Non-commutative Harmonic Analysis: Generalization of Phase Correlation to the Euclidean Motion Group

Master of Science Thesis in Applied and Computational Mathematics

Atle Loneland

Department of Mathematics
University of Bergen

June 10, 2010

Acknowledgement

First of all, I would like to thank my supervisor Hans Z. Munthe-Kaas, for letting my write a thesis about such an fascinating subject, for helping me learn the enormous amount of theory needed and for valuable ideas for how to solve the more technical details.

Also, I would like to thank those people who helped me understand some of the more advanced theory and helped proof-read my thesis. Especially, Mauricio, Hilde Kristine and Jan Magnus. Your help have been invaluable.

Lastly, a big thank you to all my fellow student at the Mathematical Department, it has been two wonderful years.

Bergen, June 2010
Atle Loneland

Contents

Chapter 1

Introduction

Noncommutative harmonic analysis is a field in pure mathematics which arises when Fourier analysis is extended to noncommutative topological groups. Until now this powerful and beautiful tool has not been extensively used in applied mathematics and in engineering applications. One of the reasons for this may be that it has historically been a field developed by and for pure mathematician and theoretical physicists. Another reason is the need for more literature that addresses engineering problems with this framework. If more engineers knew about the existence of this area of mathematics, more publications on the area of application would arise.

The application of noncommutative harmonic analysis is wide, from robotics, mechanics and Brownian motion to image analysis and tomography. For example the Euclidean motion group is used in formulating problems in image registration, deconvolution, radon transform inversion, et cetera.

In this thesis, a generalization of the phase correlation to the Euclidean motion group is proposed. The author is not aware of any work where this generalization has been done before. The Euclidean motion group has for the reason mentioned above not been extensively applied in image processing, but the number of works using this group is increasing.

Since the treatment of noncommutative harmonic analysis needs a lot of theory from pure mathematics, at least seen from an applied mathematician's viewpoint, we have chosen to give a comprehensive introduction to those topics. A good understanding of the fundamental theory is very important for understanding the more advanced topics and for the development of our own theory. Therefore, the thesis is organized as follows

- **Chapter 1**: Introduction to the thesis.
- **Chapter 2**: Introduction to group theory, including Lie groups.
- **Chapter 3**: Representation theory for finite groups.
- **Chapter 4**: Harmonic analysis on noncommutative groups, the theory in chapter 3 is generalized to include more general classes of groups. The emphasises is on the Euclidean motion group, since this is the group considered in the later chapters.

- **Chapter 5**: This chapter consists of the generalization of the phase correlation method to the Euclidean motion group, first the proof for cross-correlation on a noncommutative group is shown, then this result is used to generalize the phase correlation to the Euclidean motion group.
- **Chapter 6**: Numerical experiments, where the method proposed in chapter 5 is tested. We also make comparison with the ordinary phase correlation method. A small discussion at the end of this chapter describes some of the problems of how to handle the data in the implementation.
- **Chapter 7**: This chapter consists of some concluding remarks on the thesis and on some of the theory used in it. We also give a small summary of how well this method behaves and some ideas for the future; both for improvement and new application areas for the proposed method.

There is also a small appendix at the end where some definitions needed for understanding the theory in this thesis is included.

Chapter 2

Group Theory

2.1 Introduction

Group theory is the study of algebraic structures called groups. It is a mathematical abstraction of the study of symmetry. There are three main historical sources of group theory: Number theory, the theory of algebraic equations, and geometry. The treatment of group theory here follows [1, 2].

2.2 Groups

In this section the general theory, notation and some basic result of group theory is presented. First we start with a few standard definitions:

Definition 2.1. A (closed) binary operation is a law of composition which takes any two elements of a set and returns an element of the same set (i.e., $g_1 \circ g_2 \in G$ whenever $g_1, g_2 \in G$).

Definition 2.2. A group ⟨G,∘ ⟩ is a set G, closed under a binary operation ∘, such that for any element $g, g_1, g_2, g_3 \in G$ the following axioms holds:

- $g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3$ (Associativity)
- There exist an element $e \in G$ such that $e \circ g = g \circ e = g$
- For every element $g \in G$ there is an element $g^{-1} \in G$ such that $g^{-1} \circ g = g \circ g^{-1} = e$.

If the property $g_1 \circ g_2 = g_2 \circ g_1$ also holds, then the group is called commutative or abelian, otherwise it is called non-commutative or non-abelian. The element e is called the identity and g^{-1} is called the inverse of g. If the group operation is understood by context G refers to both the set and the group.

We define conjugation of an element h by an element g as:

$$h_g = g \circ h \circ g^{-1} \qquad \text{and} \qquad h^g = g^{-1} \circ h \circ g.$$

Both h_g and h^g is a conjugation with the relation $h^g = h_{g^{-1}}$. If the groups are abelian conjugation leaves the elements unchanged: $h_g = h^g = h$. This is usually not true in the non-commutative case.

Definition 2.3. The **order** of a group G is the number of elements in G and is denoted $|G|$.

As we can see from the definition the order of a group is defined in the same manner as the cardinality of the underlying set G, which also is denoted $|G|$.

Theorem 2.4. *If G is a group with binary operation $\circ$, then the **left and right cancellation laws** hold in G, that is, $g_1 \circ g_2 = g_1 \circ g_3$ implies $g_2 = g_3$, and $g_2 \circ g_1 = g_3 \circ g_1$ implies $g_2 = g_3$ for all $g_1, g_2, g_3 \in G$.*

Theorem 2.5. *If G is a group with binary operation $\circ$, and if g_1 and g_2 are any elements of G, then the linear equations $g_1 \circ x = g_2$ and $y \circ g_1 = g_2$ have unique solutions x and y in G.*

2.3 Subgroups

A subset H of a group G under the binary operation of G is called a **subgroup** of G if it is closed under the induced operation from G and H is itself a group. We denote a subgroup H of G as $H \leq G$ or $G \geq H$

Definition 2.6. If G is a group, then the subgroup consisting of G itself is the **improper subgroup** of G. All other subgroups are **proper subgroups**. The subgroup $\{e\}$ is the **trivial subgroup** of G. All others subgroups are **nontrivial**.[1]

Theorem 2.7. *A subset H of a group G is a subgroup of G if and only if H is a group and H is closed under the binary operation of G.*

2.3.1 Cyclic Subgroups

A subgroup of G containing g must by Theorem 2.7 contain g^n and these positive integral powers of g gives a set closed under multiplication. Since a subgroup containing an element g must also by the definition of a group, contain the inverse g^{-1}. In general it must also contain g^{-m} for all $m \in \mathbb{Z}^+$. The identity element $e = g^0$ must also be contained in the subgroup. To summarize, *a subgroup of G containing the element g must contain the element g^n for all $n \in \mathbb{Z}$*. We can put these and some more properties into the next theorem

Theorem 2.8. *Let G be a group and let $g \in G$. Then*

$$H = \{g^n | n \in \mathbb{Z}\}$$

is a subgroup of G and it is the smallest subgroup of G that contains g, that is, every subgroup containing g contains H.

Definition 2.9. Let G be a group and let $g \in G$. Then the subgroup $\{g^n | n \in \mathbb{Z}\}$ of G, characterized in Theorem 2.8, is called the **cyclic subgroup of G generated by g**, and it is denoted by $\langle g \rangle$.

Definition 2.10. An element g of a group G **generates** G and is a **generator for** G if $\langle g \rangle = G$. A group G is cyclic if there is some element g in G that generates G.

Example 2.11. Let $\mathbb{Z}_4$ be a group. Then $\mathbb{Z}_4$ is cyclic and both 1 and 3 are generators, that is

$$\langle 1 \rangle = \langle 3 \rangle = \mathbb{Z}_4$$

Theorem 2.12. *Every Cyclic group is abelian.*

A very simple, but fundamental tool for the study of cyclic group is the *division algorithm*

Algorithm 2.13 (Division Algorithm for $\mathbb{Z}$)**.** *If m is a positive integer and n is any integer, then there exist unique integers q and r such that*

$$n = mq + r \qquad \textit{and} \qquad 0 \leq r < m$$

Theorem 2.14. *A subgroup of a cyclic group is cyclic.*

Corollary 2.15. *The subgroup of $\mathbb{Z}$ under addition are precisely the groups $n\mathbb{Z}$ under addition for $n \in \mathbb{Z}$*

2.4 Finite groups

A finite group is a group G where the underlying set G has finitely many elements, i.e. the order of G, $|G|$ is finite. The case when $|G| = 1$ is not interesting since the only element of the group must be the identity element.

2.4.1 Group Tables

To identify the groups structure of a finite group with two or more elements we can use group tables to list the elements of a group and their composition:

Example 2.16. Group table of a group $G = \{e, a\}$ with $|G| = 2$:

We see from the group table (Table 2.16) that $a \circ a = e$, so a is its own inverse.

Table 2.1: Group Table

$\circ$	e	a
e	e	a
a	a	e

2.5 Permutations

A permutation of a set is a rearrangement of the element of the set. A set $\{1,2,3,4,5\}$ could be rearranged into a set $\{4,2,5,1,3\}$. Here 1 is carried to 4, 2 is carried to 2, 3 is mapped to 5, 4 to 1 and 5 to 3. Let us think of this as a function mapping of each element into a single(not necessarily different) element from the same set. We can define a permutation to be such a mapping

Definition 2.17. A **permutation of a set** A is a function $\phi : A \to A$ that is both one to one and onto

Usually, the action produced by a group element can be regarded as a *function*, and the binary operation of the group can be regarded as a *function composition.*

Theorem 2.18. *Let A be a nonempty set, and let S_A be the collection of all permutations of A. Then S_A is a group under permutation multiplication.*

Definition 2.19. Let A be the finite set $\{1, 2, , ..., n\}$. The group of all permutations of A is the **symmetric group on n letters,** and is denoted by S_n

The group S_n has $n!$ elements, where

$$n! = n(n-1)(n-2)....(3)(2)(1)$$

Example 2.20. The group S_3 of $3! = 6$ elements is an interesting example to study. Let A be the set $\{1, 2, 3\}$ We assign to each permutation of A a Greek letter for a name. Let

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Table 2.2: Group Table for S_3

	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

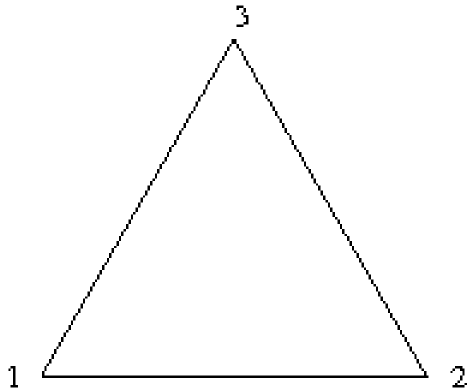


Figure 2.1: Equilateral triangle

In Table 2.2 we see the multiplication table for S_3. This group is non-abelian. It may be proved that every group of 4 elements is abelian, same is for groups of 5 elements. Thus S_3 is the smallest group which is non-abelian.

There is a natural correspondence between S_3 and the **group D_3 of symmetries of an equilateral triangle**. D_3 is called the **third dihedral group**, including both rotations and reflections (see figure 2.1). ρ_i is the rotations of the equilateral triangle, and μ_i is the reflections. So S_3 is also the group D_3. We can say that the elements of S_3 *act* on the triangle in Fig. 2.1.

Another important example is the **group of symmetries of the square**, the dihedral group D_4, also called the **octic group**.

Example 2.21. The dihedral group D_4 consist of permutations corresponding to how two

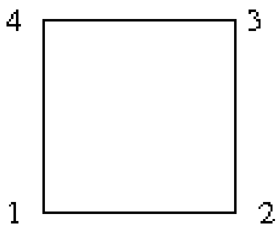


Figure 2.2: Square

Table 2.3: Group Table for D_4

	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_1	ρ_1	ρ_2	ρ_3	ρ_0	δ_1	δ_2	μ_2	μ_1
ρ_2	ρ_2	ρ_3	ρ_0	ρ_1	μ_2	μ_1	δ_2	δ_1
ρ_3	ρ_3	ρ_0	ρ_1	ρ_2	δ_2	δ_1	μ_1	μ_2
μ_1	μ_1	δ_2	μ_2	δ_1	ρ_0	ρ_2	ρ_3	ρ_1
μ_2	μ_2	δ_1	μ_1	δ_2	ρ_2	ρ_0	ρ_1	ρ_3
δ_1	δ_1	μ_1	δ_2	μ_2	ρ_1	ρ_3	ρ_0	ρ_2
δ_2	δ_2	μ_2	δ_1	μ_1	ρ_3	ρ_1	ρ_2	ρ_0

copies of a square with vertices 1,2,3 and 4 can be placed so the one covers the other with vertices on top of vertices (See Figure 2.2). We use ρ_i for rotations, δ_i for diagonal flips and μ_i for mirror images in perpendicular bisectors of sides. The total number of permutations involved are eight.

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \mu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \delta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix},$$

$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \delta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix},$$

In Table 2.3 the table for D_4 is given. Again, the group D_4 is non-abelian and the symmetries of the group table are beautiful!

An important theorem in group theory is **Cayley's Theorem** after the British mathematician Arthur Cayley. As one can observe from the group tables of finite groups it is not surprising that at least every finite group G is isomorphic to a subgroup of the group S_G of all permutations of G. Cayley's theorem states that this is also true for the infinite case, so that *every* group is isomorphic to some group consisting of permutations under permutation multiplication. This result is an intriguing result and is a classic of group theory.

Theorem 2.22 (**Cayley's Theorem**). *Every group is isomorphic to a group of permutations.*

2.5.1 Permutation Matrices

Definition 2.23. We can assign to each element $\sigma \in S_n$ an invertible $n \times n$ matrix, $D(\sigma)$, that has the property

$$D(\sigma_i \circ \sigma_j) = D(\sigma_i)D(\sigma_j). \tag{2.1}$$

The mapping $\sigma \to D(\sigma)$ is called a *matrix representation* of S_n.

To construct the matrices $D(\sigma)$ we proceed in a straightforward way: If the permutation assigns $i \to j$, put a 1 in the j, i entry of the matrix, otherwise insert a zero.

Under the mapping D, the matrix representations of the six elements of S_3 is

$$D(\sigma_0) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$D(\sigma_1) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$D(\sigma_2) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

$$D(\sigma_3) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$D(\sigma_4) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

$$D(\sigma_5) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

By direct calculation one can verify that Equation. 2.1 holds.

Since Cayley's theorem states that every group is isomorphic to a group of permutations, and these matrix representations can be generated for any permutation it follows that every finite group can be represented by square matrices composed of ones and zeros with only a single one in each row and column. These are called permutation matrices.

2.6 Orbits, Cycles and Cosets

There exist a natural partition of a set A into cells determined by each permutation σ of A. The partition has the property that $g, h \in A$ are in the same cell if and only if $h = \sigma^n(g)$ for some $n \in \mathbb{Z}$. With an appropriate equivalence relation we can establish this partition:

$$\text{For } g, h \in A, \text{ let } a \sim b \text{ if and only if } h = \sigma^n(g) \text{ for some } n \in \mathbb{Z}. \tag{2.2}$$

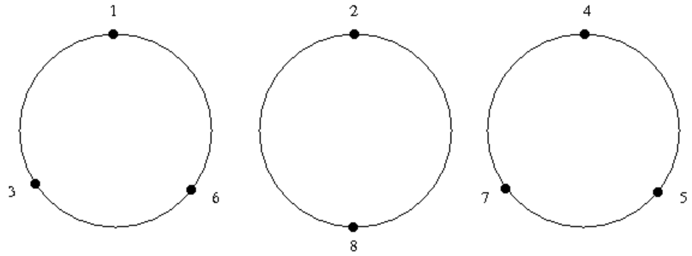


Figure 2.3: Orbits of σ

Definition 2.24. Let σ be a permutation of a set A. The equivalence classes in A determined by the equivalence relation 2.2 are the **orbits of** σ.

Definition 2.25. A permutation $\sigma \in S_n$ is a **cycle** if it has at most one orbit containing more than one element. The **length** of a cycle is the number of elements in its largest orbit.

Example 2.26. The orbits of

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix} \tag{2.3}$$

are shown in figure 2.3.

As one can see, σ acts on each integer from 1 to 8 by carrying it into the next integer. Figure 2.3 illustrates this, σ carries each integer counterclockwise. The leftmost circle indicates $\sigma(1) = 3$, $\sigma(3) = 6$ and $\sigma(6) = 1$. This makes Figure 2.3 a nice way to visualize the structure of the permutation σ. Also each circle individual in Figure 2.3 defines a permutation in S_8. For example, the rightmost circle corresponds to the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 7 & 4 & 6 & 5 & 8 \end{pmatrix} \tag{2.4}$$

that acts on 4,5 and 7, but leaves the remaining integers fixed.

To simplify notation for a cycle, we write a single-row *cyclic notation*. In this notation, the cycle in Equation (2.4) becomes

$$\mu = (4, 7, 5).$$

We understand from this notation that μ carries the number 4 to the number 7 and the number 7 to the number 5. Integers not in this notation for μ is understood to be left fixed by μ. Of course, the set $\{1, 2, 3, 4, 5, 6, 7, 8\}$ which μ acts on in our example is made clear from context.

Cycles are just special types of permutations so they can be multiplied just as any two permutations. The product of two cycles does not necessarily need to become a cycle again. The permutation in Equation (2.3) can be rewritten as a product of cycles using cyclic-notation:

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

The cycles above are **disjoint**, i.e integers are moved by at most one of the cycles. No number appears in the notation of two different cycles. We can express every permutation in S_n in an similar manner as a product of the disjoint cycles corresponding to its orbits. This is stated as a theorem below.

Theorem 2.27. *Every permutation σ of a finite set is a product of disjoint cycles.*

Multiplication of cycles is commutative, while in general permutation multiplication is not commutative.

2.6.1 Even and Odd Permutations

We have just seen that every permutation of a finite set is a product of disjoints cycles. It therefore seems reasonable that every reordering of the sequence $1, 2, ..., n$ can be achieved by interchanging the position of pairs of numbers.

Definition 2.28. A cycle of length 2 is a **transposition**.

Since a transposition is a cycle and is of length 2 it leaves all elements but two fixed, and maps each of these onto the other. The computation

$$(a_1, a_2, ..., a_n) = (a_1, a_n)(a_1, a_{n-1})...(a_1, a_3)(a_1, a_2).$$

shows that any cycle is a product of transpositions. Thus we have a corollary to Theorem 2.27.

Corollary 2.29. *Any permutation of a finite set of at least two elements is a product of transpositions.*

The transpositions need not to be disjoint, and a representation of the permutation in this way is not unique. We could for example insert the permutation $(1, 2)$ twice since $(1, 2)(1, 2)$ is the identity permutation in S_n for $n \geq 2$, but the number of transpositions used to represent a given permutation must either be even or odd. This important fact is always true.

Theorem 2.30. *No permutation in S_n can be expressed both as a product of an even number of transpositions and as a product of of an odd number of transpositions.*

Because of this theorem we can now define if an permutation is even or odd which also let us define the **Alternating group A_n on n letters**.

Definition 2.31. A permutation of a finite set is **even** or **odd** according to whether it can be expressed as a product of an even number of transpositions or the product of an odd number of transpositions.

