$$\bar{1} = \{1 + 3k \mid k \in \mathbb{Z}\}$$

$$\bar{2} = \{2 + 3k \mid k \in \mathbb{Z}\}$$

$$\bar{0} \cup \bar{1} \cup \bar{2} = \mathbb{Z}$$

On définit l'addition sur $\mathbb{Z}/n\mathbb{Z}$ *telle que :* $\bar{a} + \bar{b} = a \bar{+} b$.
On vérifie que cette définition ne dépend pas du choix des représentants.

$$\begin{aligned} \bar{a} + \bar{b} &= a + \bar{k_1} n + b + \bar{k_2} n \\ &= a + k_1 n \bar{+} b + k_2 n \\ &= a + b + (\bar{k_1} + k_2) n \\ &= a \bar{+} b \end{aligned}$$

Remarque 6. *Sur* $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$
$\bar{0} = \{2k \mid k \in \mathbb{Z}\}$, *l'ensemble des nombres pairs*
$\bar{1} = \{1 + 2k \mid k \in \mathbb{Z}\}$, *l'ensemble des nombres impairs*

$(\mathbb{Z}/n\mathbb{Z}, +)$ *est un groupe abélien.*

Remarque 7. *Comment définir une multiplication sur* $\mathbb{Z}/n\mathbb{Z}$ *?*

Notation. *Un groupe est noté G*

Notation. *notation multiplicative Il s'agit de la notation par défaut,*
"produit" du g et h : gh
élément neutre : e, 1 *ou* 1_G
l'inverse de g : g^{-1} *(et jamais* $\frac{1}{g}$*)*

Notation. *notation additive Il s'agit de la notation préférée pour les groupes abéliens,*
"somme" de a et b : $a + b$
élément neutre : 0 *ou* 0_G
l'inverse de a : $-a$

2 Les sous-groupes

Définition 3. *Soit G, un groupe.*
Un sous-ensemble $H \subset G$ *est appelé sous-groupe de G et noté* $H < G$ *si la loi sur G induit une structure de groupe sur H, c'est-à-dire :*

— $\forall h_1, h_2 \in H,\ h_1 h_2 \in H$ *(la loi est interne)*
— *l'élément neutre e de G est dans H*
— $\forall h \in H$, *h admet un symétrique* $h^{-1} \in H$ *(on dit que H est stable par passage au symétrique)*

Exemple. — $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} < \mathbb{Z}$
— $\mathbb{R}_{>0} = \{x \in \mathbb{R} \mid x > 0\} < \mathbb{R}^*$
— *Le cercle unité* $U = \{x \mid |z| = 1\} < \mathbb{C}^*$
Le groupe des racines n-ièmes de l'unité $U_n = \{z \in \mathbb{C} \mid z^n = 1\} < \mathbb{C}^*$
Remarque 8. $\forall n,\ U_n \subset U$ *mais* $\forall n,\ U_n \neq U$
— *Soit P un polygone.*
$Isom(P)$, *le groupe d'isométries préservant P (rotations et symétries).*
$Isom^+(P)$, *les isométries de* $Isom(P)$ *qui préservent l'orientation du plan (ici, seulement les rotation).*
On a $Isom^+(P) < Isom(P)$
— $Diff(\mathbb{R}) < Bij(\mathbb{R})$, *le sous-groupe des bijections de* $\mathbb{R}$ *de classe* $\mathscr{C}^\infty$
— $SL_n(\mathbb{R}) = \{M \in GL_n(\mathbb{R}) \mid det(M) = 1\} < GL_n(\mathbb{R})$

Proposition 1. *Soit G, un groupe.*
Un sous-ensemble H de G est un sous-groupe si et seulement si les deux consitions suivantes sont satisfaites :

— $H \neq \emptyset$
— $\forall h_1, h_2 \in H, h_1 h_2^{-1} \in H$

Démonstration. On suppose que H satisfait les deux points de la propriété ci-dessus.
$H \neq \emptyset$ donc $\exists h \in H$
pour vérifier que $e \in H$,
on applique la seconde propriété à h, donc $hh^{-1} = e \in H$ on vérifie ensuite que tout élément de H possède un inverse dans H,
soit $h \in H$, on applique la seconde propriété à e donc $eh^{-1} = h^{-1} \in H$
on vérifie enfin que le produit de tout élément de H appartient à H
Soient $h_1, h_2 \in H$. On applique la seconde propriété à $h_1, h_2^{-1} \in H$. Donc $h_1(h_2^{-1})^{-1} = h_1 h_2 \in H$ □

