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

Conjugtion in a group and its applications

Presented by :
Lograda Nour elhouda
Boudjellal Nadhira

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 2021/2022

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
جامعة محمد بوضياف بالمسيلة
UNIVERSITE MOHAMED BOUDIAF DE M'SILA
كلية الرياضيات و الإعلام الآلي
Faculté des Mathématiques et de l'Informatique
Département des Mathématiques
قسم الرياضيات

المسيلة في: / /

تصريح بتصحيح مذكرة الماستر 2

أنا الممضي أسفله الأستاذ: عضيان ناصر

مؤطر الطلبة الآتية أسماؤهم:

1- لقرادة نور الهدى

2- بوجلال نظيرة

3-

أصرح بأنهم قد قاموا بتصحيح مذكرتهم المعنونة بـ:

Conjugtion in group and Their applications

وذلك تبعا للنصائح الموجهة لهم من طرف لجنة التقييم.

إمضاء الأستاذ المؤطر

جامعة محمد بوضياف بالمسيلة
UNIVERSITE MOHAMED BOUDIAF DE M'SILA
كلية الرياضيات و الإعلام الآلي
Faculté des Mathématiques et de l'Informatique
Département des Mathématiques
قسم الرياضيات

المسيلة في: / /

تصريح بتصحيح مذكرة الماستر 2

أنا الممضي أسفله الأستاذ: عضيان ناصر

مؤطر الطلبة الآتية أسماؤهم:

1- لقرادة نور الهدى

2- بوجلال نظيرة

3-

أصرح بأنهم قد قاموا بتصحيح مذكرتهم المعنونة بـ:

Conjugtion in group and Their applications

وذلك تبعا للنصائح الموجهة لهم من طرف لجنة التقييم.

إمضاء الأستاذ المؤطر

Thanks

Praise be to **God**, whose good grace is completed, and thanks to him
for favoring us with this work.

I thank the supervisor professor N.Ghadbane who provided us
with guidance and reconciliation in this work.

I thank Mr. D.Mihoubi

I thank Mr. L.Heboub

I thank all the professors of the faculty of Mathematics, especially
Dr. S.Abdelkebir, who was of help and support for us,
and do not forget to have mercy on Professor R.Heraiz who is the winner,
may **God** forgive him.

Dedication

I dedicate my success as the fruit of struggle, fatigue and nights of staying up to
my mother and dear father's for their love, sacrifice and encouragement.
I pray to **God** to bless them and grant them paradise and bliss.

To the comfort of my eyes and my solid bridge, my brothers and sisters
the firm bond that does not lean.

To my friends who pull my arms and raise my head.

To everyone who encouraged me and said to me one day "I trust you".

To everyone who frustrated me and waited for my failure.

To the one who enlightened us on the path of knowledge and paved the way for my teachers
from the primary stage to the university.

To the partners of wishes ambition and beautiful memories my colleagues from the class
2017-2018, especially my colleagues in the field of Algebra and Discrete Mathematics.

Contents

Introduction

A reflection across one line in the plane is, geometrically, just like a reflection across every other line. That is, while reflections across two different lines in the plane are not strictly the same, they have the same type of effect.
Similarly, two different transpositions in S_n are not the same permutation but have the same type of effect: swap two elements and leave everything else unchanged.
The concept that makes the notion of "different, but same type of effect" precise is called conjugacy.

This work is divide in three chapters:

In chapter one, we provide some mathematical preliminaries concerning of group theory.

In chapter 2, we study the group actions and its applications.

In chapter 3, we give a conjugacy classes in some groups and its applications.

Chapter 1

Group basics

In this chapter we will study some basic concepts, theorems and proposition of groups that will help us in the following chapters.

1.1 Group and subgroup

1.1.1 Group

Definition 1.1.1 *A group G is a set provided with an internal law from an application*

$$\begin{array}{rccc} " * " : & G \times G & \to & G \\ & (x, y) & \longmapsto & x * y \end{array}$$

That satisfies the following conditions :

1. *The law " $*$ " is associative :* $\forall\, x, y, z \in G,\ (x * y) * z = x * (y * z)$.

2. *There exists an element neutral in* $G : \exists\, e \in G, \forall\, x \in G, e * x = x * e = x$.

3. *Any element in G is symmetrical :* $\forall\, x \in G, \exists\, x' \in G, x * x' = x' * x = e$.

We say that the group $(G, *)$ is commutative (or abelian) if the law is commutative i.e : $\forall\, x, y \in G, x * y = y * x$.

Examples 1.1.1

1. The sets $\mathbb{Z}\,, \mathbb{Q}\,, \mathbb{R}\,, \mathbb{C}$ provided by the adition are commutative groups.

2. The sets $\mathbb{Q}^*\,, \mathbb{R}^*\,, \mathbb{C}^*$ provided by multiplication are commutative groups.

3. $(\mathbb{R}^n, +)$ is a group for any $n \geq 2$.

Example 1.1.2

The set $GL_n(\mathbb{R})$ of squar matrices $n \times n$ provided with coefficient in $\mathbb{R}$ equipped with multiplication of matrices is a no commutative group in general. The neutral element is the identity matix.

Example 1.1.3

Let G and H be two group, the cartesian product $G \times H$ provided with a group law, called product law if : $(g, h), (g', h') \in G \times H$.
Let's pose :
$(g, h) \cdot (g', h') = (gg', hh')$ is a group.

1.1.2 Subgroup

Definition 1.1.2 *Let $(G, *)$ be a group and H a part of G, we say that $(H, *)$ a subgroup of $(G, *)$ if and only if :*

1. $e_G \in H$.

2. $\forall\, x, y \in H : x * y \in H$.

3. $\forall\, x \in H : x^{-1} \in H$.

Examples 1.1.4

1. For everything group G, $\{e_G\}$ and G are subgroups of G.

2. $(\mathbb{Z}, +)$ is subgroup of $(\mathbb{R}, +)$.

3. $(\mathbb{N}, +)$ is not a subgroup.

Examples 1.1.5

1. For $n \in \mathbb{N}$, $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}, (n\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$.

2. $\{2^n, n \in \mathbb{Z}\}, \{-1, 1\}, \mathbb{Q}_+^*$ are subgroups of $(\mathbb{Q}^*, \times)$.

lemma 1.1.1 *Let H a no empty part of a group $(G, *)$, so H is a subgroup of G if and only if :*

$$\forall\, x, y \in H \Rightarrow x * y^{-1} \in H.$$

Proof.

$\Rightarrow$) Suppose that H is a subgroup of G ie :
1. $\forall\, x, y \in h \Rightarrow x * y \in H$.
2. $\forall\, x \in H \Rightarrow x^{-1} \in H$.

Let $x, y \in H$, then from (2) we have $y^{-1} \in H$, from (1) we have $x * y^{-1} \in H$.

$\Leftarrow$) Suppose that $(\forall\, x, y \in H \Rightarrow x * xy^{-1} \in H)$, we demonstrate :
1. $\forall\, x, y \in H \Rightarrow x * y \in H$.
2. $\forall\, x \in H \Rightarrow x^{-1} \in H$.
Let $x, y \in H$, then $y^{-1} \in H$, then $x * (y^{-1})^{-1} = x * y \in H$.
Let $x \in H$ we pose $y = x$, then $x * x^{-1} = e \in H$, then $e * x^{-1} = x^{-1} \in H$.

Theorem 1.1.1 (Intersection of subgroups) *Let $(G, *)$ be a group, then any intersection of subgroups of G is a subgroup of G.*

Proof.

Let $(H_i)_{i \in I}$ be a family of subgroups of G.

$H = \cap_{i \in I} H_i$

1. $H \neq \emptyset$, because $e_G \in H_i, \forall\, i \in I$ then $e_G \in H$.

2. Let $x, y \in H$, So $\forall\, i \in I, x \in H_i, y \in H_i$, then $x * y^{-1} \in H_i \Rightarrow x * y^{-1} \in H$.

So H is a subgroup of $(G, *)$.

Remark 1.1.1 *If H is a subgroup of a group G, and if F is a subgroup of H, then F is a subgroup of G.*

Remark 1.1.2 *The union of two subgroups is not in general a subgroup.*

1.1.3 Generator subgroup

Definition 1.1.3 *Let $(G, *)$ a group, and A a part of G. The subgroup generated by A noted $\langle A \rangle$ is the smallest subgroup of G containing A.*
$\langle A \rangle$ is the intersection of all subgroups of G that contains A.

Definition 1.1.4 *Let $(G, *)$ a group, and $a \in G$, the subgroup monogeneous generated by a in G is called the subgroup generated by the singleton $\{a\}$, denoted by $\langle a \rangle$.*

Remark 1.1.3

-$\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$ *with multiplication.*

-$\langle a \rangle = \{ak \mid k \in \mathbb{Z}\}$ *with addition.*

Definition 1.1.5 *We say that a family $(x_i)_{i \in I}$ (resp.a party X of G) genarated the group G, or is a family (resp.party) generator of G, if $G = \langle x_i, i \in I \rangle$ (resp. $G = \langle X \rangle$).*
We say that a group G is of finite type if it has a finite generator family.
A group is said to be monogeneous if it exists $x \in G$ such that $G = \langle x \rangle$.

Examples 1.1.6

1. $\langle \emptyset \rangle = \{e\}$.

2. $\mathbb{Z}$ monogeneous generated by 1 or by -1.

Definition 1.1.6 ***(Order of a group, order of an element)***
A group G is said finite if it contains finite number of elements. In this case, the cardinal of G is called the order of group G, and is denoted $|G|$.
Let G be a group and a an element of G. We call order of a, denoted by $O(a)$ is the cardinal of $\langle a \rangle$(subgroup generated by a) if $\langle a \rangle$ is finite.
If this cardinal is infinite, we say that a is of infinite order.

Remark 1.1.4 *Let G is a finite group and x an element of G, $O(x) \leq |G|$.*

Remark 1.1.5 *In all groups G, the neutral element is the only one of order 1.*

1.2 Quotient group

1.2.1 Cosets

Definition 1.2.1 ***(Equivalence relation)*** *Let E be a set, and $\mathcal{R}$ a binary relation, we say that $\mathcal{R}$ is an equivalence relation on E if and only if :*

1. *$\mathcal{R}$ is reflexive : for all $x \in E$, we have $x\mathcal{R}x$.*

2. *$\mathcal{R}$ is symetric : for all $x, y \in E$, we have $x\mathcal{R}y \Rightarrow y\mathcal{R}x$.*

3. *$\mathcal{R}$ is transitive : for all $x, y, z \in E, (x\mathcal{R}y \text{ and } y\mathcal{R}x) \Rightarrow x\mathcal{R}z$.*

Example 1.2.1

We consider the relation $\mathcal{R}$ on $\mathbb{Z} \times \mathbb{Z}^*$ defined by :

$$(a, b)\mathcal{R}(c, d) \Leftrightarrow ad = bc$$

this is an equivalence relation.

Definition 1.2.2 ***(Equivalence class)*** *Let R is an equivalence relation on E, the equivalence class of element x of E is :*

$$\bar{x} = c(x) = \{\ y\ \in E,\ y\mathcal{R}x\ \}$$

The set of equivalence classes of E by $\mathcal{R}$ is called the quotient set of E by $\mathcal{R}$

$$E/\mathcal{R} = \{\ \bar{x},\ x\ \in E\ \}$$

lemma 1.2.1 *If E is a finite set provided with eqivalence relation $\mathcal{R}$, then*

$$Card\, E = \sum_{c \in E/\mathcal{R}} Card\, c$$

Definition 1.2.3 *Let H is a subgroup of group G, we define on G an equivalence relation called left equivalence relation (resp.to the right), associated to H by :*

$a \equiv_l b$ modulo $H \Leftrightarrow ab^{-1} \in H$
(resp $a \equiv_r b$ modulo $H \Leftrightarrow a^{-1}b \in H$).
Recall that an equivalence relation on a set is reflexive, symetric and transitive.