Theorem 2.32. *If $n \geq 2$, then the collection of all even permutations of $\{1, 2, 3, ..., n\}$ forms a subgroup of order $n!/2$ of the symmetric group S_n.*

Definition 2.33. The subgroup of S_n consisting of the even permutations of n letters is the **Alternating group A_n on n letters**.

A_n and S_n are both very important groups. For example Cayle's theorem states that every finite group G is structurally identical to some subgroup of S_n for $n = |G|$. Because of that it can be shown that there are no formulas involving just radicals for solution of polynomial equations of degree $n \geq 5$. Surprising as it may seem this fact is due to the structure of A_n.

2.6.2 Cosets

One thing you may have noticed is that the order of a subgroup H of a finite group G always seems to divide the order of G. If the group G is partitioned into cells with the same size as H, the cells is called **cosets of** H. Therefore, if the number of such cells are r, we have

$$r(\text{order of } H) = (\text{order of } G).$$

Definition 2.34. Let H be a subgroup of a group G. The subset $aH = \{ah | h \in H\}$ of G is the **left coset** of H containing a, while the subset $Ha = \{ha | h \in H\}$ is the **right coset** of H containing a.

If the group G is abelian, the left and right cosets of a subgroup H are the same and the number of elements in every coset (left or right) of H are the same as in H.

Theorem 2.35 (Theorem of Lagrange). *Let H be a subgroup of a finite group G. Then the order of H is a divisor of the order of G.*

This is an elegant theorem an is regarded as a counting theorem. It also gives us some important corollaries and theorems

Corollary 2.36. *Every group of prime order is cyclic.*

Corollary 2.37. *The order of an element of a finite group divides the order of the group.*

There is only one group structure, up to isomorphism, of an given primer order p, since every cyclic group of order p is isomorphic to $\mathbb{Z}_p$.

Definition 2.38. Let H be a subgroup G. The number of left cosets of H in G is the **index** (G:H) **of** H **in** G.

The index (G:H) may be finite or infinite. If G is a finite group, then (G:H) is finite and we have (G:H)=$|G|/|H|$. The index (G:H) could be equally defined as the number of right cosets of H in G.

Theorem 2.39. *Suppose H and K are subgroups of a group G such that $K \leq H \leq G$, and suppose (H:K) and (G:H) are both finite. Then (G:K) is finite, and (G:K)=(G:H)(H:K).*

We know, because of Theorem 2.35, that if there is a subgroup H of a finite group G, then the order of H divides the order of G. If the group is also abelian it can be shown that the converse is also true. I.e, if G is a group of order n, and m divides n, then there is a subgroup of order m. However, this is not true in the nonabelian case, since A_4 has no subgroup of order 6. which provides us with a counterexample.

Definition 2.40. A subgroup of H of a group G is **normal** if its left and right cosets coincide, that is, if gH=Hg for all $g \in G$.

It is easily seen that all subgroups of an abelian group is normal.

2.7 Finitely Generated Abelian Groups

Up to now we have seen a variety of groups. From the finite groups we have the cyclic group $\mathbb{Z}_n$, the symmetric group S_n, the alternating group A_n and the dihedral groups D_n. We have also seen that the subgroups of these groups exist. In the infinite case we have groups consisting of sets of numbers under familiar operation like addition, as $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$, and their nonzero version under multiplication. The goal of this section is to use known groups as building blocks to form more groups by taking the **direct product** or **direct sum** of groups.

2.7.1 Direct Products

To define the direct product we first have to generalize the well known **Cartesian product** to sets

Definition 2.41. The **Cartesian product of sets** $S_1, S_2, ..., S_n$ is the set of all ordered n-tuples $(a_1, a_2, ..., a_n)$, where $a_i \in S_i$ for i=1,2,...,n. The Cartesian product is denoted by either

$$S_1 \times S_2 \times ... \times S_n$$

or by

$$\prod_{i=1}^{n} S_i.$$

The idea now is to let $G_1, G_2, ..., G_n$ be groups and use the same multiplicative notation for all the group operations. Regarding G_i as sets corresponding to each group G_i, we form the product $\prod_{i=1}^{n} G_i$. It can then be shown that $\prod_{i=1}^{n} G_i$ can be made into a group with a binary operation of *multiplication by components*.

Theorem 2.42. *Let $G_1, G_2, ..., G_n$ be groups. For $(a_1, a_2, ..., a_n)$ and $(b_1, b_2, ..., b_n)$ in $\prod_{i=1}^n G_i$, define $(a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n)$ to be the element $(a_1b_1, a_2b_2, ..., a_nb_n)$. Then $\prod_{i=1}^n G_i$ is a group, the* ***direct product of the groups*** *G_i, under this binary operation.*

Should the operation for each G_i be commutative, it is common to use additive notation for $\prod_{i=1}^n G_i$, and refer to $\prod_{i=1}^n G_i$ as the **direct sum of the groups** G_i. Instead of $\prod_{i=1}^n G_i$ the notation $\bigoplus_{i=1}^n G_i$ is sometimes used. Also, in this case it can be shown that the direct product/sum of abelian groups is again abelian.

Theorem 2.43. *The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic and is isomorphic to $\mathbb{Z}_{mn}$ if and only if m and n are relatively prime, that is, the* ***greatest common divisor*** *(gcd) of m and n is 1.*

Of course this theorem can be extended to a product of more than two factors. The next corollary states this.

Corollary 2.44. *The $\prod_{i=1}^n \mathbb{Z}_{m_i}$ is cyclic and isomorphic to $\mathbb{Z}_{m_1 m_2 ... m_n}$ if and only if the numbers m_i for i=1,...,n are such that the gcd of any two of them is 1.*

If n is written as a product of powers of distinct prime numbers, as in

$$n = (p_1)^{n_1}(p_2)^{n_2}...(p_r)^{n_r},$$

then Corollary 2.44 shows that $\mathbb{Z}_n$ is isomorphic to

$$\mathbb{Z}_{(p_1)^{n_1}} \times \mathbb{Z}_{(p_2)^{n_2}} \times ... \times \mathbb{Z}_{(p_r)^{n_r}}.$$

For example, $\mathbb{Z}_{72}$ is isomorphic to $\mathbb{Z}_8 \times \mathbb{Z}_9$.

Definition 2.45. Let $r_1, r_2, ..., r_n$ be positive integers. Their **least common multiple**, (abbreviated lcm) is the positive generator of the cyclic group of all common multiples off the r_i, that is, the cyclic group of all integers divisible by each r_i for i=1,2,...,n.

From the last definition and the theory on cyclic groups, we see that the lcm of $r_1, r_2, ..., r_n$ is the smallest nonnegative integer that is a multiple of each of the r_i, hence the name *least common multiple.*

Theorem 2.46. *Let $(a_1, a_2, ..., a_n) \in \prod_{i=1}^n G_i$. If a_i is of finite order r_i in G_i, then the order of $(a_1, a_2, ..., a_n)$ in $\prod_{i=1}^n G_i$ is equal to the least common multiple of all the r_i.*

2.7.2 The Structure of Finitely Generated Abelian Groups

The next theorem gives us complete information about the structure of all sufficiently small abelian groups, especially, about all finite abelian groups.

Theorem 2.47 (**Fundamental Theorem of Finitely Generated Abelian Groups**). *Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups in the form*

$$\mathbb{Z}_{(p_1)^{n_1}} \times \mathbb{Z}_{(p_2)^{n_2}} \times ... \times \mathbb{Z}_{(p_r)^{n_r}} \times \mathbb{Z}^n,$$

*where the p_i are primes, not necessarily distinct, and the r_i are positive integers. The direct product is unique except for possible rearrangement of the factors; that is, the number (**Betti number** of G) of factors $\mathbb{Z}$ is unique and the prime powers $(p_i)^{r_i}$ are unique.*

We end this section with a small portion of all the theorems regarding abelian groups that follows or can be proved because of Theorem 2.47.

Definition 2.48. A group G is **decomposable** if it is isomorphic to a direct product of two proper nontrivial subgroups. Otherwise G is **indecomposable**.

Theorem 2.49. *The finite indecomposable abelian groups are exactly the cyclic groups with order a power of a prime.*

Theorem 2.50. *If m divides the order of a finite abelian group G, then G has a subgroup of order m.*

Theorem 2.51. *If m is a square free integer, that is, m is not divisible by the square of any prime, then every abelian group of order m is cyclic.*

2.8 Homomorphisms

A mapping from a group G into another group G' which relates the group structure of G to the group structure of G', gives information about one of the groups from known structural properties of the other. The known isomorphism $\phi : G \to G'$, if one exist, is an example of such a structural-relating map. If everything is known about the structure of the group G and ϕ is an isomorphism, we know all about the structure of the group G'. It is just a structurally copy of G. If the condition of an isomorphism is weakened so that we no longer require that the maps should be one to one and onto we can consider more general structure-relating maps.

Definition 2.52. A map ϕ of a group G into a group G' is a **homomorphism** if the homomorphism property

$$\phi(ab) = \phi(a)\phi(b)$$

holds for all $a, b \in G$.

In the next theorem we state some the properties which are preserved by a homomorphism $\phi : G \to G'$, but first we need to review set-theoretic definitions.

Definition 2.53. Let ϕ be a mapping of a set X into a set Y, and let $A \subseteq X$ and $B \subseteq Y$. The **image** $\phi[A]$ **of** A **in** Y **under** ϕ is $\{\phi(a)|a \in A\}$. The set $\phi[X]$ is the **range of** ϕ. The **inverse image** ϕ^{-1} **of** B **in** X is $\{x \in X|\phi(x) \in B\}$.

The *square brackets* is used when we apply a function to a subset of its domain.

Theorem 2.54. *Let ϕ be a homomorphism of a group G into a group G'.*

1. *If e is the identity element in G, then $\phi(e)$ is the identity element e' in G'.*
2. *If $a \in G$, then $\phi(a^{-1}) = \phi(a)^{-1}$.*
3. *If H is a subgroup of G, then $\phi[H]$ is a subgroup of G'.*
4. *If K' is a subgroup of G', then $\phi^{-1}[K']$ is a subgroup of G.*

In a more loose sense, ϕ preserves the identity element, inverses and subgroups. The subset $\{e'\}$ is a subgroup of G', so from property 4 in Theorem 2.54 we have that $\phi^{-1}[\{e'\}]$ is a subgroup H of G, and in the study of homomorphism this subgroup is critical.

Definition 2.55. Let $\phi : G \to G'$ be a homomorphism of groups. The subgroup $\phi^{-1}[\{e'\}] = \{x \in G | \phi(x) = e'\}$ is the **kernel of** ϕ denoted by $Ker(\phi)$.

The next theorem relates the kernel of ϕ and the cosets of the subgroup H of G.

Theorem 2.56. *Let $\phi : G \to G'$ be a group homomorphism, and let $H = Ker(\phi)$. Let $a \in G$. Then the set*

$$\phi^{-1}[\{\phi(a)\}] = \{x \in G | \phi(x) = \phi(a)\}$$

is the left coset aH of H, and is also the right coset Ha of H. Consequently, the two partitions of G into left cosets and into right cosets of H are the same.

An important corollary follows from Theorem 2.56 and is used to show when an isomorphism is a one-to-one map.

Corollary 2.57. *A group homomorphism $\phi : G \to G'$ is a one-to-one map if and only if $Ker(\phi) = \{e\}$.*

Another corollary which follows from Definition 2.40 and the last statement of Theorem 2.54 is

Corollary 2.58. *If $\phi : G \to G'$ is a group homomorphism, then $Ker(\phi)$ is a normal subgroup of G.*

Two things are of primary importance in any group homomorphism $\phi : G \to G'$: The *kernel* of ϕ and the *image* $\phi[G]$ of G in G'. The importance of $Ker(\phi)$ has been indicated and in the next section the importance of the image $\phi[G]$ will be indicated.

2.9 Factor Groups

The cosets of H can form a group called a **factor group**, if H is the kernel of a group homomorphism $\phi : G \to G'$ and the binary operation is derived from the group operation of G. More formally we can write

Theorem 2.59. *Let $\phi : G \to G'$ be a group homomorphism with kernel H. Then the cosets of H form a factor group, G/H, where (aH)(bH)=(ab)H. Also, the map $\mu : G/H \to \phi[G]$ defined by $\mu(aH) = \phi(a)$ is an isomorphism. Both coset multiplication and μ are well defined, independent of the choices a and b from the cosets.*

Knowing how to compute in factor group is very important. By choosing *any* two representative elements from the cosets we can multiply (add) two cosets by multiplying (adding) the representative elements together and find the coset in which the resulting product(sum) lies.

Example 2.60. The factor group $\mathbb{Z}/5\mathbb{Z}$ has the cosets

$$5\mathbb{Z} = \{..., -10, -5, 0, 5, 10, ..\},$$

$$1 + 5\mathbb{Z} = \{..., -9, -4, 1, 6, 11, ..\},$$

$$2 + 5\mathbb{Z} = \{..., -8, -3, 2, 7, 12, ..\},$$

$$3 + 5\mathbb{Z} = \{..., -7, -2, 3, 8, 13, ..\},$$

$$4 + 5\mathbb{Z} = \{..., -6, -1, 4, 9, 14, ..\}.$$

To find the coset we get when we add $(2 + 5\mathbb{Z}) + (4 + 5\mathbb{Z})$, we choose 2 from the first coset, 4 from the second, and find that the answer $2 + 4 = 6$ is in the coset $1 + 5\mathbb{Z}$.

We refer to cosets of $n\mathbb{Z}$ as *residue classes modulo n*. Integers in the same coset are *congruent modulo n*. This is why G/H is often called the **factor group of G modulo H**. Elements in same coset of H is said to be **congruent modulo H**.

2.9.1 Factor Groups from Normal Subgroups

Theorem 2.61. *Let H be a subgroup of a group G. Then the left coset multiplication is well defined by the equation*

$$(aH)(bH) = (ab)H$$

if and only if H is a normal subgroup of G.

Theorem 2.61 shows that $(aH)(bH) = (ab)H$ is a well-defined binary operation on cosets if the left and right cosets of H coincide. And the next corollary shows that the cosets also form a group with this coset multiplication.

Corollary 2.62. *Let H be a normal subgroup of G. Then the cosets of H form a subgroup G/H under the binary operation*

$$(aH)(bH) = (ab)H$$

.

Definition 2.63. The group G/H in the preceding corollary is the **factor group** (or **quotient group**) of G by H.

2.9.2 The Fundamental Homomorphisms Theorem

We saw in the preceding paragraph that every homomorphism $\phi : G \to G'$ gives rise to a natural factor group, $G/\mathrm{Ker}(\phi)$ by Theorem 2.59. The next theorem shows that each factor group G/H gives a natural homomorphism with H as a kernel.

Theorem 2.64. *Let H be a normal subgroup of G. Then $\gamma : G \to G/H$ given by $\gamma(x) = xH$ is a homomorphism with kernel H.*

The next theorem called **The Fundamental Homomorphisms Theorem** shows the relation between ϕ, γ and μ.

Theorem 2.65 (**The Fundamental Homomorphisms Theorem**). *Let $\phi : G \to G'$ be a group homomorphism with kernel H. Then $\phi[G]$ is a group, and $\mu : G/H \to \phi[G]$ given by $\mu(gH) = \phi(g)$ is an isomorphism. If $\gamma : G \to G/H$ is the homomorphism given by $\gamma(g) = gH$, then $\phi(g) = \mu\gamma(g)$ for each $g \in G$.*

The name of the isomorphism μ and homomorphism γ in Theorem 2.65 is referred to respectively as a *natural/canonical* isomorphism or homomorphism. To sum up, every homomorphism with domain G gives a factor group G/H, and each factor group G/H gives a homomorphism mapping G into G/H. There is a close relationship between homomorphism and factor groups. The next example indicates how useful the relationship is.

Example 2.66. To classify the group $(\mathbb{Z}_4 \times \mathbb{Z}_2)/(0 \times \mathbb{Z}_2)$ accordingly to the fundamental theorem of finitely generated abelian groups we proceed in the following manner: The projection map $\pi_1 : \mathbb{Z}_4 \times \mathbb{Z}_2 \to \mathbb{Z}_4$ given by $\pi_1(x, y) = x$ is a homomorphism $\mathbb{Z}_4 \times \mathbb{Z}_2$ onto $\mathbb{Z}_4$ with kernel $\{0\} \times \mathbb{Z}_2$. Theorem 2.65 shows that the given factor group is isomorphic to $\mathbb{Z}_4$.

2.9.3 Normal Subgroups and Inner Automorphisms

In the following theorem some alternative characterizations of normal subgroups are given. This often provides an easier way to check normality than finding the coset decompositions of both the left and right cosets.

Theorem 2.67. *The following are three equivalent conditions for a subgroup H of a group G to be a normal subgroup of G.*

1. $ghg^{-1} \in H$ *for all* $g \in G$ *and* $h \in H$.
2. $gHg^{-1} = H$ *for all* $g \in G$.
3. $gH = Hg$ *for all* $g \in G$.

The second condition of Theorem 2.67 is often used as the definition of a normal subgroup H of G. One can also easily see from Theorem 2.67 that every subgroup H of an abelian group G is normal. $gh = hg$ for all $h \in H$ and all $g \in G$, hence, $ghg^{-1} = h \in H$ for all $g \in G$ and all $h \in H$, so H is normal.

Definition 2.68. An isomorphism $\phi : G \to G$ of a group G with itself is an **automorphism** of G. The automorphism $i_g : G \to G$, where $i_g(x) = gxg^{-1}$ for all $x \in G$, is the **inner automorphism of** G **by** g. Performing i_g on x is called **conjugation of** x **by** g.

By this definition and by Theorem 2.67 $gH = Hg$ for all $g \in G$ is only satisfied if and only if $i_g[H] = H$ for all $g \in G$. i.e, if and only if H is **invariant** under all inner automorphism of G. A subgroup $K = i_g[H]$ of G is called a **conjugate subgroup** of H for some $g \in G$.

2.10 G-Set - Group Action on a Set

Earlier we have seen examples of how group acts on things, like for example the group of symmetries of a triangle or of a square. More can be named, like the group of rotations of a cube, the general linear group acting on $\mathbb{R}^n$, and so on. In this section we are going to see groups acting on sets.

2.10.1 Group Action

Definition 2.69. Let X be a set and G a group. An **action of** G **on** X is a map $\circ : G \times X \to X$ such that

1. $ex = x$ for all $x \in X$,
2. $(g_1g_2)(x) = g_1(g_2x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

Under these conditions, X is a G**-set.**

The next theorem says that for every G-set X and for every $g \in G$, the mapping $\sigma_g : X \to X$ defined by $\sigma_g(x) = gx$ is a permutation of X.

Theorem 2.70. *Let X be a G-set. For each* $g \in G$, *the function* $\sigma_g : X \to X$ *defined by* $\sigma_g(x) = gx$ *for* $x \in X$ *is a permutation of X. Also, the map* $\phi : G \to S_X$ *defined by* $\phi(g) = \sigma_g$ *is a homomorphism with the property that* $\phi(g)(x) = gx$.

From the preceding theorem and Theorem 2.56 it follows that if X is a G-set, then the subset of G which leaves every element of X fixed is a normal subgroup N of G. One can now regard X as a G/N-set where the action of a coset gN on X is given by $(gN)x = gx$ for each $x \in X$. We say that G **acts faithfully** on X if $N = \{e\}$, since the identity element of G is the only element which leaves every element $x \in X$ fixed. If for every elements $x_1, x_2 \in X$, there exist $g \in G$ that relates x_1, x_2 as $gx_1 = x_2$ we say that G **acts transitively** on X.