3 Sous-groupe engendré

Proposition 2. *Soit G, un groupe, soit de plus $S \subset G$.*

$$\exists! H < G \;/\; S \subset H \;\; et \;\; \forall F < G \;/\; S \subset F,\; H \subset F$$

Remarque 9. *Un groupe monogène est nécessairement commutatif.*

Démonstration. Si $G =< g >$, alors $G = \{g^n,\ n \in \mathbb{Z}\}$
De plus, si $k, l \in \mathbb{Z}$, on a $g^k g^l = g^{k+l} = g^{l+k} = g^l g^k$ □

Remarque 10. *En particulier, un groupe non commutatif ne peut pas être monogène (contraposée de la remarque précédente)*

Exemple. *S_3, par exemple, n'étant pas commutatif, n'est pas non plus monogène.*

3.1 Produit de groupes

Soient G_1 et G_2, deux groupes.
Le groupe produit $G = G_1 \times G_2$ est défini par l'ensemble $\{(g_1, g_2) \mid g_1 \in G_1,\ g_2 \in G_2\}$ avec l'opération $* : G \times G \to G$ définie par

$$(g_1, g_2) \times (h_1, h_2) = (g_1 h_1, g_2 h_2)$$

On définit de manière similaire le produit d'une famille de groupes.

Remarque 11.
$$G_1 \times (G_2 \times G_3) = (G_1 \times G_2) \times G_3 = G_1 \times G_2 \times G_3$$

Exemple.

—
$$\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z} = \{(m, n) \mid m, n \in \mathbb{Z}\}$$
$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$$

—
$$\begin{aligned}\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} &= \{(a, b) \mid a \in \frac{\mathbb{Z}}{2\mathbb{Z}},\ b \in \frac{\mathbb{Z}}{3\mathbb{Z}}\} \\ &= \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{0}, \bar{2}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1}), (\bar{1}, \bar{2})\} \\ &=< (\bar{1}, \bar{1}) > \text{ qui est un groupe cyclique d'ordre } 6\end{aligned}$$

— *$\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ n'est pas cyclique :*
$\{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1})\}$ *contient un élément d'ordre* 1 *et trois éléments d'ordre* 2.
$\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ *ne contient pas d'élément d'ordre* 4 *et n'est donc pas cyclique.*

3.2 Morphismes

Définition 4. *Soient $(G, \star)$ et $(\Gamma, \diamond)$, deux groupes.*
On appelle morphisme (ou homomorphisme) de groupes de G vers Γ toute application

$$\varphi : G \to \Gamma$$

telle que $\forall g, h \in G,\ \varphi(g \star h) = \varphi(g) \diamond \varphi(h)$

Remarque 12. *S'il n'y a pas d'ambiguïté, on utilisera la notation multiplicative pour G et Γ :*

$$\varphi(gh) = \varphi(g)\varphi(h)$$

Propriété 1. — $\varphi(e_G) = e_\Gamma$

Démonstration.

$$\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$$

On multiplie par $\varphi(e_G)^{-1}$ l'égalité précédente et on obtient

$$\varphi(e_G)\varphi(e_G)^{-1} = \varphi(e_G)\varphi(e_G)\varphi(e_G)^{-1}$$

$$\Rightarrow e_\Gamma = \varphi(e_G)e_\Gamma$$

Donc, $e_\Gamma = \varphi(e_G)$ □

— $\forall g \in G,\ \varphi(g^{-1}) = \varphi(g)^{-1}$
— $\forall n \in \mathbb{Z},\ \forall g \in G,\ \varphi(g^n) = \varphi(g)^n$

Démonstration. Par récurrence pour $n > 0$,
On utilise $\varphi(g^1) = \varphi(g)$
Pour $n \geq 2$,

$$\begin{aligned}\varphi(g^n) &= \varphi(g^{n-1}g)\\ &= \varphi(g^{n-1})\varphi(g)\\ &= \varphi(g)^{n-1}\varphi(g)\\ &= \varphi(g)^n\end{aligned}$$

Pour $n = 0$,
$g^0 = e_G$ et $\varphi(g)^0 = e_\Gamma$
Pour $n = 1$,

□

Définition 5. *Soit $\varphi : G \to \Gamma$, un morphisme de groupes.*
On appelle :