Example 1.2.2

$$x\mathcal{R}y \Leftrightarrow \exists\, k \in \mathbb{Z} : x - y = 5k.$$

For the relation $\equiv [5]$
Five equivalence classes : $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$
His quotient set noted $\mathbb{Z}/5\mathbb{Z}$.

Definition 1.2.4 *Let H is a subgroup of group G, the cardinal of the classes set on the left modulo H = the cardinal of classes set on the right, is called the index of H in G denoted by $[G : H]$, Then :*
$[G : H] = |(G/H)_r| = |(G/H)_l|$.

Theorem 1.2.1 (Lagrange Theorem) *Let H be a subgroup of a finite group G, the order of H divide the order of G, and we have :*
$[G : H] = |G|/|H|$.

1.2.2 Normal subgroup

Definition 1.2.5 *Let H be a subgroup of a group G, we say that H is a normal subgroup of G if :*
$gH = Hg, \forall g\ \in G$.
or
$g^{-1}Hg \subset H$.

Remark 1.2.1 *We can replace g in the definition with g^{-1}, and g^{-1} with g, then : $gHg^{-1} \subset H$.*

Remark 1.2.2 *We have in the definition gHg^{-1}, we can verify that it is true for the elements: Let $h \epsilon H, g\ \in G$, then $ghg^{-1}\ \in\ H$.*

Proposition 1.2.1 *Let G be a group, then $\{e\}$ and G are normal subgroups of G.*

Proof.

- $\{e\}$ is a normal subgroup : let $g \,\epsilon\, G$, the only element of $\{e\}$ is e and $geg^{-1} = e \,\epsilon\, \{e\}$.

- G is a normal subgroup : let $g \in G$ and $h \in G$, then $ghg^{-1} \in G$ because g, h and $g^{-1} \in G$.

1.3 Group morphism

1.3.1 Group morphism

Definition 1.3.1 *Let $(G, *)$ and $(H, \cdot)$ two groups.*
A group morphism (or homomorphism) of groups of G into H any application $f : G \longrightarrow H$ which verifies :

$$\forall g, g' \in G,\ f(g * g') = f(g) \cdot f(g')$$

- If $G = H$ we say that f is an endomorphism of G.

Examples 1.3.1

- The application *exp* of $(\mathbb{R}, +)$ in $(\mathbb{R}_+^*, \times)$ is a group morphism :
$\forall\, x, y \in \mathbb{R}$, $\exp(x + y) = \exp(x) \times \exp(y)$.

- The application ln of $(\mathbb{R}_+^*, \times)$ in $(\mathbb{R}, +)$ is a group morphism :
$\forall\, x, y \in \mathbb{R}$, $\ln(xy) = \ln(x) + \ln(y)$.

- $x \longmapsto \sqrt{x}$ of $(\mathbb{R}^*, \times)$ to $(\mathbb{R}^*, \times)$.

Proposition 1.3.1 *Let $f : G \to H$ a group morphism*

1. $f(e_G) = e_H$.

2. $\forall x \in G$, $f(x^{-1}) = f(x)^{-1}$.

Proof.

1. Let $x \in G$, $f(x) = f(xe_G) = f(x)f(e_G)$, then $f(e_G) = e_H$.

2. For all $x \in G$, $e_H = f(e_G) = f(xx^{-1}) = f(x)f(x^{-1})$, then $f(x^{-1}) = f(x)^{-1}$.

Theorem 1.3.1 *Let f and g two group morphism*

$$\begin{array}{rcl} f : G & \longrightarrow & H \\ g : H & \longrightarrow & L \end{array}$$

Then $g \circ f$ is a group morphism of G in L.

Proof.

$\forall\, x, y \in G$, $g \circ f(xy) = g[f(xy)] = g[f(x)f(y)] = g[f(x)]g[f(y)] = g \circ f(x) \cdot g \circ f(y)$.

1.3.2 Group isomorphism

Definition 1.3.2 *Let $f : G \longrightarrow H$ be a group morphism.*
- We say that f is an isomorphism of groups if f is bijective.

- We say that f is an automorphism of G if it's a isomorphism of G in himself, i.e : a bijective endmorphism.

- We say that f is an antimorphism if verified the relation $f(g * g') = f(g') \cdot f(g), \forall\, g, g' \in G$.

Example 1.3.2

1. The group $(\mathbb{R}, +)$ is isomorphic to the group $(\mathbb{R}^+, \times)$.

2. The group $(\mathbb{R}, +)$ is isomorphic to the group $(\mathbb{C}, +)$.

3. The group $\mathbb{Z}$ of integers with addition subgroup of $\mathbb{R}$, and the quotient group $\mathbb{R}/\mathbb{Z}$ is isomorphic to the group $\mathbf{S^1}$ of complex numbers of absolute value 1 with multiplication.

Proposition 1.3.2 *If f is an isomorphism of groups of G on H, then f^{-1} is an isomorphism of H on G.*

Example 1.3.3

exp is an isomorphism of the group $(\mathbb{R}, +)$ on the group $(\mathbb{R}_+^*, \times)$, and $\ln = \exp^{-1}$ is an isomorphism of the group $(\mathbb{R}_+^*, \times)$ on the group $(\mathbb{R}_+^*, \times)$.
The groups $\mathbb{R}$ and $\mathbb{R}_+^*$ are isomorphic.

1.3.3 Image and kernel

Definition 1.3.3 *Let $f : G \longrightarrow H$ be a morphism from a group $(G, *)$ to a group $(H, .)$*
- The image of f is the subset

$$Imf = f(G) = \{f(g), g \in G\} \subset H.$$

- The kernel of f is the subset

$$\ker f = f^{-1}(e_H) = \{g \in G, f(g) = e_H\} \subset G.$$

Theorem 1.3.2 *Let f be a morphism of groups of G in H.*
• *Imf is a subgroup of H.*
• *$\ker f$ is a subgroup of G.*
• *f is injective, if and only if $\ker f = e_G$.*
• *f is surjective if and only if $Imf = H$.*

Proof.

Use the criteria of a subgroup .

• Imf subgroup of H.
- $f(e_G) = e_H \Rightarrow e_H \in Imf$.
- $\forall\, y, y' \in Imf, \exists x, x' \in G, y = f(x)$ and $y' = f(x')$

$$y(y') = f(x)[f(x')]^{-1} = f(x)f(x'^{-1}) = f[x(x')^{-1}] \in Imf.$$

• $\ker f$ subgroup of H.
- $f(e_G) = e_H \Rightarrow e_G \in \ker f$.
- $\forall\, x, y \in \ker f, f(xy^{-1}) = f(x)f(y^{-1}) = f(x)[f(y)]^{-1} = e_H(e_H)^{-1} = e_H \Rightarrow xy^{-1} \in \ker f$.

• f is injective if and only if $\ker f = e_G$.
- f injective $\Rightarrow (f(x) = f(e_G) \Rightarrow x = e_G) \Rightarrow \ker f = e_G$.
- $\ker f = e_G, \forall\, x, x' \in G, f(x) = f(x') \Rightarrow f(x)[f(x')]^{-1} = e_H \Rightarrow f(x)f(x^{-1}) = e_H \Rightarrow f[x(x')^{-1}] = e_H$ (As $\ker f = e_G) \Rightarrow x(x')^{-1} = e_G \Rightarrow x = x' \Rightarrow f$ injective.

• f is surjective if and only if $Imf = H$.

Examples 1.3.4

Let :

$$\begin{array}{ccccc} f : (\mathbb{Z}, +) & \longrightarrow & (\mathbb{Z}, +) \\ x & \longmapsto & 2x \end{array}$$

• f is a morphism of groups because :
$\forall\, x, y \in \mathbb{Z}$, $f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y)$.

• $\forall\, x \,\epsilon\, \mathbb{Z}$, $2x = 0 \Rightarrow x = 0 \Rightarrow \ker(f) = \{x \in \mathbb{Z} : 2x = 0\} = \{0\}$, then f is injective.

• $Imf = \{2x, x \in \mathbb{Z}\} \neq \mathbb{Z}$, f is not surjective.

Proposition 1.3.3 *The kernel of a morphism $f : G \longrightarrow H$ is a normal subgroup.*

Proof.

For $n \in kerf$ and $g \in G$, using things from just above,

$$f(gng^{-1}) = f(g)f(n)f(g^{-1}) = f(g)e_Hf(g)^{-1} = f(g)f(g)^{-1} = e_H.$$

1.4 Cyclic group

Definition 1.4.1 *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

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

Example 1.4.1

The set $\mathbb{Z}_n = \{0, 1, ..., n - 1\}$ for $n \geq 1$ is a cyclic group under addition modulo n. Again, 1 and $-1 = n - 1$ are generators.

Theorem 1.4.1 *Cyclic group is abelian.*

Proof.

Let G be a cyclic group generated by g. Let $x, y \in G$, we want to show that $xy = yx$.
Now $x = g^m$ and $y = g^n$ for some integres m and n.
So $xy = g^mg^n = g^{m+n}$ and $yx = g^ng^m = g^{n+m}$.
But $m + n = n + m$ (addition of integres is commutative) .
So $xy = yx$.

1.5 Symmetric groups

1.5.1 Permutation groups

Definition 1.5.1 *Let E be a set. We call symmetric group of E (or group of permutations) the set of one-to-one mappings from E to E. We note it $S(E)$, $S(E)$ is a group for the composition of applications.*
A special case $E = \{1, 2, ..., n\}\ \forall\, n \in \mathbb{N}$, is a finite set, we then note S_n symmetric group of this set. The elements of S_n are called permutations.

Rating

Let $\sigma : \{1, 2, ..., n\} \longrightarrow \{1, 2, ..., n\}$ is a permutation, we denote by :

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

The neutral element Id_n is represented by :

$$\begin{pmatrix} 1 & 2 & ... & n \\ 1 & 2 & ... & n \end{pmatrix}$$

Proposition 1.5.1 *For every natural number n, the symmetric group S_n has $n!$ elements.*

Proof.

The order of S_n isthe 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 $n - 1$ choices for the image of 2. Then there are $n - 2$ choices for theimage of 3. Continuingin this way, we see tat

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

Example 1.5.1

For $n = 2$, $|S_2| = 2! = 2$

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$$

lemma 1.5.1 *Let σ be a permutation of E. Then the inverse of σ is a permutation of E.*

Example 1.5.2

Let the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$,the inverse of σ is :
$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ is permutation.

1.5.2 The compsition of permutations

Definition 1.5.2 *If σ and τ are permutations of S_n, then $\sigma\tau$ is defined to be the composition of the permutation σ and τ.*
$\sigma\tau$ is the permutation of S_n whose rule is given by :

$$\sigma\tau(x) = \sigma(\tau(x)), \forall x \in \mathbb{N}$$

Example 1.5.3

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$\sigma\tau(1) = \sigma(\tau(1)) = \sigma(2) = 1$
$\sigma\tau(2) = \sigma(\tau(2)) = \sigma(3) = 3$
$\sigma\tau(3) = \sigma(\tau(3)) = \sigma(1) = 2$

Thus we have

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Proposition 1.5.2 *The composition of permutations is not usually commutative.*

Example 1.5.4

Let :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Then

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

But

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

1.5.3 Support and cycle

Definition 1.5.3 ***(Suuport of permutation)***
We call support of a permutation $\sigma \in S_n$ the set of elements of $\{1, 2, ..., n\}$ non invariant.

$$Supp(\sigma) = \{i \in \{1, 2, ..., n\}, \sigma(i) \neq i\}.$$

Example 1.5.5

The support of $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 6 & 1 & 5 \end{pmatrix}$ is $\{1, 3, 4, 5, 6\}$.

