Not to appear in Nonlearned J., 45.

Sur les automorphismes d'un groupe cyclique

N. GHADBANE(1) et D. MIHOUBI(1)

LMPA, Département de Mathématiques, Université de M'sila, Algérie.

nacer.ghadbane@yahoo.com et Mihoubi.douadi@yahoo.fr

Subject headings: groupe cyclique, les automorphismes d'un groupe cyclique, la fonction indicatrice d'Euler, les générateurs d'un groupe cyclique.

Résumé: Pour tout entier naturel n, on note par $Aut(\mathbb{Z}/n\mathbb{Z})$ le groupe des automorphismes du groupe additif des entiers modulo n $(\mathbb{Z}/n\mathbb{Z},+)$. On sait que $Aut(\mathbb{Z}/n\mathbb{Z})$ et $(\mathbb{Z}/n\mathbb{Z})^{\times}$ le groupe des éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$ sont isomorphes.

L'objet de cette étude est de donner une généralisation de ce résultat à un groupe cyclique quelconque c'est-à-dire on va montrer le résultat suivant: si G un groupe cyclique d'ordre n et de générateur g, alors le groupe $Aut(G)$ des automorphismes de G est isomorphe au groupe $G^{\times}$ des éléments symétrisables dans G où $G^{\times}=\left\{g^{k}: p\gcd(k,n)=1\right\}$, muni de l'opération interne $*$ définie par:

$$\forall g^{k},g^{k'}\in G^{\times}: g^{k}*g^{k'}=g^{kk'}.$$

1. Introduction

Deux groupes G et G' sont dits isomorphes et on note cette relation par $G\simeq G'$, s'il existe un isomorphisme de groupes $f: G\longrightarrow G'$. Dans ce cas G et G' sont dans la même classe de la relation $\simeq$ définie sur l'ensemble des groupes. Cette notion est d'une extrême importance pour la classification des groupes. Si deux groupes G et G' sont isomorphes alors ils ont la même structure algébrique ou bien les mêmes propriétés algébriques en d'autres mots G' représente G. Par exemples, les propriétés suivantes sont les mêmes entre deux groupes isomorphes: L'ordre, commutativité, cyclicité, chaque élément a un ordre fini, ...etc.

Dans ce travail, on montre le résultat suivant:

[1]LMPA, Département de Mathématiques, Université de M'sila, Algérie.

Etant donné un groupe cyclique G, le groupe des automorphismes de G est isomorphe au groupe $G^{\times}$ des éléments générateurs de G . En d'autres mots, $Aut(G) \simeq G^{\times}$.

Notons que ce résultat est une généralisation du théorème suivant :

$$(\mathbb{Z}/n\mathbb{Z})^{\times} \simeq Aut(\mathbb{Z}/n\mathbb{Z}),$$

où $(\mathbb{Z}/n\mathbb{Z})^{\times}$ désigne le groupe des unités de $\mathbb{Z}/n\mathbb{Z}$ et $Aut(\mathbb{Z}/n\mathbb{Z})$ le groupe des automorphismes de $\mathbb{Z}/n\mathbb{Z}$.

Ce papier est subdivisé en trois sections. Dans la première section, on introduit l'importance de la notion d'isomorphisme de groupes. La seconde section sera consacrée à quelques notions algébriques nécessaires pour ce travail. Enfin, dans la troisième section, on montre le résultat essentiel de ce papier.

2. Préliminaires

Soit G un groupe et A une partie de G. Alors le groupe engendré par A, noté $\langle A \rangle$ est défini par :

$$\langle A \rangle = \bigcup_{r \in \mathbb{N}} \{a_1 a_2 ... a_r : \forall 1 \leq i \leq r, a_i \in A \cup A^{-1}\} \text{ où } A^{-1} = \{a^{-1} : a \in A\}.$$

Si $\langle A \rangle = G$, alors A est une partie génératrice de G. Si $|A| = 1$, alors G est dit monogène. Le groupe G est dit cyclique s'il est monogène et d'ordre fini, i.e $|G| = n$, $n \in \mathbb{N}^*$.

Un homomorphisme entre deux groupes G et G' est une application $f : G \longrightarrow G'$ qui satisfait:

$$f(x \cdot y) = f(x) \cdot f(y), \forall x, y \in G.$$

Notons que si G est un groupe monogène de générateur g et f est un morphisme surjectif de G vers G', alors G' est monogène aussi de générateur $f(g)$. On fait remarquer si G un groupe cyclique d'ordre n non réduit à son élément neutre et g un générateur de G, alors les autres éléments générateurs de G sont les g^k tels que $k \in \{1..., n-1\}$ avec $p\gcd(k, n) = 1$. L'ensemble des éléments générateurs de G, noté $G^{\times}$, est de cardinal $\varphi(n)$ avec $\varphi(n) = |\{k \in \{1..., n-1\} : p\gcd(k, n) = 1\}|$, où φ désigne la fonction indicatrice d'Euler.

