Group actions on a set and Pólya's Enumeration Theorem

Saad Eddine *KADI*

June 8, 2016

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, professor: **D.Mihoubi**, for his invaluable advices and suggestions.
My thanks also go to the jury members for the honor they have done me by accepting to judge this modest work.
I would like to thank my 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.

Thank you.

Contents

Index of notations

$\|G\|$	Order of a group
$\mathcal{M}_{n\times n}(\mathbb{R})$	The set of $n \times n$ matrices over $\mathbb{R}$
$\mathcal{GL}_n(\mathbb{R})$	The set of $n \times n$ invertible matrices over $\mathbb{R}$
$\mathcal{SL}_n(\mathbb{R})$	The set of $n \times n$ matrices over $\mathbb{R}$ with determinant equal to 1
$End(G)$	The set of all endomorphisms of a group G
$Aut(G)$	The set of all automorphisms of a group G
G/H	The set of all left cosets of a subgroup H in a group G
H/G	The set of all right cosets of a subgroup H in a group G
$[G : H]$	The index of a subgroup H in a group G
$\sim$	Equivalence relation
$cl(x)$	Equivalence class of an element
σ	A permutation
$cyc(\sigma)$	Cycle index of a permutation
S_n	The symmetric group of the first n natural numbers
C_n	The cyclic group of order n
D_n	The nth dihedral group
A_n	The alternating group
$\mathcal{O}_x$	The orbit of an element
$Stab(x)$	The stabilizer of an element
$Fix(g)$	The invariant of an element
$cim(\sigma)$	Cycle index monomial of a permutation
Z_G	Cycle index polynomial associated with a group
w_c	The weight of an element
$W(f)$	The weight of a function
PI_G	Pattern inventory under a group G

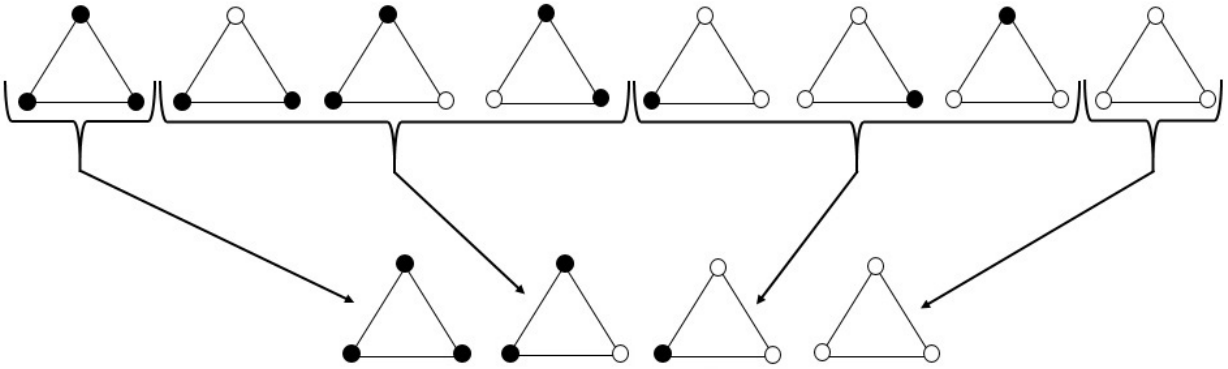
Abstract

IN this thesis we present the solutions of some counting problems using the Pólya's Enumeration Theorem. Firstly, we define a permutation and describe its properties. Next, we introduce the four symmetry groups used in Polya's Enumeration Theorem, the symmetric, cyclic, dihedral and alternating groups and example of symmetries of geometric figures in two and three dimensional spaces. After that , we introduce the notion of group actions on a set and its concepts like the orbit, the stabilizer, the invariant and describe its properties and give some simple problems in group theory solved by the notion of group action. Finaly, we give the Pólya's Enumeration Theorem and use it to solve some counting problems like the necklace problem, coloring of polytopes, the number of non-isomorphic simple graphs with n vertices, chemical compounds and give a generalization theorem of Fermat and Gauss theorems.
Key-words: Symmetric groups, group actions, Burnside's Lemma, cycle indexes, pattern inventory, Pólya's Enumeration Theorem.

Introduction

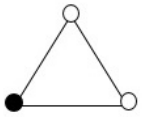
One of the central problems in combinatorics is to find the number of distinct ways in which something can be done. A simple example is to find the number of colorings of the three vertices of a triangle using two colors black and white. Clearly there are $2^3 = 8$ possibilities (see the first row of the following figure).

Suppose that the triangle is not fixed, but moved in the plane by rotations. Two colorings are the same if one can be obtained from the other by rotation, so many of these possibilities are the same and we obtained just four possibilities (see the second row of the following figure).



In passing from the first row to the second in the example, we have treated different ways of painting the triangle as being equivalent, and we have shown one representative from each equivalence class. The problem of computing the number of distinguishable ways in which something can be done is the same as that of computing the number of equivalence classes under an appropriate equivalence relation. The equivalence classes are orbits under the action of an appropriate group. In the example, the group for passing from the first row to the second is the cyclic group C_3 of rotations of the triangle.

Now, we ask a complex question. What if we want to count the number of different colorings with a specific number of vertices of each color? For example how many colorings are there with one vertice is balck and two vertices are white? There is just one coloring with 1 vertice is black and 2 vertices are white.



In 1937, the Hungarian mathematician George Pólya (1887-1985) gave one of the most important theorems in the 20-th century, called "Pólya's Enumeration Theorem", is a theorem in combinatorics that generalizes Burnside's lemma on the number of orbits of a group action on a set. The theorem was first published in 1927 by the American mathematician John Howard Redfield (1879-1944) and in 1937 it was rediscovered by the Hungarian mathematician George Pólya (1887-1985), who then greatly popularized the result by applying it to many counting problems, our simple example is one of them.

In the first chapter, we define a permutation and describe its properties. After that we introduce the four symmetry groups used in Pólya's Enumeration Theorem, the symmetric, cyclic, dihedral and alternating groups and example of symmetries of geometric figures in two and three dimensional spaces. In the second chapter, we introduce the concept of group actions on a set and its concepts like the orbit, the stabilizer, the invariant and describe its properties and give some simple problems in group theory solved by the notion of group action. In the last chapter, we give the Pólya's Enumeration Theorem and use it to solve some counting problems.

Chapter 1

Groups and Symmetry

The group theory is one of central ideas of modern algebra. In this first chapter we give an introduction to group through examples and a connection with symmetry.

1.1 General concepts of group theory

1.1.1 Groups, subgroups and homomorphisms

Definition 1.1 (Group)
A **group** *is a nonempty set G together with one binary operation, generally denoted by juxtaposition, with the following properties:*

1. *(***Closure***) For all $x, y \in G, xy \in G$.*
2. *(***Associative***) For all $x, y, z \in G, (xy)z = x(yz)$.*
3. *(***Identity***) There exists an element $1 \in G$, called the* **identity** *element of the group, for which $x1 = 1x = x$ for all $x \in G$.*
4. *(***Inverse***) For each $x \in G$, there is an element $x^{-1} \in G$, called the* **inverse** *of x, for which $xx^{-1} = x^{-1}x = 1$.*

Two elements $x, y \in G$ commute if $xy = yx$.
A group is **abelian**, *or* **commutative**, *if every pair of elements commute.*
A group is **finite** *if the set G is a finite set; otherwise, it is* **infinite**. *The* **order** *of a group is the cardinality of the set G, denoted by $|G|$.*

Example 1.1 The integers $\mathbb{Z}$ form an abelian group under addition, the identity is 0. The rational numbers $\mathbb{Q}$ form an abelian group under addition and the nonzero rational numbers $\mathbb{Q}^*$ form an abelian group under multiplication. A similar statement holds for the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$.

Example 1.2 The set $\mathcal{M}_{n\times m}(\mathbb{R})$ of all $n\times m$ matrices over $\mathbb{R}$ is an abelian group under addition of matrices. The set $GL_n(\mathbb{R})$ of all $n \times n$ matrices over $\mathbb{R}$ with non-zero determinant is a non abelian group under multiplication. This group is called the ***general linear group***. The set $SL_n(\mathbb{R})$ of all $n \times n$ matrices over $\mathbb{R}$ with determinant equal to 1 is a group under multiplication, called the ***special linear group***.

Example 1.3 Let n be a natural number. The set of integers $mod\ n$ form a group under addition modulo n; that is $\mathbb{Z}_n = \{0, 1, ..., n-1\}$.

Definition 1.2 (Subgroup)
A nonempty subset H of a group G is a **subgroup** *of G, denoted by $H \leq G$, if H is a group under the restricted product on G. If $H \leq G$ and $H \neq G$, we write $H < G$ and say that H is a* **proper subgroup** *of G.*

Example 1.4 $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ is a sequence of subgroups under addition.
The group $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$.

Definition 1.3 (Group homomorphism)
Let G and H be groups. A function $f : G \longrightarrow H$ is called **homomorphism** *if*
$f(xy) = f(x)f(y)$ *for all $x, y \in G$.*
A surjective homomorphism is an **epimorphism**, *which we denoted by $f : G \twoheadrightarrow H$.*
An injective homomorphism is a **monomorphism**, *which we denoted by $f : G \hookrightarrow H$.*
A bijective homomorphism is an **isomorphism**, *which we denoted by $f : G \approx H$.*
A homomorphism of G into itself is an **endomorphism**. *The set of all endomorphism of G is denoted by* End(G).
An isomorphism of G into itself is an **automorphism**. *The set of all automorphisms of G is denoted by* Aut(G).

Example 1.5 The map $f : (\mathbb{Z}, +) \to (\mathbb{Q}^*, \cdot)$ defined by $f(n) = 2^n$ is a homomorphism. Since

$$f(n + m) = 2^{n+m} = 2^n \cdot 2^m = f(n) \cdot f(m)$$

Example 1.6 We can define an isomorphism f from the additive group of real numbers $(\mathbb{R}, +)$ to the multiplicative group of positive real numbers $(\mathbb{R}^*_+, \cdot)$ with the exponential map; that is,

$$f(x + y) = e^{x+y} = e^x e^y = f(x)f(y)$$

Of course, f is also injective and surjective.

1.1.2 Cosets and Lagrange's Theorem

In 1770, Joseph-Louis Lagrange (1736-1813) gives one of the most important results in finite group theory, states that the order of a subgroup must divide the order of the group. This theorem provides a powerful tool for analyzing finite groups; it gives us an idea of exactly what type of subgroups we might expect a fnite group to possess. Central to understanding Lagranges's Theorem is the notion of a coset.

Definition 1.4 (Cosets)
Let $H \leq G$ and $a \in G$. The set $aH = \{ah | h \in H\}$ is called a **left coset** *of H in G. Similarly, the set $Ha = \{ha | h \in H\}$ is called a* **right coset** *of H in G. The set of all left cosets if 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 1.7 Let $H = \{0, 3\}$ be a subgroup of $\mathbb{Z}_6$. The left cosets of H in $\mathbb{Z}_6$ are

$$1 + H = \{1, 4\}$$
$$1 + H = \{1, 4\}$$
$$2 + H = \{2, 5\}$$
$$3 + H = \{0, 3\}$$
$$4 + H = \{1, 4\}$$
$$5 + H = \{2, 5\}$$

Definition 1.5 (Equivalence relation)
Let X be a set. The relation $\sim$ on X is an **equivalence relation** *if it satisfies all of the following:*

(i) (**Reflexivity**) *For all $x \in X, x \sim x$;*

(ii) (**Symmetry**) *For all $x, y \in X$, if $x \sim y$, then $y \sim x$.*

(iii) (**Associativity**) *For all $x, y, z \in X$, if $x \sim y$ and $y \sim z$, then $x \sim z$.*

Definition 1.6 (Equivalence class)
Let $\sim$ be an equivalence relation on a set X. For $x \in X$, the **equivalence class** *of x induced by $\sim$, denoted by $cl(x)$, is the set*

$$cl(x) = \{y \in X | x \sim y\}$$

.

Example 1.8 Let n be a fixed natural number. We define the relation $\sim$ on $\mathbb{Z}$ by:

$$a \sim b \Leftrightarrow a - b \; is \; divisible \; by \; n$$

Then $\sim$ is an equivalence relation and for every $x \in \mathbb{Z}$ we have:

$$cl(x) = x + n\mathbb{Z}$$

.

Proposition 1.1 *Let x and y be two elements of a group G and $H \leq G$. Then*

$$xH = yH \Leftrightarrow y^{-1}x \in H$$

Proof.

- ($\Rightarrow$): Suppose that $xH = yH$. Since $e \in H$, $xe = x \in xH$, and therefore $x \in yH$. So there exists $h \in H$ such that $x = yh$. That is, H contains $h = y^{-1}x$.
- ($\Leftarrow$): Let x and y be two elements of G such that $y^{-1}x \in H$. There exists $h \in H$ such that $y^{-1}x = h$, then there exists $h \in H$ such that $x = yh$.
  Let $z \in xH$; there exists $h' \in H$ such that

  $$z = xh' = (yh)h' = y(hh') = yh"$$

  This implies that $z \in yH$. Likewise, every element in yH is in xH. So $xH = yH$.

Theorem 1.1 *Let H be a subgroup of a group G.*
The number of left cosets of H in G is the same as the number of right cosets of H in G.

Proof. Define a map $f : G/H \to H/G$ by $f(gH) = Hg^{-1}$
We need to show that the map is well defined and bijective.