Proposition 1.5.3 *Let $n \in \mathbb{N}$, σ and τ two permutations of S_n,*
we always have :

$$Supp(\sigma\tau) \subset Supp(\sigma) \cup Supp(\tau).$$

Definition 1.5.4 ***(Cycle)***
Let $1 \leq k \in \mathbb{N}$. A cycle of length k (or k-cycle) is a permutation $\sigma \in S_n$ if it exists k distinct elements $a_1, a_2, ..., a_k \in \{1, 2, ..., n\}$ such that :

$$\sigma(a_1) = a_2, \sigma(a_2) = a_3, ..., \sigma(a_{k-1}) = a_k, \sigma(a_k) = a_1$$

And $\sigma(x) = x, \forall\, x \in \{1, 2, ..., n\} \setminus \{a_1, a_2, ..., a_k\}$.

Examples 1.5.6

Let σ, τ and ρ three permutations such that :

a) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix} = (1425)$ is a cycle of length 4.

b) $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 5 & 6 & 4 \end{pmatrix} = (13)(456)$ this permutation containing a cycle of length 2 and cycle of length 3.

Example 1.5.7

$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix} \in S_5$, we remark that $\rho = (13254) = (32541) = (25413) = (41325)$.

Figure 1.3.5. the cycle (13254)

Definition 1.5.5 ***(Transposition)*** *We call transposition any 2-cycle, i.e any permutation that exchange two elements i and $j \neq i$ leaving fixed each of $n-2$ others, we also note τ_{ij},*

$$\tau_{ij} = (i,j) = \begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ 1 & 2 & \dots & j & \dots & i & \dots & n \end{pmatrix}.$$

Example 1.5.8

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = (13)$$

is a transposition τ_{13}.

1.5.4 Signature of permutation

Definition 1.5.6 *The signature of a permutation σ is denoted $sgn(\sigma)$ or $(-1)^\sigma$ for each $\sigma \in S_n$.*
In particular, we define

$$sgn(\sigma) = (-1)^\sigma = \begin{cases} 1 & if\ \sigma \quad is\ even \\ -1 & if\ \sigma \quad is\ odd \end{cases}$$

Definition 1.5.7 *Let $n \geq 2$, $\sigma \in S_n$, the signature of σ is :*

$$\varepsilon(\sigma) = \prod_{1 \leq i \leq j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

Agreement.

If $n = 1$, $S_1 = \{Id_{\{1\}}\}$ and we pose $\varepsilon(Id_{\{1\}}) = 1$.

Example 1.5.9

If

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

Then

$$\varepsilon(\sigma) = \frac{2-4}{1-2} \times \frac{2-3}{1-3} \times \frac{2-1}{1-4} \times \frac{4-3}{2-3} \times \frac{4-1}{2-4} \times \frac{3-1}{3-4} = 1.$$

1.5.5 Alternate group

Definition 1.5.8 *The set of even permutations (of signature 1) denoted by A_n is said alternate group.*

Example 1.5.10

$S_3 = \{id, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$

$A_3 = \{id, (1,2,3), (1,3,2)\}$.

Definition 1.5.9 *The kernel of morphism $\varepsilon : S_n \longmapsto \{-1, 1\}$ is a normal subgroup of S_n. This subgroup denoted by A_n, is called alternate group.*

Proposition 1.5.4 *For $n \geq 2$ the group A_n is the distingue subgroup of index two of S_n, it contains $\frac{n!}{2}$ elements.*

Example 1.5.11

$|A_3| = \frac{3!}{2} = 3.$

Chapter 2

The group actions and its applications

In chapter 2 we study the groups actions in the sets and its applications.

2.1 Group actions on a set

Definition 2.1.1 *Let X be a set and let G be a group. A left action of G on X is a mapping*

$$f : G \times X \longrightarrow X$$

$$(g, x) \longmapsto g \cdot x$$

Such that
1. $e \cdot x = x$, $\forall\, x \in X$.

2. $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$, $\forall\, g_1, g_2 \in G, x \in X$.

A set together with a (left) action of G is called a (left) G-set. An action is trivial if $g \cdot x = x$ for all $g \in G$.
We also say that G acts or operates on X.

Definition 2.1.2 *We say that $x \in X$ is invariant under the action of G on X if*

$$\forall\, g \in G, g \cdot x = x$$

We note X^G the set of elements invariants of X under the action of G.

Example 2.1.1 ***(Action by conjugation)***
All group G operates on itself by conjugation

$$G \times G \longrightarrow G$$

$$(g, x) \longmapsto g \cdot x = gxg^{-1}$$

Verification :

1. *Let $e, x \in G$ we have $e \cdot x = exe^{-1} = exe = ex = x$.*

2. *Let $g_1, g_2 \in G$, we have :*

$$\begin{cases} g_1 \in G \Rightarrow g_1 \cdot x = g_1 x g_1^{-1} \\ \text{and} \\ g_2 \in G \Rightarrow g_2 \cdot x = g_2 x g_2^{-1} \end{cases}$$

Then

$$\begin{aligned} g_1 \cdot (g_2 . x) &= g_1 \cdot (g_2 x g_2^{-1}) \\ &= g_1 g_2 x g_2^{-1} g_1^{-1} \\ &= g_1 g_2 x (g_1 g_2)^{-1} \\ &= (g_1 g_2) \cdot x \end{aligned}$$

Example 2.1.2

Let H is a subgroup of a group G. Then G operates on the set $(G/H)_g$ of classes on the left modulo H by :

$$G \times (G/H)_g \longrightarrow (G/H)_g$$
$$(g, xH) \longmapsto g \cdot (xH) = gxH$$

Example 2.1.3

If $X = G$, then every group G acts on itself by the left regular representation, that is :

$$(g, x) \longmapsto \lambda_g(x) = gx$$

where λ_g is left multiplication :

$$e \cdot x = \lambda_e(x) = ex = x$$

$$(g_1 \cdot g_2) \cdot x = \lambda_{g_1 g_2} x = \lambda_{g_1} \lambda_{g_2} x = \lambda_{g_1}(g_2 x) = g_1 \cdot (g_2 \cdot x).$$

Example 2.1.4

Let $G = GL_2(\mathbb{R})$ and $X = \mathbb{R}^2$. Then G acts on X by left multiplication. If $v \in \mathbb{R}^2$ and I is the identity matrix, then $I \cdot v = v$. If A and B are 2×2 invertible matrices, then $(A \cdot B) \cdot v = A \cdot (B \cdot v)$ since matrix multiplication is associative.

Remarks 2.1.1

1. If a group G operates on X, so for any subgroup H of G, the canonical injection $H \to G$ induces an operation of H on X.

2. For any normal subgroup N, G acts on N and G/N by conjugation.

Definition 2.1.3 *An action of G on X is a map $G \times X \longrightarrow X$ denoted $(g, x) \longrightarrow gx$ such that $1x = x$ and $g(hx) = (gh)x$ for all x in X and g, h in G. Given an action of G on X, we call X a G-set. A G-map between G-sets X and Y is a map $f : X \longrightarrow Y$ of sets that respects the G-action, meaning that, $f(gx) = gf(x)$ for all x in X and g in G. To give an action of G on X is equivalent to giving a group homomorphism from G to the group of bijections of X. In symbols $f : G \longrightarrow Bij(X)$*

Example 2.1.5

Let X a $\mathbb{K}$-vector space. We consider its linear group $GL(X) \longrightarrow Bij(X)$.
Let G be a group. A morphism group

$$f : G \longrightarrow GL(X)$$

is called a linear representation of G on X. We also say that G operates linearly on X.

Remark 2.1.2

For any group G, $Aut(G)$ acts on G.

Proposition 2.1.1 *Such an external law of a group on a set is called the action of the group on the set .*

Proof

If $f : G \longrightarrow Bij(X)$ is a group morphism , then setting for $x \in X$and $g \in G$,

$$g \cdot x = f(g)(x),$$

We obtain an external law of G on$X$ which satisfies both properties since

$$f(gh) = f(g)f(h) \quad and \quad f(e_G) = Id_X.$$

Reciprocally, if an external law.
checks both properties ,for $g \in G$ we can define an application $f(g) : X \longmapsto X$ by :if $x \in X$ so $f(g)(x) = g \cdot x$.
by applying the conditions of an action on the left 2 then 1 at g and g^{-1} , we obtain

$$\forall x \in X, x = e_G \cdot x = (gg^{-1}) \cdot x = g \cdot (g^{-1} \cdot x),$$

either by using f :

$$\forall x \in X, Id_X(x) = f(g)(f(g^{-1})(x)),$$

which means that

$$Id_X = f(g) \circ f(g^{-1}).$$

We have thus proved that for each $g \in G$, application $f(g)$ is bijective (reciprocal $f(g^{-1})$).
So f is an application of G in Bij(X) .
The translation of 1 in terms of f gives

$$\forall g, h \in G, f(gh) = f(g) \circ f(h)$$

So f is a group morphism .

Definition 2.1.4 ***(Faithful action, transitive action)***
We say that :
1. G operates faithfully on X if we have
$(\forall\, x \in X,\ g \cdot x = x) \Rightarrow g = e.$

2. G operates transitively on X if we have
$\forall\, x, x' \in X, \exists g \in G, g \cdot x = x'.$

Example 2.1.6

Any group G operates faithfully and transitively on itself by translation

$$G \times G \longrightarrow G$$

$$(g, x) \longmapsto g \cdot x = gx$$

Theorem 2.1.1 (Cayley) *Every group of order n is isomorphic to some subgroup of symmetric group S_n.*

Proof.

We consider the action of G on itself by left multiplication. Because this action is faithful, G embeds as a subgroup of Sym(G), and because Sym$(G) \cong S_n$, G isomorphic to a subgroup of S_n.

2.2 Orbits and stabilizers

Definition 2.2.1 ***(Orbit)*** *Let G be an action group on a set X. For $x \in X$ we call orbit of x under the action of G the subset of X defined by*

$$Orb(x) = \{g \cdot x,\ g \in G\}$$

Example 2.2.1

Let G be the permutation group defined by

$$G = \{(1), (123), (132), (45), (123)(45), (132)(45)\}$$

and $X = \{1, 2, 3, 4, 5\}$. Then X is a G-set. The orbits are

$$\begin{cases} Orb(1) = Orb(2) = Orb(3) = \{1, 2, 3\} \\ Orb(4) = Orb(5) = \{4, 5\} \end{cases}$$

Example 2.2.2

Suppose G acts on X, and let $\alpha \in G$ be an element of order n. Then the orbits of $\langle \alpha \rangle$ are the sets of the form

$$\left\{x, \alpha x, ..., \alpha^{n-1} x\right\}$$

(These elements need not be distinct, and so the set may contain fewer than n elements.)

Example 2.2.3

The orbits for a subgroup H of G acting on G by left multiplication are the right cosets of H in G. We write $H \setminus G$ for the set of right cosets. Similarly, the orbits for H acting by right multiplication are the left cosets, and we write G/H for the set of left cosets. Note that the group law on G will not induce a group law on G/H unless H is normal.

Example 2.2.4

For a group G acting on itself by conjugation, the orbits are called conjugacy classes: for $\alpha \in G$, the conjugacy class of α is the set

$$\left\{g\alpha g^{-1} \mid g \in G\right\}$$

Theorem 2.2.1 *The orbits of X form a partition.*

Proof.

Consider the relation defined on X by

$$x \mathcal{R} y \Leftrightarrow \exists g \in G,\ g \cdot x = y$$

This defines an equivalence relation on X, Let $x, y, z \in X$

- As $e_G = x$, we obtain $x \mathcal{R} x$.
- If $x \mathcal{R} y$, then let $g \in G$ such that $y = g \cdot x$. We obtain $x = g^{-1} \cdot y$ so $y \mathcal{R} x$.
- If now $x \mathcal{R} y$ and $y \mathcal{R} z$, then $y = g \cdot x$ and $z = h \cdot y$ with $g, h \in G$, so $z = (h \cdot g) \cdot x$ so $x \mathcal{R} z$.