Exemple 2.1:

Soit $G = (\mathbb{Z}/n\mathbb{Z}, +)$ avec $n \in \mathbb{N}$, où $\mathbb{N}$ dénote l'ensemble des entiers naturels, dans ce cas $(G^\times, \cdot) = \left((\mathbb{Z}/n\mathbb{Z})^\times, \cdot\right)$ le groupe des unités de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ muni de la multiplication des classes d'élément neutre la classe $\overline{1}$. Pour $n = 6$, les générateurs de $(\mathbb{Z}/6\mathbb{Z}, +)$ sont $\left\{\overline{1}; \overline{5}\right\}$.

3. Les automorphismes d'un groupe cyclique

Cette section sera consacrée à la démonstration du résultat suivant:

Etant donné un groupe cyclique G, le groupe des automorphismes de G est isomorphe au groupe $G^\times$ des éléments générateurs de G . En d'autres mots, $Aut(G) \simeq G^\times$.

Un automorphisme d'un groupe G est un morphisme bijectif de G vers G. L'ensemble des automorphismes d'un groupe G, noté $Aut(G)$, muni de la composition des applications, i.e $(Aut(G), \circ)$ est un groupe.

La proposition suivante montre que les automorphismes de $\mathbb{Z}/n\mathbb{Z}$ sont de la forme $f_{\overline{m}}(\overline{x}) = \overline{mx}$, avec $\overline{m} \in (\mathbb{Z}/n\mathbb{Z})^\times$ et $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$.

Proposition 3.1

Soit $n \in \mathbb{N}^*$,

1. Pour tout $\overline{m} \in (\mathbb{Z}/n\mathbb{Z})^\times$, l'application $f_{\overline{m}} : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ définie par $\overline{x} \longmapsto \overline{mx}$ est un automorphisme de $\mathbb{Z}/n\mathbb{Z}$.

2. L'application $\Psi : Aut(\mathbb{Z}/n\mathbb{Z}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ définie par $f \longmapsto \Psi(f) = f(\overline{1})$ est un isomorphisme de groupes.

Démonstration

1. L'application $f_{\overline{m}}$ est un homomorphisme. En effet, pour $\overline{x}, \overline{y} \in \mathbb{Z}/n\mathbb{Z}$ on a:

$$f_{\overline{m}}(\overline{x} + \overline{y}) = \overline{m}(\overline{x} + \overline{y}) = \overline{mx} + \overline{my} = f_{\overline{m}}(\overline{x}) + f_{\overline{m}}(\overline{y}).$$

Montrons que $f_{\overline{m}}$ est surjectif. Soit $\overline{y} \in \mathbb{Z}/n\mathbb{Z}$, l'équation $\overline{y} = f_{\overline{m}}(\overline{x})$ est équivalente à $\overline{y} = \overline{mx}$, comme $\overline{m} \in (\mathbb{Z}/n\mathbb{Z})^\times$, il existe donc $(\overline{m})^{-1} \in (\mathbb{Z}/n\mathbb{Z})^\times$, dit l'inverse de $\overline{m}$, et on a $(\overline{m})^{-1}\,\overline{y} = (\overline{m})^{-1}\,\overline{mx}$ et par suite $\overline{x} = (\overline{m})^{-1}\,\overline{y}$, ce qui montre que $f_{\overline{m}}$ est bien surjective.

Comme $f_{\overline{m}} : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ est surjective et $\mathbb{Z}/n\mathbb{Z}$ est de cardinal fini, alors $f_{\overline{m}}$ est bien injective, et par conséquent $f_{\overline{m}}$ est un élément du groupe $(Aut(\mathbb{Z}/n\mathbb{Z}), \circ)$.

2. Il est clair que si $f \in Aut(\mathbb{Z}/n\mathbb{Z})$, alors $f(\overline{1})$ est un élément générateur de $\mathbb{Z}/n\mathbb{Z}$. En

effet, comme f est surjectif et $\mathbb{Z}/n\mathbb{Z} = \langle \overline{1} \rangle$ alors $f(\overline{1}) \in (\mathbb{Z}/n\mathbb{Z})^{\times}$.

