PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

**Mohamed Boudiaf University of M'sila**
**Faculty of Mathematics and Computer Science**
**Department of Mathematics**

# *Master Thesis*

**Domaine** : Mathematics and Computer Science
**Track** : Mathematics
**Option** : Algebra and Discrete Mathematics

# Theme

*Holomorph of the group and their applications in cryptography*

**Presented by :**
*GUAGUI* Fatima ezzahra

**Before the jury composed of :**

| | | |
|---|---|---|
| N. *GHADBANE* | University of M'sila | **Supervisor**. |
| D. *MIHOUBI* | University of M'sila | **President**. |
| L. *HEBOUB* | University of M'sila | **Examiner**. |

University Year 2020/2021

## Acknowledgements

Thanks to GOD almighty for the completion of this work. Only due to his blessings I could finish it.

I would like to express my deepest gratitude to my advisor, Mr: N.Ghadbane, for his invaluable advices and suggestions.

My thanks also ago to the jury members for the honor they have done me by accepting to judge this modest work.

I would like to thank my beloved parents for their encouragement who are so supportive to me throughout my life. My sisters, brothers deserve my wholehearted thanks as well, to all my friends and all people who have helped me during my study.

This work is only a begining of my journey.

thanks

# Table of contents

# Notations

| | |
|---|---|
| $1_G$ | The neutral element of $G$ |
| $x^{-1}$ | The invertible element of $G$ |
| $\|G\|$ | Order of a group $G$ |
| $H \leq G$ | $H$ subgroup of $G$ |
| $\langle S \rangle$ | Subgroup of $G$ generated by $S$ |
| $\Re$ | Relation |
| $[x]$ | Equivalence class defined by $x$ |
| $A/\Re$ | Quotient set of $A$ with respect to $\Re$ |
| $[G : H]$ | The index of $H$ in $G$ |
| $G \lhd H$ | $H$ normal subgroup of $G$ |
| $(G)^\star$ | Group of units |
| $S(E)$ | The set of all permutation |
| $G \times H$ | Direct product of groups |
| $G \rtimes_\theta H$ | Semidirect product of groups |
| $End(G)$ | Set of all endomorphism of a group $G$ |
| $Aut(G)$ | Set of all automorphism of a group $G$ |
| $Hol(G)$ | The holomorph of $G$ |
| $pK$ | Public key |
| $sK$ | Secret key |
| $\lambda(G)$ | The left regular representation of $G$ |

# Introduction

The creation of public key cryptography by Diffie and Hellman in 1976 and the subsequent invention of the RSA public key cryptosystem by Rivest, Shamir and Adleman in 1978 are watershed events in the long history of secret communications. Public key cryptography draws on many areas of mathematics, including number theory, abstract algebra, and information theory.

A number of public-key cryptosystems based on combinatorial group theory have been proposed since the early 1980s. The first proposal to use non-abelian groups in public key cryptography is due to Wagner and Magyarik in 1985. The cryptosystem is based on the hardness of the word problem for finitely presented monoids. The importance of Wagner and Magyarik's scheme lies in its novelty, which commenced an interplay between cryptography and combinatorial group theory.

A secure public key cryptosystem requires a mathematical operation which is easy to compute (encryption) but computationally difficult to reverse (decreption) in a realistic time without knowing a special secret information, called the trapdoor, which is the private key.

This thesis is organized as follows. In chapter 1, we begin with some elementary material concerning of group and semidirect product of groups. In chapte 2, we show that $(Aut(G), \circ) \cong ((G)^*, \triangle)$ . In chapter 3, we begin with some elementary material concerning of public key cryptography and The Diffie-Hellman key exchange (DHKE) and we present some notes on the holomorph of the group.

# Chapter 1

# Preliminaries

In this chapter we recall some basic information and concepts used in the following chapter.

# 1.1 Groups

## 1.1.1 Group

**Definition 1.1.1** *A group is an ordered pair $(G, .)$ consisting of a non-empty set $G$ together with a binary operation "." defined on $G$ such that :*

1. *for all $x, y \in G, xy \in G$ (closure).*
2. *If $x$,$y$ and $z$ in $G$, then $(xy)\, z = x\,(yz)$ (associativity).*
3. *There exists an element $1_G$ in $G$ such that, for all $x \in G, 1_G x = x 1_G = x$ (identity).*
4. *For eath $x$ in $G$, there exists $x^{-1}$ in $G$ such that $x^{-1}x = xx^{-1} = 1_G$ (inverse).*

A group $G$ is called **abelian** if the binary operation is commutative, i.e, $xy = yx$ for all $x, y \in G$.

The number of elements of a group (finite or infinite) is called its order. We will use $|G|$ to denote the order of $G$.

**Example 1.1.1** *$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ are abelian groups.*

**Example 1.1.2** *The set $\mathbb{R}^n = \{(a_1, a_2, ..., a_n), a_1, a_2, ..., a_n \in \mathbb{R}\}$ is a group under comoponentwise addition [i.e.; $(a_1, a_2, ..., a_n) + (b_1, b_2, ..., b_n) = (a_1 + b_1, a_2 + b_2, ..., a_n + b_n)$].*

**Example 1.1.3** *Let $n$ be a natural number. The set of integers $\bmod n$ form a group under addition modulo $n$, that is $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$.*

## 1.1.2 Subgroup

**Definition 1.1.2** *If $(G, .)$ is a group and $H$ is subset of $G$, then $(H, .)$ is called a **subgroup** of $(G, .)$ if the following condition hold:*

1. *$H \neq \phi$.*
2. *$x.y \in H$ for all $x, y \in H$ (closure).*

*3.* $x^{-1} \in H$ *for all* $x \in H$ *(inverse).*

*The subgroup* $H$ *of a group* $G$ *is denoted by* $H \leq G$ *.*

**Example 1.1.4** *- The set of even integers is a subgroup of the set of integers under addition.*
*-* $(\mathbb{Z}, +)$ *is a subgroup of* $(\mathbb{Q}, +)$*.*

- Given two subgroups $H$ and $F$ of a group $G$, $HF = \{hf, h \in H \text{ and } f \in F\}$ may not be a subgroup of $G$. Hence $HF$ is a subgroup of $G$ if and only if, $HF = FH$.

**Definition 1.1.3** *Tow subgroups* $H$*,* $F \leq G$ *are called complementary (to each other ) if* $H \cap F = \{1_G\}$ *and* $HF = G$*. we also note that if* $H$*,* $F \leq G$ *are complementary then each element* $g$ *of* $G$ *can be written uniquely in the form* $g = hf$ *where* $h \in H$*,* $f \in F$*.*

**Definition 1.1.4 (Centre of a group)** *The centre* $Z(G)$ *of a group* $G$ *is the subset of element in* $G$ *that commute with every element of* $G$*. In symbols,*

$$Z(G) = \{a \in G, ax = xa \text{ for all } x \text{ in } G\} .$$

**Definition 1.1.5** *Let* $G$ *be a group. The* ***centraliser*** *of* $g \in G$ *is defined to be:*

$$C_g = \{h \in G, hg = gh\}$$

*Then* $C_g$ *is a subgroup of* $G$*.*

**Proof.** Suppose that $h$ and $k$ are two elements of $C_g$. We show that the product $hk$ is an element of $C_g$. We have to prove that $(hk)\, g = g\, (hk)$.

$$\begin{aligned}
(hk)\, g &= h(kg) && \text{by associativity} \\
&= h\, (gk) && \text{as } k \in C_g \\
&= (hg)\, k && \text{by associativity} \\
&= (gh)\, k && \text{as } h \in C_g \\
&= g\, (hk) && \text{by associativity.}
\end{aligned}$$

Thus $hk \in C_g$.

Now suppose that $h \in C_g$. We show that the inverse of $h$ is in $C_g$. We have to show that $h^{-1}g = gh^{-1}$.

Suppose we start with the equality $hg = gh$.

Multiply both sides by $h^{-1}$ on the left. We get $h^{-1}(hg) = h^{-1}(gh)$, So that simplifying we get $g = (h^{-1}g)\,h$.

Now multiply both sides of this equality by $h^{-1}$ on the right. We get $gh^{-1} = (h^{-1}g)(hh^{-1})$. Simplifying we get $gh^{-1} = h^{-1}g$.

Which is what we want.

Thus $h^{-1} \in C_g$.