Example 2.71. Every group G is its own G-set with the action on $g_2 \in G$ by $g_1 \in G$ defined by left multiplication $\circ(g_1, g_2) = g_1 g_2$. If H is a subgroup of G, G is also regarded as a H-set, with the action defined by $\circ(h, g) = hg$.

2.10.2 Isotropy Subgroups

For a G-set X, and for $x \in X$ and $g \in G$, it will be important to know when $gx = x$. Let

$$X_g = \{x \in X | gx = x\}$$

and

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

The question now is if there exist cases where G_x is subgroup of G. As the next theorem will show, this is true in general.

Theorem 2.72. *Let X be a G-set. Then G_x is a subgroup of G for each $x \in X$.*

Definition 2.73. Let X be a G-set and let $x \in X$. The subgroup G_x is the **isotropy subgroup of** x.

2.10.3 Orbits

If G acts on a G-set X but not transitively, X becomes divided into multiple equivalence classes by G and these equivalence classes containing $x \in X$ is called the **orbits** of x. The next theorems shows this and some more properties.

Theorem 2.74. *Let X be a G-set. For $x_1, x_2 \in X$, let $x_1 \sim x_2$ if and only if there exist $g \in G$ such that $gx_1 = x_2$. Then $\sim$ is an equivalence relation on X.*

Definition 2.75. Let X be a G-set. Each cell in the partition of the equivalence relation described in Theorem 2.74 is an **orbit in** X **under** G. If $x \in X$, the cell containing x is the **orbit of** x. We let this cell be Gx.

Theorem 2.76. *Let X be a G-set and let $x \in X$. Then $|Gx| = (G : G_x)$. If $|G|$ is finite, then $|Gx|$ is a divisor of $|G|$.*

An interesting property of isotropy group is given in the following theorem

Theorem 2.77. *Given a group G acting on a set X, the conjugation of any isotropy group G_x by $g \in G$ for any $x \in X$ is an isotropy group, and in particular*

$$gG_xg^{-1} = G_{g \cdot x}$$

2.10.4 G-Morphisms

Given two sets X and Y on which a group G acts. We distinguish between two different kind of actions by denoting them as $g \circ x \in X$ and $g \bullet y \in Y$ for all $x \in X$ and $y \in Y$. We define a $G-$ *morphism* as the mapping $f : X \to Y$ with the property

$$f(g \circ x) = g \bullet f(x).$$

This property is often called $G-$ *equivariance.*

Example 2.78. Suppose $g \bullet y = y$ for all $y \in Y$ and $g \in G$. Then the mapping $f : X \to Y$ with the property

$$f(g \circ x) = f(x)$$

for all $x \in X$ is a G-morphism that is constant on each orbit.

2.10.5 G-sets, Counting and Burnside's Formula

One application of G-sets is to counting. The following theorem, named **Burnside's Formula** after the English mathematician William Burnside, provides us with a tool for counting the number of orbits in a G-set X under G. We let $X_g = \{x \in X \mid gx = x\}$, that is, X_g is the set of elements of X left fixed by g.

Theorem 2.79 (**Burnside's Formula**). *Let G be a finite group and X a finite G-set. If r is the number of orbits in X under G, then*

$$r \cdot |G| = \sum_{g \in G} |X_g|. \tag{2.5}$$

2.11 Conjugacy Classes and Class Functions

We remember that two elements $a, b \in G$ is said to be *conjugate* to each other if for some $g \in G$ we have $a = g^{-1}bg$. This is an equivalence relation since the *reflexivity, symmetry and transitivity* properties holds. We get a subgroup of G, called a *conjugate subgroup*, if we conjugate all the elements of a subgroup $H \leq G$ with respect to a specific $g \in G$. This subgroup is denoted $g^{-1}Hg$.

On the other hand, if we instead of fixing an element g and conjugate whole subgroups by g, we fix an element $b \in G$ and calculate $g^{-1}bg$ for *all* $g \in G$. This result is a set of elements in G called the *conjugacy class* containing b. All elements in the same conjugacy class are conjugate to every other elements in the same conjugacy class, and each elements can only belong to one class. This follows from the fact that an equivalence relation partitions a set into subsets which are disjoint. We let C_i denote the ith conjugacy class and $|C_i|$ denotes the number of group elements in this class, then

$$\sum_{i=1}^{\alpha} |C_i| = |G| \tag{2.6}$$

where α is the number of classes and Equation (2.6) is called the *class equation.* $|C_i| = 1$ for all i only when G is abelian, and thus this is the only case where $\alpha = |G|$.

2.11.1 Class Functions and Sums

A function $\mathcal{C} \; : \; G \to \mathbb{C}$ which is constant on conjugacy classes is called the *class function.* The value of a class function is the same for all elements of each conjugacy class. So we have

$$\mathcal{C}(g) = \mathcal{C}(h^{-1}gh) \qquad \text{or} \qquad \mathcal{C}(hg) = \mathcal{C}(gh)$$

for all values of $g, h \in G$. These two equations are completely equivalent since the change of variables $g \longrightarrow hg$ is invertible.

Using shifted δ-functions, we define the *class sum* function as

$$\mathcal{C}_i(g) = \sum_{a \in \mathcal{C}_i} \delta(a^{-1}g) \tag{2.7}$$

This is the characteristic function of the set $\mathcal{C}_i$, since Equation (2.7) is a class function with the property

$$\mathcal{C}_i(g) = \begin{cases} 1 & \text{for } g \in \mathcal{C}_i \,, \\ 0 & \text{for } g \notin \mathcal{C}_i . \end{cases}$$

2.11.2 Relationship between Double Cosets and Conjugacy Classes

Definition 2.80. Let $H < G$ and $K < G$. Then for any $g \in G$, the set

$$HgK = \{hgk \mid h \in H, k \in K\}$$

is called the *double coset* of H and K.

Any $g' \in HgK$ is called a *representative* of the double coset. The order of the double cosets are $|HgK| \leq \; |G|$ and in general $|HgK| \neq |H| \cdot |K|$. In some special cases $|HgK| = |H| \cdot |K| = |G|$. Like for example, when every $g \in G$ can be uniquely decomposed as $g = hk$ for $h \in H$ and $k \in K$, we then have

$$H(hk)K = H(hek)K = (Hh)e(kK) = HeK = G.$$

In general, we denote the set of all double cosets of H and K as $H \backslash G/K$. Hence, we have $g \in HgK \in H \backslash G/K$.

Theorem 2.81. *Membership in a double coset is an equivalence relation on G. That is, G is partitioned into disjoint double cosets, and for $H < G$ and $K < G$ either $Hg_1K \cap Hg_2K = \emptyset$ or $Hg_1K = Hg_2K$.*

It follows from Theorem 2.81 that for any finite group, we may write

$$G = \bigcup_{i=1}^{|H\backslash G/K|} H\sigma_i K \qquad \text{and} \qquad |G| = \sum_{i=1}^{|H\backslash G/K|} |H\sigma_i K|$$

where σ_i is an representative of the ith double coset. Unlike the single cosets case where $|gH| = |H|$, the assumption that all the double cosets have the same size is wrong. If we can make the decomposition $g = hk$, the meaning of the fact that double coset must be disjoint or identical is $H\backslash G/K = \{G\}$ and $|H\backslash G/K| = 1$.

Theorem 2.82. *Given $H < G$ and $K < G$ and $g_1, g_2 \in G$ such that $g_1K \cap Hg_2K \neq \emptyset$, then $g_1K \subseteq Hg_2K$.*

If we denote $G{\cdot}G$ as the subset of $G \times G$ (recall that $G \times G$ is the direct product of G and G of all pairs (g, h) for $g, h \in G$ with the operation defined as $(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$) consisting of all pairs of the $(g, g) \in G \times G$, we have the following theorem about the relationship between double cosets and conjugacy classes

Theorem 2.83. *Given a finite group G, there is a bijective mapping between the set of double cosets $(G \cdot G)\backslash(G \times G)/(G \cdot G)$ and the set of conjugacy classes of G, and hence*

$$\alpha = |(G \cdot G)\backslash(G \times G)/(G \cdot G)|,$$

where α is the number of conjugacy classes of G.

2.12 Lie Groups

A Lie group is a group which is also an analytic manifold. The group is named after the Norwegian Mathematician Sophus Lie, who laid the foundation of the theory of continuous transformation groups. Lie groups is the best-developed theory of continuous symmetry of mathematical objects and structures, and is an indispensable tools for many parts of contemporary mathematics, as well as for modern theoretical physics.

2.12.1 Rigorous Definitions

We start this section by giving some definitions of Lie groups

Definition 2.84. A Lie Group $(G, \circ)$ is a group for which the set G is an analytic manifold, with the operation $(g_1, g_2) \to g_1g_2$ and $g \to g^{-1}$ being analytic.

The dimension of the Lie group is the same as the dimension of the associated manifold G.

Definition 2.85. A *matrix* Lie group $(G, \circ)$ is a Lie group where G is a set of square matrices and the group operation is the usual matrix multiplication.

Another way to state Definition 2.85 is that a matrix Lie group is a closed Lie subgroup of $\mathbb{GL}(N,\mathbb{R})$ or $\mathbb{GL}(N,\mathbb{C})$. In this thesis we will deal exclusively with matrix Lie groups.

Elements of a matrix Lie group sufficiently close to the identity are written as $g(t) = e^{tX}$ for some $X \in \mathcal{G}$ (The Lie algebra of G) and t near 0. The matrix exponential is defined with the same power series as the scalar exponential function

$$e^{tX} = \mathbb{I}_{N\times N} + \sum_{n=1}^{\infty} \frac{t^n X^n}{n!}.$$

We use small letters for the corresponding Lie algebra of the matrix Lie groups. Thus, the corresponding Lie algebras of the groups $\mathbb{GL}(N,\mathbb{R}), SO(N)$ and $SE(N)$ are respectively denoted as $gl(N,\mathbb{R}), so(N)$ and $se(N)$. One of Sophus Lie's key idea, was to replace the global object, the group, with its linearized or local version, which has since become known as its Lie algebra. Lie himself called this the "infinitesimal group." Therefore, we study the matrices $\frac{dg}{dt}g^{-1}$ and $g^{-1}\frac{dg}{dt}$, which are respectively called the *tangent vectors* or *tangent elements* at g. If we evaluate it at $t = 0$, these vectors reduces to X.

Definition 2.86. The *adjoint* operator is defined as

$$Ad(g_1)X = \frac{d}{dt}(g_1 e^{tX} g_1^{-1})|_{t=0} = g_1 X g_1^{-1}.$$

Definition 2.86 gives a homomorphism $Ad : G \to \mathbb{GL}(\mathcal{G})$ from the group into the set of all invertible linear transformations of $\mathcal{G}$ onto itself. The homomorphism is shown as

$$Ad(g_1)Ad(g_2)X = g_1(g_2 X g_2^{-1})g_1^{-1} = (g_1g_2)X(g_1g_2)^{-1} = Ad(g_1g_2)X.$$

The linearity is shown as

$$Ad(g)c_1X_1+c_2X_2) = g(c_1X_1+c_2X_2)g^{-1} = c_1gX_1g^{-1}+c_2gX_2g^{-1} = c_1Ad(g)X_1+c_2Ad(g)X_2.$$

For a 1-parameter subgroup when $g = g(t)$ is an element close to $\mathbb{I}$, we may approximate $g(t) \approx \mathbb{I}_{N\times N} + tX$ for small t. We then get $Ad(\mathbb{I}_{N\times N} + tX)Y = Y + t(XY - YX)$. The *Lie Bracket* is defined as the quantity

$$XY - YX = [X,Y] = \frac{d}{dt}(Ad(g(t))Y)|_{t=0} = ad(X)Y. \tag{2.8}$$

In Equation (2.8) the last equality defines $ad(X)$ and one observes from this definition

$$Ad(exp(t \cdot ad(X)).$$

It is easily seen from Equation (2.8) that the Lie brackets is linear in each entry

$$[c_1X_1 + c_2X_2, Y] = c_1[X_1,Y] + c_2[X_2,Y]$$

and

$$[X, c_1Y_1 + c_2Y_2] = c_1[X,Y_2] + c_2[X,Y_2].$$

The Lie bracket is also anti-symmetric

$$[X, Y] = -[Y, X].$$

Thus $[X, X] = 0$. Let $\mathcal{G}$ be a Lie algebra of finite dimension, and let $\{X_1, ..., X_n\}$ be a basis for $\mathcal{G}$. The Lie bracket of any of the two elements results in a linear combination of all basis elements

$$[X_i, X_j] = \sum_{k=1}^{n} C_{ij}^k X_k.$$

The constants, real or complex numbers C_{ij}^k are called the *structure constant* of $\mathcal{G}$. Two finite-dimensional Lie Algebras are isomorphic if they have the same structure constant.

Given any three elements of the Lie algebra $\mathcal{G}$, the *Jacobi identity* is satisfied

$$[X_1, [X_2, X_3]] + [X_2, [X_3, X_1]] + [X_3, [X_1, X_2]] = 0. \tag{2.9}$$

It follows from the Jacobi identity that $ad(X)$ satisfies

$$ad([X, Y]) = ad(X)ad(Y) - ad(Y)ad(X).$$

There exist an important relationship between the Lie bracket and matrix exponential called the *Baker-Campbell-Hausdorff formula*. It allows us to express the product of two Lie group elements written as exponential of Lie algebra elements as

$$e^X e^Y = e^{Z(X,Y)}$$

where

$$Z((X, Y) = X + Y + \frac{1}{2}[X, Y] + \frac{1}{12}([X, [X, Y]] + [Y, [Y, X]] + \cdots .$$

For a connected Lie group, the matrix exponential provides us with a tool for parameterizing it.

2.12.2 Calculating Jacobians

An orthonormal basis for the Lie algebra can always be found for a finite-dimensional matrix Lie group if an appropriate inner product is defined. We can construct such a basis bye the Gram-Schmidt orthogonalization procedure given any Lie algebra basis.

The inner product between elements of the Lie algebra may be defined as

$$(X, Y) = \frac{1}{2}\mathrm{Re}[\mathrm{trace}(XWY^\dagger)] \tag{2.10}$$

where W is a Hermitian weighting matrix with positive eigenvalues. If Lie group is a real matrix Lie group, the matrices of the Lie algebra will be real, thus the inner product becomes

$$(X, Y) = \frac{1}{2}\mathrm{trace}(XWY^T),$$

where W is now a real symmetric positive defined matrix.

Definition 2.87. Given an orthonormal basis $X_1, ..., X_n$ for the Lie algebra, elements of the right- and left-Jacobian matrices is given by the projection of the left and right tangent operators onto this basis

$$(J_R)_{ij} = (g^{-1}\frac{\partial g}{\partial x_i}, X_j) \qquad \text{and} \qquad (J_L)_{ij} = (\frac{\partial g}{\partial x_i} g^{-1}, X_j)$$

Where $g = g(x_1, ..., x_n)$ and $\{x_1, ..., x_n\}$ is the set of local coordinates used to parameterize the neighbourhood of the group around the identity.

There exist, for an n-dimensional matrix Lie group, two special kinds of vector fields denoted as

$$V_L(g) = \sum_{i=1}^{n} v_i X_i g \qquad \text{and} \qquad V_R(g) = \sum_{i=1}^{n} v_i g X_i.$$

The subscript of V indicates which side of the Lie algebra the basis elements appears. Since we restrict the discussion to real vector fields, $X_i g$ and gX_i are simply matrix products, and $\{v_i\}$ are real numbers. The left- and right-shift operation for a vector field $V(g)$ on a matrix Lie group are defined as

$$L(h)V(g) = hV(g) \qquad \text{and} \qquad R(h)V(g) = V(g)h$$

where $h \in G$. It is then clear that V_L is *right-invariant* and V_R is *left-invariant* in the sense that

$$L(h)V_R(g) = V_R(hg) \qquad \text{and} \qquad R(h)V_L(g) = V_L(gh).$$

From there it follows that there are left- and right-invariant ways to extend the inner product $(\cdot, \cdot)$ on the Lie algebra over the whole group. For all $Y, Z \in \mathcal{G}$ we define the right and left inner product respectively as

$$(gY, gZ)_g^R \triangleq (Y, Z) \qquad \text{and} \qquad (Yg, Zg)_g^L \triangleq (Y, Z)$$

for any $g \in G$. Defined this way, the inner product of two invariant vector fields $Y_L(g)$ and $Z_L(g)$ (or $Y_R(g)$ and $Z_R(g)$) yields

$$((Y_L(g), Z_L(g))_g^L) = ((Y_R(g), Z_R(g))_g^R) = (Y, Z).$$

Theorem 2.88. *Given a matrix Lie group G with an orthonormal basis $\{X_i\}$ for $\mathcal{G}$. If $Y = \sum_{i=1}^n y_i X_i$ and $Z = \sum_{i=1}^n z_i X_i$, it follows that*

$$(Y, Z) = \sum_{i=1}^{n} y_i z_i.$$

The (i, j) entry of the left Jacobian, is in this notation $\frac{\partial g}{\partial x_i}$, projected on the jth basis element for the tangent space to G at g as

$$(J_L)_{ij} = (\frac{\partial g}{\partial x_i}, X_j g)_g^L = (\frac{\partial g}{\partial x_i} g^{-1}, X_j).$$

And

$$(J_R)_{ij} = (\frac{\partial g}{\partial x_i}, gX_j)_g^R = (g^{-1}\frac{\partial g}{\partial x_i}, X_j).$$

Jacobians for SE(2)

The *special Euclidean motion group* (the Euclidean motion group, Euclidean group or just the motion group) of the plane $SE(2) = \mathbb{R}^2 \rtimes_\varphi SO(2)$ is the group of rigid motion of the plane and is itself a three dimensional Lie group. The Lie algebra is denoted $se(2)$. $SE(2)$ may be parameterized as

$$g(x_1, x_2, \theta) = exp(x_1 X_1 + x_2 X_2) exp(\theta X_3) = \begin{pmatrix} \cos\theta & -\sin\theta & x_1 \\ \sin\theta & \cos\theta & x_2 \\ 0 & 0 & 1 \end{pmatrix}$$

where

$$X_1 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}; \qquad X_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}; \qquad X_3 = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

We observe that $(X_i, X_j) = \delta_{ij}$ if we use the weighting matrix

$$W = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

With this parameterization, basis and weighting matrix, the Jacobians are of the form

$$J_R = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and

$$J_L = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ x_2 & -x_1 & 1 \end{pmatrix}.$$

Observe that

$$\det(J_L) = \det(J_R) = 1.$$

In a similar manner we can examine the Jacobians for the exponential parameterization

$$g(v_1, v_2, \alpha) = \exp(v_1 X_1 + v_2 X_2 + \alpha X_3) = \begin{pmatrix} 0 & -\alpha & v_1 \\ \alpha & 0 & v_2 \\ 0 & 0 & 0 \end{pmatrix}.$$

In this case the Jacobians have the form

$$J_R = \begin{pmatrix} \frac{\sin\alpha}{\alpha} & \frac{\cos\alpha - 1}{\alpha} & 0 \\ \frac{1-\cos\alpha}{\alpha} & \frac{\sin\alpha}{\alpha} & 0 \\ \frac{\alpha v_1 - v_2 + v_2\cos\alpha - v_1 \sin\alpha}{\alpha^2} & \frac{v_1 + \alpha v_2 + v_1 \cos\alpha - v_2 \sin\alpha}{\alpha^2} & 1 \end{pmatrix}$$

and

$$J_L = \begin{pmatrix} \frac{\sin\alpha}{\alpha} & \frac{1-\cos\alpha}{\alpha} & 0 \\ \frac{\cos\alpha-1}{\alpha} & \frac{\sin\alpha}{\alpha} & 0 \\ \frac{\alpha v_1+v_2-v_2\cos\alpha-v_1\sin\alpha}{\alpha^2} & \frac{-v_1+\alpha v_2+v_1\cos\alpha-v_2\sin\alpha}{\alpha^2} & 1 \end{pmatrix}$$

and the determinant is

$$\det(J_L) = \det(J_R) = \frac{-2(\cos\alpha - 1)}{\alpha^2}.$$

2.12.3 Killing Form

If a *bilinear form* $B(X, Y)$ for $X, Y \in \mathcal{G}$ is

$$B(X, Y) = B(Ad(g)X, Ad(g)Y)$$

for any $g \in G$. Then it is said to be Ad-invariant. A symmetric and Ad-invariant bilinear form $B(X, Y) = B(Y, X)$, named the *Killing form* is defined for real matrix Lie group as

$$B(X, Y) = \text{trace}(ad(Y)ad(Y)).$$

It is named after the German mathematician Wilhelm Karl Joseph Killing. This form can be shown to be written as [3]

$$B(X, Y) = \lambda\text{trace}(XY) + \mu(\text{trace}X)(\text{trace}Y)$$

where the numbers μ and λ are some constant real numbers that are group dependent.