Vérifions tout d'abord que Ψ est un morphisme de groupes. Soit $f, g \in Aut(\mathbb{Z}/n\mathbb{Z})$, on montre qu'on a $\Psi(f \circ g) = \Psi(f) \cdot \Psi(g)$ ce qui équivaut à dire $(f \circ g)(\overline{1}) = f(\overline{1}) \cdot g(\overline{1})$.

On a $(f \circ g)(\overline{1}) = f(g(\overline{1}))$, avec $g(\overline{1}) \in (\mathbb{Z}/n\mathbb{Z})^{\times}$, alors $\exists 1 \leq k \leq n-1$ tel que: $p\gcd(k,n) = 1$ et $g(\overline{1}) = \overline{k}$.

Donc $f(g(\overline{1}) = f(\overline{k}) = f(\underbrace{\overline{1} + \overline{1} + ... + \overline{1}}_{k\ fois}) = kf(\overline{1}) = f(\overline{1}).g(\overline{1})$.

Par conséquent, l'application Ψ est un morphisme de groupes. Montrons que $Ker\Psi = \{id_{\mathbb{Z}/n\mathbb{Z}}\}$ ce qui permet d'assurer que Ψ est injectif.

On a $Ker\Psi = \{f \in Aut(\mathbb{Z}/n\mathbb{Z}) : \Psi(f) = \overline{1}\} = \{f \in Aut(\mathbb{Z}/n\mathbb{Z}) : f(\overline{1}) = \overline{1}\}$,

comme $f \in Aut(\mathbb{Z}/n\mathbb{Z})$ et $f(\overline{1}) = \overline{1}$, alors pour tout $\overline{t} \in \mathbb{Z}/n\mathbb{Z}$, on a $f(\overline{t}) = f(\underbrace{\overline{1} + \overline{1} + ... + \overline{1}}_{t\ fois}) = tf(\overline{1}) = t.\overline{1} = \overline{t}$.

Donc $f(\overline{1}) = \overline{1} \Longleftrightarrow f = id_{\mathbb{Z}/n\mathbb{Z}}$. Et par suite, $Ker\Psi = \{id_{\mathbb{Z}/n\mathbb{Z}}\}$.

Enfin, l'application Ψ est surjectif car pour tout $\overline{m} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$, $\exists f_{\overline{m}} \in Aut(\mathbb{Z}/n\mathbb{Z})$, avec $\Psi(f_{\overline{m}}) = f_{\overline{m}}(\overline{1}) = \overline{m}.\overline{1} = \overline{m}$.

Finalement, on a bien $(\mathbb{Z}/n\mathbb{Z})^{\times} \simeq Aut(\mathbb{Z}/n\mathbb{Z})$.■

Exemple 3.2

▶ Pour $n = 6$, on a $(\mathbb{Z}/6\mathbb{Z})^{\times} = \{\overline{1}; \overline{5}\}$, dont la table de Cayley du groupe est décrite ci-contre:

$\cdot$	$\overline{1}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{5}$
$\overline{5}$	$\overline{5}$	$\overline{1}$

.

▶ On a dans ce cas $Aut(\mathbb{Z}/6\mathbb{Z}) = \{f_{\overline{1}}, f_{\overline{5}}\}$, avec $f_{\overline{1}} = \begin{pmatrix} \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} \\ \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} \end{pmatrix}$ et $f_{\overline{5}} = \begin{pmatrix} \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} \\ \overline{0} & \overline{5} & \overline{4} & \overline{3} & \overline{2} & \overline{1} \end{pmatrix}$. Le groupe $Aut(\mathbb{Z}/6\mathbb{Z}), \circ)$ dont la table est

$\circ$	$f_{\overline{1}}$	$f_{\overline{5}}$
$f_{\overline{1}}$	$f_{\overline{1}}$	$f_{\overline{5}}$
$f_{\overline{5}}$	$f_{\overline{5}}$	$f_{\overline{1}}$

est identique à celle du groupe $((\mathbb{Z}/6\mathbb{Z})^{\times}, \cdot)$ ce qui montre que ces deux groupes sont bien isomorphes.

A présent, on montre que si $G = \langle g \rangle$ est un groupe cyclique d'ordre n, alors l'ensemble $G^{\times}$ des éléments générateurs de G muni de l'opération $*$ définie ci-dessous dans la proposition **3.3** a une structure de groupe commutatif d'élément neutre le générateur g.

Proposition 3.3

Soient G un groupe cyclique d'ordre n, d'élément neutre noté 1_G, et g un générateur de G, l'ensemble $G^{\times}$ des éléments générateurs de G muni de l'opération $*$ définie par:

$\forall g^k, g^{k'} \in G^{\times} : g^k * g^{k'} = g^{kk'}$, *avec* $k, k' \in \{1..., n-1\}, p\gcd(k, n) = 1, p\gcd(k', n) = 1,$

est un groupe commutatif.