Thus $C_g$ is a subgroup of $G$. ■

**Subgroup generated by subset**

**Definition 1.1.6** *Let $A$ be a subset of a group $G$. Then the subgroup of $G$ generated by $A$ denoted by $\langle A \rangle$, is defined to be the intersection*

$$\langle A \rangle = \bigcap_{\substack{A \subset B \\ B \leq G}} B$$

Then $\langle A \rangle$ is the smallest subgroup of $G$ containing $A$.

### 1.1.3 Cosets

**Definition 1.1.7 (Equivalence relation)** *Let $X$ be a set. An equivalence relation $\Re$ is a relation on $X$ wich is:*

1. *Reflexive: $x\Re x$ for every $x \in X$.*
2. *Symmetric: $x\Re y$ implies $y\Re x$ for every $x$, $y \in X$.*
3. *Transitive: $x\Re y$ and $y\Re z$ implies $x\Re z$ for every $x, y, z \in X$.*

***Example 1.1.5*** *Let $X$ be any set and consider the relation*

$$a\Re b \text{ if and only if } a = b$$

*A moments thought convince the reader this is an equivalence relation.*

***Lemma 1.1.1*** *Let $G$ be a group and let $H$ be a subgroup. Let $\Re$ be the relation on $G$ defined by the rule*

$$a\Re b \Leftrightarrow b^{-1}a \in H$$

*Then $\Re$ is an equivalence relation.*

**Proof.** There are three things to check.

First we check reflexivity: Suppose that $a \in G$, then $a^{-1}a = 1_G \in H$ since is a subgroup. But then $a\Re a$ by definition of $\Re$ and $\Re$ is reflexive.

Now we check symmetry: Suppose that $a$ and $b$ are elements of $G$ and that $a\Re b$. Then $b^{-1}a \in H$. As $H$ is closed under taking inverses $(b^{-1}a)^{-1} \in H$ . But

$$\begin{aligned} \left(b^{-1}a\right)^{-1} &= a^{-1}\left(b^{-1}\right)^{-1} \\ &= a^{-1}b \end{aligned}$$

Thus $a^{-1}b \in H$. But then by definition $b\Re a$. Thus $\Re$ is symmetric.

Finally we check transitivity. Suppose that $a\Re b$ and $b\Re c$.

Then $b^{-1}a \in H$ and $c^{-1}b \in H$. As $H$ is closed under multiplication $\left(c^{-1}b\right)\left(b^{-1}a\right) \in H$. On the other hand

$$\begin{aligned} \left(c^{-1}b\right)\left(b^{-1}a\right) &= c^{-1}\left(bb^{-1}\right)a \\ &= c^{-1}\left(1_G a\right) = c^{-1}a. \end{aligned}$$

Thus $C^{-1}a \in H$. But then $a\Re b$ and $\Re$ is transitive.

As $\Re$ is reflexive, symmetric and transitive, it is an equivalence relation. ■

**Definition 1.1.8 (Equivalence class)** *Let $\Re$ be a equivalence on a set $X$.*

*Let $a \in X$ be an element of $X$. The **equivalence class** of $a$ is*

$$[a] = \{b \in X, b\Re a\}$$

*- The set of all equivalence classes is called the **quotient set** of $X$ by $\Re$, and is denoted $A/\Re$. Hence*

$$A/\Re = \{[a], a \in X\}.$$

**Definition 1.1.9** *Let $H \leq G$ and $g \in G$. The set $[g] = gH = \{gh, h \in H\}$ is called a **left coset** of $H$ in $G$, and The set $[g] = Hg = \{hg, h \in H\}$ is called a **right coset** of $H$ in $G$.*

The set of all left cosets of $H$ in $G$ is denoted by $G/H$ and the set of all right cosets of $H$ in $G$ is denoted by $H/G$.

**Example 1.1.6** *Let $H = \{0, 3\}$ be a subgroup of $\mathbb{Z}_6$. The left cosets of $H$ in $\mathbb{Z}_6$ are*

$$0 + H = H$$

$$1 + H = \{1, 4\}$$

$$2 + H = \{2, 5\}$$

$$3 + H = \{0, 3\}$$

$$4 + H = \{1, 4\}$$

$$5 + H = \{2, 5\}$$

**Definition 1.1.10 (Index of a subgroup)** *Let $G$ be a group and let $H$ be a subgroup.*

*The index of $H$ in $G$, denoted $[G : H]$ is aqual to the number of left cosets of $H$ in $G$.*

**Example 1.1.7** *Let $G = \mathbb{Z}_6$ and $H = \{0, 3\}$. Then $[G : H] = 3$.*

**Theorem 1.1.1 (Lagrange's Theorem)** *The order of any subgroup of a finite group divides the order of the group.*

### 1.1.4 Normal subgroup

**Definition 1.1.11** *Let $(H, .)$ be a subgroup of a group $(G, .)$. $(H, .)$ is called normal of $(G, .)$ if*

$$g^{-1}hg \in H \text{ for all } g \in G \text{ and } h \in H$$

*or*

$$Hg = gH \text{ for all } g \in G.$$

*- The normal subgroup of a group $G$ is denoted by $H \lhd G$.*

**Example 1.1.8** - $H = \{1_G\} \lhd G$.

- $G \lhd G$.

### 1.1.5 Cyclic group

**Definition 1.1.12** *Let $G$ be a group. We say that $G$ is **cyclic,** if it is generated by one element $g$ in $G$.*

*Let $G = \langle g \rangle$ be a cyclic group, then*

$$G = \left\{ g^i, i \in \mathbb{Z} \right\}$$

***Example 1.1.9*** *- $(\mathbb{Z}, +)$ is a cyclic group, both $1$ and $-1$ are generators.*

*- $(\mathbb{Z}_n, +)$ is a cyclic group.*

**Lemma 1.1.2** *Let $G$ be a finite group and let $g \in G$. Then the order of $g$ divides the order of $G$.*

**Lemma 1.1.3** *Let $G$ be a finite group of order $n$ and let $g$ be an element of $G$. Then $g^n = 1_G$.*

**Proof.** We know that $g^k = 1_G$ where $k$ is the order of $g$. But $k$ divides $n$. So $n = km$. But then

$$g^n = g^{km} = \left(g^k\right)^m = 1_G^m = 1_G.$$

■

### 1.1.6 Group of units

**Definition 1.1.13** *Let $n$ be a positive integres.*

The group of units $(\mathbb{Z}_n)^*$ for the *integers modulo* $n$ is the subset of $\mathbb{Z}_n$ of integers coprime to $n$ under multiplication.

**Definition 1.1.14** *Let $n$ be a positive integre, The **Euler's function** $\varphi(n)$ of $n$ is the number of positive integers not greater than and relatively prime to $n$:*

$$\varphi(n) = \left| \{ k \in \mathbb{N}, k \leq n \text{ and } \gcd(k, n) = 1 \} \right|.$$

**Example 1.1.10** *Let $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. $\mathbb{Z}_5^* = \{k \in \mathbb{Z}_5, \ \gcd(k, 5) = 1\} = \{1, 2, 3, 4\}$ and $\varphi(5) = 4$.*

**Lemma 1.1.4** *Let $a$ be any integer, which is coprime to the positive integer $n$. Then*

$$a^{\varphi(n)} = 1 \bmod n.$$

### 1.1.7 Permutation groups

**Definition 1.1.15 (Permutation)** *Let $E$ be a set. A permutation of $E$ is simply a bijection $f : E \to E$.*

**Lemma 1.1.5** *Let $E$ be a set.*

1. Let $\sigma_1$ and $\sigma_2$ be two permutation of $E$. Then the composition of $\sigma_1$ and $\sigma_2$ is a permutation of $E$.

2. Let $\sigma$ be a permutation of $E$. Then the inverse of $\sigma$ is a permutation of $E$.

**Lemma 1.1.6** *Let $E$ be a set. The set of all permutations under the composition of permutation, forms a group $S(E)$.*

*- if $E$ is a finite set with $n$ elements. Then $S(E)$ has $n!$ elements.*

**Symmetric group** $S_n$

**Definition 1.1.16** *The group $(S_n, \circ)$ is the set of permutation of the first $n$ natural numbers.*

- Elements of the $S_n$ have the form :

$$\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix}$$

**Example 1.1.11** *Let $E = \{1, 2, 3\}$, $S_n = \{\Pi : \{1, 2, 3\} \to \{1, 2, 3\}, \Pi$ is a bijection$\}$*

$\Pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\Pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\Pi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $\Pi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\Pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $\Pi_6 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$.