The reason why the Killing form is important in the context of harmonic analysis, is because the Fourier transform and inversion formula can be explained for a large class of groups which are defined by the behaviour of their Killing form. *Cartan's criteria*, named after the French mathematician Elie Cartan, is used in the classification of Lie groups according to the properties of the Killing form. For example, a *nilpotent* Lie group has the Killing form $B(X, Y) = 0$ for all $X, Y \in \mathcal{G}$. It is called a *solvable* Lie group if and only if $B(X, [Y, Z]) = 0$ for all $X, Y, Z \in \mathcal{G}$. Those Lie groups for which $B(X, Y)$ are nondegenerate, are called *semi-simple*. Examples of such groups are the rotation groups which are semi-simple, the groups of rigid-body motion which are solvable and the Heisenberg groups which are nilpotent.

2.12.4 The Matrices of $Ad(G)$, $ad(X)$, and $B(X, Y)$

Using an appropriate inner product and concrete basis for the Lie algebra, we may, as with all linear operators, express $Ad(g)$ and $ad(X)$ as matrices. With the inner product defined as earlier for the Lie algebra we have

$$[Ad(g)]_{ij} = (X_i, Ad(g)X_j) = \left(X_i, gX_jg^{-1}\right) \tag{2.11}$$

$$[ad(X)]_{ij} = (X_i, ad(X)X_j) = (X_i, [X, X_j]). \tag{2.12}$$

There is another way to view this if we define the linear operator $\vee$ such that it converts the basis elements X_i of the Lie Algebra into elements of the natural basis element $\mathbf{e}_i \in \mathbb{R}^n$,

$$(X_i)^\vee = \mathbf{e}_i,$$

we then get the matrix element in Equation (2.11) to be

$$[Ad(g)] = \left[\left(gX_1g^{-1}\right)^\vee, ..., \left(gX_1g^{-1}\right)^\vee\right].$$

The left and right Jacobians are related with this matrix. We write

$$J_L = \left[\left(\frac{\partial g}{\partial x_1}g^{-1}\right)^\vee, ..., \left(\frac{\partial g}{\partial x_n}g^{-1}\right)^\vee\right]$$

and

$$J_R = \left[\left(g^{-1}\frac{\partial g}{\partial x_1}\right)^\vee, ..., \left(g^{-1}\frac{\partial g}{\partial x_n}\right)^\vee\right].$$

Because

$$\left(g\left(g^{-1}\frac{\partial g}{\partial x_1}\right)g^{-1}\right)^\vee = \left(\frac{\partial g}{\partial x_1}g^{-1}\right)^\vee$$

we get

$$J_L = [Ad(g)]\, J_R.$$

Likewise, if the Jacobians are known, we may write

$$[Ad(g)] = J_L J_R^{-1}.$$

By using the operator $\vee$ on Equation (2.12), the matrix elements will be

$$[ad(X)] = [(X, X_1])^\vee, ..., ([X, X_n])^\vee].$$

Now we have a concrete tool in which to calculate the $n \times n$ matrix with entries

$$[B]_{ij} = B(X_i, Y_j) = \text{trace}\left([ad(X_i)]\,[ad(X_j)]\right).$$

We see from the last equation that B is degenerate if and only if

$$\det([B]) = 0.$$

Thus, the Lie algebra is called semi-simple if $\det([B]) \neq 0$. The Lie algebra is nilpotent if for all entries i, j

$$[B]_{ij} = 0.$$

Connection between $ad(X)$, $B(X,Y)$ and the structure Constants

Remember that a real Lie algebra has a structure constants defined by

$$[X_i, X_j] = \sum_{k=1}^{n} C_{ij}^k X_k.$$

We see since the Lie bracket Equation (2.8) and the Jacobi identity Equation (2.9) are anti-symmetric that

$$C_{ij}^k = -C_{ji}^k$$

and

$$\sum_{j=1}^{N} (C_{ij}^l C_{km}^j + C_{mj}^l C_{ik}^j + C_{kj}^l C_{mi}^j) = 0.$$

The relationship between the matrix entries of $[ad(X_k)]_{ij}$ and the structure constants are

$$[ad(X_k)]_{ij} = (X_i, [X_k, X_j]) = \left(X_i, \sum_{m=1}^{N} C_{kj}^m X_m \right).$$

The inner product of a real Lie Algebra,

$$(X, Y) = \frac{1}{2} \text{trace} \left(XWY^T \right),$$

is linear in the second argument, thus

$$[ad(X_k)]_{ij} = \sum_{m=1}^{N} (X_i, X_m) C_{kj}^m = C_{kj}^i.$$

And then

$$\begin{aligned} B(X_i, X_j) &= \text{trace} \left(ad(X_i) ad(X_j) \right) \\ &= \sum_{m=1}^{N} \sum_{m=1}^{N} [ad(X_i)]_{mn} [ad(X_j)]_{nm} \\ &= \sum_{m=1}^{N} \sum_{m=1}^{N} C_{in}^m C_{jm}^n \end{aligned}$$

SE(2)

Substituting the parameterization of $SE(2)$ into the definitions gives us

$$[Ad(g)] = \begin{pmatrix} \cos\theta & -\sin\theta & x_2 \\ \sin\theta & \cos\theta & -x_1 \\ 0 & 0 & 1 \end{pmatrix}.$$

And if

$$X = \begin{pmatrix} 0 & -\alpha & v_1 \\ \alpha & 0 & v_2 \\ 0 & 0 & 0 \end{pmatrix},$$

we receive

$$[ad(X)] = \begin{pmatrix} 0 & -\alpha & v_2 \\ \alpha & 0 & -v_1 \\ 0 & 0 & 0 \end{pmatrix},$$

and

$$[B] = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -2 \end{pmatrix},$$

which is clearly degenerate. Thus, $SE(2)$ is not semi-simple. (Same goes for $SE(3)$.)

Chapter 3

Theory of Linear Representations of Finite Groups

The mathematical field of representation theory studies abstract algebraic structures in terms of representing their elements as linear transformations of vector spaces. The essence is to represent an algebraic object by matrices and the algebraic operations as matrix addition or matrix multiplication. The theory throughout this chapter follows [4].

3.1 Basic Theory of Linear Representations

We start this section by giving some basic definitions of representation theory.

3.1.1 Definitions

Given a field $\mathbb{C}$ of complex numbers, let V be a vector space over it and $GL(V)$ is the group of isomorphisms of V onto itself. Any element $a \in GL(V)$ is, by definition, a linear mapping of V into V with an linear inverse a^{-1}. When the basis $\{e_i\}$ of V is finite with n elements, each linear mapping $a : V \to V$ is defined by a square matrix $\{a_{ij}\}$ of order n. The complex coefficients a_{ij} are obtained by using the basis$\{e_i\}$ to express the image $a(e_j)$

$$a(e_j) = \sum_i a_{ij} e_i.$$

That a is an isomorphisms is equivalent to that the determinant of a $\det(a) = \det(a_{ij})$ is nonzero. Therefore, the group $GL(V)$ is recognisable as the group of **invertible square matrices of order n**.

Definition 3.1. A linear representation of a finite group G in V is a homomorphism ρ from the group G into the group $GL(V)$, $\rho : G \to GL(V)$

Thus, for every $g, h \in G$

$$\rho(gh) = \rho(g)\rho(h), \quad \rho(g^{-1}) = \rho(g)^{-1}, \quad \rho(e) = e.$$

Given a ρ, we say that V is the **support** of the representation and the **dimension of the representation** is given by the dimension of V [5].

The **trivial** (or **unit**) representation is a representation obtained by taking $\rho(g) = 1$ for all $g \in G$.

Assume now that V has a finite dimension n. Let $R(g)$ be the matrix of $\rho(g)$ with respect to a basis $\{e_i\}$ of V. We then have

$$\det(R(g)) \neq 0, \qquad R(gh) = R(g)R(h) \quad if\ g,h \in G.$$

If the coefficients of the matrix $R(G)$ is denoted $r_{ij}(g)$, the second formula becomes

$$r_{ik}(gh) = \sum_j r_{ij}(g)r_{jk}(h).$$

Two representations ρ and ρ' of the same group G are said to be similar (or isomorphic) if there exist a linear isomorphism $\tau\ :\ V \to V'$ which satisfies

$$\tau \circ \rho(g) = \rho'(g) \circ \tau \quad \text{for all } g \in G.$$

This may also be written $R'(g) = TR(g)T^{-1}$.

3.1.2 Subrepresentations

Let W be a vector subspace of V and suppose W is invariant under the action of G, i.e.

$$x \in W \Leftrightarrow\ \rho(g)x \in W \quad \text{for all } g \in G$$

where $\rho : G \to GL(V)$ is the linear representation of V. The restriction of $\rho(g)$ to W, denoted $\rho^W(g)$, is then an isomorphism of W onto W, and $\rho^W(gh) = \rho^W(g)\rho^W(h)$. We therefore get a linear representation $\rho^W : G \to GL(V)$ of G in W and this representation is called a **subrepresentation** of V.

Theorem 3.2. *Let $\rho : G \to GL(V)$ be a linear representation of G in V and let W be a vector subspace of V invariant under G. Then there exist a complement W^0 of W in V which is invariant under G.*

Using the same notation and hypothesis as in Theorem 3.2, let $x \in V$ and let w and w^0 be the projection on W and W^0. When $\rho(g)x = \rho(g)w + \rho(g)w^0$ we have $x = w + w^0$, and because W and W^0 are stable under G, we have $\rho(g)w \in W$ and $\rho(g)w^0 \in W^0$. $\rho(g)w$ and $\rho(g)w^0$ are therefore projections of $\rho(g)x$. The representation spaces W and W^0 determine the representation space V. Thus, V is the direct sum of W and W^0

$$V = W \oplus W^0.$$

Let W and W^0 be given in matrix form by $R(g)$ and $R^0(g)$, then $V = W \oplus W^0$ is given in matrix form by

$$\begin{pmatrix} R(g) & 0 \\ 0 & R^0(g) \end{pmatrix}.$$

Similarly,we define the direct sum of an arbitrary finite number of representations.

3.1.3 Irreducible Representations

We say that a linear representation $\rho : G \to GL(V)$ of G is **irreducible** or **simple** if the only vector subspaces of V invariant under G is 0 and V itself.

Theorem 3.3. *Every representation is a direct sum of irreducible representations and every representation of a finite group is finite dimensional.*

The question now: Are the decomposition into irreducible representations unique? The case where all the $\rho(g) = 1$ shows that, in general, this is not true.

3.1.4 Tensor Product of two Representations

In the same way that the direct sum operation, which formal has addition properties, there exist a "multiplication" operator: The **tensor product**, or the **kronecker** product.

Definition 3.4. Let $\rho_1 : G \to GL(V_2)$ and $\rho_2 : G \to GL(V_2)$ be two representations and V_1, V_2 is their respectively representation spaces. A space W with a map $(x_1, x_2) \to x_1 \cdot x_2$ of $V_1 \times V_2$ into W, is called a the tensor product of V_1 and V_2 if the following two conditions are satisfied

1. $x_1 \cdot x_2$ is linear in each of the variables x_1 and x_2.
2. If (e_{i_1}) is a basis for V_2 and (e_{i_2}) is a basis for V_2, the family of products $e_{i_1} \cdot e_{i_2}$ is a basis for W.

The tensor product of V_1 and V_2 is denoted $V_1 \otimes V_2$ and the tensor product of the two representations $\rho_1(g)$ and $\rho_2(g)$ is denoted $\rho_1(g) \otimes \rho_2(g)$.

The existence of such a space is easily shown and it is unique up to isomorphism. Condition 2 of Definition 3.4 shows that

$$\dim(V_1 \otimes V_2) = \dim(V_1) \cdot \dim(V_2).$$

Definition 3.5. The tensor product $\rho(g) = \rho_1(g) \otimes \rho_2(g)$ defined as in 3.4 defines a linear representation of G in $V_1 \otimes V_2$ called the tensor product of the given representations.

We may decompose the tensor product of two irreducible representations into a direct sum of irreducible representations. Hence, the tensor product is not in general irreducible.

3.2 Character Theory

3.2.1 The Character of a Representation

Let $\rho : G \to GL(V)$ be a linear representation of a finite group G in V. The character of the representation ρ is defined as the complex valued function

$$\chi_\rho = \text{trace}(\rho(g)).$$

It is an important function since it **characterizes** the representation ρ.

Theorem 3.6. *If χ is the character of a representation ρ of degree n, we have*

1. $\chi(1) = n$,
2. $\chi(g^{-1}) = \chi(g)^*$ *for* $g \in G$,
3. $\chi(hgh^{-1}) = \chi(g)$ *for* $g, h \in G$.

Recall from Section 2.11.1 that a function satisfying identity 3 of Theorem 3.6 is called a class function.

Theorem 3.7. *Let $\rho_1 : G \to GL(V_1)$ and $\rho_2 : G \to GL(V_2)$ be two linear representations of G, and let χ_1 and χ_2 be their characters. Then*

1. *The character χ of the direct sum of representation $V_1 \oplus V_2$ is equal to $\chi_1 + \chi_2$.*
2. *The character ψ of the tensor product representation $V_1 \otimes V_2$ is equal to $\chi_1 \cdot \chi_2$.*

3.2.2 Schur's Lemma

An elementary theorem in mathematics is **Schur's Lemma** named after Issai Schur. It has proven to be very useful in representation theory of groups and algebras and it admits generalizations to Lie groups and Lie algebras.

Theorem 3.8 (**Schur's Lemma**). *Let $\rho_1 : G \to GL(V_1)$ and $\rho_2 : G \to GL(V_2)$ be two irreducible representations of G, and let f be a linear mapping of V_1 into V_2 such that $\rho_2(g) \circ f = f \circ \rho_1(g)$ for all $g \in G$. Then*

1. *If ρ_1 and ρ_2 are not isomorphic, we have $f = 0$.*
2. *If $V_1 = V_2$ and $\rho_1 = \rho_2$, f is a homothety (i.e. a scalar multiple of the identity).*

Keeping the hypothesis that V_1 and V_2 are irreducible and denote as usual the order of G by $|G|$ we get a corollary to Schur's lemma.

Corollary 3.9. *Let t be a linear mapping of V_1 into V_2, and put*

$$t^0 = \frac{1}{|G|} \sum_{g \in G} (\rho_2(g))^{-1} t \rho_1(g).$$

Then

1. *If ρ_1 and ρ_2 are not isomorphic, we have $t^0 = 0$.*
2. *If $V_1 = V_2$ and $\rho_1 = \rho_2$, t^0 is a homothety of ratio $\frac{1}{n}\mathrm{trace}(t)$, where n is the dimension of V_1.*

If ρ_1 and ρ_2 are given in their matrix form

$$\rho_1(g) = (r_{i_1 j_1}(g)),\ \rho_2(g) = (r_{i_2 j_2}(g)),$$

and t is given by the matrix $(t_{i_2 i_1})$, we can rewrite Corollary 3.9 as

Corollary 3.10. *In case (1) of Corollary 3.9, we have*

$$\frac{1}{|G|}\sum_{g\in G} r_{i_2 j_2}(g^{-1}) r_{i_1 j_1}(g) = 0$$

for arbitrary i_1, i_2, j_1, j_2.

Corollary 3.11. *In case (2) of Corollary 3.9, we have*

$$\frac{1}{|G|}\sum_{g\in G} r_{i_2 j_2}(g^{-1}) r_{i_1 j_1}(g) = \frac{1}{n}\delta_{i_2 i_1}\delta_{j_2 j_1} = \begin{cases} 1/n & \text{if } i_1 = i_2 \text{ and } j_1 = j_2 \\ 0 & \text{otherwise.} \end{cases}$$

3.2.3 Orthogonality Relations

We begin by defining a **scalar product** for complex-valued functions on G as

$$(\phi|\psi) = \frac{1}{|G|}\sum_{g\in G} \phi(g)\psi(g)^*.$$

Theorem 3.12.

1. *If χ is the character of an irreducible representation, we have $(\chi|\chi) = 1$ (i.e. the norm of χ is 1)*
2. *If χ and χ' are the characters of two nonisomorphic irreducible representations, we have $(\chi|\chi') = 0$. (χ and χ' are orthogonal).*

We see from Theorem 3.12 that characters of irreducible representations form an orthonormal system. Such characters are named irreducible characters.

Theorem 3.13. *Let V be a linear representation space of G, with character ϕ, and suppose V decomposes into a direct sum of irreducible representation spaces*

$$V = W_1 \oplus \cdots \oplus W_k.$$

Then, if W is an irreducible representation space with character χ, the number of W_i isomorphic to W is equal to the scalar product $(\phi|\chi) = \langle\phi, \chi\rangle$.

Where $\langle \phi, \chi \rangle$ is defined as

$$\langle \phi, \chi \rangle = \frac{1}{|G|} \sum_{g \in G} = \phi(g^{-1})\psi(g) = \frac{1}{|G|} \sum_{g \in G} = \phi(g)\psi(g^{-1}).$$

By Theorem 3.7 we have that

$$\phi = \chi_1 + \cdots + \chi_k,$$

where χ_i is the character of W_i. Hence, $(\phi|\psi) = (\chi_1|\chi) + \cdots + (\chi_k|\chi_k)$. But, Theorem 3.12 states that $(\chi_1|\chi)$ is equal to 1 or 0, if W_i is, or is not, isomorphic to W. The result i stated as corollaries

Corollary 3.14. *The number of W_i isomorphic to W does not depend on the chosen decomposition.*

This is why one may say that there is uniqueness in the decomposition of a representation into irreducible representations.