- f is well define:

$$\begin{aligned} xH = yH &\Rightarrow y^{-1}xH = H \\ &\Rightarrow y^{-1}x \in H \\ &\Rightarrow Hy^{-1}x = H \\ &\Rightarrow Hy^{-1} = Hx^{-1} \\ &\Rightarrow f(xH) = f(yH) \end{aligned}$$

- f is injective: Suppose that $f(xH) = f(yH)$

$$\begin{aligned} f(xH) = f(yH) &\Rightarrow Hx^{-1} = Hy^{-1} \\ &\Rightarrow H = Hy^{-1}x \\ &\Rightarrow y^{-1}x \in H \\ &\Rightarrow xH = yH \end{aligned}$$

- f is surjective: Clearly that f is surjective, because for every $Hy \in H/G$ there is $xH \in G/H$ $(x = y^{-1})$ such that $f(xH) = Hy$

Proposition 1.2 *Let H be a subgroup of a group G and $g \in G$.*
The number of elements in H is the same as the number of elements in gH.

Proof. Let $H = \{h_1, h_2, ..., h_k\}$ and $g \in G$. Then $gH = \{gh_1, gh_2, ..., gh_k\}$. The elements of gH must be distinct, because for $gh_i = gh_j$ imply $h_i = h_j$. Hence, $|gH| = k$

Proposition 1.3 *The left cosets of a subgroup H in a group G constitutes a partition of the group.*

Proof. Let G be a group and H be a subgroup of G. We define a relation $\sim$ in G by:

$$x \sim y \Leftrightarrow x^{-1}y \in H$$

We need to show that $\sim$ is an equivalence relation whose equivalence classes are the left cosets of H in G.

- $\sim$ is reflexive: For every $x \in G$, $x^{-1}x = e \in H$, then $x \sim x$.
- $\sim$ is symmetric: Let $x, y \in G$ such that $x \sim y$. So $x^{-1}y \in H$, then $(x^{-1}y)^{-1} \in H$, so $y^{-1}x \in H$, then $y \sim x$.
- $\sim$ is transitive: Let $x, y, z \in G$ such that $x \sim y$ and $y \sim z$. So $x^{-1}y \in H$ and $y^{-1}z \in H$, then $x^{-1}yy^{-1}z \in H$, then $x^{-1}z \in H$, then $x \sim z$.

Now, we show that for every $x \in G$ we have $cl(x) = xH$.

- Let $y \in cl(x)$. Then

$$\begin{aligned} y \in cl(x) &\Rightarrow x^{-1}y \in H \\ &\Rightarrow x(x^{-1}y) \in xH \\ &\Rightarrow y \in xH \\ &\Rightarrow cl(x) \subseteq xH \end{aligned}$$

- Let $y \in xH$. Then

$$\begin{aligned} y \in xH &\Rightarrow y = xh \; for \; some \; h \in H \\ &\Rightarrow x^{-1}y = h \in H \\ &\Rightarrow x \sim y \\ &\Rightarrow y \in cl(x) \\ &\Rightarrow xH \subseteq cl(x) \end{aligned}$$

Definition 1.7 (Index of a subgroup)
Let G be a group, The **index** *of $H \leq G$ is the cardinality of the set G/H, denoted by $[G : H]$.*

Example 1.9 Let $G = \mathbb{Z}_6$ and $H = \{0, 3\}$. Then $[G : H] = 3$.

Example 1.10 Let n be a fixed natural number. The index of the subgroup $n\mathbb{Z}$ on the group $\mathbb{Z}$ under addition is n.

Theorem 1.2 (Lagrange's Theorem)
The order of any subgroup of a finite group divides the order of the group.

Proof. Let G be a group of order n and $H \leq G$ of order k, have r distinct left cosets. From proposition 1.1 and proposition 1.3 we have:

$$\begin{aligned} n &= |G| \\ &= |\bigcup_{i=1}^{r} g_i H| \\ &= \sum_{i=1}^{r} |g_i H| \\ &= \sum_{i=1}^{r} k \\ &= rk \end{aligned}$$

So, $|G|$ is divisible by $|H|$.

Corollary 1.1 *Let g be an element of a finite group G. Then the order of g divides the order of G.*

Remark 1.1 *The converse of Lagrange's Theorem is false. I mean that if a natrual number m divides the order of a group G, we are not guaranteed that G has a subgroup of arder m.*

1.2 Symmetry groups

In 1878, the British mathematician Arthur Cayley (1821-1895) shows that the symmetric groups form such an important class of groups: in a sense, if we understand the symmetric groups completely, then we understand all groups. We now produce an important class of groups.

Definition 1.8 (Permutation)
A **permutation** *of a nonempty set X is a bijective function on X. The set of all permutations of X is denoted by S_X.*

Lemma 1.1 *Let X be a set and σ_1 and σ_2 be two permutations of X.*
The composition of σ_1 and σ_2 is a permutation of X and The inverse of σ_1 is a permutation of X.

Theorem 1.3 *The set S_X form a group under the composition of permutations called the* **permutation group** *of X. If X is the set of the first n natural numbers, the permutation group of X is called* **symmetric group** *and denoted by S_n.*

Proof. It follows from Lemma 1.1 that the composition of two permutation is a permutation and the inverse of a permutation is a permutation; So S_X is closed under composition and closed under inverses. The composition of functions is always associative, and the identity of S_X is the identity bijection of X. Therefore, $(S_X, \circ)$ satisfies all the axioms for a group.

Theorem 1.4 (Cayley's Theorem)
Every group is isomorphic to a group of permutations.

Corollary 1.2 *If G is a finite group of order n, then G is isomorphic to a subgroup of S_n.*

How to represent a permutation? There are two ways to represent $\sigma \in S_n$.
The first is by a matrix of type $2 \times n$, that is

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

The second way is called the *cycle notation*, if $a_1, a_2, ..., a_k$ are distinct elements of the set $\{1, 2, ..., n\}$, the permutation σ, defined by

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

and $\sigma(a) = a$ for all $a \notin \{a_1, a_2, ..., a_k\}$, is called a ***cycle*** of length r or an ***r-cycle***, we denoted it by $(a_1\ a_2\ ...\ a_k)$.
A 2-cycle is called **transposition**.

Proposition 1.4 *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 $\{1, 2, \cdots, n\}$ 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

$$|S_n| = n \cdot (n-1) \cdot (n-2) \cdot (n-3) \cdots 2 \cdot 1 = n!$$

Definition 1.9 (Disjoint cycles)
Two cycles $\sigma = (a_1\ a_2\ ...\ a_k)$ and $\alpha = (b_1\ b_2\ ...\ b_m)$ are **disjoint** *if $a_i \neq b_j$ for all i, j.*

Theorem 1.5 (Cycle decomposition)
Every permutation σ in S_n is a product of disjoint cycles. This product is unique and called the **cycle decomposition** *of σ.*

How to decompose a permutation to a cycles? *Let $X = \{1, 2, ..., n\}$ and $\sigma \in S_n$. The following algorithm produces this representation:*

1. *Choose an element $i \in X$ (usually $i = 1$). Find the image of i under the mapping σ, then the image of the image, then ..., until we obtain j such that $\sigma(j) = i$. Thus the cycle $(i...j)$ has been generated.*

2. *Choose the smalest element of X not found in any one of the cycles already generated. Go back to the step 1 and use this element as element i is step 1.*

3. *Repeat step 2 until X has been exhauted.*

Example 1.11 Let us factor $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 1 & 2 & 5 & 3 & 8 & 9 & 7 \end{pmatrix}$ into a product of disjoint cycles.
$\sigma(1) = 6$, so σ is begin by (1 6; $\sigma(6) = 3$, σ continues $(1\ 6\ 3$; since $\sigma(3) = 1$, the parentheses close, and σ is begin by the cycle $(1\ 6\ 3)$. The smallest integer not having appeared is 2; write $(1\ 6\ 3)(2$, $\sigma(2) = 4$, then $(1\ 6\ 3)(2\ 4$; continuing is this way, we obtained

$$\sigma = (1\ 6\ 3)(2\ 4)(5)(7\ 8\ 9)$$

Corollary 1.3 *Every permutation σ in S_n is a product of transpositions.*

Definition 1.10 (Order of permutation)
Let σ be an element of S_n. The order of σ is the least common multiple of the lengths of its disjoint cycles.

Example 1.12 Find the order of the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 8 & 7 & 1 & 4 & 6 & 2 \end{pmatrix}$$

Solution: We can write this permutation in terms of disjoint cycles as

$$\sigma = (1\ 3\ 8\ 2\ 5)(4\ 7\ 6)$$

So, the order of σ is $lcm(5, 3) = 15$. Of course, we could calculate $\sigma^2, \sigma^3, \sigma^4, ...$ until we obtained the identity, but this would take much longer.

Definition 1.11 (Cycle type)
Let σ be any element of S_n. The **cycle type** *of σ is the vector $(k_1, k_2, ..., k_n)$ such that k_i is the number of i-cycles in the cycle decomposition of σ.*

Example 1.13 Find the cycle type of the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 1 & 2 & 5 & 3 & 8 & 9 & 7 \end{pmatrix}$$

Solution: From example 1.11, we can write this permutation in terms of disjoint cycles as $\sigma = (1\ 6\ 3)(2\ 4)(5)(7\ 8\ 9)$. So, the cycle type of σ is $(1, 1, 2, 0, 0, 0, 0, 0, 0)$.

Definition 1.12 (Cycle index)
Let G be a group of permutations and $\sigma \in G$. The **cycle index** *of σ, denoted by $cyc(\sigma)$, is the number of cycles in the cycle decomposition of σ.*

Definition 1.13 (Parity of permutation)
A permutation is **even** *or* **odd** *if it can be expressed as a product of an even or odd number of transpositions respectively.*

Example 1.14 It is easy to see that the cycle $\sigma = (123)$ is even, for there is a factorization $\sigma = (13)(12)$ into two transpositions.

Lemma 1.2 *Let $\sigma \in S_n$ be a permutation.*
Then σ is not both an even and an odd permutation.

1.3 Symmetries of geometric figures

One important source of groups is as symmetries of geometric figures, these symmetry groups play a crucial role in the application of modern algebra to physics and chemistry. In this section we introduce the finite symmetry groups in two and three dimensional spaces.

1.3.1 Symmetries in two dimensions

There are two families of groups that appear repeatedly in many combinatorial problems. The first is the cyclic group of order n and the second is the nth dihedral group.

Definition 1.14 (Cyclic group)
Let n be a natural number. The **cyclic group** *of order n, denoted by C_n, is the set of all rotations of a regular n-gon.*

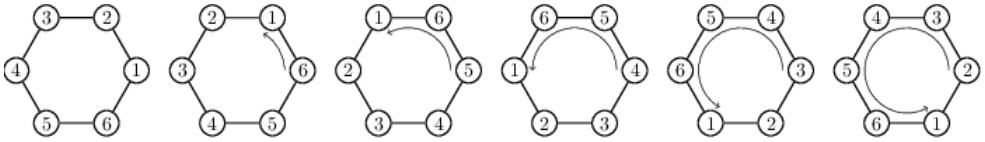


Figure 1.1: The cyclic group C_6

Example 1.15 Find the group of rotations of the hexagon.
Solution: All 6 possible rotations of the hexagon are listed in Figure 1.1 below

Definition 1.15 (Dihedral group)
Let n be a natural number. The n-th **dihedral group**, *denoted by D_n, is the set of all rotations and reflexive symmetries of a regular n-gon, its order is $2n$.*

Example 1.16 Find the group of symmeties of the hexagon.
Solution: All 12 possible symmetries of the hexagon are listed in Figure 1.2 below

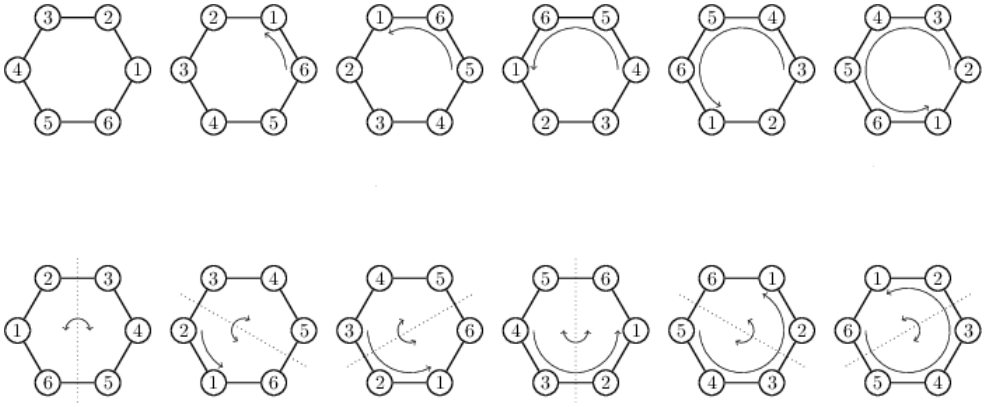


Figure 1.2: Dihedral group D_6

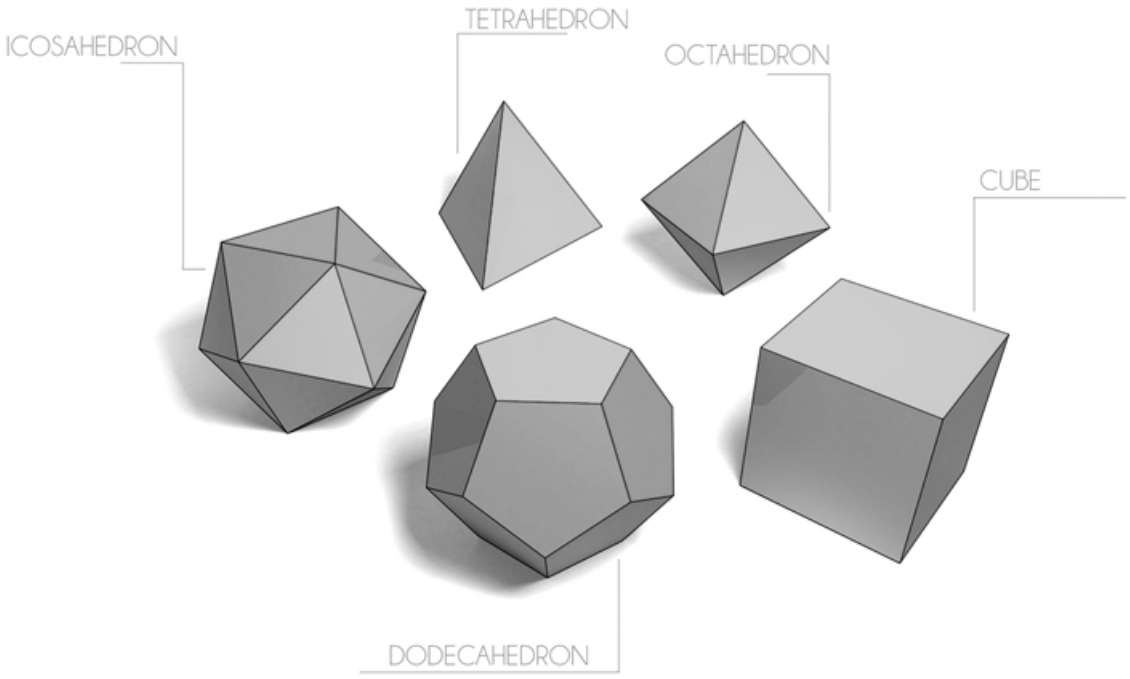
Theorem 1.6 (7) *The symmetry group of any finite plane figure is either a cyclic group C_n or a dihedral group D_n.*