**Proposition 1.1.1** *For every natural number $n$, the symmetric group $S_n$ has $n!$ elements.*

**Proof.** The order of $S_n$ is the number of bijections from the set $\{1, 2, ..., n\}$ to itself. There are $n$ possible choices for the image of 1 under a bijection. once the image of 1 has been chosen, there are $n-1$ choises for the image of 2. Then there are $n-2$ choises for the image of 3. Continuing in this way, we see that

$$|S_n| = n \cdot (n-1) \cdot (n-2) \cdot ... \cdot 2 \cdot 1 = n!.$$

■

# 1.2 Morphism

## 1.2.1 Group morphism

**Definition 1.2.1** *Let $(G,.)$ and $(H,.)$ two groups. A function $f : G \to H$ is called* ***homomorphism,*** *if*

$$f(xy) = f(x)f(y) \text{ for all } x, y \in G.$$

A homomorphism of $G$ into itself is an **endomorphism**. the set of all endomorphism of a group $G$ is denoted by $End(G)$.

- The kernel of the homomorphism $f$ is the set

$$\ker f = \{x \in G, f(x) = 1_H\}.$$

- The image of the homomorphism $f$ is the set

$$\operatorname{Im} f = \{f(x),\ x \in G\}.$$

**Proposition 1.2.1** *Let $f : G_1 \to G_2$ be a morphism of the group. The following assertions are valide*

1. $f(1_{G_1}) = 1_{G_2}$.
2. $f(g^{-1}) = f(g)^{-1}$ for $g \in G_1$.
3. $f$ is one-to-one if and only if, $\ker f = \{1_{G_1}\}$.
4. $f$ is onto if only if, $\operatorname{Im} f = G_2$.

**Lemma 1.2.1** *Let $f : G \to H$ be a homomorphism. Then the kernel of $f$ is a normal subgroup of $G$.*

**Proof.** We have already seen that the kernel is a subgroup. suppose that $g \in G$. We want to prove that $g \ker f g^{-1} \subset \ker f$. Suppose that $h \in \ker f$.
We need to prove that $ghg^{-1} \in \ker f$. Now

$$f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)1_H f(g)^{-1} = f(g)f(g)^{-1} = 1_H.$$

Thus $ghg^{-1} \in \ker f$. ■

## 1.3 Isomorphism

### 1.3.1 Group isomorphism

**Definition 1.3.1** *We say that $G$ and $H$ are **isomorphic** if there is a bijection map $f : G \to H$, which respects the group structure. That is to say, for every $g_1$ and $g_2$ in $G$*

$$f(g_1 g_2) = f(g_1) f(g_2).$$

the map $f$ is called an isomorphism.

- An isomorphism of $G$ into itself is an **automorphism**. The set of all automorphism of $G$ is denoted by $Aut(G)$.

**Example 1.3.1** *Let $G = (\mathbb{R}, +)$ and $H = (\mathbb{R}^+, \times)$. The map $f : G \longrightarrow H$ defined by $f(n) = 2^n$ is a isomorphism.*

**Theorem 1.3.1 (Cayley Theorem)** *Every group is isomorphic to a group of permutations.*

**Lemma 1.3.1** *Let $G$ and $H$ be two cyclic groups of the same order. Then $G$ and $H$ are isomorphic.*

**Corollary 1.3.1** *If $G$ is a finite group of order $n$, then $G$ is isomorphic to a subgroup of $S_n$.*

## 1.4 Product of groups

### 1.4.1 Direct product

**Proposition 1.4.1** *If $(G, \circ)$ and $(H, *)$ are two groups, then $(G \times H, \cdot)$ is a group under the binary operation. defined by*

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2) \text{ where } g_1, g_2 \in G, h_1, h_2 \in H$$

*The group $(G \times H, \cdot)$ is called the direct product of the group $(G, \circ)$ and $(H, *)$.*

**Proof.** We will prove that $(G \times H, \cdot)$ is a group

1. For the fact that $(G, \circ)$ and $(H, *)$ are associative we have

$$\begin{aligned}((g_1, h_1) \cdot (g_2, h_2)) \cdot (g_3, h_3) &= (g_1 \circ g_2, h_1 * h_2) \cdot (g_3, h_3) \\ &= ((g_1 \circ g_2) \circ g_3, (h_1 * h_2) * h_3) \\ &= (g_1 \circ (g_2 \circ g_3), h_1 * (h_2 * h_3)) \\ &= (g_1, h_1) \cdot (g_2 \circ g_3, h_2 * h_3) \\ &= (g_1, h_1) \cdot ((g_2, h_2) \cdot (g_3, h_3))\end{aligned}$$

   Where $g_1, g_2, g_3 \in G$ and $h_1, h_2, h_3 \in H$.

   Then the operation "$\cdot$" is associative on $G \times H$.

2. The identity element of $G \times H$ is $(1_G, 1_H)$, where $1_G$ is the identity element of $G$ and $1_H$ is the identity element of $H$.

3. The inverse of $(g, h)$ is $(g^{-1}, h^{-1})$, where $(g, h) \in G \times H$.

   Hence $(G \times H, \cdot)$ is a group.

■

### 1.4.2 Semidirect product

**Proposition 1.4.2** *Given any groups $G$ and $H$ and a morphism $\theta : G \to Aut(H)$, denote the automorphism $\theta(g)$ by $\theta_g$, then $G \times H$ is a group with the multiplication*

$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 \theta_{g_1}(h_2))$ *where* $g_1, g_2 \in G$; $h_1, h_2 \in H$; $\theta_{g_1} \in Aut(H)$ *and* $\theta_{g_1}(h_2) \in H$.

*The group $(G \times H, \cdot)$ is called the semidirect product of $G$ and $H$ with respect $\theta$ to and it is denoted by $G \ltimes_\theta H$.*

***Proof.*** *-we will prove that the operation "$\cdot$" is associative on $G \times H$. Let $g_1, g_2, g_3 \in G$; $h_1, h_2, h_3 \in H$*

$$\begin{aligned}
((g_1,h_1)(g_2,h_2)) \cdot (g_3,h_3) &= (g_1g_2, h_1\theta_{g_1}(h_2)) \cdot (g_3,h_3) \\
&= (g_1g_2g_3, h_1\theta_{g_1}(h_2)\theta_{g_1g_2}(h_3)) \\
&= (g_1g_2g_3, h_1\theta_{g_1}(h_2)\theta_{g_1}(\theta_{g_2}(h_3)))\text{ , as } \theta \text{ is a group morphism} \\
&= (g_1g_2g_3, h_1\theta_{g_1}(h_2\theta_{g_2}(h_3)))\text{ , as } \theta_{g_1} \in Aut(H) \\
&= (g_1g_2g_3, h_1\theta_{g_1}(h_2\theta_{g_2}(h_3)))\text{ , as } G \text{ is a group} \\
&= (g_1,h_1)(g_2g_3, h_2\theta_{g_2}(h_3)) \\
&= (g_1,h_1) \cdot ((g_2,h_2) \cdot (g_3,h_3)).
\end{aligned}$$

*Then "$\cdot$" is associative on $G \times H$.*

*-The identity element of $G \times H$ is $(1_G, 1_H)$*

$$\begin{aligned}
(g,h)(1_G,1_H) &= (g1_G, h\theta_g(1_H)) \\
&= (g, h1_H)\text{ , as } \theta_g \in Aut(H) \\
&= (g,h).
\end{aligned}$$

*and*

$$\begin{aligned}
(1_G,1_H) \cdot (g,h) &= (1_Gg, 1_H\theta_{1_G}(h)) \\
&= (g, 1_H id(h))\text{ , as } \theta \text{ is a morphism} \\
&= (g,h).
\end{aligned}$$

*-The inverse of $(g,h)$ is $(g^{-1}, \theta_{g^{-1}}(h^{-1}))$ where $(g,h) \in G \times H$*

*Its easy to find this inverse so*

*First because of the bijectivity of $\theta_g$, there exist an element $h' \in H$ such that $\theta_g(h') = h^{-1}$, then*

$$\begin{aligned}
(g,h) \cdot \left(g^{-1}, h'\right) &= \left(gg^{-1}, h\theta_g(h')\right) \\
&= \left(gg^{-1}, hh^{-1}\right) \\
&= (1_G, 1_H).
\end{aligned}$$