— *Image de φ, l'ensemble*

$$Im(\varphi) = \{\varphi(g) \mid g \in G\} = \{\gamma \in \Gamma \mid \exists g \in G \ /\ \varphi(g) = \Gamma\} \subset \gamma$$

— *noyau de φ,*

Remarque 13. — *Les exemples 1, 3 et 4 sont des isomorphismes*
— *Le déterminant n'est pas bijectif pour $n > 1$*

Définition 6. *Soit G un groupe.*
Un sous-groupe H de G est distingué (ou normal) dans G si

$$\forall g \in G,\ \forall h \in H,\ ghg^{-1} \in H$$

Notation. *On note alors* $H \triangleleft G$

Un élément de type ghg^{-1} *est dit conjugué de* h *par* g.

Proposition 3. *Soit* $\varphi : G \to \Gamma$, *un morphisme.*

- $Im(\varphi)$ *est un sous-groupe de* Γ
- $Ker(\varphi)$ *est un sous-groupe distingué de* G

Démonstration. — — $\varphi(e_G) = e_\Gamma$ donc $e_\Gamma \in Im(\varphi)$

□

Proposition 4. *Soit* $\varphi : G \to \Gamma$, *un morphisme.*
Alors φ *est injectif si et seulement si* $Ker(\varphi) = \{e_G\}$

Démonstration. Dans le sens direct :
On suppose que φ, est injectif, i.e.

$$\forall g_1, g_2 \in G,\ \varphi(g_1) = \varphi(g_2) \Rightarrow g_1 = g_2$$

Soit $g \in Ker(\varphi)$. On sait que $e_G \in Ker(\varphi)$
On a alors, $\varphi(g) = e_\Gamma = \varphi(e_G)$.
Par l'injectivité de φ, on a $g = e_G$.
Donc $Ker(\varphi) = \{e_G\}$

Dans le sens indirect :
On suppose que $Ker(\varphi) = \{e_G\}$
On veut montrer que φ est injectif.
Soient $g_1, g_2 \in G$ tels que $\varphi(g_1) = \varphi(g_2)$

$$\begin{aligned} \varphi(g_1 g_2^{-1}) &= \varphi(g_1)\varphi(g_2^{-1}) \\ &= \varphi(g_2)\varphi(g_2)^{-1} \\ &= e_\Gamma \end{aligned}$$

Donc $g_1 g_2^{-1} \in Ker(\varphi) = \{e_G\}$
Donc $g_1 g_2^{-1} = e_G$
Donc $g_1 = g_2$
Donc φ est injectif. □

Proposition 5. *Si* $\varphi : G \to \Gamma$ *est un morphisme bijectif, alors l'application* $\varphi^{-1} : \Gamma \to G$ *est un morphisme (lui aussi bijectif).*
Autrement dit, si $\varphi : G \to \Gamma$ *est un isomorphisme, alors* $\varphi^{-1} : \Gamma \to G$ *est aussi un isomorphisme.*

Démonstration. Soient $\gamma_1, \gamma_2 \in \Gamma$
Il existe $g_1, g_2 \in G$ tels que $\gamma_1 = \varphi(g_1)$ et $\gamma_2 = \varphi(g_2)$

$$\begin{aligned} \varphi^{-1}(\gamma_1\gamma_2) &= \varphi^{-1}(\varphi(g_1)\varphi(g_2)) \\ &= \varphi^{-1}(\varphi(g_1 g_2)) \\ &= g_1 g_2 \\ &= \varphi^{-1}(\gamma_1)\varphi^{-1}(\gamma_2) \end{aligned}$$

Donc φ^{-1} est un morphisme. $\square$

Définition 7. *Deux groupes G et F sont isomorphes s'il existe un isomorphisme $\varphi : G \to \Gamma$.*

Notation. *On note alors $G \cong \Gamma$*

Remarque 14. *Deux groupes sont isomorphes quand ils possèdent la même structure de groupe.*

Exemple.