Démonstration

1. La loi de composition $*$ est interne sur $G^{\times}$. En effet,

pour $g^k, g^{k'} \in G^{\times}$, on a $g^k * g^{k'} = g^{kk'}$, et comme $k, k' \in \{1..., n-1\}$ avec $p\gcd(k, n) = 1$ et $p\gcd(k', n) = 1$, on a $p\gcd(kk', n) = 1$, et par suite $g^k * g^{k'} = g^{kk'} \in G^{\times}$.

2.La loi $*$ est commutative, pour $g^k, g^{k'} \in G^{\times}$, on a $g^k * g^{k'} = g^{kk'} = g^{k'k} = g^{k'} * g^k$.

3. La loi $*$ est associative. En effet, soient $g^k, g^{k'}, g^{''} \in G^{\times}$,

on a $g^k * (g^{k'} * g^{k''}) = g^k * g^{k'k''} = g^{k(k'k'')} = g^{(kk')k''} = (g^k * g^{k'}) * g^{k''}$.

4. L'élément g^1 est neutre pour la loi $*$, en effet, pour $g^k \in G^{\times}$ on a $g^k * g = g * g^k = g^k$.

5. L'élément $g^{k'}$ de $G^{\times}$ est le symétrique de g^k si, et seulement si $g^k * g^{k'} = g^{k'} * g^k = g$.

Comme $g^k \in G^{\times}$, on $p\gcd(k, n) = 1$ et d'après l'identité de Bézout il existe $(u, v) \in \mathbb{Z}^2$ tels que $uk + nv = 1$ et par suite $g^{uk+nv} = g^1$, ceci ce traduit dans le groupe G par $g^{uk} \cdot g^{nv} = g$, comme g est d'ordre n on a $(g^n)^v = 1_G$, et par suite $g^{uk} \cdot 1_G = g^{uk} = g$, qui s'écrit $g^u * g^k = g$ dans le groupe $G^{\times}$. Donc on prend k' le seul entier u qui vérifie $uk \equiv 1\,[n]$ et par suite $g^{k'} = g^u$ est le symétrique de g^k dans $G^{\times}$.■

Exemple 3.4

Soit G un groupe cyclique d'ordre 6, donc $G = \{1_G, g, g^2, g^3, g^4, g^5\}$ et $G^\times = \{g, g^5\}$, dont la table de Cayley du groupe $(G^\times, *)$ est décrite ci-contre:

$*$	g	g^5
g	g	g^5
g^5	g^5	g

. On a par exemple $g^5 * g^5 = g^{25} = g^{4\times 6+1} = (g^6)^4 \cdot g^1 = 1_G \cdot g^1 = g$.

Proposition 3.5

Soit G un groupe cyclique d'ordre $n \in \mathbb{N}^*$ de générateur g.

1. *Pour tout $g^k \in G^\times$, l'application $f_{g^k} : G \longrightarrow G$, définie par: $g^t \longmapsto g^{kt}$, avec $0 \leq t \leq n-1$ est un automorphisme de G.*

2. *L'application $\Psi : Aut(G) \longrightarrow (G)^\times$, définie par $f \longmapsto \Psi(f) = f(g)$, est un isomorphisme de groupes.*

Démonstration

1. l'application f_{g^k} est un homomorphisme. En effet, pour $g^t, g^{t'} \in G$, on a:

$f_{g^k}(g^t g^{t'}) = f_{g^k}(g^{t+t'}) = g^{k(t+t')} = g^{kt+kt'} = g^{kt} \cdot g^{kt'} = f_{g^k}(g^t) \cdot f_{g^k}(g^{t'})$.

Montrons que f_{g^k} est injectif: soit $\left(g^t, g^{t'}\right) \in G^2$, alors,

$f_{g^k}(g^t) = f_{g^k}(g^{t'}) \Longleftrightarrow g^{kt} = g^{kt'} \Leftrightarrow g^{k(t-t')} = 1_G \Longleftrightarrow n$ divise $k(t-t')$,

On a $\left\{\begin{array}{c} n \text{ divise } k(t-t') \\ \text{et} \\ p\gcd(k,n) = 1 \end{array}\right.$ d'après le lemme de Gausse, alors n divise $t - t'$, donc $\exists q \in \mathbb{Z}$: $t - t' = qn$.

Et comme $1 \leq t \leq n-1$ et $1 \leq t' \leq n-1$, alors $t - t' = 0$, donc $t = t'$.