*Second we know that* $\theta_{g^{-1}} = (\theta_g)^{-1}$ *,as* $\theta$ *is a morphism,then*

$$\begin{aligned} \theta_{g^{-1}}(h^{-1}) &= \theta_{g^{-1}}(\theta_g(h')) \\ &= (\theta_g)^{-1}(\theta_g(h')) \\ &= h'. \end{aligned}$$

*And this give us*

$$\begin{aligned} \theta_{g^{-1}}(h) &= \theta_{g^{-1}}((h^{-1})^{-1}) \\ &= \left(\theta_{g^{-1}}(h^{-1})^{-1}\right) \\ &= h'^{-1} \end{aligned}$$

*Then*

$$\begin{aligned} \left(g^{-1}, h'\right) \cdot (g, h) &= \left(g^{-1}g, h'\theta_{g^{-1}}(h)\right) \\ &= \left(g^{-1}g, h'h'^{-1}\right) \\ &= (1_G, 1_H). \end{aligned}$$

*Then the inverse element of* $(g, h)$ *is* $(g^{-1}, \theta_{g^{-1}}(h^{-1}))$*.Hence* $(G \times H, \cdot)$ *is a group.* ■

# Chapter 2

# On the automorphism of a cyclic group

In this chapter, we show that $(Aut(G), \circ) \cong ((G)^*, \triangle)$ with $G^\star = \{g^s : \gcd(s, n) = 1\}$ epuipped with the operation $\triangle$ defined by: $\forall g^s, g^t \in G^\star : g^s \triangle g^t = g^{st}$. We give many examples to illustrate the above result.

## 2.1 Automorphism group of $\mathbb{Z}_n$

**Proposition 2.1.1** *Let $n \in \mathbb{N} - \{0\}$,*

1. *For all $\overline{m} \in (\mathbb{Z}_n)^*$ the mapping $f_{\overline{m}} : \mathbb{Z}_n \to \mathbb{Z}_n$, defined by $\overline{x} \longmapsto \overline{mx}$ is a automorphism of $(\mathbb{Z}_n, \oplus)$.*

2. *The mapping $\Psi : Aut(\mathbb{Z}_n) \to (\mathbb{Z}_n)^*$ defined by $f \mapsto f(\overline{1})$ is an isomorphism of groups.*

**Proof.**

1. The mapping $f_{\overline{m}}$ is morphism because for all $\overline{x}, \overline{y} \in \mathbb{Z}_n$, we have

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

   Now we show that $f_{\overline{m}}$ is onto: Let $\overline{y} \in \mathbb{Z}_n$, since $\overline{m} \in (\mathbb{Z}_n)^*$, there exists $(\overline{m})^{-1} \in (\mathbb{Z}_n)^*$ such that $\overline{m} \cdot (\overline{m})^{-1} = (\overline{m})^{-1} \cdot \overline{m} = \overline{1}$, then we have $\overline{y} = f_{\overline{m}}(\overline{x}) = \overline{mx}$ implies $\overline{x} = (\overline{m})^{-1} \cdot \overline{y}$.

   Since $f_{\overline{m}}$ is onto and $\mathbb{Z}_n$ is finite, then $f_{\overline{m}}$ is one-to-one. Finally $f_{\overline{m}} \in Aut(\mathbb{Z}_n)$.

2. It is clear that if $f \in Aut(\mathbb{Z}_n)$, then $f\left(\overline{1}\right)$ is a generator of $\mathbb{Z}_n$, because $f$ is onto and $\mathbb{Z}_n = \left\langle \overline{1} \right\rangle$, then $f\left(\overline{1}\right) \in (\mathbb{Z}_n)^*$. The mapping $\Psi : Aut(\mathbb{Z}_n) \to (\mathbb{Z}_n)^*$ is morphism because for all $(f, h) \in Aut(\mathbb{Z}_n)$, We have $\Psi(f \circ h) = (f \circ h)\left(\overline{1}\right) = f\left(h\left(\overline{1}\right)\right)$, since $h\left(\overline{1}\right) \in (\mathbb{Z}_n)^*$, then there exists $1 \leq k \leq n-1$ with $\gcd(k, n) = 1$ such that $h\left(\overline{1}\right) = \overline{k}$, then $f\left(h(\overline{1})\right) = f\left(\overline{k}\right) = kf\left(\overline{1}\right) = f\left(\overline{1}\right) \cdot h\left(\overline{1}\right) = \Psi(f) \cdot \Psi(h)$.

   Now we show that $\ker \Psi = \{id_{\mathbb{Z}_n}\}$, we have $\ker \Psi = \left\{f \in Aut(\mathbb{Z}_n) : f\left(\overline{1}\right) = \overline{1}\right\}$

   Since $f \in Aut(\mathbb{Z}_n)$ and $f\left(\overline{1}\right) = \overline{1}$, then for all $\overline{t} \in \mathbb{Z}_n : f\left(\overline{t}\right) = \overline{t}$.
   Finally $\ker \Psi = \{id_{\mathbb{Z}_n}\}$.

   The mapping $\Psi$ is onto because for all $\overline{m} \in (\mathbb{Z}_n)^*$, there exists $f_{\overline{m}} \in Aut(\mathbb{Z}_n)$ such that $\Psi(f_{\overline{m}}) = \overline{m}$.

■

**Example 2.1.1** *Let $n = 6$, we have $(\mathbb{Z}_6)^* = \{\overline{1}, \overline{5}\}$, the Cayley table of $((\mathbb{Z}_6)^*, \times)$ is defined as follows (see Tabel 1):*

| $\times$ | $\overline{1}$ | $\overline{5}$ |
|---|---|---|
| $\overline{1}$ | $\overline{1}$ | $\overline{5}$ |
| $\overline{5}$ | $\overline{5}$ | $\overline{1}$ |

(Table 1)

*In this example $Aut(\mathbb{Z}_6) = \{f_{\overline{1}}, f_{\overline{5}}\}$, with $f_{\overline{1}} = id_{\mathbb{Z}_6} = \begin{pmatrix} \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} \\ \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} \end{pmatrix}$, $f_{\overline{5}} = \begin{pmatrix} \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} \\ \overline{0} & \overline{5} & \overline{4} & \overline{3} & \overline{2} & \overline{1} \end{pmatrix}$.*
*The Cayley table of $(Aut(\mathbb{Z}_6), \circ)$ is defined as follows (see Table 2):*

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

(Table 2)

*Finally we have $(Aut(\mathbb{Z}_6), \circ) \cong ((\mathbb{Z}_6)^*, \times)$.*

In following proposition, we show that any cyclic group $G = \langle g \rangle$ of order $n$, $(G^*, \triangle)$ is an abelian group.

**Proposition 2.1.2** *Let $G = \langle g \rangle$ be a cyclic group of order $n$. $G^* = \{g^s : \gcd(s, n) = 1\}$ equipped with the operation $\triangle$ defined by:*

$$\forall g^s, g^t \in G^* : g^s \triangle g^t = g^{st}.$$

*is an commutative group.*

**Proof. closure:** for all $g^s, g^t \in G^*$, we have $g^s \triangle g^t = g^{st}$, since $s, t \in \{1, ..., n-1\}$ with $\gcd(s, n) = 1$ and $\gcd(t, n) = 1$, then $\gcd(st, n) = 1$, consequently $g^{st} \in G^*$.

**commutative:** for all $g^s, g^t \in G^*$, We have $g^s \triangle g^t = g^{st} = g^t \triangle g^s$.

**Associativity:** for all $g^s, g^t, g^r \in G^*$, We have $\left(g^S \triangle g^t\right) \triangle g^r = g^{st} \triangle g^r = g^{(st)r} = g^{s(tr)} = g^s \triangle (g^t \triangle g^r)$.