1.3.2 Symmetries in three dimensions

We turm now to three-dimensional figures. One class of symmetries that we know occurs in three dimensions is the class of rotation groups of the regular solids: the tetrahedron, cube, octahedron, dodecahedron, and icosahedron. In this subsection we produce this solids and its rotation groups.

Definition 1.16 (Regular solid)
A **regular solid** *is a polyhedron in which all faces are congruent regular polygons and all vertices are incident with the same number of faces.*

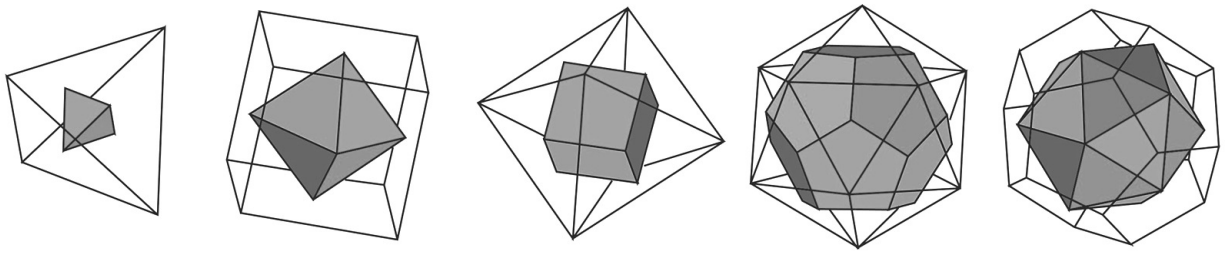
Lemma 1.3 *There are exactly five platonic solids. These are tetrahedron, cube, octahedron, dodecahedron and icosahedron.*



Polyhedron	Number of Vertices	Number of Edges	Number of Faces	Faces	Number of Faces at Each Vertex
Tetrahedron	4	6	4	Triangles	3
Cube	8	12	6	Squares	3
Octahedron	6	12	8	Triangles	4
Dodecahedron	20	30	12	Pentagons	3
Icosahedron	12	30	20	Triangles	5

Definition 1.17 (Dual polyhedron)
For any polyhedron, we can construct its **dual polyhedron** *in the following way. The vertices of the dual are the centers of the faces of the original polyhedron. Two centers are joined by an edge if the corresponding faces meet in an edge*

The dual of a regular tetrahedron is another regular tetrahedron. The cube and octahedron are duals of each other. The dodecahedron and icosahedron are also duals of each other.



Lemma 1.4 *Dual polyhedra have the same symmetry group.*

We now produce the rotation groups of the regular solids, but after lemma 1.5, we give just the rotation groups of tetrahedron, cube and dodecahedron.

Definition 1.18 (Alternating group)
Let n be a natural number. The **Alternating group**, *denoted by A_n, is a subgroup of S_n contain all even permutations.*

Example 1.17 Find the elements of A_3.
Solution: The symmetric group S_3 has 6 elements, the following table gives the parity of these elements *:*

	permutation	*produit of transpositions*	*number of transpositions*	*the parity*
i	$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$		*0*	*even*
σ_1	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$(2\ 3)$	*1*	*odd*
σ_2	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$(1\ 2)$	*1*	*odd*
σ_3	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$(2\ 3)(1\ 2)$	*2*	*even*
σ_4	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$(1\ 2)(2\ 3)$	*2*	*even*
σ_5	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$(1\ 3)$	*1*	*odd*

So, $A_3 = \{i, \sigma_3, \sigma_4\}$.

Proposition 1.5 *If* $n \geq 2$, *then* $|A_n| = \dfrac{n!}{2}$.

Theorem 1.7

- *The group of rotations of a regular tetrahedron is isomorphic to* A_4.
- *The group of rotations of a cude is isomorphic to* S_4.
- *The group of rotations of a regular dodecahedron is isomorphic to* A_5.

Theorem 1.8 *The group of rotations of any finite three-dimensional figure is isomorphic to one of*

$$C_n\ (n \geq 1), D_n\ (n \geq 2), A_4, S_4 \text{ or } A_5$$

.

Chapter 2

Group actions on a set

In this chapter we introduce the concept of an action of a group G on a non-empty set X and study such actions.

2.1 Group actions and representation map

In this section we give the notion of an action of a group G on a nonempty set X.

Definition 2.1 (The action)
An **action** *of a group G on a nonempty set X is a function $f : G \times X \longrightarrow X$, denoted by $(g, x) \longmapsto g \cdot x$ for all $g \in G$, $x \in X$ such that:*

(i) for any $x \in X$, $1 \cdot x = x$, where 1 is the identity of G;

(ii) for any $x \in X$, $g_1, g_2 \in G$, $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$.

Under these conditions X is said to be a G-set.

Definition 2.2 (Representation map)
Let G be a group and X a nonempty set. The group G is said to be **acts** *on the set X if there is a morphism λ from G to S_X. The morphism $\lambda : G \longrightarrow S_X$ is called the* **representation map** *of G on X.*

Proposition 2.1 *The action of a group G on a set X is equivalente to a group homomorphism from G to S_X the group of all permutations on X.*

Proof. Let G be a group acts on a set X. Define a map $\lambda_g : X \to X$ by $\lambda_g(x) = g \cdot x$, and we show that λ_g is a permutation for all $g \in G$.

- Clearly that for every element $y \in X$, there is an element $x \in X$ ($x = g^{-1} \cdot y$) such that $\lambda_g(x) = y$.

$$\begin{aligned} \lambda_g(x) &= \lambda_g(g^{-1} \cdot y) \\ &= g \cdot (g^{-1} \cdot y) \\ &= (gg^{-1})y \\ &= 1 \cdot y \\ &= y \end{aligned}$$

  Then λ_g is surjective.

- Let $x, y \in X$ such that $\lambda_g(x) = \lambda_g(y)$.

$$\begin{aligned} \lambda_g(x) = \lambda_g(y) &\Rightarrow g^{-1} \cdot \lambda_g(x) = g^{-1} \cdot \lambda_g(y) \\ &\Rightarrow g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g \cdot y) \\ &\Rightarrow (g^{-1}g) \cdot x = (g^{-1}g) \cdot y \\ &\Rightarrow 1 \cdot x = 1 \cdot y \\ &\Rightarrow x = y \end{aligned}$$

Then λ_g is injective.
Now we show that the map $\lambda : G \to S_X$ defined by $\lambda(g) = \lambda_g$ is a group homomorphism. For all $g, h \in G$ and $x \in X$, we have

$$\begin{aligned} (\lambda_g \circ \lambda_h)(x) &= \lambda_g(\lambda_h(x)) \\ &= \lambda_g(h \cdot x) \\ &= g \cdot (h \cdot x) \\ &= (gh) \cdot x \\ &= \lambda_{gh}(x) \end{aligned}$$

So, λ is a group homomorphism.
Let λ be a group homomorphism from G to S_X. We can define an action of G on X by $g \cdot x = \lambda(g)(x)$ for all $g \in G$ and $x \in X$.

- $g \cdot (h \cdot x) = g \cdot (\lambda(h)(x)) = \lambda(g)(\lambda(h)(x)) = (\lambda(g) \circ \lambda(h))(x) = \lambda(gh)(x) = (gh) \cdot x$
- $1 \cdot x = \lambda(1)(x) = Id_X(x) = x$.

Then $g \cdot x = \lambda(g)(x)$ define an action of G on X.

Example 2.1 Let G be a group. Then G acts on itself by left multiplication.
If $x \in G$ and e the identity element, then $ex = x$. If $g_1, g_2 \in G$ and $x \in G$, then $(g_1g_2)x = g_1(g_2x)$ because the multiplication is associative.

Example 2.2 Let $G = GL_2(\mathbb{R})$ the set of all 2×2 invertible matrices and $X = \mathbb{R}^2$. Then G acts on X by left multiplication. If $u \in \mathbb{R}^2$ and I the identity matrix, then $Iu = u$. If A and B are 2×2 invertible matrices, then $(AB)u = A(Bu)$ since matrix multiplication is associative.

Example 2.3 Let G be a group and H a sub group of G. Then G is an H-set under the conjugation, we can define an action of H on G by:

$$(h, g) \longrightarrow hgh^{-1}$$

for $h \in H$ and $g \in G$. Clearly, the first axiom is satisfied. Observing that

$$(h_1h_2, g) = h_1h_2g(h_1h_2)^{-1} = h_1(h_2gh_2^{-1})h_1^{-1} = (h_1, (h_2, g))$$

we see that the second condition is also satisfied.

Example 2.4 Let $G = D_4$, the symmetry group of a square and $X = \{1, 2, 3, 4\}$ the set of vertices of the square. D_4 consist of the following permutations:

$$\{(1), (13), (24), (1432), (1234), (12)(34), (14)(23), (13)(24)\}$$

The elements of D_4 act on X as functions. For example, the permutation $(13)(24)$ acts on vertex 1 by sending it to vertex 3, on vertex 2 by sending it to vertex 4, and so on. It is easy to see that the axioms of a group action are satisfied.
In general, if X be a nonempty set and G a subgroup of S_X. then X is a G-set under the group action $(\sigma, x) \longrightarrow \sigma(x)$ *for* $\sigma \in G$ *and* $x \in X$.

Example 2.5 Let H be a subgroup of G and G/H the set of all left cosets of H in G. The set G/H is a G-set under the action $(g, aH) \longrightarrow gaH$ for $g \in G$ and $aH \in G/H$. Again, it is easy to see that the first axiom is true. Since $(g_1g_2)aH = g_1(g_2aH)$, the second axiom is also true.

Remark 2.1

1. *In general* $g_1x = g_2x \nRightarrow g_1 = g_2$.
   For example in the actions of S_4 *on the set* $\{1, 2, 3, 4\}$, *let* $\sigma_1 = (12)$ *and* $\sigma_2 = (13)$. *We have* $\sigma_1(4) = 4 = \sigma_2(4)$ *but* $\sigma_1 \neq \sigma_2$.

2. *If* H *is a subgroup of* G *and* G *acts on* X, *then* H *acts on* X *(by the same action).*

2.2 Orbit and stabilizer

We now proceed to develop the theory of groups actions, introducing the fundamental concepts of orbit and stabilizer.

Definition 2.3 (Orbit)
Let X be a G-set and $x \in X$. The **orbit** *of x, denoted by $\mathcal{O}_x$, is the set*

$$\mathcal{O}_x = \{gx | g \in G\}$$

The set of all the orbits is called **orbit space** *and denoted by X/G.*

Example 2.6 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 and the orbits are $\mathcal{O}_1 = \mathcal{O}_2 = \mathcal{O}_3 = \{1, 2, 3\}$ and $\mathcal{O}_4 = \mathcal{O}_5 = \{4, 5\}$.

Proposition 2.2 *Let X be a G-set.*
The orbits form a partition of X.

Proof. Define the relation $\sim$ in X by:

$$x \sim y \; if \; and \; only \; if \; y = gx \; for \; some \; g \in G$$

We proved that the relation $\sim$ is an equivalence relation whose equivalence classes are the orbits.

- $\sim$ is reflexive: For each $x \in X$, $ex = x$. then $x \sim x$.
- $\sim$ is symmetric: Let $x, y \in X$ such that $x \sim Y$. So $y = gx$ for some $g \in G$, then $x = g^{-1}y$, then $y \sim x$.
- $\sim$ is transitive: Let $x, y, z \in X$ such that $x \sim Y$ and $y \sim z$. There exists $g, h \in G$ such that $y = gx$ and $z = hy$, then $z = h(gx) = (gh)x$, then $x \sim z$.