Comme $f_{g^k} : G \longrightarrow G$ est injectif et G est de cardinal fini, alors f_{g^k} est surjectif, et par conséquent f_{g^k} est un élément du groupe $(Aut(G), \circ)$.

2. L'application Ψ est bien définie car si $f \in Aut(G)$, alors $f(g)$ est un élément de $G^\times$ de sorte que $f(g)$ est un générateur de $(G, .)$.

De plus si $f, h \in Aut(G)$ avec $f = h$, on a donc $f(g^t) = h(g^t)$ pour tout $t \in \{0, 1, ..., n-1\}$ en particulier $f(g) = h(g)$ ce qui montre qu'on bien $\Psi(f) = \Psi(h)$.

L'application Ψ est un morphisme, en effet, Soit $f, h \in Aut(G)$, avec $f(g) = g^{k'}, h(g) = g^k$

et $g^{k'}, g^k$ appartiennent à $G^{\times}$.

On a $(f \circ h)(g) = f(h(g)) = f(g^k) = (f(g))^k = (g^{k'})^k = g^{kk'} = g^{k'} * g^k = f(g) * h(g)$ ce qui montre $\Psi(f \circ h) = \Psi(f) * \Psi(h)$.

Montrons que $Ker\Psi = \{id_G\}$ ce qui permet d'assurer que Ψ est injectif.

On a $Ker\Psi = \{f \in Aut(G) : \Psi(f) = g\} = \{f \in Aut(G) : f(g) = g\}$,

comme $f \in Aut(G)$ et $f(g) = g$, alors pour tout $1 \leq t \leq n-1$,

$f(g^t) = f(\underbrace{g.g.....g}_{t\ fois}) = (f(g))^t = g^t$.

Donc $f(g) = g \Longleftrightarrow f = id_G$. Et $Ker\Psi = \{id_G\}$, par conséquent Ψ est injectif.

L'application Ψ est surjectif, car pour tout $g^k \in (G)^{\times}, \exists f_{g^k} \in Aut(G)$, avec $\Psi(f_{g^k}) = f_{g^k}(g) = g^k$.

Finalement $(G)^{\times} \simeq Aut(G)$.■

Exemple 3.6

Soit G un groupe cyclique d'ordre 5, donc $G = \{1_G, g, g^2, g^3, g^4\}$ et $G^{\times} = \{g, , g^2, g^3, g^4\}$.

Le groupe $(G^{\times}, *)$ dont la table est

$*$	g	g^2	g^3	g^4
g	g	g^2	g^3	g^4
g^2	g^2	g^4	g	g^3
g^3	g^3	g	g^4	g^2
g^4	g^4	g^3	g^2	g

.

Dans ce cas $Aut(G) = \{f_g, f_{g^2}, f_{g^3}, f_{g^4}\}$, avec $f_g = \begin{pmatrix} 1_G & g & g^2 & g^3 & g^4 \\ 1_G & g & g^2 & g^3 & g^4 \end{pmatrix}$,

$f_{g^2} = \begin{pmatrix} 1_G & g & g^2 & g^3 & g^4 \\ 1_G & g^2 & g^4 & g & g^3 \end{pmatrix}$, $f_{g^3} = \begin{pmatrix} 1_G & g & g^2 & g^3 & g^4 \\ 1_G & g^3 & g & g^4 & g^2 \end{pmatrix}$ et $f_{g^4} = \begin{pmatrix} 1_G & g & g^2 & g^3 & g^4 \\ 1_G & g^4 & g^3 & g^2 & g \end{pmatrix}$

.

Le groupe $(Aut(G), \circ)$ dont la table est

$\circ$	f_g	f_{g^2}	f_{g^3}	f_{g^4}
f_g	f_g	f_{g^2}	f_{g^3}	f_{g^4}
f_{g^2}	f_{g^2}	f_{g^4}	f_g	f_{g^3}
f_{g^3}	f_{g^3}	f_g	f_{g^4}	f_{g^2}
f_{g^4}	f_{g^4}	f_{g^3}	f_{g^2}	f_g

.

REFERENCES

[1] M. Demazure. Cours d'algèbre, Paris, Cassini, 1997.

[**2**] Daniel Guin, Thomas Hausberger. Groupes, Corps et théorie de Galois, EDP sciences, 2008.

[**3**] F. Pécastaings. Chemins vers l'algèbre tome 1, Vuibert,1993.

[**4**] L. Schwartz, Algèbre $3^{ième}$ Année. Dunod, 2003.

This preprint was prepared with the AAS LATEX macros v5.2.