Now the orbirs are the equivalence classes for this relation, so then they form a partition of X.

Definition 2.2.2 *We say that G acts transitive on X if there is only one orbit in X under G.*

Example 2.2.5

S_n acts transitively on $\{1, 2, ..., n\}$.

Theorem 2.2.2 *For $y \in Orb(x)$, the orbit of y is equal to the orbit of x.*

Proof.

For $y \in Orb(x)$, there exists some $g_1 \in G$ such $g_1 x = y$. We can also write this as $x = g_1^{-1} y$ by left multiplication with g^{-1}. For $z \in Orb(y)$, there exists some $h \in G$ such that $hy = z$. By substituting $gx = y$ into the equation, we get $ghx = z$. By closure, $gh \in G$, so $z \in Orb(x)$ and $Orb(x) \subseteq Orb(y)$.
Similarly, for $w \in Orb(x)$ where $w \neq y$ there exists some $g_2 \in G$ such that $g_2 x = w$. Substituting $x = g_1^{-1} y$, we see that $g_2 g_1^{-1} y = w$. By closure, $g_2 g_1^{-1} \in G$ so $w \in Orb(y)$ and $Orb(x) \subseteq Orb(y)$. Since $Orb(x) \subseteq Orb(y)$ and $Orb(y) \subseteq Orb(x)$, $Orb(y) = Orb(x)$.

Definition 2.2.3 ***(stabilizer)*** *Let G acts on X. The stabilizer (or isotropy group) of an element $x \in X$ denoted Stab(x) is*

$$Stab(x) = \{g \in G \mid g \cdot x = x\} \subset G$$

For a subset S of X, we define the stabilizer of S to be

$$Stab(S) = \{g \in G \mid g \cdot S = S\}$$

Example 2.2.6

Let G be the permutation group defined by

$$G = \{(1), (12)(3456), (35)(46), (12)(3654)\}$$

and $X = \{1, 2, 3, 4, 5, 6\}$. Then X is a G-set. The stabilizers are

$$\begin{cases} Stab(1) = Stab(2) = \{(1), (35)(46)\} \\ Stab(3) = Stab(4) = Stab(5) = Stab(6) = \{(1)\} \end{cases}$$

Example 2.2.7

Let G acts on G by conjugation, and let H be a subgroup of G. The stabilizer of H is called the normalizer $N_G(H)$ of H in G :

$$N_G(H) = \left\{g \in G \mid gHg^{-1} = H\right\}$$

Proposition 2.2.1 *Let G be a group acting on a set X and $x \in X$. The stabilizer group of x $Stab(x)$ is a subgroup of G.*

Proof.

Clearly, $e \in Stab(x)$ since the identity fixes every element in the set X. Let $g_1, g_2 \in Stab(x)$. Then $g_1 \cdot x = x$ and $g_2 \cdot x = x$. So $(g_1 g_2)x = g_1 \cdot (g_2 \cdot x) = g_1 \cdot x = x$, hence, the product of two elements in $Stab(x)$ is also in $Stab(x)$. Finally, if $g \in Stab(x)$, then $x = e \cdot x = (g^{-1}g) \cdot x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x$. So g^{-1} is in $Stab(x)$.

Definition 2.2.4 *Let G be a group acting on set X. The fixer of an element $g \in G$ is*

$$Fix(g) = \{x \in X \mid g \cdot x = x\}$$

Definition 2.2.5 *The transporter from x to y is the set of elements that send x to y*

$$Trans(x, y) = \{g \in G \mid g \cdot x = y\} \subset G$$

Remark 2.2.1

$Fix(g) \subset X$ and $Stab(x) \subset G$.

2.3 Class formula

Definition 2.3.1 *The **center** $Z(G)$ of a group G is defined to be :*

$$Z(G) = \{g \in G \mid gx = xg, \forall x \in G\}$$

$Z(G) = G$ if G is commutative.

Definition 2.3.2 *Let G be a group and H be a subgroup of G The **centralizer** of H is defined to be :*

$$C_G(H) = \{g \in G \mid hg = gh, \forall\, h \in H\}$$

Then $C_G(H)$ is a subgroup of G.

lemma 2.3.1 *Let G be a group acting on a finite set X.*

$$\sum_{Orb_i \in X/G} |Orb_i| = |X|$$

X/G is the set of orbits in action, i.e :

$$X/G = \{Orb(x) \mid x \in X\}.$$

Theorem 2.3.1 *When a group G acts on a set X, the length of the orbit of any point is equal to the index of its stabilizer in G.*

$$|Orb(x)| \ = [G : Stab(x)]$$

Proof.

The first thing we wish to prove is that for any two group elements g_1 and g_2, $g_1 \cdot x = g_2 \cdot x$ if and only if g_1 and g_2 are in the same left coset of $Stab(x)$.
We know this because if $g_1 \cdot x = g_2 \cdot x$, then $g_1^{-1} \cdot g_2$ fixes x. Thus, $g_2 \in g_1 \cdot Stab(x)$, and since g_2 also lies in its own left coset of $Stab(x)$, $g_1 \cdot Stab(x) = g_2 \cdot Stab(x)$.

Now define a mapping $f : G/Stab(x) \longrightarrow Orb(x)$ by $f(g \cdot Stab(x)) = g \cdot x$. This map is surjective because for$y \in Orb(x)$, we can choose a $g \in Trans(x, y)$, for which $g \cdot Stab(x)$ maps to y under f. Our previous result proves that this map is injective, and thus, we have a bijection.$|Orb(x)| = |G/Stab(x)| = [G : Stab(x)]$.

Corollary 2.3.1 *Let G be a group acting on a finite set X.*
If $X = \cup_{i=1}^{n} X_i$ is the partition of X in orbits under the action of G and if $x_i \in X_i$ is an element of the orbit X_i, then

$$|X| = \sum_{i=1}^{n} [G : Stab(x_i)]$$

Proof.

The orbits form a partition of X, then $X = \cup_{i=1}^{n} Orb(x_i)$, so

$$|X| = \sum_{x_i \in X} |Orb(x_i)|$$

according to (Theorem 2.3.1)

$$|Orb(x_i)| = [G : Stab(x_i)]$$

Then

$$|X| = \sum_{i=1}^{n} [G : Stab(x_i)].$$

For the action of G on itself by conjuction, we conclude the following class formula :

$$|G| = |Z(G)| + \sum_{h_i \notin Z(G)} [G : C(h_i)].$$

Example 2.3.1

It is easy to check that the conjugacy classes in S_3 are the following:

$$\{(1)\}, \{(123), (132)\}, \{(12), (13), (23)\}.$$

The class equation is $6 = 1 + 2 + 3$.

Theorem 2.3.2 (Burnside's theorem) *Let G be a group acting on a finite set X.Then the numbrer N of orbits is calculated by*

$$N = |X/G| = \frac{1}{|G|} \sum_{g \in G} |Fix(g)| = \frac{1}{|G|} \sum_{x \in X} |Stab(x)|.$$

In particular, the number of fixed peak average number of orbits of the elements of G.

Proof.

Let $A = (g, x) \in G \times X, g \cdot x = x$. We can write by denoting by X/G all the orbits:

$$|A| = \sum_{x \in X} |\{g \in G \mid g \cdot x = x\}| = \sum_{x \in X} |Stab(x)| = \sum_{Orb_i \in X/G} \sum_{x \in Orb_i} |Stab(x)|, \forall\, i \in \{1, 2, ..., k\}.$$

However, it results from the class formula that for each orbit Orb_i

$$\sum_{x \in Orb_i} |Stab(x)| = \sum_{x \in Orb_i} |G|/|Orb_i| = |G|,$$

Then

$$|A| = |(X/G)| \cdot |G|.$$

But we can also calculate $|A|$ by grouping the elements differently:

$$|A| = \sum_{g \in G} |\{x \in X \mid g \cdot x = x\}| = \sum_{g \in G} |Fix(g)|.$$

And by writing the equlity of the two expressions of $|A|$ found, we obtaion the announced formula:

$$|(X/G)| = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|.$$

Example 2.3.2

Let $X = \{1, 2, 3, 4, 5\}$ and suppose that G is a permutation group $G = \{(1), (13), (13)(25), (25)\}$. The orbits of X are $\{1, 3\}, \{2, 5\}$ and $\{4\}$.
We have

$$\begin{array}{rcl} Orb(1) & = & \{\sigma(1), \sigma \in G\}. \\ Orb(2) & = & \{\sigma(2), \sigma \in G\}. \\ Orb(4) & = & \{\sigma(4), \sigma \in G\}. \end{array}$$

$\circ$	(1)	(13)	(25)	(13)(25)
(1)	(1)	(13)	(25)	(13)(25)
(13)	(13)	(1)	(13)(25)	(25)
(25)	(25)	(13)(25)	(1)	(13)
(13)(25)	(13)(25)	(25)	(13)	(1)

The sets of fixed points are :

$$\begin{array}{rcl} Fix((1)) & = & X \\ Fix((13)) & = & \{2, 4, 5\} \\ Fix((13)(25)) & = & \{4\} \\ Fix((25)) & = & \{1, 3, 4\} \end{array}$$

Burnside's theorem says :

$$N = \frac{1}{|G|} \sum_{g \in G} |Fix(g)| = \frac{1}{4}(5 + 3 + 1 + 3) = 3.$$

2.4 p-groups

Definition 2.4.1 *A finite p-group is a finite group which has p^n elements for a certain n, with p is a prime number.*

Examples 2.4.1

1. The trivial group $G = \{e\}$ is a p-group for any prime number p.

2. $\mathbb{Z}/8\mathbb{Z}$ is a 2-group (it is of order 2^3 with 2 prime).

Proposition 2.4.1 *Let p be a prime number, n nonzero integer and G a finite group of order p^n acts on a finite set X. Then*

$$|X^G| \equiv |X| \ (mod\, p).$$

With

$$X^G = \{x \in X \mid g \cdot x = x, \forall g \in G\}.$$

Proof.

An element $x \in X^G$ if and only if $g \cdot x = x$, then $|X^G|$ is the number of punctual orbits. Let $(x_i)_{i\in I}$ a family of representatives of non-punctual orbit. Then

$$|X| = |X^G| + \sum_{i\in I} |Orb(x_i)| \ \ such\, that\, |Orb(x_i)| = [G : Stab(x_i)]$$

is different from 1 and divides p^n, it is therefore of the form p^{α_i}, with $\alpha_i \geq 1$. Then $(|X| - |X^G|)$ is divisible by p.

lemma 2.4.1 *Every group of prime order is cyclic.*

Proof

By Lagrange's theorem, we know that for any element of G, we have $|\langle g\rangle|/|G|$. However, if G has prime order and g is not the identity, then this can only be satisfied if $\langle g\rangle = G$, making G cyclic.

Theorem 2.4.1 (Cauchy) *Let G be a finite group and p a prime such that p divides the order of G. Then G contains a subgroup of order p.*

Proof.

We will use induction on the order of G. If $|G| = p$, then clearly G must have an element of order p.
Now assume that every group of order k, where $p \leq k < n$ and p divides k, has an element of order p.
Assume that $|G| = n$ and $p \mid n$ and consider the class equation of G :

$$|G| = |Z(G)| + \sum_{h_i \notin Z(G)} [G : C(h_i)]\,.$$

We have two cases :

Case 1. The order of one of the centralizer subgroups $C(h_i)$ is divisible by p for some i, $i = 1, ..., k$. In this case, by our induction hypothesis, we are done. Since $C(h_i)$ is a proper subgroup of G and p divides $|C(h_i)|$, $C(h_i)$ must contain an element of order p. Hence, G must contain an element of order p.

Case 2. The order of no centralizer subgroup is divisible by p. Then p divides $[G : C(h_i)]$, the order of each conjugacy class in the class equation, hence p must divide the center of G, $Z(G)$. Since $Z(G)$ is abelian, it must Then, the center of G contains an element of order p.