For each $x \in X$ we have:

$$\begin{aligned} cl(x) &= \{y \in X / y \sim x\} \\ &= \{y \in X / y = gx \; where \; g \in G\} \\ &= \{gx / g \in G\} \\ &= \mathcal{O}_x \end{aligned}$$

Definition 2.4 (Stabilizer)
Let X be a G-set and $x \in X$. The **stabilizer** *of x, denoted by $Stab(x)$, is the set*

$$\{g \in G | gx = x\}$$

Example 2.7 Let $X = \{1, 2, 3, 4, 5, 6\}$ and suppose that G is the permutation group given by the permutations

$$\begin{aligned} e &= \quad (1)(2)(3)(4)(5)(6) \\ \sigma_1 &= \quad (12)(3456) \\ \sigma_2 &= \quad (1)(2)(35)(46) \\ \sigma_3 &= \quad (12)(3654) \end{aligned}$$

Find the stabilizer of each element in X under the action of G on X.
Solution: The Stabilizers are given in the following table:

The elements	*The stabilizers*
1	$\{e, \sigma_2\}$
2	$\{e, \sigma_2\}$
3	$\{e\}$
4	$\{e\}$
5	$\{e\}$
6	$\{e\}$

Proposition 2.3 *Let X be a G-set. For every $x \in X$, the stabilizer of x is a sub group 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 $g_1 x = x$ and $g_2 x = x$. So $(g_1 g_2)x = g_1(g_2 x) = g_1 x = x$; hence, the product of two elements in $Stab(x)$ is also in $Stab(x)$. Finally, if $g \in Stab(x)$, then
$x = ex = (g^{-1}g)x = g^{-1}(gx) = g^{-1}x$. So $g^{-1}x$ is in $Stab(x)$.

Lemma 2.1 *Let X be a G-set and $x, y \in X$. If $y = gx$ for some $g \in G$, then $Stab(x)$ is isomorphic to $Stab(y)$. In particular, $|Stab(x)| = |Stab(y)|$.*

Proof. Let X be a G-set and suppose that $y = gx$.
We can define a map $f : Stab(x) \to Stab(y)$ by $f(a) = gag^{-1}$.
The map f is a homomorphism since

$$f(ab) = gabg^{-1} = gaebg^{-1} = gag^{-1}gbg^{-1} = f(a)f(b).$$

Let $a, b \in Stab(x)$. Suppose that $f(a) = f(b)$. Then $gag^{-1} = gbg^{-1}$, so $a = b$; hence, the map is injective.
Let $b \in stab(y)$. Then $by = y \Rightarrow bgx = gx \Rightarrow g^{-1}bgx = x$, so $g^{-1}bg \in Stab(x)$ and $f(g^{-1}bg) = b$; hence, the map is surjective.

Definition 2.5 (Kernel of an action)
Let G be a group and X be a set. The **kernel** *of the action of G on X is the kernel of the homomorphism $\lambda : G \longrightarrow S_X$, denoted by $Ker(\lambda)$.*

Theorem 2.1 *The kernel of an action $\lambda : G \longrightarrow S_X$ is the intersection of stabilizers of all elements of X,*

$$Ker(\lambda) = \bigcap_{x \in X} Stab(x)$$

Proof. Let G be a group acts on a set X and λ be the representation map. Let g be an element of $Ker(\lambda)$. Then

$$\begin{aligned} g \in Ker(\lambda) &\Leftrightarrow \lambda(g) = Id_X \\ &\Leftrightarrow \lambda(g)(x) = Id_X \; for \; all \; x \in X \\ &\Leftrightarrow \lambda(g)(x) = x \; for \; all \; x \in X \\ &\Leftrightarrow g \cdot x = x \; for \; all \; x \in X \\ &\Leftrightarrow g \in Stab(x) \; for \; all \; x \in X \\ &\Leftrightarrow g \in \bigcap_{x \in X} Stab(x) \end{aligned}$$

Now we give an important connection between the number of elements in the orbit of a point x and the stabilizer of that point.

Theorem 2.2 (Orbit-Stabilizer Theorem)
Let G be a group acts on a set X. For each $x \in X$,

$$|G| = |Stab(x)||\mathcal{O}_x|$$

Proof. We know that for every $x \in X$, the $Stab(x)$ is a subgroup of G, our plan is to produce a bijection between $\mathcal{O}_x$ and the set $G/Stab(x)$ of all left cosets of $Stab(x)$. Let $u \in \mathcal{O}_x$; i.e., $u = gx$ for some $g \in G$. Consider the map $f : \mathcal{O}_x \longrightarrow G/Stab(x)$ defined by $u \mapsto gStab(x)$.

- f is surjective. If $gStab(x) \in G/Stab(x)$, we have $gx = y$ ($y \in \mathcal{O}_x$). So, for each $gStab(x) \in G/Stab(x)$, there exists $y \in \mathcal{O}_x$ ($y = gx$) such that $f(y) = gStab(x)$.
- f is injective. Let u and v be two elements of $\mathcal{O}_x$: $u = gx$ and $v = hx$, for $g, h \in G$. Soppose that $f(u) = f(v)$, $f(gx) = f(hx)$, $gStab(x) = hStab(x)$.
  Then $h^{-1}g \in Stab(x)$, which implies

$$(h^{-1}g)x = x \Rightarrow h^{-1}(gx) = x \Rightarrow gx = hx \Rightarrow u = v$$

So, for avery $x \in X$ we have $|\mathcal{O}_x| = |G/Stab(x)|$, and because $|G/Stab(x)| = \frac{|G|}{|Stab(x)|}$, then $|\mathcal{O}_x| = \frac{|G|}{|Stab(x)|}$, which implies $|G| = |Stab(x)||\mathcal{O}_x|$

Theorem 2.3 (Class Formula)
Let X be a finite G-set. Then

$$|X| = \sum_{x \in X} \frac{|G|}{|Stab(x)|}$$

Proof. The orbits form a partition of X, so $X = \bigcup_{x \in X} \mathcal{O}_x$, then $|X| = \sum_{x \in X} |\mathcal{O}_x|$. From theorem 2.2 $|\mathcal{O}_x| = \frac{|G|}{|Stab(x)|}$, then $|X| = \sum_{x \in X} \frac{|G|}{|Stab(x)|}$.

Definition 2.6 (Invariant)
Let G be a group acts on a set X and $g \in G$. The **invariant** *of g, denoted by $Fix(g)$, is the set of all elements of X fixed by g, that is*

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

Example 2.8 Let $X = \{1, 2, 3, 4, 5, 6\}$ and suppose that G is the permutation group given by the permutations

$$\begin{aligned} e &= (1)(2)(3)(4)(5)(6) \\ \sigma_1 &= (12)(3456) \\ \sigma_2 &= (1)(2)(35)(46) \\ \sigma_3 &= (12)(3654) \end{aligned}$$

Find the invariant of each permutation under the action of G on X.
Solution: The invariants are given in the following table:

The permutations	*The invariants*
e	X
σ_1	$\emptyset$
σ_2	$\{1, 2\}$
σ_3	$\emptyset$

Remark 2.2 *It is important to remember that $Fix(g) \subset X$ and $Stab(x) \subset G$.*

Lemma 2.2 (Burnside)
The number of orbits under the action of a finite group G on a finite set X is

$$\frac{1}{|G|} \sum_{g \in G} |Fix(g)|$$

Proof. We count the set $S = \{(g, x) \in G \times X | g.x = x\}$ in two different ways. The set S contains all pairs (g, x) such that $g.x = x$. We recall that the set $Fix(g)$ for each fixed $g \in G$ contains all $x \in X$ such that $g.x = x$. Thus, for each fixed $g \in G$, there are $|Fix(g)|$ elements such that $g.x = x$, so

$$|S| = \sum_{g \in G} |Fix(g)|$$

The stabilizer $St(x)$ contains all $g \in G$ such that $g.x = x$. So, for every fixed $x \in X$, there are $|Stab(x)|$ elements such that $g.x = x$, so

$$|S| = \sum_{x \in X} |Stab(x)|$$

From the theorem 2.2, we have

$$\sum_{x \in X} |Stab(x)| = \sum_{x \in X} \frac{|G|}{|\mathcal{O}_x|} = |G| \sum_{x \in X} \frac{1}{|\mathcal{O}_x|}$$

let $\mathcal{O}_1, \mathcal{O}_2, ..., \mathcal{O}_k$ denote all orbits in X. For every $x \in X$ we have $\mathcal{O}_x = \mathcal{O}_i$ for some $i \in \{1, 2, ..., k\}$. The orbits form a partition of X, so $X = \cup_{i=1}^{k} \mathcal{O}_i$ and $\mathcal{O}_i \cap \mathcal{O}_j = \emptyset$ for $i \neq j$, we obtain:

$$\sum_{x \in X} \frac{1}{|\mathcal{O}_x|} = \sum_{x \in \mathcal{O}_1} \frac{1}{|\mathcal{O}_1|} + \sum_{x \in \mathcal{O}_2} \frac{1}{|\mathcal{O}_2|} + ... + \sum_{x \in \mathcal{O}_k} \frac{1}{|\mathcal{O}_k|}$$

But for each $i \in \{1, 2, ..., k\}$

$$\sum_{x \in \mathcal{O}_i} \frac{1}{|\mathcal{O}_i|} = |\mathcal{O}_i| \times \frac{1}{|\mathcal{O}_i|} = 1,$$

and therefore

$$|S| = |G| \sum_{x \in X} \frac{1}{|\mathcal{O}_x|} = |G|(1 + 1 + ... + 1) = k \times |G|.$$

In the beginning of the proof we also found that $|S| = \sum_{g \in G} |Fix(g)|$, we obtain the Burnside's Lemma, which is

$$k = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|$$

Example 2.9 Let $X = \{1, 2, 3, 4, 5, 6, 7\}$ and $G = C_7$. Find the number of orbits under the action of G on X.

Solution: Every element of X is invariant under the identity, so $|Inv(e)| = 7$. If $\sigma \in C_7$ and $\sigma \neq e$, then every element of X is moved by σ, $|Inv(\sigma)| = 0$ for all $\sigma \in G$ such that $\sigma \neq e$. From the Burside's lemma we obtain the number of orbits is

$$\frac{1}{|C_7|} \sum_{\sigma \in C_7} |Inv(\sigma)|$$

$$= \frac{1}{|7|}(7 + 0 + 0 + 0 + 0 + 0 + 0) = 1$$

Remark 2.3 *In general, for every natural number n, there is exactly one orbit under the action of C_n on the set $\{1, 2, ..., n\}$*

Example 2.10 *let $X = \{1, 2, 3, 4\}$ and $G = \{e, \sigma_1, \sigma_2, \sigma_3\}$ where*

$$e = (1)(2)(3)(4), \quad \sigma_1 = (1, 2)(3)(4),$$

$$\sigma_2 = (1)(2)(3, 4), \quad \sigma_3 = (1, 2)(3, 4).$$

Find the number of orbits of G.
Solution: The set of invariants for each permutation is precisely the set of fixed points in each permutation. So,

$$|Inv(e)| = |1, 2, 3, 4| = 4, \quad |Inv(\sigma_1)| = |1, 2| = 2,$$

$$|Inv(\sigma_2)| = |3, 4| = 2, \quad |Inv(\sigma_3)| = |\emptyset| = 0.$$

Burnside's Lemma gives the number of orbits:

$$\frac{1}{|G|} \sum_{\sigma \in G} |Inv(\sigma)|$$

$$= \frac{1}{|4|}(4 + 2 + 2 + 0) = 2$$

There are two orbits in the above example. The first orbit is $\{1, 2\}$ and the second orbit is $\{3, 4\}$.

2.3 Types of actions

Definition 2.7 (Transitive action)
An action of a group G on a set X is said to be **transitive** *if it has only one orbit.*

Example 2.11 *Any group G acts transitively on itself by left multiplication, because $\mathcal{O}_e = \{ge / g \in G\} = G$.*

Example 2.12 *Let G be a group and H a subgroup of G. Then G acts on the set G/H of left cosets of H in G by left multiplication $g(aH) = (ga)H$. This action is transitive.*

Example 2.13 *The action of the cyclic group C_n on the set $X = \{1, 2, \cdots, n\}$ is transitive.*

Proposition 2.4 *An action of a group G on a set X is transitive if and only if for any x and y in X, there is some $g \in G$ such that $y = g \cdot x$.*

Proof. Let X be a G-set.

($\Rightarrow$): Suppose that the action is transitive, so there is one orbit. For any $x \in X$, its orbit is X, so every element $y \in X$ has the form $g \cdot x$ for some $g \in G$.

($\Leftarrow$): Converselysuppose that for any $x, y \in X$ we can write $y = g \cdot x$ for some $g \in G$. Fix $x \in X$. Beacuse every $y \in X$ has the form $g \cdot x$ for some $g \in G$, every y is in the orbit of x. Thus X has only one orbit.

Corollary 2.1 *If G acts transitively on X, then $|X|$ devide $|G|$.*

Definition 2.8 (Faithful action)
The action of G on X is called **faithful** *if its kernel is trivial.*

Example 2.14 *The action of a group G on itself by left multiplication is faithful.*

Example 2.15 *The action of the symmetric group S_n on the set $\{1, 2, \cdots, n\}$ is faithful.*

Proposition 2.5
An action of G on X is faithful if and only if the homomorphism $\lambda : G \longrightarrow S_X$ is injective.

Proof. Let G be a group acts on a set X.

($\Rightarrow$): Suppose that the action is faithful, so $Ker(\lambda) = e$. Let $x, y \in G$ such that $\lambda(x) = \lambda(y)$. we have

$$\begin{aligned} \lambda(x)\lambda^{-1}(x) = e &\Rightarrow \lambda(y)\lambda(x^{-1}) = e \\ &\Rightarrow \lambda(yx^{-1}) = e \\ &\Rightarrow yx^{-1} \in Ker(\lambda) \\ &\Rightarrow yx^{-1} = e \\ &\Rightarrow y = x \end{aligned}$$

Then the homomorphism λ is injective.