**Identity:** we show that $g$ is the identity, we have for all $g^s \in G^* : g^s \triangle g = g \triangle g^s = g^s$.

**Inverse:** let $g^s \in G^*$, since $\gcd(s, n) = 1$, there exists $(u, v) \in \mathbb{Z}^2$ such that $us + vn = 1$, $g^u$ is the inverse of $g^s$. ■

**Example 2.1.2** *Let $G = \langle g \rangle$ be a cyclic group of order 6, then $G = \{1, g, g^2, g^3, g^4, g^5\}$ and $(G)^* = \{g, g^5\}$.*

*The Cayley table of $(G^*, \triangle)$ is defined as follows (see Table 3):*

| $\triangle$ | $g$ | $g^5$ |
|---|---|---|
| $g$ | $g$ | $g^5$ |
| $g^5$ | $g^5$ | $g$ |

(Table 3)

## 2.2 Automorphism group of a cyclic group

In following proposition, we show that any cyclic group $G = \langle g \rangle$ of order $n$, the groups $(Aut(G), \circ)$ and $(G^*, \triangle)$ are isomorphic.

**Proposition 2.2.1** *Let $G = \langle g \rangle$ be a cyclic group of order $n$, we have*

1. *For all $g^s \in G^*$ the mapping $f_{g^s} : G \to G$, defined by $g^k \mapsto g^{ks}$ is a automorphism of $(G, \cdot)$.*
2. *The mapping $\theta : Aut(G) \to (G)^*$ defined by $f \mapsto f(g)$ is an isomorphism of groups.*

**Proof.**

1. The mapping $f_{g^s}$ is morphism because for all $g^k, g^l \in G$, we have

$$f_{g^s}(g^k \cdot g^l) = f_{g^s}(g^{k+l}) = g^{s(k+l)} = g^{ks} \cdot g^{ls} = f_{g^s}(g^k) \cdot f_{g^s}(g^l).$$

   Now we show that $f_{g^s}$ is one -to-one: let $g^k, g^l \in G$, we have $f_{g^s}(g^k) = f_{g^s}(g^l) \iff g^{ks} = g^{ls} \Leftrightarrow g^{s(k-l)} = 1 \Leftrightarrow n$ divides $s(k-l)$, we have: $n$ divides $s(k-l)$ and $\gcd(s, n) = 1$, since the lemma of Gausse, then $n$ divides $(k-l)$, i.e.; there exists $\alpha \in \mathbb{Z}$ such that $k - l = \alpha$, and since $k, l \in \{1, 2, ..., n-1\}$, we have $\alpha = 0$ and $k = l$.

   Since $f_{g^s}$ is one-to-one and $G$ is finite, then $f_{g^s}$ is onto.

   Finally $f_{g^s} \in Aut(G)$.

2. The mapping $\theta : Aut(G) \to (G)^*$ is morphism because for all $(f, h) \in Aut(G)$, we have $\theta(f \circ h) = (f \circ h)(g) = f(h(\overline{1}))$, since $h(g) \in (G)^*$, then there exists $1 \leq k \leq n-1$

with $\gcd(k,n)=1$, such that $h(g)=g^k$, then $f(h(g))=f(g^k)=k(f(g))^k=g^{k+l}=\theta(f)\triangle\theta(h)$.

Now we show that $\ker\theta=\{id_{\mathbb{Z}_n}\}$, we have $\ker\theta=\{f\in Aut(G):f(g)=g\}$.

Since $f\in Aut(\mathbb{Z}_n)$ and $f(g)=g$, then for all $g^k\in G: f(g^k)=g^k$.

Finally $\ker\theta=\{id_G\}$.

The mapping $\Psi$ is onto because for all $g^s\in(G)^*$, there exists $f_{g^s}\in Aut(G)$ such that $\theta(f_{g^s})=g^s$.

■

**Example 2.2.1** *Let $G=\langle g\rangle$ be a cyclic group of order 5, then $G=\{1,g,g^2,g^3,g^4\}$ and $(G)^*=\{g,g^2,g^3,g^4\}$. The cayley table of $(G^*,\triangle)$ is defined as follows (see Table 4):*

| $\triangle$ | $g$ | $g^2$ | $g^3$ | $g^4$ |
|---|---|---|---|---|
| $g$ | $g$ | $g^2$ | $g^3$ | $g^4$ |
| $g^2$ | $g^2$ | $g^4$ | $g$ | $g^3$ |
| $g^3$ | $g^3$ | $g$ | $g^4$ | $g^2$ |
| $g^4$ | $g^4$ | $g^3$ | $g^2$ | $g$ |

(Table 4)

*In this example $Aut(G)=\{f_g,f_{g^2},f_{g^3},f_{g^4}\}$, with*

$$f_g=id_G=\begin{pmatrix}1 & g & g^2 & g^3 & g^4\\ 1 & g & g^2 & g^3 & g^4\end{pmatrix},\ f_{g^2}=\begin{pmatrix}1 & g & g^2 & g^3 & g^4\\ 1 & g^2 & g^4 & g & g^3\end{pmatrix},\ f_{g^3}=\begin{pmatrix}1 & g & g^2 & g^3 & g^4\\ 1 & g^3 & g & g^4 & g^2\end{pmatrix},\ f_{g^4}=\begin{pmatrix}1 & g & g^2 & g^3 & g^4\\ 1 & g^4 & g^3 & g^2 & g\end{pmatrix}.$$

*The cayley table of $(Aut(G),\circ)$ is defined as follows (see Table 5):*

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

(Table 5)

*Finally we have $(Aut(G),\circ)\cong((G)^*,\times)$.*

### 2.2.1 Order of Automorphism Group of cyclic Group

**Theorem 2.2.1** *Let $G$ a group cyclic of order $n$.*

*Let $Aut(G)$ denote the automorphism group of $G$. Then:*

$$|Aut(G)| = \varphi(n).$$

**Proof.** Let $g$ be a generator of $G$.

Let $f$ be an automorphism on $G$.

By homomorphic image of cyclic group is cyclic group, $f(g)$ is a generator of $G$.

By homomorphic of generated group, $f$ is uniquely determined by $f(g)$.

By finite cyclic group has Euler phi generators, there $\varphi(n)$ possible values for $f(g)$.

Therefor there are $\varphi(n)$ automorphism on $G$ :

$$|Aut(G)| = \varphi(n).$$

■

# Chapter 3

# The public key exchange using the holomorph of the group

In this chaptre, we show that $(\lambda(G)Aut(G), \star) \cong (Hol(G), \cdot)$ and we present the public key exchange using the group $(\lambda(G)Aut(G), \star)$.

Public key cryptography (or asymmetric cryptography) has been the most significant and striking development in the history of cryptography. This revolutionary concept has been introduced in the famous paper "New Directions in Cryptography". Public Key cryptography, was invented by Diffie and Hellman more than forty years ago. In Public Key cryptography, a user $U$ has a pair of related keys $(pK, sK)$: the key $pK$ is public and should be available to everyone, while the key $sK$ must be kept secret by $U$. The fact that $sK$ is kept secret by a single entity creates an asymmetry, hence the name asymmetric cryptography.

A function $f$ is one-way if it is computationally easy to compute the function $f(x) = y$, but computationally infeasible to invert the function $f^{-1}(y) = x$.

The Diffie -Hellman key exchange (DHKE), proposed by Whitfield Diffie and Martin Hellman in 1976. The DHKE is a very impressive application of the discrete logarithm problem. A more general descriptions of the protocol uses an arbitrary finite cyclic group. We now recall this protocol as following:

1. Alice and Bob agree on a finite cyclic group $G$ and a generating element $g$ in $G$.
2. Alice picks a random natural number $a$ and sends $g^a$ to Bob.
3. Bob picks a random natural number $b$ and sends $g^b$ to Alice.
4. Alice computes $K_A = (g^b)^a = g^{ba}$.
5. Bob computes $K_B = (g^a)^b = g^{ab}$.

   Since $ab = ba$, both Alice and Bob are now in possession of the same group element $K = K_A = K_B$ which can serve as the shared secret key.

**Definition 3.0.1** *Let $S(G)$ be the group of permutations on the set $G$. Consider the right and the left regular representations of $G$:*

$$\begin{cases} \rho : G \to S(G) \\ g \mapsto (x \mapsto xg) \end{cases} \quad \begin{cases} \lambda : G \to S(G) \\ g \mapsto (x \mapsto gx) \end{cases}$$

**Definition 3.0.2** *Let $H$, $Q$ be two groups and let $\theta : H \to Aut(Q)$ be a homomorphism. Denote $\theta(h)$ by $\theta_h$. Then the semidirect product of $H$ and $Q$ is the set*

$\Gamma = H \rtimes_\theta Q = \{(h,q), h \in H, q \in Q\}$ *where the group operation is given by* $(h,q)\left(h^{'},q^{'}\right) = \left(hh^{'}, q\theta_h(q^{'})\right)$.