Corollary 3.15. *Two representations with the same character are isomorphic.*

This result reduces the study of representations to that of their character. Let $\chi_1 \cdots, \chi_s$ be the the distinct characters of G, and let $W_i, \cdots, W_k$ denote the corresponding representations. Then, each representation V is isomorphic to a direct sum

$$V = m_1 V_1 \oplus \cdots \oplus m_s W_s \quad m_i \text{ are integers } \neq 0.$$

The corresponding character ϕ of V is equal to $m_1\chi_1 + \cdots m_s\chi_s$, and the scalar m_i is equal to $(\phi|\chi_i)$.

Theorem 3.16. *If ϕ is the character of a representation V, $(\phi|\phi)$ is a positive integer and we have $(\phi|\phi) = 1$ if and only if V is irreducible.*

Thus, we have a very convenient irreducibility criterion.

3.2.4 The Regular Representation

The **regular representation** of G is defined as the linear representation afforded by the group action of G on itself. That is, let V be a vector space of dimension equal to the order of G with a basis $\{e_h\}_{h \in G}$. For $g \in G$, then the regular representation is the linear map, $p(g)$, of V into V which sends e_h to e_{gh}.

Assume now for the rest of this section that the irreducible characters of G are denoted $\chi_1, \cdots \chi_h$ with degrees $n_1, \cdots, n_k$.

Theorem 3.17. *The character r_G of the regular representation is given by the formulas*

$$r_G(1) = n, \qquad \textit{order of } G$$

$$r_G(g) = 0 \qquad \textit{if } s \neq 1.$$

Corollary 3.18. *Every irreducible representation W_i is contained in the regular representation with multiplicity equal to its degree n_i.*

Corollary 3.19.

1. *The degrees n_i satisfy the relation $\sum_{i=1}^{s} n_i^2 = n$.*
2. *If $g \in G$ is different from 1, we have $\sum_{i=1}^{s} n_i \chi_i(g) = 0$.*

The result of Corollary (3.19) is important, and it is used in determining the irreducible representations of a group G.

3.2.5 The Number of Irreducible Representations

As we have seen many times earlier a class function f on G is a function which satisfies $f(hgh^{-1}) = f(g)$ for all $g, h \in G$.

Theorem 3.20. *Let f be a class function on a group G of order $|G|$, and let $\rho : G \to GL(V)$ be a linear representation of G. Let ρ_f be the linear mapping of V into itself defined by*

$$\rho_f = \sum_{g \in G} f(g)\rho_g.$$

If V is irreducible of degree n and character χ, then ρ_f is a homothety of ratio λ given by

$$\lambda = \frac{1}{n}\sum_{g \in G} f(g)\chi(g) = \frac{|G|}{n}(f|\chi^*).$$

We now let K be the space of class functions on G; The irreducible characters $\chi_1, \cdots, \chi_s$ belong to K and the next theorem gives us a basis for this space.

Theorem 3.21. *The characters $\chi_1, \cdots, \chi_s$ form an orthonormal basis of K.*

Recall from Chapter 2 that two elements of G is said to be conjugate if there exist an $h \in G$ such that $g' = hgh^{-1}$ for $g', g \in G$. This equivalence relation partitions G into conjugacy classes. The following theorems are a consequence of Theorem (3.21)

Theorem 3.22. *The number of irreducible representations of G (up to isomorphism) is equal to the number of conjugacy classes of G.*

Theorem 3.23. *Let $g \in G$, and let c(g) be the number of elements in the conjugacy class of g.*

1. *We have $\sum_{i=1}^{s} \chi_i(g)^*\chi_i(g) = |G|/c(g)$.*
2. *For $h \in G$ not conjugate to g, we have $\sum_{i=1}^{s} \chi_i(g)^*\chi_i(h) = 0$.*

3.3 Subgroups, Products and Induced Representations

3.3.1 Abelian Subgroups

Recall from Chapter 2 that an abelian group (or a commutative group) is a group where $gh = hg$ for all $g, h \in G$. Each conjugacy class of G have one element, and every function on G is a class function. This gives us very simple linear representations

Theorem 3.24. *The following properties are equivalent*

1. *G is abelian*
2. *All the irreducible representations of G have degree 1.*

Corollary 3.25. *Let A be an abelian subgroup of G, let $|A|$ be its order and let $|G|$ be that of G. Each irreducible representation of G has degree $\leq \frac{|G|}{|A|}$*

3.3.2 Product of Two Groups

Given two groups G_1 and G_1, let the product $G_1 \times G_2$ be the set of pairs (g_1, g_2) with $g_1 \in G_1$ and $g_2 \in G_2$. We define a group structure on $G_1 \times G_2$ by putting

$$(g_1, g_2) \cdot (h_1, h_2) = (g_1 g_2, h_1 h_2).$$

If this structure is used, $G_1 \times G_2$ is called the **group product**. The order of $G_1 \times G_2$ is $n_{G_1} n_{G_2}$. If G is the direct product of its subgroups G_1 and G_2 we may under certain conditions identify it with $G_1 \times G_2$

1. Each $g \in G$ can be written uniquely in the form $g = g_1 g_2$ with $g_1 \in G_1$ and $g_1 \in G_2$.
2. For $g_1 \in G_1$ and $g_2 \in G_2$ we have $g_1 g_2 = g_2 g_1$.

Now we can define a linear representation $\rho_1 \otimes \rho_2$ of $G_1 \times G_2$ into $V_1 \otimes V_2$, where $\rho_1 : G_1 \to GL(V_1)$ and $\rho_2 : G_2 \to GL(V_2)$, by setting

$$(\rho_1 \otimes \rho_2)(g_1, g_2) = \rho_1(g_1) \otimes \rho_2(g_2).$$

This representation is named the **tensor product** of ρ_1 and ρ_2. The character χ of $\rho_1 \otimes \rho_2$ is given by

$$\chi(g_1, g_2) = \chi_1(g_1) \cdot \chi_2(g_2),$$

where χ_i is the character of ρ_i.

Theorem 3.26.

1. *If ρ_1 and ρ_2 are irreducible, $\rho_1 \otimes \rho_2$ is an irreducible representation of $G_1 \times G_2$.*
2. *Each irreducible representation of $G_1 \times G_2$ is isomorphic to a representation $\rho_1 \otimes \rho_2$, where ρ_i is an irreducible representation of G_i (i=1,2).*

The last theorem is a powerful tool in the study of the representations of $G_1 \otimes G_2$. It completely reduces it to the study of the representation of G_1 and G_2.

3.3.3 Induced Representations

Let H be a subgroup of G. We obtain a subset R of G if we choose an element from each left cosets of H. This subset of G is called a system of representatives of G/H and each $g \in G$ can be written uniquely as $g = rh$, where $r \in R$ and $h \in H$.

We define a induces representation in the following way

Definition 3.27. Let $\rho : G \to GL(V)$ be a linear representation of G and let $\theta : H \to GL(W)$ be a linear representation of H in W. We say that the linear representation ρ of G in V is **induced** by the representation θ of H in W if V is equal to the sum of the W_σ ($\sigma \in G/H$) and if this sum is direct (i.e. if $V = \oplus_{\sigma \in G/H} W_\sigma$).

This condition may be reformulated in several ways

1. We may write uniquely each $x \in V$ as $\sum_{\sigma \in G/H} x_\sigma$ with $x_\sigma \in W_\sigma$ for each σ.

2. We have a direct sum of the vector space V equal to $\rho_r W$, with $r \in R$, if R is a system of representatives of G/H.

For the existence and uniqueness of induced representations we have

Lemma 3.28. *Suppose that (V, ρ) is induced by (W, θ). Let $\rho' : G \to GL(V')$ be a linear representation of G, and let $f : W \to V'$ be a linear map such that $f(\theta_h w) = \rho'_h f(w)$ for all $h \in H$ and $w \in W$. Then there exists a unique linear map $F : V \to V'$ which extends f and satisfies $F \circ \rho_g = \rho'_g \circ F$ for all $g \in G$.*

Theorem 3.29. *Let (W, θ) be a linear representation of H. There exists a linear representation (V, ρ) of G which is induced by (W, θ), and it is unique up to isomorphism.*

The character of an induced representation may be calculated using the procedure below: If we have (V, ρ) induced by (W, θ) and corresponding characters χ_ρ and χ_θ of G and H. There should be a way to compute the character χ_ρ from χ_θ. The next theorem tells us how

Theorem 3.30. *Let $|H|$ be the order of H and let R be a system of representatives of G/H. For each $u \in G$, we have*

$$\chi_\rho(u) = \sum_{\substack{r \in R \\ r^{-1}ur \in H}} \chi_\theta(r^{-1}ur) = \frac{1}{|H|} \sum_{\substack{g \in G \\ g^{-1}ug \in H}} \chi_\theta(g^{-1}ug).$$

(We have that $\chi_\rho(u)$ is a linear combination of the values χ_θ when χ_θ takes its values on the intersection of H with the conjugacy class of $u \in G$.)

3.4 The Group Algebra

If not stated otherwise, we assume that all the groups here to be finite, and all vectors spaces (resp., all modules) are assumed to have finite dimension.

3.4.1 Representations and Modules

Given a group G of finite order $|G|$ and a commutative ring K, we denote the **algebra of** G **over K** by $K[G]$; the basis for this algebra is indexed by the elements of G. Thus, each element f of $K[G]$ may be written uniquely in the form as

$$f = \sum_{g \in G} a_g g, \qquad \text{with } a_g \in K,$$

and multiplication in $K[G]$ extends that in G.

Definition 3.31. Let V be a K-module and let $\rho : G \to GL(V)$ be a linear representation of G in V. For $g \in G$ and $x \in V$, we set $gx = \rho(g)x$; This defines by linearity fx, for $f \in K[G]$ and $x \in V$. Therefore, V is endowed with the structure of a **left** $K[G]$**-module**.

On the contrary, such a structure defines a linear representation of G in V and we will use the terminology "linear representation" or "module" indiscriminately.

Theorem 3.32. *If K is a field of characteristic zero, the algebra $K[G]$ is semisimple.*

Corollary 3.33. *The algebra $K[G]$ is a product of matrix algebras over skew fields of finite degree over K.*

3.4.2 Decomposing $C[G]$

From now on we take $K = \mathbb{C}$, so that each skew field of finite degree over $\mathbb{C}$ is equal to $\mathbb{C}$. We then have from Corollary 3.33 that $\mathbb{C}[G]$ is a product of matrix algebras $M_{n_j}(\mathbb{C})$. More accurate, let $\rho_i : G \to GL(W_i)$, for $1 \leq i \leq s$, be the distinct irreducible representations of G (up to isomorphism). We set $n_i = \dim(W_i)$ so that the ring $\mathrm{End}(W_i)$ is isomorphic to $M_{n_i}(\mathbb{C})$. Therefore, the map $\rho_i : G \to GL(W_i)$ extends to an algebra homomorphism $\tilde{\rho}_i : \mathbb{C}[G] \to \mathrm{End}(W_i)$, and the family $(\tilde{\rho})$ defines the homomorphism

$$\tilde{\rho} : \mathbb{C}[G] \to \prod_{i=1}^{s} \mathrm{End}(W_i) \simeq \prod_{i=1}^{s} M_{n_i}(\mathbb{C}).$$

Theorem 3.34. *The homomorphism $\tilde{\rho}$ defined above is an isomorphism.*

The inverse of $\tilde{\rho}$ may be used to describe the isomorphism and it also give us a little taste of the next chapter

Theorem 3.35 (Fourier Inversion Formula). *Let $(u_i)_{1 \leq i \leq s}$ be an element of $\prod_{i=1}^{s} \mathrm{End}(W_i)$, and let $u = \sum_{g \in G} u(g)g$ be the element of $\mathbb{C}[G]$ such that $\tilde{\rho}(u) = u_i$ for all i. The gth coefficient $u(g)$ of u is given by the formula*

$$u(g) = \frac{1}{|G|} \sum_{i=1}^{s} n_i \mathrm{trace}_{W_i}(\rho_i(g^{-1})u_i), \qquad \text{where } n_i = \dim(W_i).$$

3.4.3 The Center of $\mathbb{C}[G]$

The center of $\mathbb{C}[G]$ is the set of elements which commute with all elements in $\mathbb{C}[G]$ (or, conversely, with all elements of G). If c is a conjugacy class of G, the set $e_c = \sum_{g \in G} g$ form a basis for the center of $\mathbb{C}[G]$ with dimension s, where s is the number of conjugacy classes of G. Assume that

$$\rho_i : G \to GL(W_i)$$

is an irreducible representation of G with character χ_i of degree n_i, and that $\tilde{\rho}_i : \mathbb{C}[G] \to \mathrm{End}(W_i)$ is the corresponding algebra homomorphism.

Theorem 3.36. *The homomorphism $\tilde{\rho}_i$ maps the center $\mathbb{C}[G]$ into set of homotheties of W_i and defines an algebra homomorphism*

$$\omega_i : \mathrm{Cent.}\ \mathbb{C}[G] \to \mathbb{C}.$$

If $u = \sum u(g)g$ is an element of Cent.$\mathbb{C}[G]$, *we have*

$$\omega(u) = \frac{1}{n_i} \mathrm{trace}_{W_i}(\tilde{\rho}(u)) = \frac{1}{n_i} \sum_{g \in G} u(g)\chi_i(g).$$

We see that this is just a reformulation of Theorem 3.20.

Theorem 3.37. *The family $(\omega_i)_{1 \le i \le s}$ defines an isomorphism of* Cent. $\mathbb{C}[G]$ *onto the algebra $\mathbb{C}^s = \mathbb{C} \times \cdots \times \mathbb{C}$.*

If $\mathbb{C}$ is the center of G, the following theorem gives us information about the degrees of the irreducible representations of G.

Theorem 3.38. *Let $\mathbb{C}$ be the center of G. The degrees of the irreducible representations of G divide $(G : \mathbb{C})$.*

3.5 Mackey's Criterion for Induced Representations

3.5.1 Induction

Let R be a system of left cosets representations for a subgroup H of G. If V is a $\mathbb{C}[G]$-module and W is a sub-$\mathbb{C}[H]$-module of V, then from Definition 3.27 the module V (or the representation V) is said to be induced by W if $V = \oplus_{r \in R} rW$. That is, if V is the direct sum of the images rW, $r \in R$. This condition is independent of the choice of R. Another way to formulate this is:

Given a $\mathbb{C}[G]$-module

$$W' = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} W$$

obtained from W by scalar extension from $\mathbb{C}[H]$ to $\mathbb{C}[G]$. Then the injection $W \to V$ extends by linearity to a $\mathbb{C}[G]$-homomorphism $i : W' \to V$.

Theorem 3.39. *In order for that V be induced by W, it is necessary and sufficient that the homomorphism*

$$i : \mathbb{C}[G]_{\mathbb{C}[H]}W \to V$$

is an isomorphism.

This follows from the fact that elements of R form a basis of $\mathbb{C}[G]$ considered as a right $\mathbb{C}[H]$-module.

From Theorem 3.29 we see that this characterization of the representation induced by W makes it clear that the induced representation exist and are unique. For the rest of this section, we will denote the representation of G induced by W as $\mathrm{Ind}_H^G(W)$, or simply $\mathrm{Ind}(W)$ if no confusion can be made. The last remark to make is that the induction is transitive. That is, if G is a subgroup of a group K, we have

$$\mathrm{Ind}_G^K(\mathrm{Ind}_H^G(W)) \cong \mathrm{Ind}_H^K(W).$$

Theorem 3.40. *Let V be a $\mathbb{C}[G]$-module which is a direct sum $V = \oplus_{i\in I}W_i$ of vector subspaces permuted transitively by G. Let $i_0 \in I$, $W = W_{i_0}$ and let H be the stabilizer of W in G (Recall from 2 that this means the set $g \in G$ such that $gW = W$). Then W is stable under the subgroup H and the $\mathbb{C}[G]$-module V is induced by the $\mathbb{C}[H]$-module W.*

3.5.2 The Character of an Induced Representation and the Reciprocity Formula

Keeping the preceding notation we let f be a class function on H and f' is the function on G defined by the formula

$$f'(g) = \frac{1}{|H|} \sum_{\substack{h\in G \\ h^{-1}gh}} f(h^{-1}gh).$$

f' is said to be induced by f and we denote is by $\mathrm{Ind}_H^G(f)$ or $\mathrm{Ind}(f)$.

Theorem 3.41.

1. *The function $\mathrm{Ind}(f)$ is a class function on G.*
2. *If f is the character of a representation W of H, $\mathrm{Ind}(f)$ is the character of the induced representation $\mathrm{Ind}(W)$ of G.*

Lemma 3.42. *If φ_1 and φ_2 are the characters of V_1 and V_2, we have*

$$\langle \varphi_1, \varphi_2 \rangle_G = \langle V_1, V_2 \rangle_G .$$

We write Res φ for the **restriction** of the function φ on G to the subgroup H, and Res V for the restriction of the representation V of G to H.

Theorem 3.43 (**Frobenius Reciprocity**). *If ψ is a class function on H and φ a class function on G, we have*

$$\langle \psi, \mathrm{Res}\ \varphi \rangle_H = \langle \mathrm{Ind}\ \psi, \varphi \rangle_G .$$

We see that Theorem 3.43 expresses the fact that the maps Res and Ind are adjoints of each other. Another useful relation between them are

$$\mathrm{Ind}(\psi \cdot \mathrm{Res}\ \varphi) = (\mathrm{Ind}\ \psi) \cdot \varphi.$$

Theorem 3.44. *Let W be an irreducible representation of H and E and irreducible representation of G. Then the number of times that W occurs in* Res E *is equal to the number of times that E occurs in* Ind W.

3.5.3 Restriction to Subgroups

Given two subgroups H and K of G, let $\rho : H \to GL(V)$ be a linear representation of H, and $V = \mathrm{Ind}_H^G(W)$ is the corresponding induced representation of G. To determine the restriction $\mathrm{Res}_K(V)$ of V to K, we first need to choose a set of representatives S for the (H, K) double cosets of G; This makes G the disjoint union of the KsH for $s \in S$ (which could also be written $g \in K\backslash G/H$ as in subsection 2.11.2). We get a subgroup H_s of K if we for $s \in S$, let $H_s = sHs^{-1} \cap K$. We obtain a homomorphism $\rho_s : H_s \to GL(W)$ if we set

$$\rho^s(x) = \rho(s^{-1}xs), \quad \text{for } x \in H_s,$$

and hence the homomorphism is a linear representation of H_s, denoted W_s. Since H_s is a subgroup of K, this defines the induced representation $\mathrm{Ind}_{H_s}^K(W)$.

Proposition 3.45. *The representation* $\mathrm{Res}_K\mathrm{Ind}_H^G(W)$ *is isomorphic to the direct sum of the representations* $\mathrm{Ind}_{H_s}^K(W_s)$*, for $s \in S \simeq K\backslash G/H$.*

Notice, that since $V(s)$ depends only on the image of s in $K\backslash G/H$, it is clear that the representation $\mathrm{Ind}_{H_s}^K(W_s)$ is only depended (up to isomorphism) on the double coset of s.

3.5.4 Mackey's Irreducibility Criterion

Now we apply the preceding result to the case $K = H$. The subgroup $sHs^{-1} \cap H$ is still denoted by H_s for $s \in G$. The representation $\mathrm{Res}_s(\rho)$ is defined by the restriction of the representation ρ of H to H_s, which is not the same representation as the representation ρ^s defined in the previous section.