($\Leftarrow$): Suppose that λ is injective. Let $g \in Ker(\lambda)$. So $\lambda(g) = e = \lambda(e)$, then $g = e_G$, so the kernel of λ is trivial, then the action is faithful.

Theorem 2.4 (Every action induces a faithful action)
Let $\lambda : G \longrightarrow S_X$ be the representation map of the action of G on X. There is a faithful action given by the representation map $\bar{\lambda} : G/ker\lambda \longrightarrow S_X$ defined by $\bar{\lambda}(\bar{g}) = \lambda(g)$.

Proof. Let $\lambda : G \longrightarrow S_X$ be the representation map of the action of G on X. From The First Isomorphism Theorem, There is a momomorphism $\bar{\lambda}$ from $G/Ker(\lambda)$ to S_X defined by $\bar{\lambda}(\bar{g}) = \lambda(g)$, so we define a new faithful action.

Definition 2.9 (Free action)
Let X be a G-set. The action of G on X is said to be **free** *if for every $x \in X$, $Stab(x) = \{e\}$, where e is the identity of G.*

Example 2.16 *The action of a group G on itselt by left multiplication is free.*

Example 2.17 *The action of a group G on itselt by conjugation is not free.*

Definition 2.10 (Regular action)
Let X be a G-set. The action of G on X is **regular** *if it is transitive and free. In this case, we also say that G is* **regular** *on X.*

Example 2.18 *The action of a group G on itselt by left multiplication is regular.*

2.4 Some applications

In this final section we give some proofs in group theory used the theory of group actions. Particularly, in the next chapter, we use group actions to solve some counting problems.

Proof of Cayley's Representation.
Let G be a group. Consider the action of G on it self by left multiplication. From the example 2.14 this action is faithful, so the homomorphism $\lambda : G \to S_G$ is injective, then G is isomorphic to $\lambda(G)$, where $\lambda(G)$ is a subgroup of S_G.

Proof of Lagrange's Theorem.
Let G be a finite group and H be a subgroup of G. We know that G acts on itself by left multiplication, we can restrict this action to the subgroup H.
From the class formula, we have

$$|G| = \sum_{x \in G} \frac{|H|}{|Stab(x)|}$$

But this action is free, so the stabilizer of any element in G is trivial, then

$$|Stab(x)| = 1 \; for \; all \; x \in G$$

So,

$$\begin{aligned} |G| &= \sum_{x \in G} |H| \\ &= k \times |H| \end{aligned}$$

Then, the order of H divide the order of G

The center of a p-group is not trivial.
Let G be a group action of a set X. Define the set X^G by

$$X^G = \{x \in X / \mathcal{O}_x = \{x\}\}$$

From the class formula, we have

$$|X| = |X^G| + \sum_{|\mathcal{O}_x \geq 2|} \frac{|G|}{Stab(x)}$$

Proposition 2.6 *Let G be a p-group (i.e. $|G| = p^\alpha$) acts on a set X. Then*

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

Proof. Let G be a p-group acts on a set X. Suppose that $\mathcal{O}_x$ an orbit has at last two elements.

$$|\mathcal{O}_x| = \frac{|G|}{|Stab(x)|}$$

$|Stab(x)|$ divise $|G|$, then $|Stab(x)| = p^\beta$ where $0 \leq \beta < \alpha$.
So, $|\mathcal{O}_x| = p^{\alpha-\beta}$, we have $\sum\limits_{|\mathcal{O}_x \geq 2|} \frac{|G|}{Stab(x)} \equiv 0 (mod\ p)$, then $|X^G| \equiv |X| (mod\ p)$.

Corollary 2.2 *Let G be a finite group acts on itself by conjugation, then*

$$|G| = |Z(G)| + \sum_{|\mathcal{O}_x \geq 2|} \frac{|G|}{Stab(x)},$$

where $Z(G)$ is the center of G.

Proof. Consider the action of a finite group G on it self by conjugation. L et $x \in G$.

$$\begin{aligned} \mathcal{O}_x = \{x\} &\Leftrightarrow gxg^{-1}\ for\ all\ g \in G \\ &\Leftrightarrow gx = xg\ for\ all\ g \in G \end{aligned}$$

So, $G^G = Z(G)$. Then

$$|G| = |Z(G)| + \sum_{|\mathcal{O}_x \geq 2|} \frac{|G|}{Stab(x)}$$

Theorem 2.5 *For every prime number p, the center of a p-group is not trivial.*

Proof. Let G be a p-group. G acts on itself by conjugation. From the last proposition and corollary, we see that the prime number p divide $|Z(G)|$, so $|Z(G)| \neq 1$, then the center of G is not trivial.

Every group of order p^2 is abelian.

Lemma 2.3 *Let G be a group. If $G/Z(G)$ is cyclic, then G is abelian.*

Theorem 2.6 *Every group of order p^2 is abelian.*

Proof. Let p be a prime number and G be a group of order p^2. From the theorem 2.5, the center of G is not trivial, and because the center is a subgroup, then $|Z(G)| = p$ *or* p^2.
In the two cases, the group $G/Z(G)$ is cyclic, so from lemma 2.3, we obtain that every group of order p^2 is abelian.

Chapter 3

Counting under the action of symmetry groups

Group actions can be used to solve certain types of counting problems. Begining by these questions. How many distinct ways can you color the beads of a n bead necklace using m colors? How many ways is it possible to color the faces or the vertices of a cube if m colors are available? How many different chemical compounds can be obtained by remplacing the hydrogen atoms by OH in the benzene? What is the number of non-isomorphic simple graphs with n vertices? To solve these problems we need to introduce the cycle indexes.

3.1 Cycles indexes

Definition 3.1 (Cycle index monomial)
Let G be a subgroup of S_n and $\sigma \in G$. If the cycle type of σ is $\{k_1, k_2, ..., k_n\}$, then the **cycle index monomial** *associated with the permutation σ is*

$$cim(\sigma) = \prod_{i=1}^{n} x_i^{k_i}$$

Example 3.1 Determine the cycle index monomial for each element of C_5.
Solution: The following table gives the cycle index monomial of each $\sigma \in C_5$

Permutation	*Cycle decomposition*	*Cycle index monomial*
e	$(1)(2)(3)(4)(5)$	x_1^5
σ_1	(12345)	x_5
σ_2	(13524)	x_5
σ_3	(14253)	x_5
σ_4	(15432)	x_5

Example 3.2 For each element of D_6, determine the associated cycle index monomial.
Solution: The following table gives the cycle index monomial of each $\sigma \in D_6$

Permutation	*Cycle decomposition*	*Cycle index monomial*
e	$(1)(2)(3)(4)(5)(6)$	x_1^6
σ_1	(123456)	x_6
σ_2	$(135)(246)$	x_3^2
σ_3	$(14)(25)(36)$	x_2^3
σ_4	$(153)(264)$	x_3^2
σ_5	(165432)	x_6
σ_6	$(1)(26)(35)(4)$	$x_1^2x_2^2$
σ_7	$(12)(36)(45)$	x_2^3
σ_8	$(13)(2)(46)(5)$	$x_1^2x_2^2$
σ_9	$(14)(23)(56)$	x_2^3
σ_{10}	$(15)(24)(3)(6)$	$x_1^2x_2^2$
σ_{11}	$(16)(25)(34)$	x_2^3

Definition 3.2 (Cycle index polynomial)
Let G be a subgroup of S_n. The **cycle index polynomial** *of G is a polynomial of n variables $x_1, x_2, ..., x_n$, , denoted by Z_G, that is*

$$Z_G(x_1, x_2, ..., x_n) = \frac{1}{\mid G \mid} \sum_{\sigma \in G} cim(\sigma)$$

Equivalently, we can write

$$\frac{1}{\mid G \mid} \sum_{\pi \in G} \left(\prod_{i=1}^{n} x_i^{k_i(\pi)} \right)$$

Example 3.3 Find the cycle index polynomial associated with C_5.
Solution: In Example 3.1, we found the cycle index monomial associated with each permutation in C_5. To find the cycle index polynomial, we need only average these monomials.

$$Z_{C_5}(x_1, x_2, x_3, x_4, x_5) = \frac{1}{5}(x_1^5 + 4x_5)$$

Example 3.4 Find the cycle index polynomial associated with D_6.
Solution: In Example 3.2, we found the cycle index monomial associated with each permutation in D_6. In order to find the cycle index polynomial, we need only average these monomials. Hence,

$$Z_{D_6}(x_1, x_2, x_3, x_4, x_5, x_6) = \frac{1}{12}(x_1^6 + 3x_1^2x_2^2 + 4x_2^3 + 2x_3^2 + 2x_6)$$

Example 3.5 Find the cycle index polynomial associated with the group S_3.
Solution: The elements of S_3 and the cycle index monomial associated with each permutation are given in the following table:

Permutation	*Cycle decomposition*	*Cycle index monomial*
e	$(1)(2)(3)$	x_1^3
σ_1	$(1)(23)$	x_1x_2
σ_2	$(12)(3)$	x_1x_2
σ_3	(123)	x_3
σ_4	(132)	x_3
σ_5	$(13)(2)$	x_1x_3

So, the cycle index polynomial is

$$Z_{S_3}(x_1, x_2, x_3) = \frac{1}{6}(x_1^3 + 3x_1x_2 + 2x_3)$$

To compute the cycle index polynomial of a permutation group we need to know the type of each permutation. This can be difficult when the group size increases. There are formulas to compute the cycle index polynomial for certain groups. Now we produce the cycle index polynomial for the groups C_n and D_n.

Theorem 3.1 *Let φ be the Euler's function given by*

$$\varphi(n) = |\{d \in \mathbb{N}/1 \leq d \leq n \text{ and } gcd(d, n) = 1\}|$$

The cycle index polynomial of C_n is

$$Z_{C_n}(x_1, x_2, ..., x_n) = \frac{1}{n}\sum_{d|n} \varphi(d)x_d^{n/d}$$

Example 3.6 Find the cycle index polynomial of the cyclic group C_6.
Solution: Using the last theorem, we have:

$$\begin{aligned} Z_{C_6}(x_1, x_2, x_3, x_4, x_5, x_6) &= \frac{1}{6}\sum_{d|6} \varphi(d)x_d^{6/d} \\ &= \frac{1}{6}(\varphi(1))x_1^6 + \varphi(2)x_2^3 + \varphi(3)x_3^2 + \varphi(6)x_6) \\ &= \frac{1}{6}(x_1^6 + x_2^3 + 2x_3^2 + 2x_6) \end{aligned}$$

Proposition 3.1 *If p is a prime number, then the cycle index polynomial of C_p is given by*

$$Z_{C_p}(x_1, x_2, ..., x_p) = \frac{1}{p}(x_1^p + (p-1)x_p)$$

Theorem 3.2 *The cycle index polynomial of the nth dihedral group, D_n, is given by*

$$Z_{D_n}(x_1, x_2, ..., x_n) = \frac{Z_{C_n}(x_1, x_2, ..., x_n)}{2} + \begin{cases} \frac{1}{2}x_1 x_2^{(n-1)/2} & n \text{ is odd} \\ \frac{1}{4}(x_1^2 x_2^{(n-2)/2} + x_2^{n/2}) & n \text{ is even.} \end{cases}$$

Example 3.7 Find the cycle index polynomial of the dihedral group D_5.
Solution: 5 is an odd number. So from the last theorem, we have:

$$\begin{aligned} Z_{D_5}(x_1, x_2, x_3, x_4, x_5) &= \frac{1}{2}Z_{C_5}(x_1, x_2, x_3, x_4, x_5) + \frac{1}{2}x_1 x_2^2 \\ &= \frac{1}{2}\left(\frac{1}{5}\sum_{d|5}\varphi(d)x_d^{5/d}\right) + \frac{1}{2}x_1 x_2^2 \\ &= \frac{1}{2}\left(\frac{1}{5}(\varphi(1)x_1^5 + \varphi(5)x_5)\right) + \frac{1}{2}x_1 x_2^2 \\ &= \frac{1}{2}\left(\frac{1}{5}(x_1^5 + 4x_5)\right) + \frac{1}{2}x_1 x_2^2 \\ &= \frac{1}{10}\left(x_1^5 + 5x_1 x_2^2 + 4x_5\right) \end{aligned}$$

3.2 Pólya's Enumeration Theorems

Let X and Y be two finite sets. If G is a group acts on X, then G acts on the set Y^X of all functions from X to Y. In this extended action, two functions $f_1, f_2 \in Y^X$ are in the same orbit if there is $g \in G$ such that $f_1(gx) = f_2(x)$ for all $x \in X$.

Definition 3.3 (Patterns)
Let G be a group acts on a set X and Y be a nonempty set. The orbits under the extended action of G on the set Y^X are called **patterns**.

The following theorem gives the number of patterns.