**Example 3.0.2**

1. *Let $H, Q$ two groups. if $\theta : H \to Aut(Q)$ is the trivial homomorphism, so $\theta_h = id_Q$ for all $h \in H$, then the group law on $H \rtimes_\theta Q$ is the direct product: $(h,q)(h',q') = (hh', q\theta_h(q')) = (hh', qq')$.*

2. *Let $H = \mathbb{R}$, $K = \mathbb{R}^\times$, and $\theta : \mathbb{R} \to Aut(\mathbb{R}^\times)$ where $\theta_h : \mathbb{R}^\times \to \mathbb{R}^\times$ by $\theta_h(q) = hq$ is homomorphism.*

   *The group $\mathbb{R} \rtimes_\theta \mathbb{R}^\times$ has the operation*

$$(h,q)(h',q') = (h+h', q\theta_h(q')) = (h+h', qhq').$$

**Definition 3.0.3** *The holomorph of $G$, usually denoted by $Hol(G)$, is the set of all pairs $(g,f)$, where $g \in G$, $f \in Aut(G)$, with the group operation given by:*

$$(g,f)\left(g^{'},f^{'}\right) = \left(f^{'}(g)g^{'}, ff^{'}\right).$$

**Example 3.0.3** *Let $G = \mathbb{Z}_6$ and $Aut(G) = \{f_{\overline{1}}, f_{\overline{5}}\}$. We have*

$$Hol(G) = \left\{\left(\overline{0}, f_1\right), \left(\overline{1}, f_1\right), \left(\overline{2}, f_1\right), \left(\overline{3}, f_1\right), \left(\overline{4}, f_1\right), \left(\overline{5}, f_1\right), \left(\overline{0}, f_{\overline{5}}\right), \left(\overline{1}, f_{\overline{5}}\right), \left(\overline{2}, f_{\overline{5}}\right), \left(\overline{3}, f_{\overline{5}}\right), \left(\overline{4}, f_{\overline{5}}\right), \left(\overline{5}, f_{\overline{5}}\right)\right\}$$

## 3.1 The holomorph of the group

In this section, we present some notes on the holomorph of the group.

**Proposition 3.1.1** *Let $G$ be a group and let* $\begin{cases} \lambda : G \longrightarrow S(G) \\ g \longmapsto f_g : (x \longmapsto gx). \end{cases}$ *the left regular representation of $G$. Consider the set*

$$\lambda(G) = \{f_g : g \in G\}.$$

*Then the following hold:*
*(i) for all $\psi \in Aut(G)$ and $f_g \in \lambda(G)$; $\psi f_g \psi^{-1} = f_{\psi(g)}$.*

*(ii)* $Aut(G) \cap \lambda(G) = \{id_G\}$.

*(iii) each element of* $\lambda(G)Aut(G)$ *can be written uniquely in the form* $f_g\psi$ *where* $f_g \in \lambda(G)$, $\psi \in Aut(G)$, *i.e., for all* $\psi, \varphi \in Aut(G)$ *and* $f_g, f_h \in \lambda(G)$; $f_g\psi = f_h\varphi \Longrightarrow f_g = f_h$ *and* $\psi = \varphi$.

**Proof.** Let $\psi \in Aut(G)$ and $f_g \in \lambda(G)$. For each $x \in G$

$$\psi f_g \psi^{-1}(x) = \psi f_g(\psi^{-1}(x)) = \psi(f_g(\psi^{-1}(x))) = \psi(g\psi^{-1}(x)) = \psi(g)\psi(\psi^{-1}(x)) = \psi(g)x = f_{\psi(g)}(x).$$

Then

$$\psi f_g \psi^{-1} = f_{\psi(g)}$$

Which completes the proof of (i). If $\varphi \in Aut(G) \cap \lambda(G)$, then there exists an element $g$ in $G$ such that $\varphi = f_g$. Since $f_g \in \lambda(G)$ then we have for all $x, x^{'} \in G$, $\varphi(xx^{'}) = gxx^{'}$. Also, since $\varphi \in Aut(G)$, then we have for all $x, x^{'} \in G$,$\varphi(xx^{'}) = \varphi(x)\varphi(x^{'}) = gxgx^{'}$. Therefore $gxx^{'} = gxgx^{'}$, implies $g = 1_G$ and $\varphi = f_g = id_G$. So the proof of (ii) is completed.

For (iii), we only need the uniqueness. But $f_g\psi = f_h\varphi$ implies $f_h^{-1}f_g = \varphi\psi^{-1}$.

This is in $Aut(G) \cap \lambda(G)$. Since $Aut(G) \cap \lambda(G) = \{id_G\}$, so $f_h^{-1}f_g = \varphi\psi^{-1} = id_G$. Then $\varphi = \psi$ and $f_h = f_g$. ■

**Proposition 3.1.2** *Let* $G$ *be a group. Consider the set*
$\lambda(G)Aut(G) = \{f_g\psi : f_g \in \lambda(G), \psi \in Aut(G)\}$.

*Define an operation "*$\star$*" on* $\lambda(G)Aut(G)$ *by* $f_g\psi \star f_h\varphi = f_{g\psi(h)}(\psi\varphi)$.
*Then the following hold:*

*(i)* $(\lambda(G)Aut(G), \star)$ *is a group.*

*(ii) the mapping* $\delta : (\lambda(G)Aut(G), \star) \to (Hol(G), \cdot)$, $f_g\psi \mapsto (g, \psi)$ *is an isomorphism of groups.*

***Proof.*** *Let* $f_g\psi, f_h\varphi \in \lambda(G)Aut(G)$, *since* $f_{g\psi(h)} \in \lambda(G)$ *and* $\psi\varphi \in Aut(G)$ *then* $f_{g\psi(h)}\psi\varphi \in \lambda(G)Aut(G)$. *Moreover the set* $\lambda(G)Aut(G)$ *is closed under operation "*$\star$*".*

*By considering elements* $f_g\psi, f_h\varphi$ *and* $f_k\zeta$ *of* $\lambda(G)Aut(G)$ *we have*

$$(f_g\psi \star f_h\varphi) \star f_k\zeta = f_{g\psi(h)}(\psi\varphi) \star f_k\zeta = f_{g\psi(h)(\psi\varphi)(k)}(\psi\varphi)\zeta.$$

*Also,we get*

$$f_g\psi \star (f_h\varphi \star f_k\zeta) = f_g\psi \star f_{h\varphi(k)}(\varphi\zeta) = f_{g\psi(h\varphi(k))}\psi(\varphi\zeta) = f_{g\psi(h)(\psi\varphi)(k)}(\psi\varphi)\zeta.$$

*This shows that the operation "$\star$" is associative. If $f_g\psi \in \lambda(G)Aut(G)$ then*

$$f_g\psi \star f_{1_G}id_G = f_g\psi \star id_Gid_G = id_Gid_G \star f_g\psi = f_g\psi$$

*So, the identity element for $(\lambda(G)Aut(G), \star)$ is $id_Gid_G$. For the elements $f_g\psi$ and $f_{\psi^{-1}(g^{-1})}\psi^{-1}$ of $\lambda(G)Aut(G)$ we have*

$$f_g\psi \star f_{\psi^{-1}(g^{-1})}\psi^{-1} = f_{\psi^{-1}(g^{-1})}\psi^{-1} \star f_g\psi = id_Gid_G.$$

*Which show that $f_{\psi^{-1}(g^{-1})}\psi^{-1}$ is an inverse of $f_g\psi$ in the group $(\lambda(G)Aut(G), \star)$. So the proof of (i) is completed.*

*For (ii), it is easy to see that the mapping $\delta$ is onto. Since each element of $\lambda(G)Aut(G)$ can be written uniquely in the form $f_g\psi$ where $f_g \in \lambda(G)$, $\psi \in Aut(G)$ (see proposition 3.1.1), then $\delta$ is one-to-one . Also for all $f_g\psi, f_h\varphi \in \lambda(G)Aut(G)$ :*

$$\begin{aligned}
\delta(f_g\psi \star f_h\varphi) &= \delta(f_{g\psi(h)}\psi\varphi) \\
&= (g\psi(h), \psi\varphi) \\
&= (g, \psi) \cdot (h, \varphi) \\
&= \delta(f_g\psi) \cdot \delta(f_h\varphi).
\end{aligned}$$

■

## 3.2 On public key exchange using the group $(\lambda(G)Aut(G), \star)$

In this section, we present the public key exchange using the group $(\lambda(G)Aut(G), \star)$.