— $exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$ *est un isomorphisme.*
  Donc $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$
— $\begin{aligned} f : Isom(T) &\to S_3 \\ g &\mapsto f(g) \ / \ g(x_i) = x_{f(g)(i)} \end{aligned}$ *est un isomorphisme*
  Donc $Isom(T) \cong S_3$
— *Les trois groupes suivants sont deux à deux isomorphes :*
  $\mathbb{Z}/n\mathbb{Z}$*, les racines n-ièmes de l'unité* U_n *et* $Isom(n-$*gônes réguliers*$)$
— $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
—
$$\begin{aligned} f_1 : \mathbb{Z}/n\mathbb{Z} &\to U_n \\ \bar{k} &\mapsto e^{i\frac{2k\pi}{n}} \end{aligned}$$
  est un isomorphisme
—
$$\begin{aligned} f_2 : U_n &\to Isom(n-\textit{gônes réguliers}) \\ e^{i\frac{2k\pi}{n}} &\mapsto r_{\frac{2k\pi}{n}} \end{aligned}$$

Proposition 6. *Soit G un groupe.*

1. *Si $\varphi : (\mathbb{Z}, +) \to G$ est un morphisme, alors il existe un unique élément de G tel que $\forall n \in \mathbb{Z},\ \varphi(n) = g^n$ l'élément neutre est donné par $\varphi(1) = g$.*

   Démonstration. $g = \varphi(1)$ est unique.
   Puis on se sert de la troisième propriété (qui nous donne $\varphi(n) = \varphi(1)^n = g^n$) $\square$

2. *Si g est un élément quelconque de G, alors il existe un unique morphisme $\varphi_g : (\mathbb{Z}, +) \to G$, tel que $\varphi(1) = g^n$*

   Démonstration. φ est un morphisme de groupes car
   $$\varphi(m+n) = g^{m+n} = g^m g^n = \varphi(m)\varphi(n)$$
   $\square$

Rappel 2. *Pour $\varphi : G \to \Gamma$, un isomorphisme $(\forall g, h \in G,\ \varphi(gh) = \varphi(g)\varphi(h))$*
φ est un isomorphisme si et seulement s'il est un morphisme bijectif.

Proposition 7. *Soit $\varphi : G \to Gamma$, un isomorphisme :*

1. *Si G est abélien, alors Γ est abélien.*
2. *Si $g \in G$ est d'ordre n, alors $\varphi(g) \in \Gamma$ est d'ordre n.*

Démonstration.

1. Soient $\gamma_1 = \varphi(g_1), \gamma_2 = \varphi(g_2) \in \Gamma(g_1, g_2 \in G)$

$$\begin{aligned}\gamma_1\gamma_2 &= \varphi(g_1)\varphi(g_2)\\ &= \varphi(g_1 g_2)\\ &= \varphi(g_2 g_1)\\ &= \varphi(g_2)\varphi(g_1)\\ &= \gamma_2\gamma_1\end{aligned}$$

   Donc Γ est abélien.
2. Soit $g \in G$ d'ordre n, c'est-à-dire que n est le plus petit entier naturel non nul tel que $g^n = e^g$.
   On veut montrer que $\varphi(g)$ est d'ordre n.
   —
$$\begin{aligned}\varphi(g)^n &= \varphi(g^n)\\ &= \varphi(e_G)\\ &= e_\Gamma\end{aligned}$$
   — Il reste à montrer que $\forall k \in \mathbb{Z},\ 0 < k < n,\ \varphi(g)^k \neq e_\Gamma$

$$\varphi(g)^k = \varphi(g^k) = e_\Gamma \Leftrightarrow g^k \in ker(\varphi) = \{e_G\}$$

   Donc $\varphi(g)^k = e_\Gamma$ si et seulement si $g^k = e_G$
   Ainsi, $\varphi(g)$ et g ont le même ordre.

□

Exemple.

1. *$\mathbb{Z}/6\mathbb{Z}$ n'est pas isomorphe à $Isom(T)$*
   — *$\mathbb{Z}/6\mathbb{Z}$ contient un élément d'ordre G et les ordres possibles pour les éléments de $Isom(T)$ sont 1, 2 et 3.*
   — *$\mathbb{Z}/6\mathbb{Z}$ est abélien mais $Isom(T)$ ne l'est pas.*
2. *$\mathbb{Z}/4\mathbb{Z}$ (d'ordre 4) n'est pas isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (dont l'ordre maximal est 2).*
   Si G est cyclique d'ordre n, alors il existe un $g \in G$ d'ordre n.
   Donc $\varphi(g)$ est d'ordre n.
   Ainsi, si φ est bijective, Γ est d'ordre n.

Remarque 15. *De façon générale, si $\varphi : G \to \Gamma$, est un isomorphisme et G, un groupe cyclique, alors Γ est aussi un groupe cyclique.*