Theorem 3.3 (Pólya's First Enumeration Theorem)
Let C be the set of all functions from an $n-$set X to an $m-$set Y and G be a subgroup of S_n with cycle index polynomial $Z_G(x_1, x_2, ..., x_n)$. Then the number of patterns in C under G is

$$Z_G(m, m, ..., m)$$

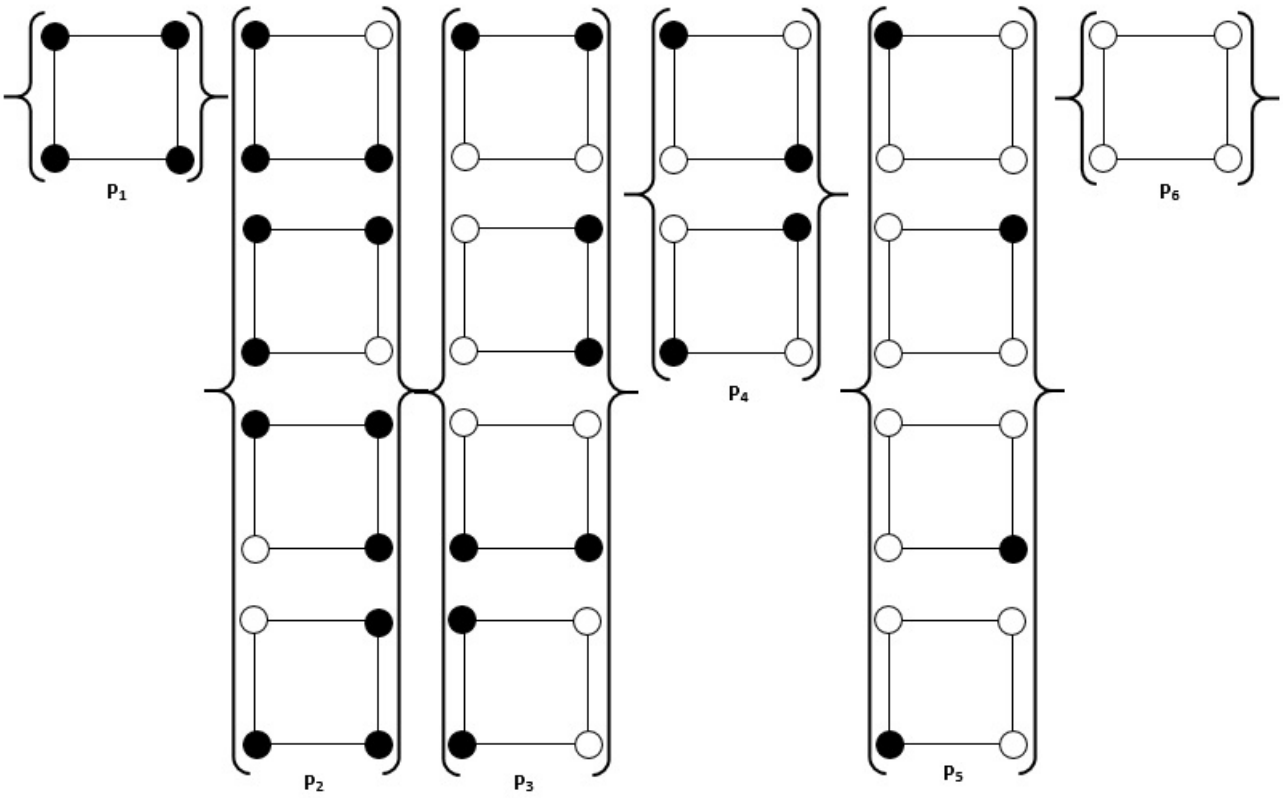
Proof. See [16, p. 149]

Example 3.8 Suppose that we want to coloring the vertices of a square using two colors black and white under rotations. The total number of colorings is $2^4 = 16$.

The cyclic group C_4 acts on the set of the vertices of the square and the number of distinct colorings under rotations is

$$Z_{C_4}(2,2,2,2) = \frac{1}{4}(2^4 + 2 \cdot 2 + 2^2) = 6$$

These patterns are:



Example 3.9 How many different colorings of the sides of a regular pentagon using three colors under rotations and reflexions.
Solution: In this case $X = \{1,2,3,4,5\}$, $Y = \{c_1, c_2, c_3\}$ and $G = D_5$.
From the example 3.6 the cycle index polynomial of D_5 is

$$\frac{1}{10}(x_1^5 + 5x_1x_2^2 + 4x_5)$$

The number of different colorings of the sides of a regular pentagon using three colors under rotations and reflexions is

$$Z_{D_5}(3,3,3,3,3) = \frac{1}{10}(3^5 + 5 \cdot 3 \cdot 3^2 + 4 \cdot 3) = 39$$

We can also using the Burnside's Lemma to count the number of patterns because the patterns are orbits under an appropriate group action.

Proposition 3.2 *Let G be a subgroup of S_n and X be an n-set and Y be an m-set. If G acts on the set Y^X of all functions from X to Y, then the number of functions invariant under σ is given by*

$$|Inv(\sigma)| = m^{cyc(\sigma)}$$

The beauty of this is to find the invariant, we only need to know the cycle index of each permutation in G. Using the above proposition, we give a version of Burnside's Lemma incorporating the cycle index.

Theorem 3.4 (Burnside's Lemma-Cycle index version)
Let C be the set of all m^n functions from X to Y. If G is a group of permutations acting on C, then the number of orbits is given by

$$\frac{1}{|G|}\sum_{\sigma\in G} m^{cyc(\sigma)}$$

Example 3.10 Find the number of distinct colorings of the vartices of a square using two colors black and white under rotations and reflexions.
Solution: In this case, the group is the 4th dihedral group D_4. The following table gives the elements of D_4, the cycle decomposition, the cycle index and the invariant of each element.

Permutation	*Cycle decomposition*	*Cycle index*	*Number of invariants*
e	$(1)(2)(3)(4)$	4	$2^4 = 16$
σ_1	(1234)	1	$2^1 = 2$
σ_2	$(13)(24)$	2	$2^2 = 4$
σ_3	(1432)	1	$2^1 = 2$
σ_4	$(14)(23)$	2	$2^2 = 4$
σ_5	$(12)(34)$	2	$2^2 = 4$
σ_6	$(13)(2)(4)$	3	$2^3 = 8$
σ_7	$(1)(24)(3)$	3	$2^3 = 8$

So, from Burnside's Lemma-Cycle index version the number of orbits is

$$\frac{1}{|D_4|}\sum_{\sigma\in D_4} 2^{cyc(\sigma)}$$

$$= \frac{1}{8}(16+2+4+2+4+4+8+8) = 6$$

With the Pólya's First Enumeration Theorem we can count the number of possible coloring of a square with m colors. What if we want to know the number of possible colorings with a specific number of vertices of each color? For example, how many colorings are possible with 2 black and 2 white? We need to know weights.

Definition 3.4 (Weight of a function)
Let f be a function from X to Y. We can assign a weight w_y *to each element $y \in Y$ (A weight can be a symbol). The* **weight of** f*, denoted by $W(f)$, is the product of the weights of the elements of Y used in f, that is*

$$W(f) = \prod_{i=1}^{n} w_{f(x_i)}$$

Example 3.11 Let f be a coloring of a square (Function from the set of the vertices {1,2,3,4} to the set of colors {black, white}) defined by

$$f(1) = black \quad f(2) = white \quad f(3) = white \quad f(4) = black$$

Suppose that the colors have the following weights:

$$w_{black} = b \qquad w_{white} = w$$

So, the weight of the coloring f is

$$W(f) = \prod_{i=1}^{4} w_{f(i)} = b^2 w^2$$

Proposition 3.3 *Two colorings in the same pattern have the same weight.*

Proof. Let P be a pattern and $f_1, f_2 \in P$.
By definition there is $g \in G$ such that $f_1(gx) = f_2(x)$ for all $x \in X$

$$\begin{aligned} W(f_1) &= \prod_{x \in X} w_{f_1(x)} \\ &= \prod_{x \in X} w_{f_1(gx)} \\ &= \prod_{x \in X} w_{f_2(x)} \\ &= W(f_2) \end{aligned}$$

So, from this proposition, we can define the weight of a pattern.

Definition 3.5 (Weight of a pattern)
Let P be a pattern. The **Weight** *of P, denoted by $W(P)$, is the common weight of all functions in P.*

Example 3.12 Find the weight of all patterns in the example 3.7.
Solution: Suppose that the colors have the weights $w_{black} = b$ and $w_{white} = w$
The weights are:

The patterns	*The weights*
P_1	b^4
P_2	b^3w
P_3	b^2w^2
P_4	b^2w^2
P_5	bw^3
P_6	w^4

Definition 3.6 (Pattern inventory)
The **pattern inventory** *is the sum of the weights of all patterns, that is a polynomial with m vaiables (The variables are the weights of the colors), denoted by $PI_G(w_{y_1}, w_{y_2}, ..., w_{y_m})$.*

Example 3.13 With weight "b" for black and "w" for white, the pattern inventory of the colorings of a square in example 3.5 is

$$PI_{C_4}(b,w) = W(P_1)+W(P_2)+W(P_3)+W(P_4)+W(P_5)+W(P_6) = b^4+b^3w+2b^2w^2+bw^3+w^4$$

Theorem 3.5 (Pólya's Second Enumeration Theorem)
Let C be the set of all functions from an $n-$set X to an $m-$set Y and G be a subgroup of S_n with cycle index polynomial $Z_G(x_1, x_2, ..., x_n)$. The pattern inventory under G is

$$Z_G\left(\sum_{i=1}^{m} w_{y_i}, \sum_{i=1}^{m} w_{y_i}^2, \cdots, \sum_{i=1}^{m} w_{y_i}^n\right)$$

Proof. See [16, p. 151]

Example 3.14 Continuing with the 2-coloring of a square with the weight "b" and "w". the pattern inventory is given by

$$\begin{aligned} Z_G\left(\sum_{i=1}^{m} w_{y_i}, \sum_{i=1}^{m} w_{y_i}^2, \cdots, \sum_{i=1}^{m} w_{y_i}^n\right) &= Z_{C_n}\left(b+w, b^2+w^2, b^3+w^3, b^4+w^4\right) \\ &= \frac{1}{4}\left((b+w)^4 + (b^2+w^2)^2 + 2(b^4+w^4)\right) \\ &= \frac{1}{4}(4b^4 + 4b^3w + 8b^2w^2 + 4bw^3 + 4w^4) \\ &= b^4 + b^3w + 2b^2w^2 + bw^3 + w^4 \end{aligned}$$

Remark 3.1 *The Pólya's First Enumeration theorem is a special case of the Pólya Second Enumeration Theorem. If we chose $w_y = 1$ for all $y \in Y$, we have the number of patterns*

$$PI_G(1,1,...,1) = Z_G\left(\sum_{i=1}^{m} 1, \sum_{i=1}^{m} 1^2, \cdots, \sum_{i=1}^{m} 1^n\right) = Z_G(m,m,...,m)$$

3.3 Applications

Now, we give the solutions of the problems in the begining of this chapter.

3.3.1 Coloring polytopes in 2 and 3 dimensional spaces

In this subsection, we give an application of Polya's Enumeration Theorem to the necklace problems and coloring of polyhedra.

Necklace problems:

How many disitnct colorings of a 7 bead necklace using two colors black and white under rotational symmetries? In this case $X = \{1, 2, 3, , 4, 5, 6, 7\}$, $Y = \{black, white\}$ and $G = C_7$.
Firstly we need to count the cycle index polynomial of C_7.
7 is a prime number, so

$$Z_{C_7}(x_1, \cdots, x_7) = \frac{1}{7}(x_1^7 + 6x_7)$$

The number of distinct colorings is

$$Z_{C_7}(2, \cdots, 2) = \frac{1}{7}(2_1^7 + 6 \cdot 2) = 20$$

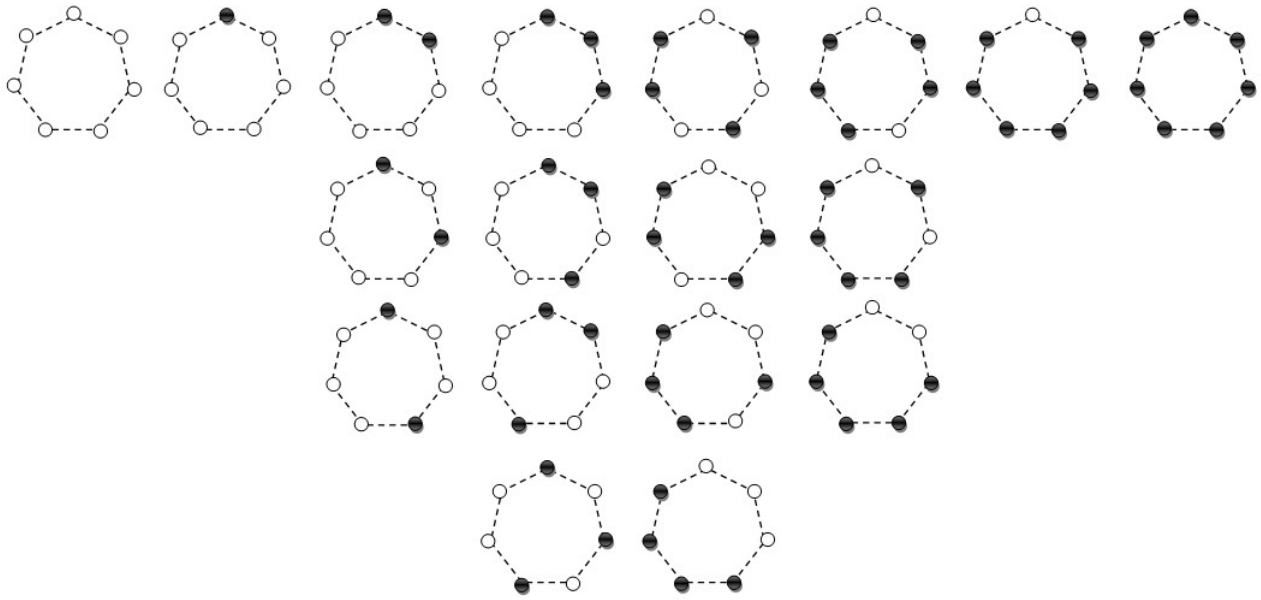
What about reflexional symmetries?
In this case $G = D_7$. The cycle index polynomial of D_7 is

$$\begin{aligned} Z_{D_7}(x_1, \cdots, x_7) &= \frac{1}{2} Z_{C_7}(x_1, \cdots, x_7) + \frac{1}{2} x_1 x_2^3 \\ &= \frac{1}{2}\left(\frac{1}{7}(x_1^7 + 6x_7)\right) + \frac{1}{2} x_1 x_2^3 \\ &= \frac{1}{14}\left(x_1^7 + 7x_1 x_2^3 + 6x_7\right) \end{aligned}$$