Let G be a group, consider the group $(\lambda(G)Aut(G), \star)$. In our key exchange protocol, $G$,$Aut(G)$,$f_g\psi \in \lambda(G)Aut(G)$ are public information.

Bob chooses a private $n \in \mathbb{N}$, while Alice chooses a private $m \in \mathbb{N}$. Both Alice and Bob are going to work with elements of the form $f_g\psi^r$, where $f_g \in \lambda(G), \psi \in Aut(G), r \in \mathbb{N}$. Note that two elements of this form are multiplied as follows:

$$f_g\psi^r \star f_h\psi^s = f_{\psi^s(g)h}\psi^{r+s}.$$

**Proposition 3.2.1** *1.* ***Alice:*** *Alice computes $(f_g\psi)^m$, where $(f_g\psi)^0 = 1_{\lambda(G)Aut(G)}$, and for all $m \geq 0$,*

$$(f_g\psi)^{m+1} = f_g\psi \star (f_g\psi)^m.$$

*Then $(f_g\psi)^m = f_{\psi^{m-1}(g)\ldots\psi^2(g)\psi^1(g)g}\psi^m \in \lambda(G)Aut(G)$.*

*And sends to Bob the element $a = f_{\psi^{m-1}(g)\ldots\psi^2(g)\psi^1(g)g}$ of the group $\lambda(G)$.*

*2.* ***Bob:*** *Bob computes $(f_g\psi)^n$, where $(f_g\psi)^0 = 1_{\lambda(G)Aut(G)}$, and for all $n \geq 0$,*

$$(f_g\psi)^{n+1} = f_g\psi \star (f_g\psi)^n.$$

*Then $(f_g\psi)^n = f_{\psi^{n-1}(g)\ldots\psi^2(g)\psi^1(g)g}\psi^n \in \lambda(G)Aut(G)$. And sends to Alice the element $b = f_{\psi^{n-1}(g)\ldots\psi^2(g)\psi^1(g)g}$ of the group $\lambda(G)$.*

*3.* ***Alice:*** *let $x \in Aut(G)$. Alice computes*

$$\begin{aligned} bx \star a\psi^m &= f_{\psi^{n-1}(g)\ldots\psi^2(g)\psi^1(g)g}x \star f_{\psi^{m-1}(g)\ldots\psi^2(g)\psi^1(g)g}\psi^m \\ &= f_{\psi^m(\psi^{n-1}(g)\ldots\psi^2(g)\psi^1(g)g)\psi^{m-1}(g)\ldots\psi^2(g)\psi^1(g)g}x\psi^m. \end{aligned}$$

*His key is now $K_A = f_{\psi^m(\psi^{n-1}(g)\ldots\psi^2(g)\psi^1(g)g)\psi^{m-1}(g)\ldots\psi^2(g)\psi^1(g)g}$.*

*4.* ***Bob:*** *let $y \in Aut(G)$. Bob computes*

$$\begin{aligned} ay \star b\psi^n &= f_{\psi^{m-1}(g)\ldots\psi^2(g)\psi^1(g)g}y \star f_{\psi^{n-1}(g)\ldots\psi^2(g)\psi^1(g)g}\psi^n \\ &= f_{\psi^n(\psi^{m-1}(g)\ldots\psi^2(g)\psi^1(g)g)\psi^{n-1}(g)\ldots\psi^2(g)\psi^1(g)g}y\psi^n. \end{aligned}$$

*His key is now $K_B = f_{\psi^n(\psi^{m-1}(g)\ldots\psi^2(g)\psi^1(g)g)\psi^{n-1}(g)\ldots\psi^2(g)\psi^1(g)g}$.*

*We have $K_A = K_B = K$, the shared secret key.*

**Proof.** We have

$$\begin{aligned} K_A &= f_{\psi^m(\psi^{n-1}(g)\ldots\psi^2(g)\psi^1(g)g)\psi^{m-1}(g)..\psi^2(g)\psi^1(g)g} \\ &= f_{\psi^{m+n-1}(g)\ldots\psi^{m+2}(g)\psi^{m+1}(g)\psi^m(g)\psi^{m-1}(g)\ldots\psi^2(g)\psi^1(g)g} \\ &= (f_g\psi)^{m+n}(\psi^{m+n})^{-1}, \text{ where } (\psi^{m+n})^{-1} \text{ is the inverse of the element } \psi^{m+n} \text{ in } Aut(G). \end{aligned}$$

And

$$\begin{aligned} K_B &= f_{\psi^n(\psi^{m-1}(g)...\psi^2(g)\psi^1(g)g)\psi^{n-1}(g)...\psi^2(g)\psi^1(g)g} \\ &= f_{\psi^{n+m-1}(g)...\psi^{n+2}(g)\psi^{n+1}(g)\psi^n(g)\psi^{n-1}(g)...\psi^2(g)\psi^1(g)g} \\ &= (f_g\psi)^{n+m}(\psi^{n+m})^{-1}, \text{ where } (\psi^{n+m})^{-1} \text{ is the inverse of the element } \psi^{n+m} \text{ in } Aut(G). \end{aligned}$$

Then

$$K_A = K_B = K.$$

■

**Security of this protocol**

The security of this protocol relies on the difficulty of recovering the element of the group $\lambda(G)$.

**Proposition 3.2.2** *Let $H$,$Q$ be two groups. In our key exchange protocol, $H$,$Q$,$Aut(Q)$,$(h,q) \in H \times Q$, and $n \in \mathbb{N}$ are public information.*

***Bob:*** *Bob begins by choosing an embedding $\theta : H \longrightarrow Aut(Q)$, which he keeps secret. He then computes $X = (h,q)^n$, where $(h,q)^0 = 1_{H \rtimes_\theta Q}$, and for all $n \geq 0$, $(h,q)^{n+1} = (h,q)^n(h,q)$.*

*Then*

$$\begin{aligned} X &= (h,q)^n \\ &= (h^n, q\theta_h(q)\theta_{h^2}(q)...\theta_{h^{n-1}}(q)) \in H \rtimes_\theta Q \end{aligned}$$

*Bob then sends $X$ to Alice.*

***Alice:*** *Alice begins by choosing an embedding $\mu : H \longrightarrow Aut(Q)$, which he keeps secret. He then computes $Y = (h,q)^n$, where $(h,q)^0 = 1_{H \rtimes_\mu Q}$, and for all $n \geq 0, (h,q)^{n+1} = (h,q)^n(h,q)$.*

*Then*

$$Y = (h,q)^n = (h^n, q\mu_h(q)\mu_{h^2}(q)...\mu_{h^{n-1}}(q)) \in H \rtimes_\mu Q.$$

*Alice then sends $Y$ to Bob.*

***Bob:*** *by multiplying the second coordinate of $Y$ by $q^{-1}$, Bob can find the element $\mu_h(q)\mu_{h^2}(q)...\mu_{h^{n-1}}(q) \in Q$.*

***Alice:*** *by multiplying the second coordinate of $X$ by $q^{-1}$, Alice can find the element $\theta_h(q)\theta_{h^2}(q)...\theta_{h^{n-1}}(q) \in Q$.*

***Bob:*** *Bob can now compute*

$$\begin{aligned}\prod_{i=1}^{n-1} \theta_{h^i}(\mu_h(q)\mu_{h^2}(q)...\mu_{h^{n-1}}(q)) &= \prod_{i=1}^{n-1} \theta_h^i(\mu_h(q)\mu_h^2(q)...\mu_h^{n-1}(q)) \\ &= \prod_{i=1}^{n-1} (\theta_h^i \circ \mu_h)(q)(\theta_h^i \circ \mu_h^2)(q)...(\theta_h^i \circ \mu_h^{n-1})(q).\end{aligned}$$