Proposition 2.4.2 ***(Center of p-group)*** *Let p be a prime nmber and G a finite non-trivial p-group. Then the center $Z(G)$ of G does not reduce to the trivial group $\{e\}$. In particular, a finite p-group of non-prime order is never a simple group.*

Proof.

Consider the action of the p-group G on itself by conjugation. Thus, the set X is G and the fixed points X^G are the elements of the center of G.
The relation $|X^G| \equiv |X| \ (mod\, p)$ (Proposition 2.4.1) gives $|Z(G)| = |G| \ (mod\, p)$ and, as p divides $|G|$, we obtain $|Z(G)| \equiv 0 \ (mod\, p)$. The center, being a subgroup, cannot be empty

and therefore contains at least p elements. So we have $Z(G) \neq \{e\}$.
Suppose now that the order of G is not a prime number. As $Z(G)$ is normal in G and $Z(G) \neq \{e\}$, if $Z(G)$ is not equal to G then the group G is not simple. If $Z(G) = G$ then the group is commutative and an element of order p (Theorem cauchy 2.4.1) generates a normal subgroup H of order p. As G is not of prime order we obtain $H \neq G$, what ends the proof.

Corollary 2.4.1 *A group of order p^n has normal subgroups of order p^m for all $m \leq n$.*

Proposition 2.4.3 *Every group of order p^2 is commutative.*

Proof.

We know that the centre $Z(G)$ of G is nontrivial, and that $G = Z(G)$ therefore has order 1 or p. In either case it is cyclic, and the next result implies that G is commutative.

Chapter 3

Conjugacy classes in some groups and its applications

In chapter 3 we study the conjugacy classes in some groups and its applications.

3.1 Conjugacy classes in some groups and its applications

3.1.1 Definition and examples

Definition 3.1.1 *Let G be a group, and let g and h two elements of G are called conjugate if*

$$h = xgx^{-1},\ for\ some\ x \in G.$$

We define the conjugacy class of g by the set

$$cl(g) = \left\{xgx^{-1} \mid x \in G\right\}.$$

Example 3.1.1

The matrix group $GL_n(\mathbb{R})$ contains all $n \times n$ invertible matrices with real entries. In this group, two matrices A and B are conjugates if there is a matrix P such that $A = PBP^{-1}$ which corresponds to matrix similarity. The conjuygacy classes of this group then are the sets of matrices that represent the same linear transfomation in different bases.

Example 3.1.2

If G is abelian then every element is its own conjugacy class : $xgx^{-1} = g$ for all $x \in G$. In fact this characterizes abelian groups, to say every $g \in G$ is its own conjugacy class means $xgx^{-1} = g$ for every x and every g, which says $xg = gx$ for all x and g in G, so G is abelian.

Example 3.1.3

$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$.

There are five conjugacy classes in Q_8 :

$$\{1\}, \{-1\}, \{i, -i\}, \{j, -j\}, \{k, -k\}.$$

Example 3.1.4

There are four conjugacy classes in A_4 :

$$\{(1)\}, \{(12)(34), (13)(24), (14)(23)\},$$

$$\{(123), (243), (134), (142)\}, \{(132), (234), (143), (124)\}.$$

Notice the 3-cycles (123) and (132) are not conjugate in A_4. All 3-cycles in A_4 are conjugate in the larger group S_4, $(132) = (23)(123)(23)^{-1}$ and the conjugating permutation (23) is not in A_4.

Example 3.1.5

Let G be an group, and let $x, g_1, g_2, \ldots, g_n \in G$, for any n, the conjugate of $g_1g_2 \ldots g_n$ by x is the product of the conjugate by x of $g_1, g_2, \ldots, g_n$.

Proposition 3.1.1 *Let G be a group, let H be a subgroup of G and $g \in G$, the set*

$$gHg^{-1} = \left\{ghg^{-1} \mid h \in H\right\}$$

is a subgroup of G, called naturally enough a conjugate subgroup to H.

Proof.

It's a subgroup since it contains the identity ($e = geg^{-1}$) and is closed under multiplication and inversion : $(ghg^{-1})(gh'g^{-1}) = g(hh')g^{-1}$ and $(ghg^{-1})^{-1} = gh^{-1}g^{-1}$. Unlike different conjugacy classes, different conjugate subgroups are not disjoint : they all contain the identity.

3.1.2 Some basic properties of conjugacy classes

Proposition 3.1.2 *If G is abelian then $xgx^{-1} = g$ for all $x, g \in G$ (and the converse is also true : if all conjugacy classes are singletons then G is abelian).*

Proposition 3.1.3 *An element $g \in G$ lies the center $Z(G)$ of G if and only if its conjygacy class has only one element, g itself.*

Remarks

1. In any group, $cl(e) = e$, because $xex^{-1} = e$ for any $x \in G$.

2. If g and x commute, then $xgx^{-1} = g$. This, when computing $cl(g)$, we only need to check xgx^{-1} for those $x \in G$ that do not commute with g.

3. Moreover, $cl(g) = g$ iff g commutes with everythingin G.

2. A subgroup is conjugate only to itself precisely when it is a normal subgroup.

Proposition 3.1.4 *The conjugacy class is an equivalence relation.*

Proof.

We define the relation " $\sim$ " by

$$g \sim h \Leftrightarrow \exists\, x \in G,\ h = xgx^{-1}.$$

1. Reflexive : $\exists\, g \in G,\ g \sim g$.
This follows from $g = ege^{-1}$, where e is the identity element of the group G
$\Rightarrow$ " $\sim$ " is reflexive i.e conjygacy is reflexive.

2. Symmetric : if $g \sim h$ then $h \sim g$.
Let $g \sim h \Leftrightarrow \exists\, x \in G,\ h = xgx^{-1}$.
$x^{-1}hx = x^{-1}xgx^{-1}x \Rightarrow x^{-1}hx = g \Rightarrow g = x^{-1}h(x^{-1})^{-1} \Rightarrow h \sim g$
$\Rightarrow$ " $\sim$ " is symmetric i.e conjugacy is symmetric.

3. Transitive : if $g \sim h$ and $h \sim f$ then $g \sim f$.
Let $g \sim h$ and $h \sim f \Leftrightarrow \exists\, x \in G,\ h = xgx^{-1}$ and $\exists\, y \in G,\ f = yhy^{-1}$
$\Rightarrow f = yxgx^{-1}y^{-1} = yxg(yx)^{-1}$
$\Rightarrow \exists\, c \in G,\ f = cgc^{-1}$ $(c = yx \in G)$.
$\Rightarrow g \sim f \Rightarrow$ " $\sim$ " is transitive i.e conjugacy is transitive.
Finally " $\sim$ " is equivalence relation i.e the conjugacy class is an equivalence relation.

lemma 3.1.1 *In a group, $(xgx^{-1})^n = xg^nx^{-1}$ for all positive integers n.*

Theorem 3.1.1 *All the elements of a conjugacy class have the same order*

Proof.

This is saying g and xgx^{-1} have the same order. By Lemma 3.1.1, $(xgx^{-1})^n = xg^nx^{-1}$ for all $n \in \mathbb{Z}^+$, so if $g^n = 1$ then $(xgx^{-1})^n = xg^nx^{-1} = xx^{-1} = e$, and if $(xgx^{-1})^n = 1$ then $xg^nx^{-1} = e$, so $g^n = x^1x = e$. Thus $(xgx^{-1})^n = 1$ if and only if $g^n = 1$, so g and xgx^{-1} have the same order.

Corollary 3.1.1 *If H is a cyclic subgroup of G then every conjugate subgroup to H is cyclic.*

Proof.

Writing $H = \langle y \rangle = \{y^n \mid n \in \mathbb{Z}\}$,

$$gHg^{-1} = \left\{gy^ng^{-1} \mid n \in \mathbb{Z}\right\} = \left\{(gyg^{-1})^n \mid n \in \mathbb{Z}\right\} = \langle gyg^{-1} \rangle,$$

so a generator of gHg^{-1} is a conjugate (by g) of a generator of H.

Theorem 3.1.2 *Let G be a group and $g, h \in G$. If the conjugacy classes of g and h overlap, then the conjugacy classes are equal.*

Proof.

We need to show every element conjugate to g is also conjugate to h, and vice versa. Since the conjugacy classes overlap, we have $xgx^{-1} = yhy^{-1}$ for some x and y in the group. Therefore

$$g = x^{-1}yhy^{-1}x = (x^{-1}y)h(x^{-1}y)^{-1},$$

so g is conjugate to h. Each element conjugate to g is zgz^{-1} for some $z \in G$, and

$$zgz^{-1} = z(x^{-1}y)h(x^{-1}y)^{-1}z^{-1} = (zx^{-1}y)h(zx^{-1}y)^{-1},$$

which shows each element of G that is conjugate to g is also conjugate to h. To go the other way, from $xgx^{-1} = yhy^{-1}$ write $h = (y^{-1}x)g(y^{-1}x)^{-1}$ and carry out a similar calculation.

Theorem 3.1.2 says each element of a group belongs to just one conjugacy class. We call an element of a conjugacy class a representative of that class.
A conjugacy class consists of all xgx^{-1} for fixed g and varying x. Instead we can look at all xgx^{-1} for fixed x and varying g. That is, instead of looking at all the elements conjugate to g we look at all the ways x can conjugate the elements of the group. This "conjugate-by-x" function is denoted

$$\gamma_x : G \longrightarrow G$$
$$\gamma_x(g) = xgx^{-1}$$

Theorem 3.1.3 *Each conjugation function $\gamma_x : G \longrightarrow G$ is an automorphism of G.*

Proof.

For all g and h in G,

$$\gamma_x(g)\gamma_x(h) = xgx^{-1}xhx^{-1} = xghx^{-1} = \gamma_x(gh),$$

so γ_x is a homomorphism. Since $h = xgx^{-1}$ if and only if $g = x^{-1}hx$, the function γ_x has inverse $\gamma_{x^{-1}}$, so γ_x is an automorphism of G.

Theorem 3.1.3 explains why conjugate elements in a group are "the same except for the point

of view" : they are linked by an automorphism of the group, namely one of the maps γ_x. This means an element and its conjugates have the same group-theoretic properties.
Automorphisms of G having the form γ_x are called inner automorphisms. That is, an inner automorphism of G is a conjugation-by-x operation on G, for some $x \in G$. Inner automorphisms are about the only examples of automorphisms that can be written down without knowing extra information about the group (such as being told the group is abelian or that it is a particular matrix group). For some groups every automorphism is an inner automorphism. This is true for the groups S_n when $n \neq 2, 6$ (that's right: S_6 is the only nonabelian symmetric group with an automorphism that isn't conjugation by a permutation).The groups $GL_n(\mathbb{R})$ when $n \geq 2$ have extra automorphisms : since $(AB)^T = B^T A^T$ and $(AB)^{-1} = B^{-1}A^{-1}$, the function $f(A) = (A^T)^{-1}$ on $GL_n(\mathbb{R})$ is an automorphism and it is not inner. Here is a simple result where inner automorphisms tell us something about all automorphisms of a group.

Theorem 3.1.4 *If G is a group with trivial center, then the group $Aut(G)$ also has trivial center.*

Proof.

Let $\varphi \in Aut(G)$ and assume φ commutes with all other automorphisms. We will see what it means for φ to commute with an inner automorphism γ_x. For $g \in G$,

$$(\varphi \circ \gamma_x)(g) = \varphi(\gamma_x(g)) = \varphi(xgx^{-1}) = \varphi(x)\varphi(g)\varphi(x)^{-1}$$

and

$$(\gamma_x \circ \varphi)(g) = \gamma_x(\varphi(g)) = x\varphi(g)x^{-1},$$

so having φ and γ_x commute means, for all $g \in G$, that

$$\varphi(x)\varphi(g)\varphi(x)^{-1} = x\varphi(g)x^{-1} \Leftrightarrow x^{-1}\varphi(x)\varphi(g) = \varphi(g)x^{-1}\varphi(x).$$

so $x^{-1}\varphi(x)$ commutes with every value of φ. Since φ is onto, $x^{-1}\varphi(x) \in Z(G)$. The center of G is trivial, so $\varphi(x) = x$. This holds for all $x \in G$, so φ is the identity automorphism. We have proved the center of $Aut(G)$ is trivial.