Proposition 3.46. *In order for that the induced representation $V = \mathrm{Ind}_H^G(W)$ is irreducible, it is necessary and sufficient that the following two conditions are satisfied:*

1. *W is irreducible*
2. *For each $s \in G - H$ the two representations ρ^s and $\mathrm{Res}_s(\rho)$ of H_s are disjoint.*

Corollary 3.47. *Suppose H is normal in G. In order for that $\mathrm{Ind}_H^G(\rho)$ is irreducible, it is necessary and sufficient that ρ is irreducible and not isomorphic to any of its conjugates ρ^s for $s \notin H$.*

Clearly, since we then have $H_s = H$ and $\mathrm{Res}_s(\rho) = \rho$.

3.6 Useful Examples of Induced Representations

In this section we give some examples of induced representations using the theory so far. Since the Euclidean motion group is the the group of most interest in this thesis, we show an example of how to find induced representations of semidirect products.

3.6.1 Normal Subgroups; The degree of the Irreducible Representations

Proposition 3.48. *Let A be a normal subgroup of a group G, and let $\rho : G \to GL(V)$ be an irreducible representation of G. Then*

1. *Either there exist a subgroup of H of G, unequal to G and containing A, and an irreducible representation σ of H such that ρ is induced by σ;*

2. *or else the restriction of ρ to A is isotypic.*

(An isotypic representation is a representation that is a direct sum of isomorphic irreducible representations.)

Condition (2) of Proposition 3.48 is equivalent to saying that if A is abelian, then $\rho(A)$ is a homothety for each $a \in A$.

Corollary 3.49. *If A is an abelian normal subgroup of G, the degree of each irreducible representation ρ of G divides the index $(G : A)$ of A in G.*

3.6.2 Semidirect Products by an Abelian Group

We have now come to the cornerstone of the theory presented so far, the theory of semidirect product by an abelian group. We make the following hypothesis for two subgroups A and H of G, with A normal

1. A is abelian.

2. G is the semidirect product of H by A.

[This means that $G = A \rtimes H$ and that $A \cap H = \{e\}$, or equivalently, that each elements of the group G, may be written uniquely as a product ah with $a \in A$ and $h \in H$.]

We show now that the irreducible representations of G may be constructed from those of certain subgroups of H (The method is the "little group" method of Wigner and Mackey).

The irreducible characters of the abelian subgroup A have degree 1 and the form a group $X = \mathrm{Hom}(A, \mathbb{C}^*)$. The group G acts on X as

$$(g\chi)(a) = \chi(g^{-1}ag) \quad \text{for } g \in G, \chi \in X, a \in A.$$

Now we let $(\chi_i)_{i \in X/H}$ be a system of representatives for the orbits of H in X. For each $i \in X/H$, we let H_i be the subgroup of H consisting of those elements h such that $h\chi_1 = \chi_1$, and $G_i = A \rtimes H_i$, is the corresponding subgroup of G. The function χ_i may be extended to G_i by setting

$$\chi_i(ah) = \chi_i(a) \quad \text{for } a \in A, h \in H_i.$$

We see that χ_i is a character of degree 1 of G_i, since $h\chi_i = \chi_i$ for all $h \in H$. By composing the irreducible representation ρ of H_i with the canonical projection $G_i \to H_i$ we obtain an irreducible representation $\tilde{\rho}$ of G_i. If we take the tensor product of χ_i and $\tilde{\rho}$ we receive an irreducible representation $\chi_i \otimes \tilde{\rho}$ of G_i, and finally, we let $\theta_{i,\rho}$ be the corresponding induced representations of G.

Proposition 3.50.

1. *$\theta_{i,\rho}$ is irreducible.*

2. *If $\theta_{i,\rho}$ and $\theta_{i',\rho'}$ are isomorphic, then $i = i'$ and ρ is isomorphic to ρ'.*

3. *Every irreducible representation of G is isomorphic to one of the $\theta_{i,\rho}$.*

(And thus, we have all the irreducible representations of G.)

3.6.3 An example, a discrete model of $SE(2)$

Let $G = H \ltimes A$ with the product

$$(h, a)(\tilde{h}, \tilde{a}) = (h\tilde{h}, a + h\tilde{a}),$$

where $A = (Z_N)^2$, $H = \{S^j\}_{j=0}^5$, and $S = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$. We find $\widehat{A} = (Z_N)^2$ with the pairing $\langle k, j \rangle = \exp(2\pi \mathrm{i} k^T j/N)$. Note that since $S^6 = \mathbb{I}$ we have $H \simeq Z_6$. The irreducible representations on H are thus the six characters $S^j \mapsto \exp(2\pi \mathrm{i} kj/6)$ for $k = 0, 1, \ldots, 5$. The action of H on $\widehat{A}$ is given as $\langle k, S^\ell j \rangle = \langle (S^T)^\ell k, j \rangle$. The exact structure of the H-orbits in $\widehat{A}$ depends on N.

N not divisible by 2 or 3

If neither 2 or 3 divide N, then all orbits are full of length 6, except the orbit $\{(0,0)\}$. Let $\chi_0 = (0,0)^T$. We find $H_0 = H = Z_6$ and since χ_0 is fixed by any element of G, we have $G_0 = G$. We find the 1-D representations

$$\overline{R}_{0,\ell}(S^k, a) = \exp(2\pi \mathrm{i}\ell k/6) \quad \text{for } \ell = 0, \dots, 5.$$

All the other orbits are full. Representatives of these can be taken as

$$\chi_1 = (1,0)^T, \chi_2 = (2,0)^T, \chi_3 = (1,2)^T, \chi_4 = (2,1)^T, \chi_5 = (3,0)^T, \quad \text{etc. depending on } N.$$

For each of these we have $H_i = \{e\}$ and $G_i = e \ltimes (Z_N)^2$. Since H_i is the trivial group, the construction yields only one representation for each of these,

$$\rho_i(h, a) = \langle \chi_i, a \rangle.$$

Now we lift these to G. Coset representatives of G_i in G can be taken as all $(\widetilde{h}, 0)$ where $\widetilde{h} \in H$. Here V is 1-dimensional and we let W be the six dimensional space of functions $\phi(x)$ defined for $x = h^{-T}\chi_i \in \mathrm{Orb}(\chi_i)$. The inverse on h is chosen to obtain a left action of H on $\widehat{A}$. We may then write $\phi = \sum_{\widetilde{h} \in H} \widetilde{h}\phi(\widetilde{h}^{-T}\chi_i)$ and compute the intertwining of coset representatives $(\widetilde{h}, 0)$ with $g = (h, a) \in G$

$$(h, a)(\widetilde{h}, 0) = (h\widetilde{h}, 0)(0, (h\widetilde{h})^{-1}a),$$

which yields

$$\mathrm{ind}_{G_i}^G \rho_i(h, a)\phi = \sum_{\widetilde{h} \in H} h\widetilde{h}\langle \chi_i, (h\widetilde{h})^{-1}a\rangle \phi(\widetilde{h}^{-T}\chi_i) = \sum_{\overline{h} \in H} \overline{h}\langle \overline{h}^{-T}\chi_i, a\rangle \phi(h^T\overline{h}^{-T}\chi_i),$$

thus the induced representation becomes

$$\overline{R}_i(h, a)\phi(x) = \langle x, a\rangle \phi(h^T x) \quad \text{for } x = \overline{h}^{-T}\chi_i \in \mathrm{Orb}(\chi_i).$$

This way we get $(N^2 - 1)/6$ 6-dimensional irreducible representations, one for each full orbit. In addition we get 6 one-dimensional representations for the orbit consisting of the origin. These are given as

$$\rho_{0,k}(S^j, a) = \exp(2\pi \mathrm{i}kj/6) \quad \text{for } k = 0, 1, \dots, 5.$$

Matrix Representations

We may present the representation $\bar{R}_i$ given above as 6×6 matrices. If we let $(S^{-T})^r\chi_i = x_r$ for $r = 0, \dots, 5$, we find

$$\bar{R}_i(S, 0) = \phi(x_r) = \phi(x_{i+1}),$$

thus $\bar{R}_i(S, 0) = C$, where C is the cyclic shift matrix

$$C = \begin{pmatrix} & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \\ 1 & & & & & \end{pmatrix}.$$

Furthermore, $\bar{R}_i(\mathbb{I}, A)\phi(x_i) = \langle x_i, a\rangle$, therefore

$$\bar{R}_i(\mathbb{I}, a) = D_a = \begin{pmatrix} \langle \chi_i, a\rangle & & & \\ & \langle S^{-T}\chi_i, a\rangle & & \\ & & \ddots & \\ & & & \langle (S^{-T})^5\chi_i, a\rangle \end{pmatrix}.$$

We now have the proper machinery to continue with the next chapter. Almost all of the theorems in this chapter can be generalized in some sense to a more wider class of groups.

Chapter 4

Harmonic Analysis on Groups

In this section we present Fourier analysis on noncommutative groups. We start with simple finite groups and then consider compact ones and at last we discuss how to handle noncompact noncommutative unimodular groups. In the last case we emphasize on the Euclidean motion group. The theory in this chapter follows [2] and other references cited throughout this chapter.

4.1 Introduction

Given two square integrable functions $f_i(g)$ for $i = 1, 2$ with respect to an invariant integration measure μ on a group G which are unimodular, i.e.,

$$\mu(|f_i(g)|^2) = \int_G |f_i(g)|^2 \, d(g) < \infty$$

and

$$\mu(f_i(hg)) = \mu(f_i(gh)) = \mu(f_i(g)) \qquad \forall \qquad h \in G,$$

the convolution product can be defined as

$$(f_1 * f_2)(g) = \int_G f_1(h) f_2(h^{-1}g) \, d(h),$$

and the Fourier transform

$$\mathcal{F}(f) = \hat{f}(p) = \int_G f(g) U(g^{-1}, p) \, d(g).$$

Here $U(\cdot, p)$ is called an irreducible unitary representation(IUR) for each value of the parameter p. Defined this way, the Fourier transform has a corresponding inversion, convolution and Parseval theorem

$$f(g) = \int_{\hat{G}} \text{trace}[\hat{f}(p) U(g, p)] \, dv(p),$$

$$\mathcal{F}(f_1 * f_2) = \hat{f}_2(p)\hat{f}_1(p)$$

and

$$\int_G |f(g)|^2 d(g) = \int_{\hat{G}} \|\hat{f}(p)\|^2 \, dv(p),$$

Where $\|\cdot\|$ is the Hilbert-Schmidt norm and $\hat{G}$ is the dual of the group G (space of all p values). v is an integration measure on $\hat{G}$.

Throughout this section we will assume functions to be as well-behaved as required for the given context and the condition of square integrability is assumed to hold as well. In the Lie-group case with elements parameterized as $g(x_1, \cdots, x_n)$, all the partial derivatives of $f(g(x_1, \cdots, x_n))$ for all the parameters x_i is assumed to exist. In the noncompact case, all the functions $f(g)$ are in $\mathcal{L}^p(G)$ for all $p \in \mathbb{Z}^+$ and they are rapidly decreasing in the sense that

$$\int_G |f(g(x_1, \cdots, x_n))| x_1^{p_1} \cdots x_n^{p_n} \, d(g(x_1, \cdots, x_n)) < \infty$$

for all $p_i \in \mathbb{Z}^+$.

4.2 Fourier Analysis on Finite Groups

Let G be a finite group of order $|G|$. Given a function $f(g)$ which assigns a complex value to each group element, that is, $f : G \to \mathbb{C}$, then the convolution of two such functions $f_i(g)$ on G may be written as

$$(f_1 * f_2)(g) = \sum_{h \in G} f_1(h) f_2\left(h^{-1} g\right). \tag{4.1}$$

The convolution of two functions on a noncommutative group G does not in general commute: $(f_1 * f_2)(g) \neq (f_2 * f_1)(g)$. Some of the exception of this are if one of the functions $f_i(g)$ are scalar multiple of the other, or if one or both of the functions are class functions. In these cases the convolution will commute.

4.2.1 Fourier Transform, Inversion formula and Convolution Theorem

Definition 4.1. Let $\pi_j(g)$ be a irreducible unitary representation of a group G. The Fourier transform of a complex-valued function $f : G \to \mathbb{C}$ is the matrix-valued function with the representation-valued argument defined as

$$\mathcal{F} = \hat{f}(\pi_j) = \sum_{g \in G} f(g) \pi_j(g^{-1}). \tag{4.2}$$

The matrix-valued function $\hat{f}(\pi_j)$ is referred to as the Fourier Transform at the representation π_j and the collection $\{\hat{f}(\pi_j)\}$ for $i = 1, \cdots \alpha$ is called the spectrum of f.

Theorem 4.2. *Let d_j be the dimension of the irreducible unitary representation π_j. The following inversion formula reproduces f from its spectrum*

$$f(g) = \frac{1}{|G|} \sum_{j=1}^{\alpha} d_j \mathrm{trace} \left[\hat{f}(\pi_j) \pi_j(g) \right], \tag{4.3}$$

where the sum is taken over all inequivalent irreducible representations.

Because of the trace, this formula will still work with representations which are not unitary.

Theorem 4.3. *The Fourier transform of the convolution of two functions on G is the matrix product of the Fourier transform matrices*

$$\mathcal{F}((f_1 * f_2)(g))(\pi_j) = \hat{f}_2(\pi_j)\hat{f}_1(\pi_j),$$

where the order of the product matters.

Proof. By definition we have

$$\mathcal{F}((f_1 * f_2))(g)(\pi_j) = \sum_{g \in G} \left(\sum_{h \in G} f_1(h) f_2\left(h^{-1}g\right) \right) \pi_j\left(g^{-1}\right).$$

Setting $k = h^{-1}g$ and substituting $g = hk$, the expression becomes

$$\sum_{k \in G} \sum_{h \in G} f_1(h) f_2(k) \pi_j\left(k^{-1}h^{-1}\right).$$

The homomorphism property of π_j and the commutative nature of the scalar-matrix multiplication and summation lets us split this into

$$\left(\sum_{k \in G} f_2(k) \pi_j\left(k^{-1}\right) \right) \left(\sum_{h \in G} f_1(h) \pi_j\left(h^{-1}\right) \right) = \hat{f}_2(\pi_j)\hat{f}_1(\pi_j).$$

□

The choice of how the Fourier transform is defined decides if the order of the matrix product of Fourier matrices is reversed or not. In some literature the Fourier transform is defined using $\pi_j(g)$, instead of $\pi_j(g^{-1})$, which keeps the order of the product of the Fourier transform matrices the same as the order of the convolution in Theorem 4.3. Nevertheless, the order of the product still matters, and cannot be interchanged.

Lemma 4.4. *The generalization of the Parseval equality (called the Plancherel theorem in the context of group theory) is written as*

$$\sum_{g \in G} |f(g)|^2 = \frac{1}{|G|} \sum_{j=1}^{\alpha} d_j \left\| \hat{f}(\pi_j) \right\|_2^2,$$

where $\|\cdot\|_2$ is the Hilbert-Schmidt norm of a matrix. A more general form of this equation is

$$\sum_{g \in G} f_1\left(g^{-1}\right) f_2(g) = \frac{1}{|G|} \sum_{j=1}^{\alpha} d_j \mathrm{trace} \left[\hat{f}_1(\pi_j)\hat{f}_2(\pi_j) \right].$$

4.2.2 Fast Fourier Transform for Finite Groups

The classical fast Fourier transform has in a series of papers by Diaconis and Rockmore [6], Rockmore [7], Maslen [8] and Maslen and Rockmore [9] been extended to the context of finite groups. We shall only go into the key enabling concept of fast Fourier transform for groups and leave out the more technical detail.

A function $F : S \to V$, where S is a finite set and V is a vector space, may be decomposed as

$$\sum_{s\in S} F(s) = \sum_{[s]\in S/\sim} \left(\sum_{x\in[s]} F(x) \right) \tag{4.4}$$

for any equivalence relation $\sim$.

Two natural equivalence classes are evident; conjugacy classes and cosets. In the first case Equation (4.4) is written as

$$\sum_{g\in G} F(g) = \sum_{i=1}^{\alpha} \sum_{g\in \mathcal{C}_i} F(g).$$

Recall that α is the number of conjugacy classes. In the last case, the decomposition with the equivalence classes as cosets may be written as

$$\sum_{g\in G} F(g) = \sum_{\sigma\in G/H} \left(\sum_{s\in\sigma} F(s) \right) \tag{4.5}$$

Each left coset of G is of the form $\sigma = gH$, so $|\sigma| = |H|$ and we have $|G| = |G/H| \cdot |H|$, where $|G/H| = |G|/|H|$ is the number of left cosets.

If we choose a an element $s_\sigma \in \sigma$ for each $\sigma \in G/H$ called a coset representation, and use the observation that

$$\sum_{s_\sigma\in\sigma} F(s) = \sum_{h\in H} F(s_\sigma h),$$

Equation (4.5) may be rewritten as

$$\sum_{g\in G} F(g) = \sum_{\sigma\in G/H} \left(\sum_{h\in H} F(s_\sigma h) \right). \tag{4.6}$$

This is an important step in making a recursive computation for the Fourier transform for groups. Unfortunately, this alone does not enable fast evaluation of the arbitrary sum $\sum_{g\in G} F(g)$. Another key step is to use the special property of the Fourier transform of a function on a finite group

$$F(g) = f(g)\pi\left(g^{-1}\right)$$

where $\pi(g)$ is an irreducible matrix representation of the group. We may then use the homomorphism property $\pi(g_1 g_2) = \pi(g_1)\pi(g_2)$ of the representation and write the Fourier transform in Equation (4.2) as

$$\sum_{g\in G} f(g)\pi\left(g^{-1}\right) = \sum_{\sigma G/H}\left(\sum_{h\in H} f_\sigma(h)\pi\left(h^{-1}\right)\right)\pi\left(s_\sigma^{-1}\right) \tag{4.7}$$

where $f_\sigma(h) = f(s_\sigma h)$. Since the restriction of an irreducible representation to a subgroup is not always irreducible, we write it as a direct sum of irreducible representations

$$\pi(h) \cong \sum_k \oplus_k \pi_k^H(h). \tag{4.8}$$

By choosing a special kind of basis (called "H-adapted"), the equivalence in Equation (4.8) becomes an equality. Recall from the previous chapter that c_k is the number of times $\pi_k^H(h)$ appears in the decomposition. Since $\sum_k c_k \mathrm{dim}(\pi_k^H) = \mathrm{dim}(\pi)$, we see that it is more efficient to compute the Fourier transform of all the functions $f_\sigma(\sigma)$ on H using the irreducible representations as $\sum_{h\in H} f_\sigma(h)\pi_k^H(h^{-1})$ for all $\sigma \in G/H$ and for all values of k, and then use Equations (4.7) and (4.8) to recompose the Fourier transform on the whole group. If G can be decomposed into a "tower of subgroups"

$$G_n \subset \cdots \subset G_2 \subset G_1 \subset G,$$

Equation (4.6 may be written as

$$\sum_{g\in G} F(g) = \sum_{\sigma_1\in G/G_1}\sum_{\sigma_2\in G_1/G_2}\cdots\sum_{\sigma_1\in G_{n-1}/G_n}\sum_{h\in G_n} F(s_{\sigma_1}\cdots s_{\sigma_n}h) \tag{4.9}$$

and the representation $\pi(g)$ is recursively decomposed into smaller and smaller representations as we restrict them to smaller and smaller subgroups.