So, the number of distinct colorings is

$$Z_{D_7}(2, 2, ..., 2) = \frac{1}{14}\left(2^7 + 7 \cdot 2 \cdot 2^3 + 6 \cdot 2\right) = 18$$

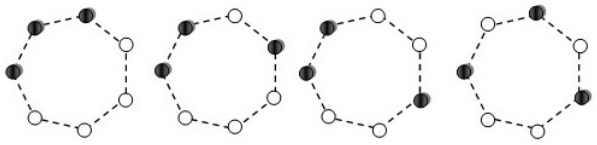
These colorings are:



Now, we will present more complex version of the necklace problem.
How many 7 bead necklaces are possible with 3 black beads and 4 white beads under rotations and reflexions? We need to determine the coefficient of b^3w^4 in the pattern inventory.
The pattern inventory is

$$\begin{aligned} PI_{D_7}(b,w) &= Z_{D_7}(b+w, b^2+w^2, ..., b^7+w^7) \\ &= \frac{1}{14}((b+w)^7 + 7(b+w)(b^2+w^2)^3 + 6(b^7+w^7)) \\ &= \frac{1}{14}(14b^7 + 14b^6w + 42b^5w^2 + 56b^4w^3 + 56b^3w^4 + 42b^2w^5 + 14bw^6 + 14w^7) \\ &= b^7 + b^6w + 3b^5w^2 + 4b^4w^3 + 4b^3w^4 + 3b^2w^5 + bw^6 + w^7 \end{aligned}$$

Hence the number of distinct 7 bead necklaces with 3 black beads and 4 white beads under rotations and reflexions is 4.



Coloring of a cube:

Suppose that we want to paint the 6 faces of a cube such that three faces are white, two faces are black and 1 face is red. How many distinct ways we can do this under rotations?

The group G of rotations of a cube and the cycle index monomial associated to each permutation are given in [3]. see the two following tables:

Permutation	Cycle decomposition	Cycle index monomial
e	$(1)(2)(3)(4)(5)(6)$	x_1^6
σ_1	$(1)(2354)(6)$	$x_1^2x_4$
σ_2	$(1)(2453)(6)$	$x_1^2x_4$
σ_3	$(1)(25)(34)(6)$	$x_1x_2^2$
σ_4	$(12)(34)(56)$	x_2^3
σ_5	$(123)(465)$	x_3^2
σ_6	$(124)(365)$	x_3^2
σ_7	$(1265)(3)(4)$	$x_1^2x_4$
σ_8	$(132)(456)$	x_3^2
σ_9	$(1364)(2)(5)$	$x_1^2x_4$
σ_{10}	$(13)(25)(46)$	x_2^3
σ_{11}	$(135)(264)$	x_3^2
σ_{12}	$(142)(356)$	x_3^2
σ_{13}	$(1463)(2)(5)$	$x_1^2x_4$
σ_{14}	$(14)(25)(36)$	x_2^3
σ_{15}	$(145)(263)$	x_3^2
σ_{16}	$(1562)(3)(4)$	$x_1^2x_4$
σ_{17}	$(154)(236)$	x_3^2
σ_{18}	$(153)(246)$	x_3^2
σ_{19}	$(15)(26)(34)$	x_2^3
σ_{20}	$(16)(34)(2)(5)$	$x_1^2x_2^2$
σ_{21}	$(16)(23)(45)$	x_2^3
σ_{22}	$(16)(24)(35)$	x_2^3
σ_{23}	$(16)(25)(3)(4)$	$x_1^2x_2^2$

Therfore, the cycle index polynomial associated with G is

$$Z_G(x_1, x_2, x_3, x_4) = \frac{1}{24}(x_1^6 + 6x_1^2x_4 + 3x_1^2x_2^2 + 6x_2^3 + 8x_3^2)$$

Suppose that the wieght of the colors are $w_{white} = w$, $w_{black} = b$ and $w_{red} = r$.
To compute our pattern inventory, we evaluate $Z_G(x_1, x_2, x_3, x_4)$ at $x_i = w^i + b^i + r^i$.

$$
\begin{aligned}
PI_G(w,b,r) &= Z_G(w+b+r,...,w^4+b^4+r^4) \\
&= \frac{1}{24}\left[\begin{array}{l}(w+b+r)^6+6(w+b+r)^2(w^4+b^4+r^4)+\\ 3(w+b+r)^2(w^2+b^2+r^2)^2+\\ 6(w^2+b^2+r^2)^3+8(w^3+b^3+r^3)^2\end{array}\right] \\
&= \frac{1}{24}\left[\begin{array}{l}24b^6+24b^5+24b^5w+48b^4r^2+48b^4rw+48b^4w^2+\\ 48b^3r^3+72b^3r^2w+72b^3rw^2+48b^3w^3+48b^2r^4+\\ 72b^2r^3w+144b^2r^2w^2+72b^2rw^3+48b^2w^4+24br^5+\\ 48br^4w+72br^3w^2+72br^2w^3+48brw^4+24bw^5+24r^6+\\ 24r^5w+48r^4w^2+48r^3w^3+48r^2w^4+24rw^5+24w^6\end{array}\right] \\
&= \begin{array}{l}b^6+b^5+b^5w+2b^4r^2+2b^4rw+2b^4w^2+2b^3r^3+3b^3r^2w+\\ 3b^3rw^2+2b^3w^3+2b^2r^4+3b^2r^3w+6b^2r^2w^2+3b^2rw^3+\\ 2b^2w^4+br^5+1br^4w+3br^3w^2+3br^2w^3+2brw^4+bw^5+r^6+\\ r^5w+2r^4w^2+2r^3w^3+2r^2w^4+rw^5+24w^6\end{array}
\end{aligned}
$$

The coefficient of w^3b^2r is 3, thus there are 3 distinct colorings of the faces of a cube such that three faces are white, two faces are black and 1 face is red.
The total number of distinct colorings of the 6 faces of a cube using 3 colors is

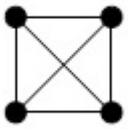
$$Z_G(3,\cdots,3)=\frac{1}{24}(3^6+6\cdot 3^2\cdot 3+3\cdot 3^2\cdot 3^2+6\cdot 3^3+8\cdot 3^2)=57$$

3.3.2 Graphical Enumeration

The Pólya's Enumeration Theorem can be used to calculate the number of non-isomorphic simple graphs with a fixed number of vertices. Let V be a set of n vertices. Two graphs $\mathcal{G}_1=(V,E_1)$ and $\mathcal{G}_2=(V,E_2)$ are isomorphic if there is a permutation $\sigma\in S_V$ such that $(x,y)\in E_1\Leftrightarrow(\sigma(x),\sigma(y))\in E_2$. To apply the Pólya's Enumeration Theorem we identify each graph $\mathcal{G}=(V,E)$ with a function f from the set X of all edges to the set $Y=\{present,absent\}$, so the set of all graphs is identify with the set of all functions from X to Y. Hence the problem of finding the number of non-isomorphic graphs is equivalent to find the number of distinct colorings of the edges of the complete simple graph on n vertices using two colors present and absent. In this case, the method of finding the group of permutations (denoted by S_n^2) and its cycle index polynomial is given in [11].

In the following two examples we give the number of non-isomorphic simple graphs of 4 and 5 vertices.

Example 3.15 Find the number of non-isomorphic simple graphs on 4 vertices.
Solution: Consider the complete simple graph of 4 vertices, wich has 6 edges.



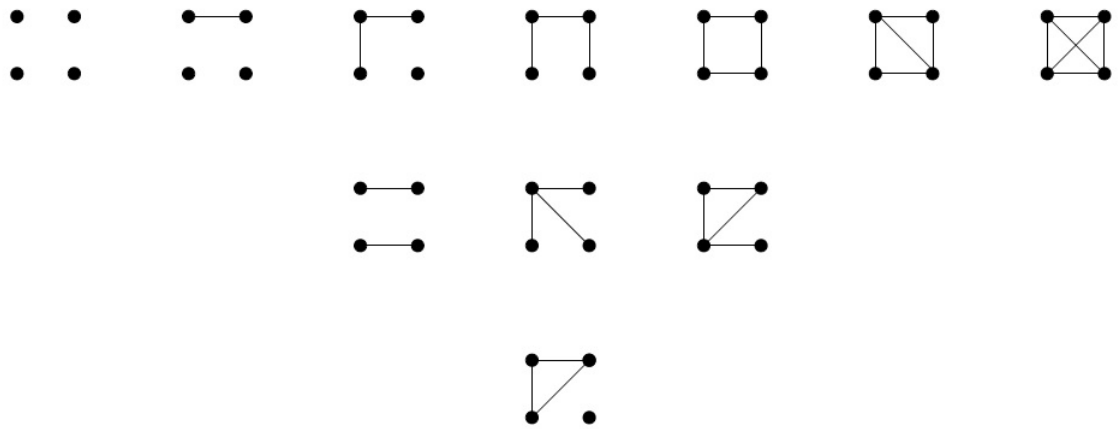
The cycle index polynomial of the action in this case is

$$Z_{S_4^2}(x_1, ..., x_6) = \frac{1}{24}(x_1^6 + 9x_1^2x_2^2 + 8x_3^2 + 6x_2x_4)$$

For the weights $w_{present} = p$ and $w_{absent} = a$, the pattern inventory is

$$\begin{aligned} PI_{S_4^2}(p, a) &= Z_{S_4^2}(a + b, a^2 + b^2, ..., a^6 + b^6) \\ &= \frac{1}{24}((a + b)^6 + 9(a + b)^2(a^2 + b^2)^2 + 8(a^3 + b^3)^2 + 6(a^2 + b^2)(a^4 + b^4)) \\ &= \frac{1}{24}(24a^6 + 24a^5b + 48a^4b^2 + 72a^3b^3 + 48a^2b^4 + 24ab^5 + 24b^6) \\ &= a^6 + pa^5 + 2p^2a^4 + 3p^3a^3 + 2p^4a^2 + p^5a + p^6 \end{aligned}$$

We obtain 11 non-isomorphic graphs. See the following figure



Example 3.16 Find the number of non-isomorphic simple graphs on 5 vertices.
Solution: Consider the complete simple graph of 5 vertices, wich has 10 edges.

The cycle index polynomial of the action in this case is

$$Z_{S_5^{(2)}}(x_1,...,x_{10}) = \frac{1}{120}(x_1^{10} + 10x_1^4x_2^3 + 20x_1x_3^3 + 15x_1^2x_2^4 + 30x_2x_4^2 + 20x_1x_3x_6 + 24x_5^2)$$

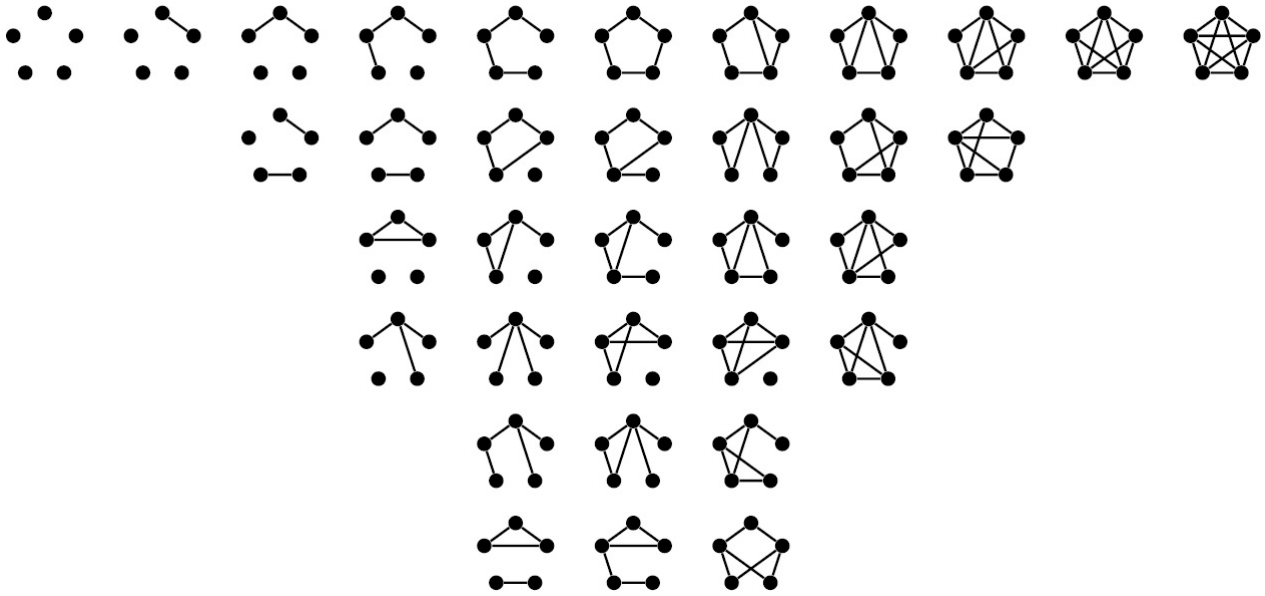
The pattern inventory is

$$\begin{aligned}
PI_{S_5^2}(p,a) &= Z_{S_5^{(2)}}(a+b, a^2+b^2, ..., a^{10}+b^{10}) \\
&= \frac{1}{120}\left[\begin{array}{l} (p+a)^{10} + 10(p+a)^4(p^2+a^2)^3 + 20(p+a)(p^3+a^3)^3 + \\ 15(p+a)^2(p^2+a^2)^4 + 30(p^2+a^2)(p^4+a^4)^2 + \\ 20(p+a)(p^3+a^3)(p^6+a^6) + 24(p^5+a^5)^2 \end{array}\right] \\
&= \frac{1}{120}\left[\begin{array}{l} 120a^{10} + 120a^9 + 240a^8p^2 + 480a^7p^3 + 720a^6p^4 + \\ 720a^5p^5 + 720a^4p^6 + 480a^3p^7 + 240a^2p^8 + 120ap^9 + \\ 120p^{10} \end{array}\right] \\
&= a^{10} + a^9 + 2a^8p^2 + 4a^7p^3 + 6a^6p^4 + 6a^5p^5 + 6a^4p^6 + 4a^3p^7 + 2a^2p^8 + ap^9 + p^{10}
\end{aligned}$$

The Polya's Enumeration Threorem gives the number of non-isomorphic simple graphs of 5 vertices with a specific number of edges. From the pattern inventory there are:

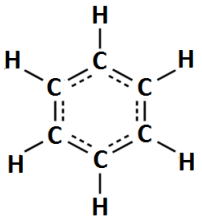
1 graph without any vertice.
1 graph with one vertice.
2 non-isomorphic graphs with 2 vertices.
4 non-isomorphic graphs with 3 vertices.
6 non-isomorphic graphs with 4 vertices.
6 non-isomorphic graphs with 5 vertices.
6 non-isomorphic graphs with 6 vertices.
4 non-isomorphic graphs with 7 vertices.
2 non-isomorphic graphs with 8 vertices.
1 graph with 9 vertices.
1 graph with 10 vertices.