Theorem 3.1.5 *Let G be a finite group and let g be an element of G. Then,*

$$|cl(g)| = |G : C_G(g)|.$$

Proof.

Consider the function T that sends the coset $xC_G(g)$ to the conjugate xgx^{-1} of g. A routine calculation shows that T is well-defined, is one-to-one, and maps the set of left cosets onto the conjugacy class of g. Thus, the number of conjugates of g is the index of the centralizer of g.

Corollary 3.1.2 *In a finite group, $|cl(g)|$ divides $|G|$.*

3.2 Conjygacy classes in S_n

Definition 3.2.1 *If $\sigma \in S_n$ and σ is written as the product of the disjoint cycles of lengths $n_1, \ldots, n_k$ which $n_i \leq n_{i+1}$ for each $i < k$, then $n_1, \ldots, n_k$ is the cycle type of σ*

Theorem 3.2.1 *The conjugacy classes of S_n are determined entirely by the cycle type. That is, the conjugacy class of an element x of S_n consists of all the elements of S_n whose cycle type is the same as the cycle type of x.*

Example 3.2.1

In S_3, for all $\sigma \in S_3$.

σ	(1)	(12)	(13)	(23)	(123)	(132)
$\sigma(1)\sigma^{-1}$	(1)	(1)	(1)	(1)	(1)	(1)

The conjugacy class of (1) is : (1).

σ	(1)	(12)	(13)	(23)	(123)	(132)
$\sigma(12)\sigma^{-1}$	(12)	(12)	(23)	(13)	(23)	(13)

The conjugacy class of (12) is : $\{(12), (13), (23)\}$.

σ	(1)	(12)	(13)	(23)	(123)	(132)
$\sigma(123)\sigma^{-1}$	(123)	(132)	(132)	(132)	(123)	(123)

The conjugacy class of (123) is : $\{(123), (132)\}$.
So S_3 has three conjugacy classes :

$$\{(1)\}, \{(12), (13), (23)\}, \{(123), (132)\}$$

The following tables list a representative from each conjugacy class in S_n for $3 \leq n \leq 6$, along with the size of the conjugacy classes. Conjugacy classes disjointly cover a group, by Theorem 3.1.2, so the conjugacy class sizes add up to $n!$ for S_n.

	S_3		
Rep.	(1)	(123)	(12)
Size	1	2	3

	S_4				
Rep.	(1)	(12)(34)	(12)	(1234)	(123)
Size	1	3	6	6	8

	S_5						
Rep.	(1)	(12)	(12)(34)	(123)	(12)(345)	(12345)	(1234)
Size	1	10	15	20	20	24	30

	S_6					
Rep.	(1)	(12)	(12)(34)(56)	(123)	(123)(456)	(1234)
Size	1	15	15	40	40	45
Rep.	(1234)	(12)(3456)	(123456)	(12)(345)	(12345)	
Size	90	90	120	120	144	

Theorem 3.2.2 *For each cycle $(i_1 i_2 \dots i_k)$ in S_n and each $\sigma \in S_n$,*

$$\sigma(i_1 i_2 \dots i_k)\sigma^{-1} = (\sigma(i_1)\sigma(i_2)\dots\sigma(i_k)).$$

Proof.

Let $\pi = \sigma(i_1 i_2 \dots i_k)\sigma^{-1}$. We want to show π is the cyclic permutation of the numbers $\sigma(i_1), \sigma(i_2), \dots \sigma(i_k)$. That means two things :

- Show π sends $\sigma(i_1)$ to $\sigma(i_2)$, $\sigma(i_2)$ to $\sigma(i_3)$, . . . , $\sigma(i_{k-1})$ to $\sigma(i_k)$ and finally $\sigma(i_k)$ to $\sigma(i_1)$.

- Show π does not move a number other than $\sigma(i_1)$, . . . , $\sigma(i_k)$.

The second step is essential. Just knowing a permutation cyclically permutes certain numbers does not mean it is the cycle built from those numbers, since it could move other numbers we haven't looked at yet. (For instance, if $\pi(1) = 2$ and $\pi(2) = 1$, π need not be (12). The permutation (12)(345) also has that behavior.)
What does π do to $\sigma(i_1)$? The effect is

$$\pi(\sigma(i_1)) = (\sigma(i_1 i_2 \dots i_k)\sigma^{-1})(\sigma(i_1)) = ((\sigma(i_1 i_2 \dots i_k)\sigma^{-1}\sigma)(i_1) = \sigma(i_1 i_2 \dots i_k)(i_1) = \sigma(i_2).$$

(The "(i_1)" at the ends is not a 1-cycle, but denotes the point where a permutation is being evaluated.) Similarly, $\pi(\sigma(i_2)) = \sigma(i_1 i_2 \dots i_k)(i_2) = \sigma(i_3)$, and so on up to $\pi(\sigma(i_k)) = \sigma(i_1 i_2 \dots i_k)(i_k) = \sigma(i_1)$.

Now pick a number a that is not among $\sigma(i_1) \dots \sigma(i_k)$. We want to show $\pi(a) = a$. That means we want to show $\sigma(i_1 i_2 \dots i_k)\sigma^{-1}(a) = a$. Since $a \neq \sigma(i_j)$ for $j = 1, \dots, k$, also $\sigma^{-1}(a)$ is not i_j for $j = 1, \dots, k$. Therefore the cycle $(i_1 i_2 \dots i_k)$ does not move $\sigma^{-1}(a)$, so its effect on $\sigma^{-1}(a)$ is to keep it as $\sigma^{-1}(a)$. Hence

$$\pi(a) = \sigma(i_1 i_2 \dots i_k)\sigma^{-1}(a) = \sigma(\sigma^{-1}(a)) = a.$$

Example 3.2.2

In S_5, let $\sigma = (13)(254)$. Then

$$\sigma(1432)\sigma^{-1} = (13)(254)(1432)(245)(13) = (1532)$$

while $(\sigma(1)\sigma(4)\sigma(3)\sigma(2)) = (3215)$ since $\sigma(1) = 3, \sigma(4) = 2, \sigma(3) = 1$, and $\sigma(2) = 5$. Clearly $(1532) = (3215)$.

Example 3.2.3

In S_7, let $\sigma = (13)(265)$. Then

$$\sigma(73521)\sigma^{-1} = (13)(265)(73521)(256)(13) = (12637)$$

and $(\sigma(7)\sigma(3)\sigma(5)\sigma(2)\sigma(1)) = (71263) = (12637)$.

Theorem 3.2.3 *All cycles of the same length in S_n are conjugate.*

Proof.

Pick two k-cycles, say

$$(a_1 a_2 \dots a_k), \quad (b_1 b_2 \dots b_k).$$

Choose $\sigma \in S_n$ so that $\sigma(a_1) = b_1, \dots, \sigma(a_k) = b_k$, and let σ be an arbitrary bijection from the complement of $\{a_1 \dots a_k\}$ to the complement of $\{b_1 \dots b_k\}$. Then, using Theorem 3.2.2, we see conjugation by σ carries the first k-cycle to the second.

For instance, the transpositions (2-cycles) in S_n form a single conjugacy class, as we saw for S_3 in the introduction.
Now we consider the conjugacy class of an arbitrary permutation in S_n, not necessarily a cycle. It will be convenient to introduce some terminology. Writing a permutation as a product of disjoint cycles, arrange the lengths of those cycles in increasing order, including 1-cycles if there are fixed points. These lengths are called the cycle type of the permutation. For instance, in S_7 the permutation $(12)(34)(567)$ is said to have cycle type $(2, 2, 3)$. When discussing the cycle type of a permutation, we include fixed points as 1-cycles. For instance, $(12)(35)$ in S_5 is $(4)(12)(35)$ and has cycle type $(1, 2, 2)$. If we view $(12)(35)$ in S_6 then it is $(4)(6)(12)(35)$ and has cycle type $(1, 1, 2, 2)$.
The cycle type of a permutation in S_n is just a set of positive integers that add up to n, which is called a partition of n. There are 7 partitions of 5 :

$$5,\ 1+4,\ 2+3,\ 1+1+3,\ 1+2+2,\ 1+1+1+2,\ 1+1+1+1+1.$$

Thus, the permutations of S_5 have 7 cycle types. Knowing the cycle type of a permutation tells us its disjoint cycle structure except for how the particular numbers fall into the cycles. For instance, a permutation in S_5 with cycle type $(1, 2, 2)$ could be $(1)(23)(45), (2)(35)(14)$, and so on. This cycle type of a permutation is exactly the level of detail that conjugacy measures in Sn: two permutations in S_n are conjugate precisely when they have the same cycle type. Let's understand how this works in an example first.

Example 3.2.4

We consider two permutations in S_5 of cycle type $(2, 3)$:

$$\pi_1 = (24)(153),\ \pi_2 = (13)(425).$$

To conjugate π_1 to π_2, let σ be the permutation in S_5 that sends the terms appearing in π_1 to the terms appearing in π_2 in exactly the same order :

$$\sigma = \begin{pmatrix} 2 & 4 & 1 & 5 & 3 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix} = (14352).$$

Then

$$\sigma\pi_1\sigma^{-1} = \sigma(24)(153)\sigma^{-1} = \sigma(24)\sigma^{-1}\sigma(153)\sigma^{-1} = (\sigma(2)\sigma(4))(\sigma(1)\sigma(5)\sigma(3)) = (13)(425).$$

so $\sigma\pi_1\sigma^{-1} = \pi_2$.
If we had written π_1 and π_2 differently, say as

$$\pi_1 = (42)(531),\ \pi_2 = (13)(542).$$

then $\pi_2 = \sigma\pi_1\sigma^{-1}$ where

$$\sigma = \begin{pmatrix} 4 & 2 & 5 & 3 & 1 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix} = (1234).$$

lemma 3.2.1 *If π_1 and π_2 are disjoint permutations in S_n, then $\sigma\pi_1\sigma^{-1}$ and $\sigma\pi_2\sigma^{-1}$ are disjoint permutations for all $\sigma \in S_n$.*

Proof.

Being disjoint means no number is moved by both π_1 and π_2. That is, there is no i such that $\pi_1(i) \neq i$ and $\pi_2(i) \neq i$. If $\sigma\pi_1\sigma^{-1}$ and $\sigma\pi_2\sigma^{-1}$ are not disjoint, then they both move some number, say j. Then (check!) $\sigma^{-1}(j)$ is moved by both π_1 and π_2, which is a contradiction.

Theorem 3.2.4 *Two permutations in S_n are conjugate if and only if they have the same cycle type.*

Proof.

Pick $\pi \in S_n$. Write π as a product of disjoint cycles. By Theorem 3.1.3 and Lemma 3.2.1 , $\sigma\pi\sigma^{-1}$ will be a product of the σ-conjugates of the disjoint cycles for π, and these σ-conjugates are disjoint cycles with the same respective lengths. Therefore $\sigma\pi\sigma^{-1}$ has the same cycle type as π.

lemma 3.2.2 *In general, the number of conjugacy classe in the symmetric group S_n is equal to the number of integer partitions of n.*

Proof

this is because each conjugacy class corresponds to exactly one partition of $\{1, 2, ..., n\}$ into cycles,up to permutation of the elements of $\{1, 2, ..., n\}$.