If the direct evaluation of the whole spectrum of a function on a finite group is used, the computational performance is done in $\mathcal{O}(|G|^2)$ computations. The procedure given above is in general better and for some classes of groups $\mathcal{O}(|G|\mathrm{log}|G|)$ or $\mathcal{O}(|G|(\mathrm{log}|G|)^2)$. At least $\mathcal{O}(|G|^{\frac{3}{2}})$ performance is possible.

Theorem 4.5. *Let $G = G_1\times G_2\times\cdots\times G_k$ be the direct product of finite groups $G_1, \cdots, G_k$. Then the Fourier transform and its inverse may be computed in $\mathcal{O}(|G|\sum_{i=1}^k |G_i|)$ arithmetic operations.*

4.3 Harmonic Analysis on Lie groups

Except for some cases, the theory presented in Chapter 3 may be generalized in a straightforward way to numerous kinds of groups which has invariant integration measures.

4.3.1 Representations of Lie Groups

The physical applications of Lie groups representations are many. When quantum mechanics saw the light of day, Lie groups evolved with it and today serves as the natural language to express the quantum theory of angular momentum. Also, the connection to the theory of special functions are of great importance in this thesis. It provides us with a concrete treatment of harmonic analysis on the Euclidean motion group.

The Left Quasi-Regular Representation

Denote K as either $\mathbb{R}^N$ or $\mathbb{C}^N$, and consider for all $g \in G$ a transformation group G that acts on $\mathbf{x} \in K$ as $g\mathbf{x} \in K$. The **left-regular representation** of G is then the the group $GL(\mathcal{L}^2(K))$ [i.e., the set of all linear transformations of $\mathcal{L}^2(K)$ with composition as operator]. The group has elements $L(g)$ and group operation $L(g_1)L(g_2)$, defined such that the linear operator $L(g)$ act on scalar-valued functions $f(\mathbf{x}) \in \mathcal{L}^2(K)$ as

$$L(g)f(\mathbf{x}) = f(g^{-1}\mathbf{x}).$$

To prove that L is a representation of G we only need to show that $L : G \to GL(\mathcal{L}^2(K)$ is a homomorphism, since $GL(\mathcal{L}^2(K))$ is a group of linear transformations.

$$\begin{aligned}
(L(g_1)L(g_2)f)(\mathbf{x}) &= (L(g_1)(L(g_2)f))(\mathbf{x}) = (L(g_1)f_{g_2})(\mathbf{x}) \\
= f\left(g_2^{-1}g_1^{-1}\mathbf{x}\right) &= f\left((g_1g_2)^{-1}\mathbf{x}\right) = L(g_1g_2)f(\mathbf{x}).
\end{aligned}$$

The notation $f_{g_2}(\mathbf{x}) = f(g_2^{-1}\mathbf{x})$ is used here, so we have $L(g_1g_2) = L(g_1)L(g_2)$. In the same manner it can be shown that the **right quasi-regular representation** of a matrix Lie group G defined by

$$R(g)f(\mathbf{x}) = f\left(\mathbf{x}^T g\right)$$

is also a representation.

With an appropriate basis for the invariant subspaces of $\mathcal{L}^2(K)$, the matrices corresponding to these operators may be generated. Thus, we have the irreducible representations of the group. On the other hand, the invariant subspaces for noncompact noncommutative groups will have an infinite number of basis elements, which makes the representation matrices infinite dimensional.

4.3.2 Compact Lie Groups

As already mentioned in the start of this section: The formulation for representation theory for finite groups carries over almost word-for-word to compact Lie groups with invariant integration replacing summation over the group. Therefore, we only state the most important facts.

The Fourier transform of a function f on a compact Lie group is defined as

$$\hat{f}(\lambda) = \int_G f(g)U(g^{-1}, \lambda)\, d(g),$$

or in component form

$$\hat{f}_{i,j}(\lambda) = \int_G f(g) U_{i,j}(g^{-1}, \lambda)\, d(g).$$

The dual group of G is $\hat{G}$ and it is the collection of all λ values. The spectrum of the function f is the collection of Fourier transforms $\{\hat{f}(\lambda)\}$ for all $\lambda \in \hat{G}$.

The corresponding inversion formula is

$$f(g) \sum_{\lambda \in \hat{G}} d(\lambda) \text{trace} \left(\hat{f}(\lambda) U(g, \lambda) \right).$$

For two square-integrable functions on a compact Lie group the convolution product can be defined as

$$(f_1 * f_2) = \int_G f_1(h) f_2(h^{-1} g)\, d(h).$$

The Plancherel formulae is

$$\int_G f_1(g) \overline{f_2(g)}\, d(g) = \sum_{\lambda \in \hat{G}} d(\lambda) \text{trace} \left(\hat{f}_1(\lambda) \hat{f}_2^{\dagger}(\lambda) \right)$$

and

$$\int_G |f(g)|^2\, d(g) \sum_{\lambda \in \hat{G}} d(\lambda) \|\hat{f}(\lambda)\|^2.$$

Theorem 4.6 (Peter-Weyl). *The collection of functions $\{\sqrt{d(\lambda)} U_{i,j}(g, \lambda)\}$ for all $\lambda \in \hat{G}$ and $1 \leq i, j \leq d(\lambda)$ form a complete orthonormal basis for $\mathcal{L}^2(G)$. The Hilbert space $\mathcal{L}^2(G)$ can be decomposed into orthogonal subspaces*

$$\mathcal{L}^2(g) = \sum_{\lambda \in \hat{G}} \oplus V_\lambda. \tag{4.10}$$

For each fixed value of λ, the functions $U_{i,j}(g, \lambda)$ form a basis for the subspace V_λ. Analogous to the finite-group case, the left and right regular representations of the group are defined on the space of square integrable functions on the group $\mathcal{L}^2(G)$ as

$$(L(g)k)(h) = k\left(g^{-1} h\right) \qquad \text{and} \qquad (R(g)k)(h) = k(hg),$$

where $k \in \mathcal{L}^2(G)$. Both of these representations can be decomposed as

$$T(g) \cong \sum_{\lambda \in \hat{G}} \oplus d(\lambda) U(g, \lambda),$$

where $d(\lambda)$ is the dimension of $U(g, \lambda)$. Here $T(g)$ stands for either $L(g)$ or $R(g)$. Each of the irreducible representations $U(g, \lambda)$ acts only on the corresponding subspace V_λ.

4.3.3 Induced Representations of Lie Groups

The Homogeneous space G/H have dimension $\dim(G/H) = \dim(G) - \dim(H)$ and is in general a manifold. The matrix elements of a representation $U(g)$ are therefore calculated as

$$U_{i,j}(g) = (e_i, U(g)e_j)\,,$$

where $\{e_k\}$ is a complete set of orthonormal eigenfunctions for $\mathcal{L}^2(G/H)$ for $k = 1, 2\cdots$ and the inner product is defined as

$$(\phi_1, \phi_2) = \int_{G/H} \overline{\phi_1(\sigma)}\phi_2(\sigma)\; d(\sigma).$$

Note that $d(\sigma)$ is in this context an integration measure of G/H.

Analogously as in Chapter 3 we have a test for determining if a representation is irreducible

Theorem 4.7. *A representation $U(g)$ of a compact Lie group G with invariant integration measure $d(g)$ normalized so that $\int_G d(g) = 1$ is irreducible if and only if the character $\chi(g) = \mathrm{trace}(U(g))$ satisfies*

$$\int_G \chi(g)\overline{\chi(g)}\; d(g) = 1. \tag{4.11}$$

Given a Lie group, we evaluate a given representation $U(g)$ at a one-parameter subgroup generated by exponentiating an element of the Lie algebra as $U(exp(tX_i))$. The linear term in t will have constant coefficient matrix

$$u(X_i))\; \left.\frac{d(exp(tX_i))}{dt}\right|_{t=0}. \tag{4.12}$$

if we expand the matrix function of t in a Taylor series. We have then another test for irreducibility.

Theorem 4.8. *Given a Lie group G, associated Lie algebra $\mathcal{G}$, and finite-dimensional $u(X_i)$ as defined in Equation (4.12), then*

$$U(exp(tX_i)) = \exp[tu(X_i)], \tag{4.13}$$

where $X_i \in \mathcal{G}$. Furthermore, if the matrix exponential parameterization

$$g(x_1, \cdots, x_n) = \exp\left(\sum_{i=1}^{n} x_i X_i\right) \tag{4.14}$$

is surjective, then when the $u(X_i)$'s are not simultaneously block-diagonalizable,

$$U(g) = \exp\left(\sum_{i=1}^{n} x_i u(X_i)\right) \tag{4.15}$$

is an irreducible representation for all $g \in G$.

The irreducibility may also be checked by considering how the representation operators acts on subspaces of function spaces, which is essentially the same argument in a different terminology. This method will be used to determine the irreducibility of the representations of $SE(2)$.

Since $SE(N)$ is a solvable Lie group there exist general methods for construction of unitary representations for it.

4.4 Harmonic Analysis on the Euclidean Motion Groups

The semidirect product of $\mathbb{R}^N$ and the special orthogonal group $SO(N)$ is called the Euclidean motion group, the special Euclidean group or just the motion group, and is denoted $SE(N) = \mathbb{R}^N \rtimes_\varphi SO(N)$. The elements of this group is denoted as $g = (\mathbf{a}, A) \in SE(N)$ where $A \in SO(N)$ and $a \in +\mathbb{R}^N$ and the group law is written for any $g = (\mathbf{a}, A)$ and $h = (\mathbf{r}, R) \in SE(N)$ as $gh = (\mathbf{a} + A\mathbf{r}, AR)$ and $g^{-1} = (-A^T\mathbf{a}, A^T)$. We may also represent any element of $SE(N)$ as as a $(n+1)(n+1)$ homogeneous transformation matrix of the form

$$H(g) = \begin{pmatrix} A & \mathbf{a} \\ \mathbf{0}^T & 1 \end{pmatrix}.$$

4.4.1 Parameterization and IURs of $SE(2)$

We may parameterize each element of $SE(2)$ as either

Rectangular coordinates:

$$g(a_1, a_2, \theta) = \begin{pmatrix} \cos\theta & -\sin\theta & a_1 \\ \sin\theta & \cos\theta & a_2 \\ 0 & 0 & 1 \end{pmatrix}$$

Polar coordinates:

$$g(a_1, a_2, \theta) = \begin{pmatrix} \cos\theta & -\sin\theta & a\cos\phi \\ \sin\theta & \cos\theta & a\sin\phi \\ 0 & 0 & 1 \end{pmatrix}$$

where $a = \|\mathbf{a}\|$.

The unitary representations of $SE(2)$ may be defined by the unitary operator

$$U(g, p)\tilde{\varphi}(\mathbf{x}) \triangleq e^{-ip(\mathbf{a}\cdot\mathbf{x})}\tilde{\varphi}\left(A^T\mathbf{x}\right) \triangleq \tilde{\varphi}_g(\mathbf{x}), \tag{4.16}$$

for each $g(\mathbf{a}, A) = g(a_1, a_1, \theta) \in SE(2)$. The parameter $p \in \mathbb{R}^+$ and $\mathbf{x}$ is a unit vector.

Using the fact that $\mathbf{x}$ is a unit vector we have that $\tilde{\varphi}(\mathbf{x}) \triangleq \tilde{\varphi}(\cos\psi, \sin\psi) \equiv \varphi(\psi)$ and we will therefore not distinguish between the two functions $\tilde{\varphi}$ and φ.

Like with any function $\varphi(\psi) \in \mathcal{L}^2(S^1)$ the matrix elements of the operator $U(g,p)$ can be expressed as a weighted sum of orthonormal basis functions. With the basis $e^{in\psi}$ the expression becomes

$$U_{mn}(g,p) = \left(e^{im\psi}, U(g,p)e^{in\psi}\right) = \frac{1}{2\pi}\int_0^{2\pi} e^{-im\psi}e^{-i(a_1 p\cos\psi + a_2 p \sin\psi)}e^{in(\psi-\theta)}\, d\psi \tag{4.17}$$

$\forall m,n \in Z$. With the inner product $(\cdot,\cdot)$ defined as

$$(\varphi_1,\varphi_2) = \frac{1}{2\pi}\int_0^{2\pi} \overline{\varphi_1(\psi)}\varphi_2(\psi)\, d\psi.$$

The work of [10, 11, 12] and more, have proved that we may express the matrix elements of this representation as

$$U_{mn}(g(a,\phi,\theta),p) = i^{n-m}e^{-i[n\theta+(m-n)\phi]}J_{n-m}(pa) \tag{4.18}$$

where $J_\nu(x)$ is the ν^{th} order Bessel function.

Since $U(g,p)$ is a unitary representation we have from this expression that

$$\begin{aligned} U_{mn}(g^{-1}(a,\phi,\theta),p) &= U^{-1}_{mn}(g(a,\phi,\theta),p) \\ &= \overline{U_{mn}(g(a,\phi,\theta),p)} = i^{n-m}e^{-i[n\theta+(n-m)\phi]}J_{m-n}(pa) \end{aligned} \tag{4.19}$$

Hereafter we will not distinguish between the operator $U(g,p)$ and the infinite dimensional matrix, $U_{mn}(g,p)$ corresponding to it.

Symmetry Properties of U_{mn}

The symmetries of the matrix elements are

$$\overline{U_{mn}(g,p)} = (-1)^{m-n}U_{-m,-n}(g,p),$$

$$U_{mn}(g(-a,\phi,\theta),p) \triangleq U_{mn}(g(a,\phi,\pm\pi,\theta),p) = (-1)^{m-n}U_{mn}(g(a,\phi,\theta),p)$$

and

$$(-1)^{m-n}U_{mn}(g(a,\phi-\theta,-\theta),p) = \overline{U_{mn}(g(a,\phi,\theta),p)}.$$

Irreducibility of $U(g,p)$

The representation matrices of $SE(2)$ will be infinite dimensional since the group is neither compact nor commutative. Thus, it is convenient to study the operator $U(g,p)$ rather than the corresponding matrix to show the irreducibility. Using the basis

$$X_1 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}; \qquad X_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}; \qquad X_3 = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix};$$

one parameter subgroups generated by exponentiating linearly independent basis elements of the Lie algebra $se(2)$ is examined and one finds that

$$\begin{aligned}
g_1(t) &= \exp(tX_1) = \begin{pmatrix} 1 & 0 & t \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}; \\
g_2(t) &= \exp(tX_2) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix}; \\
g_3(t) &= \exp(tX_3) = \begin{pmatrix} \cos t & -\sin t & 0 \\ \sin t & \cos t & 0 \\ 0 & 0 & 1 \end{pmatrix}.
\end{aligned}$$

The differential operator $\tilde{X}_i^R$ and $\tilde{X}_i^L$ in polar coordinates becomes

$$\begin{aligned}
\tilde{X}_1^R &= \cos(\theta-\phi)\frac{\partial}{\partial a} + \frac{\sin(\theta-\phi)}{a}\frac{\partial}{\partial \phi} \\
\tilde{X}_2^R &= -\sin(\theta-\phi)\frac{\partial}{\partial a} + \frac{\cos(\theta-\phi)}{a}\frac{\partial}{\partial \phi} \\
\tilde{X}_3^R &= \frac{\partial}{\partial \theta}
\end{aligned}$$

and

$$\begin{aligned}
\tilde{X}_1^L &= \cos\phi\frac{\partial}{\partial a} - \frac{\sin\phi}{a}\frac{\partial}{\partial \phi} \\
\tilde{X}_2^L &= \sin\phi\frac{\partial}{\partial a} - \frac{\cos\phi}{a}\frac{\partial}{\partial \phi} \\
\tilde{X}_3^L &= \frac{\partial}{\partial \theta} + \frac{\partial}{\partial \phi}.
\end{aligned}$$

From Equation (4.16) it follows that

$$\begin{aligned}
U(g_1(t),p)\varphi(\psi) &= e^{-ipt\cos\psi}\varphi(\psi); \\
U(g_2(t),p)\varphi(\psi) &= e^{-ipt\sin\psi}\varphi(\psi); \\
U(g_3(t),p)\varphi(\psi) &= \varphi(\psi-t).
\end{aligned}$$

By differentiating with respect to t at $t=0$, we define the operators

$$\hat{X}_i(p)\varphi(\psi) \triangleq \left.\frac{dU(\exp(tX_i),p)\varphi(\psi)}{dt}\right|_{t=0}.$$

I.e,

$$\begin{aligned}\hat{X}_1\varphi &= -ip\cos\psi\varphi(\psi);\\ \hat{X}_2\varphi &= -ip\sin\psi\varphi(\psi);\\ \hat{X}_3\varphi &= -\frac{d\varphi}{d\psi}.\end{aligned}$$

It is convenient to define the operators

$$\hat{Y}_+(p) = \hat{X}_1(p) + i\hat{X}_2(p); \quad \hat{Y}_-(p) = \hat{X}_1(p) - i\hat{X}_2(p); \quad \hat{Y}_+(p) = \hat{X}_3$$

to show how the basis elements are transformed by these operators. For functions $\varphi \in \mathcal{L}^2(S^1)$ we have basis elements of the form $e^{ik\psi}$ and they are transformed as [12]

$$\hat{Y}_+(p)e^{ik\psi} = -ipe^{i(k+1)\psi}; \quad \hat{Y}_-(p)e^{ik\psi} = -ipe^{i(k-1)\psi}; \quad \hat{Y}_3(p)e^{ik\psi} = -ike^{ik\psi}.$$

We see here that that subspaces of functions that consist of scalar multipliers of $e^{ik\psi}$ are stable under $\hat{Y}_3$, and it is clear that no subspaces (except of the zero subspace and the whole supspace) can be be left invariant under $\hat{Y}_\pm$ and $\hat{Y}_3$ simultaneously since $\hat{Y}_\pm$ always "push" basis elements to "adjacent" subspaces. Hence the representation operator $U(g,p)$ are irreducible, and there their corresponding matrices are irreducible as well.

4.4.2 The Fourier Transform for $SE(2)$

Using the representations from the previous section we are ready to define the Fourier transform for $SE(2)$.

Definition 4.9. [13] The Fourier transform of a rapidly decreasing function $f \in \mathcal{L}(G)$ [Where $G = SE(2)$] and its inverse transform are defined as

$$\mathcal{F}(f) = \hat{f}(p) = \int_G f(g)U\left(g^{-1},p\right)\, d(g)$$

and

$$\mathcal{F}^{-1}(\hat{f}) = f(g) = \int_0^\infty \text{trace}\left(\hat{f}(p)U(g,p)\right)\, pdp.$$

We have the same property as the Fourier transform of functions on $\mathbb{R}^N$,ie.,

$$\mathcal{F}\mathcal{F}^{-1}\left(\hat{f}\right) = \hat{f} \quad \text{and} \quad \mathcal{F}^{-1}\mathcal{F}(f) = f,$$

so we may write symbolically

$$\mathcal{F}\mathcal{F}^{-1} = \mathcal{F}^{-1}\mathcal{F} = id$$

where id is the identity operator. The proof for this identity is given in [13]. Because $\{U(g,p)\}$ are a complete set of irreducible representations and the property that it is unitary lets us write $U(g^{-1},p) = U^\dagger(g,p)$, and we therefore may use this instead of computing the inverse of an infinite dimensional matrix.