***Alice:*** *similarly, Alice can compute*

$$\begin{aligned}\prod_{i=1}^{n-1} \mu_{h^i}(\theta_h(q)\theta_{h^2}(q)...\theta_{h^{n-1}}(q)) &= \prod_{i=1}^{n-1} \mu_h^i(\theta_h(q)\theta_h^2(q)...\theta_h^{n-1}(q)) \\ &= \prod_{i=1}^{n-1} (\mu_h^i \circ \theta_h)(q)(\mu_h^i \circ \theta_h^2)(q)...(\mu_h^i \circ \theta_h^{n-1})(q).\end{aligned}$$

*If in addition to $Q$ being abelian, we require that for all $h$ in $H$, $\theta_h$ and $\mu_h$ commute in $Aut(Q)$, then we have the following equality:*

$$\begin{aligned}k &= \prod_{i=1}^{n-1} \left(\theta_h^i \circ \mu_h\right)(q)(\theta_h^i \circ \mu_h^2)(q)...(\theta_h^i \circ \mu_h^{n-1})(q) \\ &= \prod_{i=1}^{n-1} (\mu_h^i \circ \theta_h)(q)(\mu_h^i \circ \theta_h^2)(q)...(\mu_h^i \circ \theta_h^{n-1})(q).\end{aligned}$$

*The element $k$ is computable by both Bob and Alice as shown above, giving them a shared key.*

***Proof.*** *We have*

$$\begin{aligned}\prod_{i=1}^{n-1} \theta_{h^i}(\mu_h(q)\mu_{h^2}(q)...\mu_{h^{n-1}}(q)) &= \prod_{i=1}^{n-1} \theta_h^i(\mu_h(q)\mu_h^2(q)...\mu_h^{n-1}(q)) \\ &= \prod_{i=1}^{n-1} (\theta_h^i\mu_h)(q)(\theta_h^i\mu_h^2)(q)...(\theta_h^i\mu_h^{n-1})(q).\end{aligned}$$

*And*

$$\begin{aligned}\prod_{i=1}^{n-1} \mu_{h^i}(\theta_h(q)\theta_{h^2}(q)...\theta_{h^{n-1}}(q)) &= \prod_{i=1}^{n-1} \mu_h^i(\theta_h(q)\theta_h^2(q)...\theta_h^{n-1}(q)) \\ &= \prod_{i=1}^{n-1} (\mu_h^i\theta_h)(q)(\mu_h^i\theta_h^2)(q)...(\mu_h^i\theta_h^{n-1})(q).\end{aligned}$$

*As $\theta_h$ and $\mu_h$ commute in $Aut(Q)$, then*

$$\prod_{i=1}^{n-1} \theta_{h^i}(\mu_h(q)\mu_{h^2}(q)...\mu_{h^{n-1}}(q)) = \prod_{i=1}^{n-1} \mu_{h^i}(\theta_h(q)\theta_{h^2}(q)...\theta_{h^{n-1}}(q)) = k.$$

■

**Security of this ptotocol**

The security of this protocol relies on the difficulty of recovering the homomorphism $\theta$ and $\mu$ from $(h, q) \in H \times Q, X$ and $Y$.

**Conclusion**

In this work, we present some notes on the group $(\lambda(G)Aut(G), \star)$ . Also we construct the public key exchange in this group.

# Bibliography


[1] Caranti, A., & Dalla Volta, F. (2018). Groups that have the same holomorph as a finite perfect group. Journal of Algebra, 507, 81-102.

[2] Egri-Nagy, A., & Nehaniv, C. L. (2013). Cascade Product of Permutation Groups. arXiv preprint arXiv:1303.0091.

[3] Clifford, A. H., & Preston, G. B. (1967). The algebraic theory of semigroups, Volume II (Vol. 2). American Mathematical Soc..

[4] Audu, M. S. (2001). Wreath Product of Permutation Groups. A Research Oriented Course In Arithmetics of Elliptic Curves, Groups and Loops. Lecture Notes Series, National Mathematical Centre, Abuja.

[5] Baumslag, B., Chandler, B., & Schaum's outline Series. (1968). Theory and problems of group theory. New York: McGraw-Hill.

[6] Meshram, C., & Li, X. (2018). New efficient key authentication protocol for public key cryptosystem using DL over multiplicative group. Journal of Information and Optimization Sciences, 39(2), 391-400.

[7] Paar, C., & Pelzl, J. (2009). Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media.

[8] Tsang, C. (2019). On the multiple holomorph of a finite almost simple group. arXiv preprint arXiv:1904.09754.

[9] Guin, D., & Hausberger, T. (2008). Groupes, corps et théorie de Galois. EDP sciences.

[10] Ghadbane, N. (2019). The inverse monoid associated to a group and the semidirect product of groups. Journal of Algebra and Related Topics, 7(1), 25-34.

[11] Ghadbane, N. (2020). On public key cryptosystem based on the word problem in a group. Journal of Discrete Mathematical Sciences and Cryptography, 1-6.

[12] Ghadbane, N. (2020). Decomposition of groups and the wreath product of permutation groups. Applied Sciences, 22, 83-93.

[13] Kreher, D. L. (2012). Group theory notes. Univ of Nebraska, Lincoln.

[14] F. Pécastaings, "Chemins vers l'algébre", tome 1, Vuibert, (1993).

[15] Ibrahim, A. A., & Audu, M. S. (2007). On wreath product of permutation groups. Proyecciones (Antofagasta), 26(1), 73-90.

[16] Meldrum, J. D. (1995). Wreath products of groups and semigroups (Vol. 74). CRC Press.

[17] Hoffstein, J., Pipher, J., Silverman, J. H., & Silverman, J. H. (2008). An introduction to mathematical cryptography (Vol. 1). New York: Springer.

[18] Habeeb, M., Kahrobaei, D., Koupparis, C., & Shpilrain, V. (2013, June). Public key exchange using semidirect product of (semi) groups. In International Conference on Applied Cryptography and Network Security (pp. 475-486). Springer, Berlin, Heidelberg.

[19] Mumtaz, M., & Ping, L. (2019). Forty years of attacks on the RSA cryptosystem: A brief survey. Journal of Discrete Mathematical Sciences and Cryptography, 22(1), 9-29.

[20] Adhikari, M. R., & Adhikari, A. (2014). Basic modern algebra with applications. Springer India.

[21] Bogopolski, O. (2008). Introduction to group theory, European Math. Soc., Zurich.

[22] Ruelle, P. Théorie des groupes. Cours Université Catholique de Louvain.

[23] Diffie, W., & Hellman, M. (1976). New directions in cryptography. IEEE transactions on Information Theory, 22(6), 644-654.

[24] W. Ledermann, "Introduction to Group Theory, Longman, (1973).

# ملخص

**الهولومورف للمجموعة $G$ التي يشار إليها عادة بواسطة $Hol(G)$ هي الجداء الطبيعي شبه المباشر $Aut(G)GofG$ بواسطة مجموعة التشكل الآلي $Aut(G)$. ليكن $(x \to gx)\lambda : G \to S(G), g \to fg$ التمثيل المنتظم الأيسر ل $G$ . في هذه المذكرة سنبرهن أن المجموعة $Hol(G)$ متشابهة للمجموعة:$\lambda(G)Aut(G)$ أيضا، نصف تبادل المفتاح العام في المجموعة :$\lambda(G)Aut(G)$**

**الكلمات المفتاحية: مجموعة التشاكل الذاتي، الجداء الشبه المباشر للمجموعات، تبادل المفتاح العام.**

# Abstract

The holomorph of the group G, usually denoted by Hol(G), is the naturel semidirect Product Aut(G)G of G by its automorphism group Aut(G). Let $\lambda : G \to S(G), g \to fg : (x \to gx)$ the left regular representation of G. In this paper we will show that the group Hol(G) is isomorphic to the group:$\lambda(G)Aut(G)$ Also, we describe the public Key exchange in the group: $\lambda(G)Aut(G)$

**Keywords:** Group of automorphism, semidirect products of groups, public key exchange.

# Résumé

L'holomorphe du group G généralement désigné par Hol(G), est le produit semi-direct naturel Aut(G)G de G par son groupe Aut(G). Soit $(x \to gx)\lambda : G \to S(G), g \to fg$ la représentation régulière gauche de G. Dans cet article, nous montrons que le groupe Hol(G) est isomorphe au groupe : $\lambda(G)Aut(G)$ .Nous décrivons également l'échange de clé publique dans le groupe : $\lambda(G)Aut(G)$

**Les mots clés :** Groupe d'automorphism, produits semi-directs des groupes, l'échange de clé publique.