3.3 Dihedral group

3.3.1 Introduction

For $n \geq 3$ the dihedral group D_n is defined as the rigid motions taking a regular n-gon back to itself, with the operation being composition. These polygons for $n = 3, 4, 5$ and 6 are pictured below . The dotted lines are lines of reflection : reflecting the polygon across each line brings the polygon back to itself, so these reflections are in D_3, D_4, D_5 and D_6

Figure 3.3.1

In addition to reflections, a rotation by a multiple of $2\pi/n$ radians around the center carries the polygon back to itself, so D_n contains some rotations.

3.3.2 Finding the elements of D_n

Points in the plane at a specifed distance from a given point form a circle, so points with specifed distances from two given points are the intersection of two circles, which is two points (non-tangent circles) or one point (tangent circles). For instance, the blue points in the figure below have the same distances to each of the two black points.

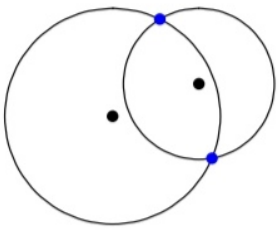

Figure 3.3.2

lemma 3.3.1 *Every point on a regular polygon is determined, among all points on the polygon, by its distances from two adjacent vertices of the polygon.*

Proof.

In the picture above, let the blue dots be adjacent vertices of a regular polygon. The line segment connecting them is an edge of the polygon and the polygon is entirely on one side of the line through the blue dots. So the two black dots can't both be on the polygon, which means each point on the polygon is distinguished from all other points on the polygon (not from all other points in the plane!) by its distances from two adjacent vertices.

Theorem 3.3.1 *The size of D_n is $2n$.*

Proof

Our argument has two parts: an upper bound and then a construction of enough rigid motions to achieve the upper bound.

Step1 : $|D_n| \leq 2n$.

Pick two adjacent vertices of a regular n-gon, and call them A and B as in the figure below. An element g of D_n is a rigid motion taking the n-gon back to itself, and it must carry vertices to vertices (how are vertices unlike other points in terms of their distance relationships with all points on the polygon?) and g must preserve adjacency of vertices, so $g(A)$ and $g(B)$ are adjacent vertices of the polygon.

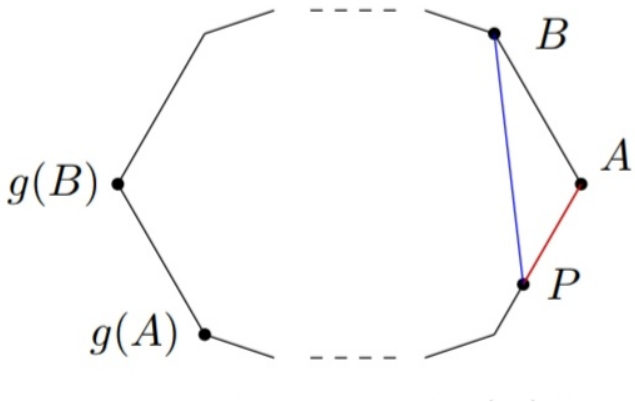

Figure 3.3.3

For each point P on the polygon, the location of $g(P)$ is determined by $g(A)$ and $g(B)$, because the distances of $g(P)$ from the adjacent vertices $g(A)$ and $g(B)$ equal the distances of P from A and B, and therefore $g(P)$ is determined on the polygon by Lemma 3.3.1 To count $|D_n|$ it thus suffices to find the number of possibilities for $g(A)$ and $g(B)$.
Since $g(A)$ and $g(B)$ are a pair of adjacent vertices, $g(A)$ has at most n possibilities (there are n vertices), and for each choice of that g(B) has at most 2 possibilities (one of the two vertices adjacent to $g(A)$). That gives us at most $n \cdot 2 = 2n$ possibilities, so $|D_n| \leq 2n$.

Step2 : $D_n = 2n$

We will describe n rotations and n reflections of a regular n-gon.
A regular n-gon can be rotated around its center in n different ways to come back to itself (including rotation by 0 degrees). Specifically, we can rotate around the center by $2k\pi/n$ radians where $k = 0, 1, \ldots, n-1$. This is n rotations.
To describe reflections taking a regular n-gon back to itself, look at the pictures 3.3.1 and

3.3.2: if n is 3 or 5 there are lines of reflection connecting each vertex to the midpoint of the opposite side, and if n is 4 or 6 there are lines of reflection connecting opposite vertices and lines of reflection connecting midpoints of opposite sides. These descriptions of reflections work in general, depending on whether n is even or odd :

• For odd n, there is a reflection across the line connecting each vertex to the midpoint of the opposite side. This is a total of n reflections (one per vertex). They are different because each one fixes a different vertex.
• For even n, there is a reflection across the line connecting each pair of opposite vertices ($n/2$ reflections) and across the line connecting midpoints of opposite sides (another $n/2$ reflections). The number of these reflections is $n/2+n/2 = n$. They are different because they have different tyon : different pairs of opposite vertices or different pairs of midpoints of opposite sides. The rotations and reflections are different in D_n since a non-identity rotation fixes no point on the polygon, the identity rotation fixes all points, and a reflection fixes two points.
In D_n it is standard to write r for the counterclockwise rotation by $2\pi/n$ radians. This rotation depends on n, so the r in D_3 means something different from the r in D_4. However, as long as we are dealing with one value of n, there shouldn't be confusion.

Theorem 3.3.2 *The n rotations in D_n are $1, r, r^2, \ldots, r^{n-1}$.*
Here and below, we designate the identity rigid motion as 1.

Proof.

The rotations $1, r, r^2, \ldots, r^{n-1}$ are different since r has order n.
Let s be a reflection across a line through a vertex. See examples in the polygons below.
A reflection has order 2, so $s^2 = 1$ and $s^{-1} = s$.

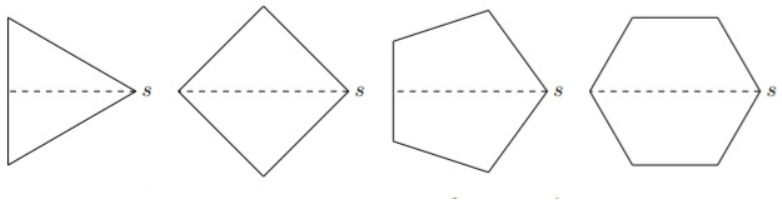

Figure 3.3.4

Theorem 3.3.3 *The n reflections in D_n are $s, rs, r^2s, \ldots, r^{n-1}s$.*

Proof.

The rigid motions $s, rs, r^2s, \ldots, r^{n-1}s$ are different since $1, r, r^2, \ldots, r^{n-1}$ are different and we just multiply them all on the right by s. No r^ks is a rotation because if $r^ks = r^l$ then $s = r^{l-k}$, but s is not a rotation.
Since D_n has n rotations and n reflections, and no r^ks is a rotation, they're all reflections.

Since each element of D_n is a rotation or reflection, there is no "mixed rotation-reflection" : the product of a rotation r^i and a reflection r^js (in either order) is a reflection. The geometric interpretation of the reflections s, rs, r^2s, and so on is this : drawing all lines of reflection for a regular n-gon and moving clockwise around the polygon starting from a vertex fixed by s, we meet successively the lines fixed by $rs, r^2s, \ldots, r^{n-1}s$. See the polygons below. Convince yourself, for instance, that if s is the reflection across the line through the rightmost vertex then rs is the next line of reflection counterclockwise.

Figure 3.3.5

Theorem 3.3.4 *The group D_n has $2n$ elements. As a list,*

$$D_n = \left\{1, r, r^2, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\right\},$$

In particular, all elements of D_n with order greater than 2 are powers of r.

Watch out : although each element of D_n with order greater than 2 has to be a power of r, because each element that isn't a power of r is a reflection, it is false in general that the only elements of order 2 are reflections. When n is even, $r^{n/2}$ is a 180-degree rotation, which has order 2. Clearly a 180-degree rotation is the only rotation with order 2, and it lies in D_n only when n is even.

3.3.3 Relations between rotations and reflections

The rigid motions r and s do not commute. Their commutation relation is a fundamental formula for computations in D_n, and goes as follows.

Theorem 3.3.5 *The dihedral group D_n is a subgroup of S_n of order $2n$.*

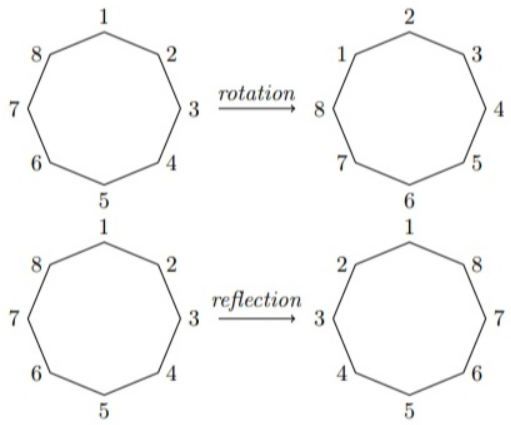

Figure 3.3.6. Rotations and reflections of a regular n-gon

Theorem 3.3.6 *In D_n,*

$$srs^{-1} = r^{-1}. \tag{3.3.1}$$

Proof.

A short proof comes from rs being a reflection : $(rs)^2 = 1 \Rightarrow rsrs = 1 \Rightarrow srs = r^{-1}$, and $s = s^{-1}$ since s has order 2.
We now want to prove (3.3.1) in a longer way using a geometric interpretation of bothsides. Since every rigid motion of a regular n-gon is determined by its effect on two adjacent vertices, to prove $srs^{-1} = r^{-1}$ in D_n it suffces to check srs^{-1} and r^{-1} have the same values at a pair of adjacent vertices.
Recall s is a reflection fixing a vertex of the polygon. Let A be a vertex fixed by s and write its adjacent vertices as B and B', with B appearing counterclockwise from A and B' appearing clockwise from A. This is illustrated in the figure below, where the dashed line through A is fixed by s. We have $r(A) = B$, $r^{-1}(A) = B'$, $s(A) = A$, and $s(B) = B'$.

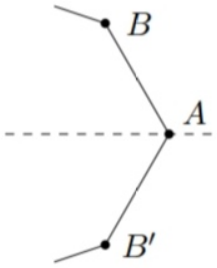

Figure 3.3.7

The values of srs^{-1} and r^{-1} at A are

$$(srs^{-1})(A) = (srs)(A) = sr(s(A)) = sr(A) = s(B) = B' \quad and \quad r^{-1}(A) = B',$$

while their values at B are

$$(srs^{-1})(B) = (srs)(B) = sr(s(B)) = sr(B') = s(A) = A \quad and \quad r^{-1}(B) = A.$$

Since srs^{-1} and r^{-1} agree at A and at B, they agree on the polygon, so $srs^{-1} = r^{-1}$. Equivalent ways of writing $srs^{-1} = r^{-1}$ are (since $s^{-1} = s$)

$$sr = r^{-1}s, \; rs = sr^{-1}. \tag{3.3.2}$$

What these mean is that when calculating in D_n we can move r to the other side of s by inverting it. By induction (or by raising both sides of (3.3.1) to an integral power) check

$$sr^k = r^{-k}s, \quad r^k s = sr^{-k} \tag{3.3.3}$$

for every integer k. In other words, every power of r can be moved to the other side of s by inversion. This also follows from $r^k s$ being a reflection :

$$1 = (r^k s)^2 = r^k s r^k s \Rightarrow sr^k = r^{-k}s^{-1} = r^{-k}s.$$

Example 3.3.1

In D_7 using (3.3.3)

$$r^2 sr^6 sr^3 = r^2(sr^6)sr^3 = r^2(r^{-6}s)sr^3 = r^2 r^{-6} ssr^3 = r^{-4}r^3 = r^{-1} = r^6$$

and

$$sr^4 sr^3 sr^2 = s(r^4 s)r^3(sr^2) = s(sr^{-4})r^3(r^{-2}s) = ssr^{-4}r^3 r^{-2}s = r^{-3}s = r^4 s.$$

The relation (3.3.2) involves a particular rotation and a particular reflection in D_n. In (3.3.3), we extended (3.3.2) to any rotation and a particular reflection in D_n. We can extend (3.3.3) to any rotation and any reflection in D_n : a general reflection in D_n is $r^i s$, so by (3.3.3)

$$\begin{aligned} (r^i s)r &= r^i r^{-j} s \\ &= r^{-j} r^i s \\ &= r^{-j}(r^i s) \end{aligned}$$

In the other order,

$$\begin{aligned} r^j(r^i s) &= r^i r^j s \\ &= r^i s r^{-j} \\ &= (r^i s)r^{-j} \end{aligned}$$

This has a nice geometric meaning : when multiplying in D_n, every rotation can be moved to the other side of every reflection by inverting the rotation. This geometric description makes such algebraic formulas easier to remember

Theorem 3.3.7 *When $n \geq 3$ is odd, the center of D_n is trivial. When $n \geq 3$ is even, the center of D_n is trivial. When $n \geq 3$ is even, the center of D_n is $1, r^{n/2}$.*

Proof.