Hence, the number of all non-isomorphic simple graphs with 5 vertices is 34. see the following figure .



3.3.3 Chemical compounds

How many different chemical compounds can be obtained by remplacing the hydrogen atoms by OH in the benzene? Also how many different chemical compounds can be obtained by remplacing just 3 hydrogen atoms?



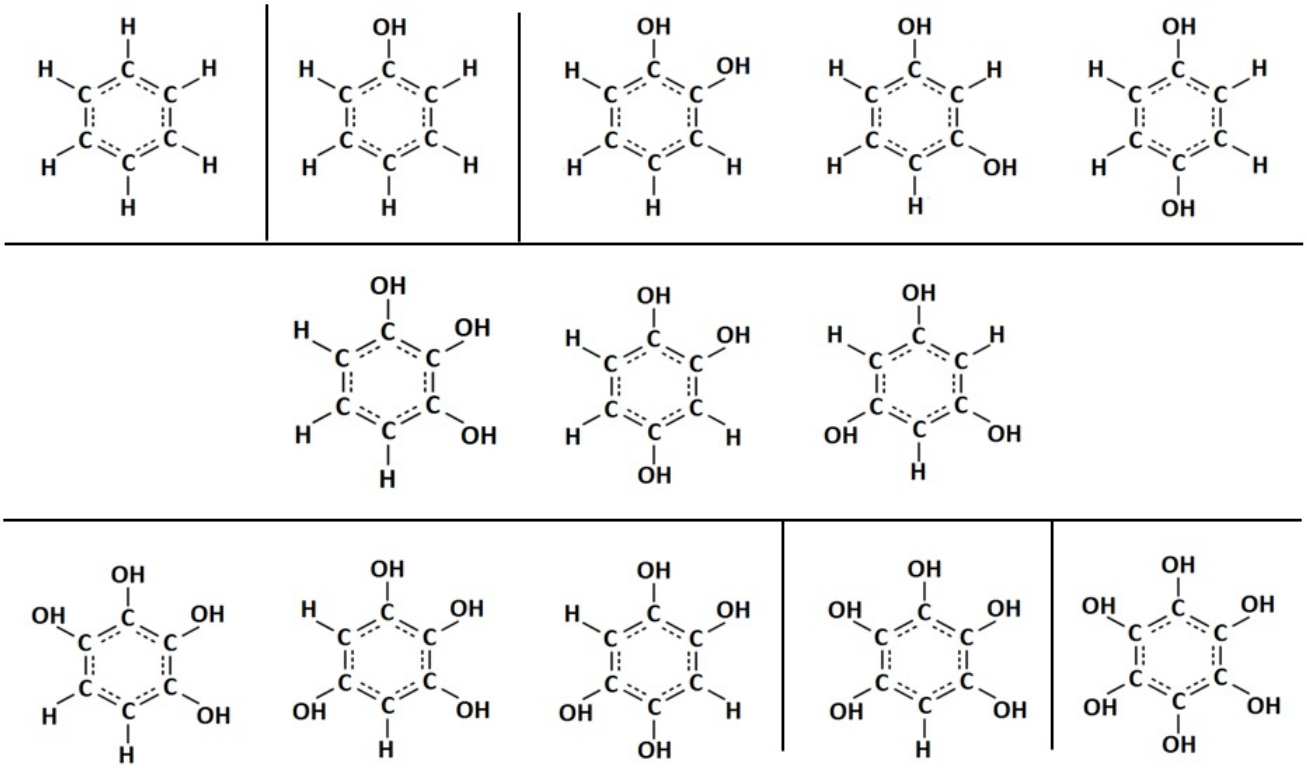
The carbon atoms are placed at the six vertices of a regular hexagon and there are 2^6 ways of attaching OH or H radicals. The dihedral group D_6 acts on the set of the vertices of the the hexagon, and we wish to find the number of patterns under D_6.

$$\begin{aligned} Z_{D_6}(x_1,\cdots,x_6) &= \frac{1}{2}Z_{C_6}(x_1,\cdots,x_6)+\frac{1}{4}(x_1^2x_2^2+x_2^3) \\ &= \frac{1}{2}\left(\frac{1}{6}(x_1^6+x_2^3+2x_3^2+2x_6)\right)+\frac{1}{4}(x_1^2x_2^2+x_2^3) \\ &= \frac{1}{12}(x_1^6+x_2^3+2x_3^2+2x_6)+\frac{3}{12}(x_1^2x_2^2+x_2^3) \\ &= \frac{1}{12}(x_1^6+3x_1^2x_2^2+4x_2^3+2x_3^2+2x_6) \end{aligned}$$

So, the number of different chemical compounds can be obtained by attaching OH or H radical to each carbon atom in the benzene ring is

$$Z_{D_6}(2,2,2,2,2,2) = \frac{1}{12}(2^6 + 3 \cdot 2^2 \cdot 2^2 + 4 \cdot 2^3 + 2 \cdot 2^2 + 2 \cdot 2) = 13$$

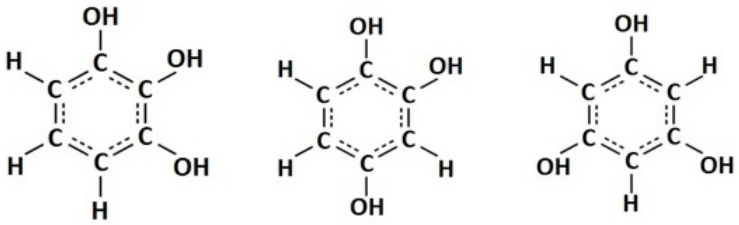
These chemical compounds are:



With weights "h" for H and "o" for OH, The pattern inventory in this case is

$$\begin{aligned} PI_{D_6}(h,o) &= Z_{D_6}(h+o, h^2+o^2, \cdots, h^6+o^6) \\ &= \frac{1}{12}((h+o)^6 + 3(h+o)^2(h^2+o^2)^2 + 4(h^2+o^2)^3 + 2(h^3+o^3)^2 + 2(h^6+o^6)) \\ &= \frac{1}{12}(12h^6 + 12h^5o + 36h^4o^2 + 36h^3o^3 + 36h^2o^4 + 12ho^5 + 12o^6) \\ &= h^6 + h^5o + 3h^4o^2 + 3h^3o^3 + 3h^2o^4 + ho^5 + o^6 \end{aligned}$$

So, the number of different chemical compounds by remplacing 3 hydrogen atoms is the coefficient of h^3o^3 is the pattern inventory, that is 3.



3.3.4 Number theory

Now we give a generalisation of both Fermat's theorem and Gauss's theorem. This work wasdone by Chong-Yun Chao and published in the journal of Number Theory in 1982.
Firstly we present the theorems of Fermat and Gauss.

Theorem 3.6 (Fermat) *Let p be a prime number.*
For every integer a

$$a^p \equiv a \pmod{p}$$

Theorem 3.7 (Gauss) *If n is a positif integer, then*

$$\sum_{d|n} \varphi(d) = n$$

where φ is the Euler's function.

These two theorems are both generalized in the following theorem.

Theorem 3.8 *Let a and n be two positive integers. Then*

$$\sum_{d|n} \varphi(d) a^{n/d} \equiv 0 \pmod{n}$$

Proof: Consider the sets $X = \{1, 2, ..., n\}$ and $Y = \{1, 2, ..., a\}$.
The cyclic group C_n of order n acts of X. By Pólya's Enumeration Theorem, the number of patterns in Y^X under C_n is

$$Z_{C_n}(a, a, ..., a) = \frac{1}{n} \sum_{d|n} \varphi(d) a^{n/d}$$

Since the total number of patterns is a positive integer k. Then

$$\frac{1}{n} \sum_{d|n} \varphi(d) a^{n/d} = k \Rightarrow \sum_{d|n} \varphi(d) a^{n/d} = kn \Rightarrow \sum_{d|n} \varphi(d) a^{n/d} \equiv 0 \pmod{n}$$

Example 3.17 *let $a = 2$ and $n = 6$. We have*

$$\begin{aligned} \sum_{d|n} \varphi(d) a^{n/d} &= \sum_{d|6} \varphi(d) 2^{6/d} \\ &= \varphi(1)2^6 + \varphi(2)2^3 + \varphi(3)2^2 + \varphi(6)2 \\ &= 84 \\ &= 6 \cdot 14 \\ &\equiv 0 \bmod 6 \end{aligned}$$

Now we see that Fermat's Theorem ane Gauss's Theorem are consequences from theorem 3.9
Let $n = p$ be a prime number. Then

$$\begin{aligned}
\sum_{d|p} \varphi(d) a^{p/d} &\equiv 0 \pmod{p} \\
a^p + (p-1)a &\equiv 0 \pmod{p} \\
a^p - a + pa &\equiv 0 \pmod{p} \\
a^p - a &\equiv 0 \pmod{p} \\
a^p &\equiv a \pmod{p}
\end{aligned}$$

Let $a = 1$, i.e., $Y = \{1\}(|Y^X| = 1)$. So there is only one pattern, then

$$\begin{aligned}
\frac{1}{n} \sum_{d|n} \varphi(d) 1^{n/d} &= 1 \\
\frac{1}{n} \sum_{d|n} \varphi(d) &= 1 \\
\sum_{d|n} \varphi(d) &= n
\end{aligned}$$

Bibliography

[1] Jonathan D.H. Smith. (2016) *Introduction to Abstract Algebra*. 2^{nd} ed. CRC Press.

[2] Robert A. Beeler. (2015) *How to Count: An Introduction to Combinatorics and Its Applications*. Switzerland: Springer.

[3] J. McKernan. (2013) *Course of Modern Algebra*. Massachusetts institute of technology.

[4] A. Tucker. (2012) *Applied Combinatorics*. 6^{th} ed. United States of America: John Wiley & Sons.

[5] R. Steven. (2012) *Fundamentals of Group Theory: An Advanced Approach*. New York: Springer.

[6] A. Camina & B. Lewis. (2011) *An Introduction to Enumeration*. London: Springer.

[7] Durbin John R. (2009) *Modern Algebra: An introduction*. 6^{th} ed. United States of America: John Wiley & Sons.

[8] Thomas W. Judson. (2009) *Abstract Algebra: Theory and Application*. Unite state of america: Stephen F. Austin State University.

[9] H. Algafly. (2009) *Application of Pólya's Theorem to Some Special Compounds of Chemical Graph Theory*. Master's thesis. University of Nebraska at Omaha.

[10] Martin Aigner. (2007) *A Course in Enumeration*. Berlin: Springer.

[11] William J. Gilbert & W. Keith Nicholson. (2004) *Modern Algebra with Applications*. 2^{nd} ed. Canada: John Wiley & Sons.

[12] B. Gross. (2003) *Course of abstract algebra*. Harvard University.

[13] S. Anand. (2002) *How to count-An Exposition of Pólya Theory of Enumeration*. Resonance, 7(9), 19-35.

[14] Joseph J. Rotman. (1995) *An Introduction to the Theory of groups*. 4^{th} ed. New York: Springer.

[15] V. K. Balakrishnan. (1995) *Combinatorics: Including concepts of graph theory*. United States of America: McGraw-Hill.

[16] G. Pólya and R. C. Read. (1987) *Combinatorial enumeration of groups, graphs and chemical compounds*. New York: Springer.

[17] Chong-Yun Cho. *Generalization of Theorems of Wilson, Fermat and Euler*. Journal of Number Theory 15.1 (1982): 95-114.

[18] F. Edgar & M. Palmer. (1973) *Graphical Enumeration* . New York and London: ACADEMIC PRESS.

[19] W. Cherowitzo. *Combinatoris Lecture Notes*. University of Colorado at Denver.