No reflections are in the center of D_n since reflections do not commute with r :

$$(r^i s)r = r^i(sr) = r^i r^{-1} s = r^{i-1}s, \quad r(r^i s) = r^{i+1}s$$

so if $r^i s$ commutes with r then $r^{i-1} = r^{i+1}$, which implies $r^2 = 1$, but r has order $n \geq 3$.
Which rotations r^j could be in the center of D_n? Without loss of generality $0 \leq j \leq n-1$.
We would need r^j to commute with s, so $r^j s = sr^j$, which is equivalent to $r^j s = r^{-j}s$, which implies $r^{2j} = 1$. Since r has order n,$r^{2j} = 1$ only if $n \mid 2j$. For odd n this implies $n \mid j$, so j is a multiple of n and thus $r^j = 1$. Hence for odd n the only rotation that could be in the center of D_N is 1. Certainly 1 is in the center, so for odd n the center of D_n is $\{1\}$. For even n, the condition $n \mid 2j$ is equivalent to $n/2 \mid j$, and for $0 \leq j \leq n-1$ the only choices for j are $j = 0$ and $j = n/2$. Thus $r^j = r^0 = 1$ or $r^j = r^{n/2}$. Certainly 1 is in the center, and to show $r^{n/2}$ is in the center we check it commutes with every rotation and reflection in D_n. That $r^{n/2}$ commutes with rotations is obvious since all rotations are powers of r and thus they all commute with each other. To check $r^{n/2}$ commutes with every reflection in D_n, the key point is that $r^{n/2} = r^{-n/2}$, which follows from $r^n = 1$. (This also makes sense geometrically since $r^{n/2}$ is a 180° rotation, and rotating by 180° or -180° has the same effect.) Now we check $r^{n/2}$ commutes with each reflection $r^i s$:

$$r^{n/2}(r^i s) = r^{n/2+i}s, \quad (r^i s)r^{n/2} = r^i r^{-n/2}s = r^i r^{n/2}s = r^{i+n/2}s = r^{n/2+i}s.$$

Example 3.3.2

The group D_3 has trivial center. The group D_4 has center $\{1, r^2\}$.
For even n, the rotation $r^{n/2}$ on a regular n-gon is by 180 degrees. Theorem 3.3.7 says this rotation for even n is the only nontrivial rigid motion of a regular n-gon that commutes with all other rigid motions of the n-gon. A 180-degree rotation around the origin commutes with all rigid motions of $\mathbf{R}$ fixing the origin, but a 180-degree rotation is not in D_n for odd n because a regular n-gon for odd n is not carried back to itself by a 180-degree rotation.

Example 3.3.3

In $D_4 = \langle r, s\rangle$, there are five conjugacy classes :

$$\{1\}, \left\{r^2\right\}, \left\{s, r^2 s\right\}, \left\{r, r^3\right\}, \left\{rs, r^3 s\right\}.$$

The members of a conjugacy class of D_4 are different but have the same type of effect on a squaren : r and r^3 are a 90 degree rotation in some direction, s and r^s are a reflection across a diagonal, and rs and $r^3 s$ are a reflection across an edge bisector.

Example 3.3.4

While D_4 has 5 conjugacy classes of elements, it has 8 conjugacy classes of subgroups. In total there are 10 subgroups of D_4 :

$$\langle 1\rangle = \{1\}, \langle s\rangle = \{1, s\}, \langle rs\rangle = \{1, rs\}, \langle r^2 s\rangle = \left\{1, r^2 s\right\}, \langle r^3 s\rangle = \left\{1, r^3 s\right\},$$

$$\langle r\rangle = \left\{1, r, r^2, r^3\right\}, \langle r^2\rangle = \left\{1, r^2\right\}, \langle r^2, s\rangle = \left\{1, r^2, s, r^2 s\right\}, \langle r^2, rs\rangle = \left\{1, r^2, rs, r^3 s\right\}, D4.$$

In this list the subgroups $\langle s\rangle$ and $r^2 s$ are conjugate, as are $\langle rs\rangle$ and $r^3 s$, check : $r\langle s\rangle r^{-1} = \langle r^2 s\rangle$ and $r\langle rs\rangle r^{-1} = \langle r^3 s\rangle$. The other six subgroups of D_4 are conjugate only to themselves.

3.4 Conjygacy classes in D_n

In the group D_n we will show rotations are conjugate only to their inverses and reflections are either all conjugate or fall into two conjugacy classes.

Theorem 3.4.1 *The conjugacy classes in D_n are as follows.*
1. If n is odd,
- *the identity element :* $\{1\}$
- $(n-1)/2$ *conjugacy classes of size 2 :* $\{r^{\pm 1}\}, \{r^{\pm 2}\}, \ldots, \{r^{\pm(n-1)/2}\}$
- *All the reflections :* $\{r^i s : 0 \leq i \leq n-1\}$.

2. If n is even
- *Two conjugacy classes of size 1 :* $\{1\}, \{r^{\frac{n}{2}}\}$
- $n/2-1$ *conjugacy classes of size 2 :* $\{r^{\pm 1}\}, \{r^{\pm 2}\}, \ldots, \{r^{\pm \frac{n}{2}-1}\}$
- *The reflections fall into two conjugacy classes :* $\{r^{2i}s : 0 \leq i \leq \frac{n}{2}-1\}$ *and* $\{r^{2i+1}s : 0 \leq i \leq \frac{n}{2}-1\}$.

Proof.

Every element of D_n is $r^i \circ r^i s$ for some integer i. Therefore to find the conjugacy class of an element g we will compute $r^i g r^{-i}$ and $(r^i s)g(r^i s)^{-1}$.
The formulas

$$r^i r^j r^{-i} = r^j, \quad (r^i s)r^j(r^i s)^{-1} = r^{-j}$$

as i varies show the only conjugates of r^j in D_n are r^j and r^{-j}. Explicitly, the basic formula $sr^j s^{-1} = r^{-j}$ shows us r^j and r^{-j} are conjugate, we need the more general calculation to be sure there is nothing further that r^j is conjugate to.
To find the conjugacy class of s, we compute

$$r^i s r^{-i} = r^{2i}s, \quad (r^i s)s(r^i s)^{-1} = r^{2i}s.$$

As i varies, $r^{2i}s$ runs through the reflections in which r occurs with an exponent divisible by 2. If n is odd then every integer modulo n is a multiple of 2 (since 2 is invertible mod n we can solve $k \equiv 2i \bmod n$ for i given k). Therefore when n is odd

$$\{r^{2i}s : i \in \mathbb{Z}\} = \{r^k s : k \in \mathbb{Z}\},$$

so every reflection is conjugate to s. When n is even, however, we only get half the reflections as conjugates of s. The other half are conjugate to rs :

$$r^i(rs)r^{-i} = r^{2i+1}s, \quad (r^i s)(rs)(r^i s)^{-1} = r^{2i-1}s.$$

As i varies, this gives us $\{rs, r^3 s, \ldots, r^{n-1}s\}$.

That reflections in D_n form either one or two conjugacy classes, depending on the parity of n, corresponds to a geometric feature of reflections : for odd n all reflections in D_n look the same (Figure 3.4.1) − reflecting across a line connecting a vertex and the midpoint on the opposite side − but for even n the reflections in D_n fall into two types − the $r^{even}s$ reflect across a line through pairs of opposite vertices and the $r^{odd}s$ reflect across a line through midpoints of opposite sides (Figure 3.4.1).

Figure 3.4.1. Lines of Reflection for $n = 3$ and $n = 5$.

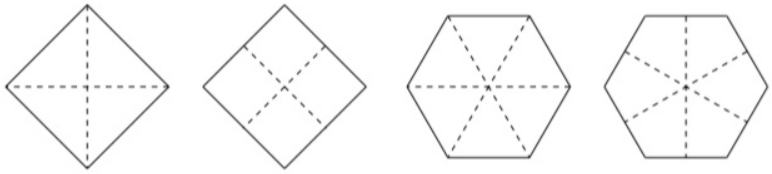

figure 3.4.2. Lines of Reflection for $n = 4$ *and* $n = 6$.

Bibliography

[1] Alexander Paulin. Introduction to Abstract Algebra (Math 113).

[2] Amin Idelhaj. (July 2016).

[3] Anne Cortella. (octobre 2011). Théorie des groupes.

[4] B.Selikh and M. Abdelhafid. (2020/2021). Memoire de fin d'etude : Action d'un groupe et symétrie.

[5] D.Schaub. (1997/98). Elements of Group Theory, University of Angers.

[6] D.S Dummit, R.M. Foote. Wiley, 2004. Abstract Algebra.

[7] F1.3YR1 Abstract Algebra Introduction To Group Theory Lecture Notes and Exercises.

[8] Felix Ulmer. (octobre 2012). Théorie des groupes.

[9] F.Guagui.(2020/2021). Master Thesis : Holomoroh of the group and their applications in cryptography.

[10] Grillet, Pierre Antoine. (2007). Abstract Algebra. Graduate texts in mathematics.

[11] Jean Delcourt. (2001). Théorie des groupes, Université de Cergy-Pontoise.

[12] Jean Louis Rouget. (2018).

[13] Joseph A. Gallian. Contemporary Abstract Algebra, University of Minnesota Duluth.

[14] J. Poland. (1968). Finite groups with a given number of conjugate classes, Canadian J. Math.

[15] J.S. Milne. (23 June 2021). Group Theory, Version 4.00.

[16] Keith Conrad. Conjugation in a group.

[17] N.Ghadbane,Decomposition of groups and the wreath product of permutation groups, Applied Sciences, vol.22, No 2, p.83-93,(2020).

[18] N.Ghadbane, The inverse monoid associated to a group and the semidirect product of groups, journal of Algebra and Related Topics, vol. 7,No 1,p.25-34,(2020).

[19] N.Ghadbane, Wreath product of permutation groups and their actions on a sets, Caspian Journal of Mathematical Sciences (CJMS),vol.10,No 2,p.142-155, (2021).

[20] Paul.Garrett. (June, 2007, Minneapolis). Abstract Algebra.

[21] Paul Milan. (2017). Cpge-L1-Algebre.

[22] Samir Siksek. Introduction to Abstract Algebra.MA136, Mathematics Institute, University of Warwick.

[23] Thomas W. Judson Stephen F. (16 August 2013). Abstract Algebra, Theory and Applications, Austin State University.

Abstract

In this work we are intersted with the study of conjugtion in group and its applications.

Key words:

Conjugacy class, group action, symmetric group, dihedral group, rotation, reflection.

Résumé

Dans ce travail nous intéressons à l'étude de la conjugaison en groupe et ses applications.

Mot-clés:

Classe de conjugaison, action de groupe, groupe symétrique, groupe dièdre, rotation, réflexion.