The Fourier transform has matrix elements

$$\hat{f}_{mn}(p) = \left(e^{im\psi}, \hat{f}(p)e^{in\psi}\right) = \int_G f(g)U_{mn}\left(g^{-1}, p\right)\ d(g)$$

which may be calculated using the matrix elements of $U(g,p)$ in Equation(4.18). The inverse transformation is written as

$$f(g) = \sum_{n,m\in\mathbb{Z}} \int_0^\infty \hat{f}_{mn}(p)U_{nm}(g,p)\ pdp.$$

4.4.3 The Convolution Theorem and Parseval's Equality for $SE(2)$

Convolution on $SE(2)$ is defined as

$$(f_1 * f_2)(g) = \int_{SE(2)} f_1(h)f_2(h^{-1}\circ g)\ d(h),$$

and by taking the Fourier transform we get the convolution theorem

$$\mathcal{F}(f_1 * f_2) = \hat{f}_2(p)\hat{f}_1(p).$$

Again, we emphasis that the order of the product of Fourier transforms matters.

Parseval's Equality (also referred to as the Plancherel formula) for $SE(2)$ is

$$\int_{SE(2)} |f(g)|^2 d(g) = \int_0^\infty \left\|\hat{f}(p)\right\|_2^2\ pdp.$$

4.4.4 IURs of $SE(3)$

There are several ways of defining unitary irreducible representations (IURs) of $SE(3)$. In this section, the same notation for the Fourier transform of a function $\varphi(\mathbf{p})$ and the the function itself $\varphi(\mathbf{r})$ is used. Therefore, the argument $\mathbf{r}$ or $\mathbf{p}$ specifies which are considered.

First, we begin by constructing the representation of the motion group in the space of functions $\varphi(\mathbf{p}) \in \mathcal{L}^2(\hat{T})$, where $\hat{T}$ is the frequency (dual) space of the $\mathbb{R}^3$ subgroup. The Fourier transform of the function $\varphi(\mathbf{r}) \in \mathcal{L}^2(T)$, for $T = \mathbb{R}^3$ is defined as

$$\varphi(\mathbf{p}) = \frac{1}{(2\pi)^{3/2}} \int_T e^{-i\mathbf{p}\cdot\mathbf{r}} \varphi(\mathbf{r}\ d\mathbf{r}.$$

The action of the rotation subgroup $SO(3)$ of the motion group on $\hat{T}$ is rotation and it divides $\hat{T}$ into orbits S_p, where S_p are S^2 spheres of radius $p = |\mathbf{p}|$. The action of the translation operator on a function $\varphi(\mathbf{p})$ is

$$(U(\mathbf{a}, \mathbb{I})\varphi)(\mathbf{p}) = e^{-i\mathbf{p}\cdot\mathbf{a}}\varphi(\mathbf{p}).$$

Thus, we may build the irreducible representations of the motion group on spaces $\varphi(\mathbf{p}) \in \mathcal{L}^2(S_p)$, with the inner product defined as

$$(\varphi_1, \varphi_2) = \int_{\Theta=0}^{\pi} \int_{\Phi=0}^{2\pi} \overline{\varphi_1(\mathbf{p})} \varphi_2(\mathbf{p}) \ \sin\Theta d\Theta d\Phi, \tag{4.20}$$

where $\mathbf{p} = (p\sin\Theta\cos\Phi, p\sin\Theta\sin\Phi, p\cos\Theta)$, and $p > 0, 0 \leq \Theta \leq \pi, 0 \leq \Phi \leq 2\pi$.

For $A \in SO(3)$ and $0 \leq \alpha \leq 2\pi$, the inner product defined above is invariant with respect to transformations of the type

$$\varphi(\mathbf{p}) \rightarrow e^{i\alpha} \varphi\left(A^{-1}\mathbf{p}\right).$$

The parameter α may have a dependency on p and group element $A \in SO(3)$. If so, different nonlinear functions of group element A, $\alpha_s(p, A)$ (s enumerates the irreducible representations of $SO(2)$), correspond to different irreducible representations of the motion group.

The representations of $G = SE(3) \simeq \hat{T} \rtimes_\varphi SO(3)$ may be constructet with the help of the function $\alpha_s(p, A)$ from the representations of its subgroup $G' = \hat{T} \rtimes_\varphi SO(2)$ by using the method of induced representations. Therefore, if we diregard the translation group for a moment, we have in our case $G = SO(3)$, $H = SO(2)$ and $\sigma = \mathbf{p} \in S_p \simeq SO(3)/SO(2)$.

By choosing a particular vector $\hat{\mathbf{p}} = (0, 0, p)$ on each orbit S_p we may construct the representations of the motion group explicitly. The vector $\hat{\mathbf{p}}$ is invariant under the action from the rotation subgroup $SO(2)$ of $SO(3)$

$$\Lambda\hat{\mathbf{p}} = \mathbf{p}; \quad \Lambda H_{\hat{\mathbf{p}}} = SO(2),$$

where $H_{\hat{\mathbf{p}}}$ is a little group of $\hat{\mathbf{p}}$. We may find $R_{\mathbf{p}} \in SO(3)/SO(2)$ for each $\mathbf{p} \in S_p$, such that

$$R_{\mathbf{p}}\hat{\mathbf{p}} = \mathbf{p}.$$

Then, it may be checked that for any $A \in SO(3)$

$$\left(R_{\mathbf{p}}^{-1} A R_{A^{-1}\mathbf{p}}\right) \hat{\mathbf{p}} = \hat{\mathbf{p}}$$

Thus, we have $\mathcal{Q}(\mathbf{p}, A) \triangleq \left(R_{\mathbf{p}}^{-1} A R_{A^{-1}\mathbf{p}}\right) \in H_{\hat{\mathbf{p}}}$, and the representations of $H_{\hat{\mathbf{p}}}$ may be chosen to be of the form

$$\Delta_s : \phi \rightarrow e^{is\phi} \ , \ 0 \leq \phi \leq 2\pi$$

for $s = 0, \pm 1, \pm 2, \cdots$

Therefore, the induced representation $\mathrm{Ind}_{\hat{T} \rtimes_\varphi \Delta_s(H_{\hat{\mathbf{p}}}))}^{SE(3)}$ of the motion group may be constructed from its subgroup $\hat{T} \rtimes_\varphi H_{\hat{\mathbf{p}}}$.

Definition 4.10. The unitary representations $U^s(\mathbf{a}, A)$ of $SE(3)$, which act on the space of functions $\varphi(\mathbf{p}$ with the inner product Equation (4.20), are defined by

$$(U^s(\mathbf{a}, A)\varphi)(\mathbf{p}) = e^{-i\mathbf{p}\cdot\mathbf{a}} \Delta_s \left(R_{\mathbf{p}}^{-1} A R_{A^{-1}\mathbf{p}}\right) \varphi\left(A^{-1}\mathbf{p}\right), \tag{4.21}$$

where $A \in SO(3)$, Δ_s are representations of $H_{\hat{\mathbf{p}}}$, and $s = 0, \pm 1, \pm 2, \cdots$

The representations characterized by $p = \|\mathbf{p}\|$ and s is irreducible and they are unitary since $(U^s(\mathbf{a}, A)\varphi_1, U^s(\mathbf{a}, A)\varphi_2) = (\varphi_1, \varphi_2)$.

Equation (4.21) may be written as

$$(U^s(\mathbf{a}, A)\varphi)(\mathbf{u}) = e^{-ip\mathbf{u}\cdot\mathbf{a}} \Delta_s \left(R_{\mathbf{u}}^{-1} A R_{A^{-1}\mathbf{u}}\right) \varphi \left(A^{-1}\mathbf{u}\right), \tag{4.22}$$

where $\mathbf{p} = p\mathbf{u}$ and $\mathbf{u}$ is an unit vector and $\varphi(\cdot)$ is defined on the unit sphere. And this representation Equation (4.22) lets us write the matrix elements of the IURs of $SE(3)$ in integral form and apply FFT methods for fast numerical computations [14].

4.4.5 Matrix Elements of $SE(3)$

If we use the group property

$$U^s(\mathbf{a}, A) = U^s(\mathbf{a}, \mathbb{I}) \cdot U^s(0, A). \tag{4.23}$$

we may obtain the matrix elements of the unitary representation of $SE(3)$. We enumerate the basis eigenfunctions of the irreducible representation Equation (4.21) by the integers l, m for each s and p.

The basis functions are expressed in the same form as in [15]

$$h_{ms}(\mathbf{u}(\Theta, \Psi)) = \mathcal{O}^l_{sm}(\cos\Theta) e^{i(m+s)\Psi}, \tag{4.24}$$

where

$$\mathcal{Q}^l_{-s,m}(\cos\Theta) = (-1)^{l-s}\sqrt{\frac{2l+1}{4\pi}} P^l_{sm}(\cos\Theta), \tag{4.25}$$

and generalized Legendre functions $P^l_{ms}(\cos\Theta)$ are given as in Vilenkin and Klimyk [3]. Θ and Ψ are the polar and azimuthal angles of $\mathbf{p}$.

These basis function transform under the rotation $h^l_{ms}(\mathbf{u}) \to \Delta_s(\mathcal{Q}(\mathbf{u}, A))h^l_{ms}(A^{-1}\mathbf{u})$ as

$$\left(U^s(0, A), h^l_{ms}\right)(\mathbf{u}) = \sum_{n=-1}^{l} \tilde{U}^l_{nm}(A) h^l_{ns}(\mathbf{u}, \tag{4.26}$$

where the matrix elemens $\tilde{U}^l_{mn}(A)$ are

$$\tilde{U}_{mn}(A) = e^{-im\alpha}(-1)^{n-m} P^l_{mn}(\cos\beta) e^{-in\gamma}, \tag{4.27}$$

where α, β and γ are ZXZ Euler angles of the rotation and the rotation matrix is not dependent on s.

Now we turn to the translation matrix which is given by the integral [15]

$$\begin{aligned} \left(h^{l'}_{m's}, U^s(\mathbf{a}, \mathbb{I})h^l_{ms}\right) &= [l', m' \mid p, s \mid l, m](\mathbf{a}) \\ &= \int_{\Theta=0}^{\pi}\int_{\Psi=0}^{2\pi} \mathcal{Q}^{l'}_{s,m'}(\cos\Theta) e^{-i(m'+s)\Phi} e^{-i\mathbf{p}\cdot\mathbf{a}} \\ &\quad \mathcal{Q}^l_{s,m}(\cos\Theta) e^{i(m+s)\Phi} \sin\Theta \, d\Theta d\Phi. \end{aligned} \tag{4.28}$$

In closed form these are written as

$$[l',m' \mid p,s \mid l,m](\mathbf{a}) = (4\pi)^{1/2} \sum_{k=|l'-l|}^{l'+l} i^k \sqrt{\frac{(2l'+1)(2k+1)}{(2l+1)}} j_k(pa) C(k,0;l',s \mid l,s) \\ C(k,m-m';l',m' \mid l,m) Y_k^{m-m'}(\theta,\phi), \tag{4.29}$$

where θ, ϕ are polar and azimuthal angles of $\mathbf{a}$, and $C(k,m-m';l',m' \mid l,m)$ are Clebsch-Gordan coefficients (For more details see [16]).

By using the group property Equation (4.23), we may express the matrix elements of the unitary representation $U^s(g,p)$ Equation (4.21) as

$$U^s_{l',m';l,m}(\mathbf{a},A;p) = \sum_{j=-l}^{l} [l',m' \mid p,s \mid l,j] \, (\mathbf{a}) \tilde{U}^l_{jm}(A). \tag{4.30}$$

for $s = 0, \pm 1 \pm 2, \cdots$.

Symmetry Properties

The matrix elements have symmetries properties and by using the Clebsch-Gordan coefficients

$$C(l_1,m_1;l_2,m_2 \mid l,m) = (-1)^{(1_1+l_2+l)} C(l_1,-m_1;l_2,-m_2 \mid l,-m), \tag{4.31}$$

the property

$$Y_l^{-m}(\theta,\phi) = (-1)^m \overline{Y}_l^m(\theta,\phi)$$

and the symmetry relation

$$P^l_{mn}(x) = (-1)^{(m-n)} P^l_{-m,-n}(x),$$

it may be shown that

$$\overline{U^s_{l',m';l,m}(-\mathbf{a},A;p)} = (-1)^{(l'-l)}(-1)^{(m'-m)} U^s_{l',-m';l,-m}(\mathbf{a},A;p). \tag{4.32}$$

From the transformation law Equation (4.28) it may observed that the complex conjugate transformation is related with the $(-s)$ transformation as

$$\overline{U^{-s}_{l',m';l,m}(-\mathbf{a},A;p)} = (-1)^{(m'-m)} U^s_{l',-m';l,-m}(\mathbf{a},A;p), \tag{4.33}$$

when the representation is evaluated at $(-\mathbf{a},A)$.

There exist also a unitary relation

$$U^s_{l',m';l,m}\left(-A^{-1}\mathbf{a},A^{-1};p\right) = \overline{U^s_{l,m;l',m'}(\mathbf{a},A;p)}. \tag{4.34}$$

Orthogonality

If we use the orthogonality of the rotation matrix elements U^l_{mn}, the integral expression Equation for the translation matrix elements (4.28), and the integral representation for the δ-function

$$\int_{\mathbb{R}^3} e^{i(\mathbf{p}-\mathbf{p}')\cdot\mathbf{r}}\, d^3\mathbf{r} = (2\pi)^3\delta(\mathbf{p}-\mathbf{p}')$$

it shows that the $SE(3)$ matrix elements satisfy the orthogonality relation

$$\begin{aligned}&\int_{\mathbb{R}^3} d\mathbf{a} \int_{SO(3)} dA\, \overline{U^s_{l_1,m_1;j_1,k_1}(\mathbf{a},A;p_1)}U^s_{l,m;j,k}(\mathbf{a},A;p)\\ &= 2\pi^2\delta_{l_1 l}\delta_{j_1 j}\delta_{m_1 m}\delta_{k_1 k}\delta_{s_1 s}\,\frac{\delta(p_1-p)}{p^2}\end{aligned} \tag{4.35}$$

where $d\mathbf{a} = a^2\, da\, \sin\theta\, d\theta d\phi$.

4.4.6 The Fourier Transform for $SE(3)$

The inner product for two functions $f_i(\mathbf{a},A) \in \mathcal{L}^2(SE(3))$ is given by

$$(f_1, f_2) = \int_{\mathbb{R}^3}\int_{SO(3)} \overline{f_1(\mathbf{a},A)}f_2(\mathbf{a},A)\, dAd\mathbf{a}. \tag{4.36}$$

We have to use a complete orthogonal basis for functions on the group $SE(3)$ to define the Fourier transform on it. This completeness of the matrix elements Equation (4.30) depends in part on the completeness of the rotation matrix $\tilde{U}^l_{mn}$ on $SO(3)$. We may define the Fourier transform of functions on the motion group by using the unitary representations $U(g,p)$ Equation (4.10)

Definition 4.11. For any absolutely- and square-integrable complex-valued function $f(\mathbf{a},A)$ on $SE(3)$ we define the Fourier transform as

$$\mathcal{F}(f) = \hat{f}(p)\int_{SE(3)} f(g)U\left(g^{-1},p\right)\, d(g)$$

where $g = (\mathbf{a},A) \in SE(3)$ and $d(g) = dAd\mathbf{a}$.

The Fourier transform has matrix elements given in terms by the matrix elements in Equation (4.30)

$$\hat{f}^s_{l',m';l,m}(p) = \int_{SE(3)} f(\mathbf{a},A)\overline{U_{l,m;l',m'}(\mathbf{a},A;p)}\, dAd\mathbf{a} \tag{4.37}$$

where the unitary property is used. The inverse Fourier transform is given by

$$f(g) = \mathcal{F}^{-1}(\hat{f}) = \frac{1}{2\pi^2}\int_{Se(3)} \mathrm{trace}(\hat{f}(p)U(g,p))\, p^2\, dp. \tag{4.38}$$

Written out explicitly

$$f(\mathbf{a}, A) = \frac{1}{2\pi^2} \sum_{s=-\infty}^{\infty} \sum_{l'=|s|}^{\infty} \sum_{l=|s|}^{\infty} \sum_{m'=-l'}^{l'} \sum_{m=-l}^{l} \int_0^{\infty} p^2 \, dp \; \hat{f}^s_{l',m';l,m}(p) U_{l',m';l,m}(\mathbf{a}, A; p). \tag{4.39}$$

4.4.7 The Convolution Theorem and Parseval's Equality for $SE(3)$

Convolution on $SE(3)$ is defined as

$$(f_1 * f_2)(g) = \int_{SE(2)} f_1(h) f_2(h^{-1} \circ g) \; d(h),$$

and by taking the Fourier transform we get the convolution theorem

$$\mathcal{F}(f_1 * f_2) = \hat{f}_2(p) \hat{f}_1(p).$$

Again, we emphasis that the order of the product of Fourier transforms matters.

Parseval's Equality (also referred to as the Plancherel formula) for $SE(3)$ is

$$\begin{aligned}
&\int_{SE(3)} |f(\mathbf{a}, A)|^2 \; dA\mathbf{a} \\
&= \frac{1}{2\pi^2} \sum_{s=-\infty}^{\infty} \sum_{l'=|s|}^{\infty} \sum_{l=|s|}^{\infty} \sum_{m'=-l'}^{l'} \sum_{m=-l}^{l} \int_0^{\infty} |\hat{f}^s_{l',m';l,m}(p)|^2 \; p^2 \; dp \\
&= \frac{1}{2\pi^2} \int_0^{\infty} \left\| \hat{f}(p) \right\|_2^2 \; p^2 \; dp.
\end{aligned} \tag{4.40}$$

Here the Hilbert-Schmidt norm of $\hat{f}(p)$ is given by

$$\left\| \hat{f}(p) \right\|_2^2 \sum_{s=-\infty}^{\infty} \sum_{l'=|s|}^{\infty} \sum_{l=|s|}^{\infty} \sum_{m'=-l'}^{l'} \sum_{m=-l}^{l} \int_0^{\infty} |\hat{f}^s_{l',m';l,m}(p)|^2.$$

4.5 Algorithm for Fast Fourier Transform on the 2D Motion Group

We present here a continuous algorithm for the 2D motion group. This algorithm is similar to the algorithm presented in the next section, but uses $\exp(im\Phi)$ as a basis function instead of pulse functions. The representation operator for the 2D Motion group is

$$U(g, p)\tilde{\varphi}(\mathbf{x}) = e^{-ip(\mathbf{r}\cdot\mathbf{x})} \tilde{\varphi}\left(R^T \mathbf{x}\right), \tag{4.41}$$

which is defined for each $g = (\mathbf{r}, R(\theta) \in SE(2)$. Since the vector $\mathbf{x}$ is a unit vector, $\tilde{\varphi}(\mathbf{x})$ is a function on the unit circle. Henceforth $\tilde{\varphi}(\mathbf{x}) = \tilde{\varphi}(\cos\psi, \sin\psi) \equiv \varphi(\psi)$, so we will not distinguish between $\tilde{\varphi}$ and φ.

Like with any function $\varphi(\psi) \in L^2([0, 2\pi))$ the matrix elements of the operator $U(g, p)$ can be expressed as a weighted sum of orthonormal basis functions. With our basis the expression becomes:

$$U_{mn}(g,p) = \left(e^{im\psi}, U(g,p)e^{in\psi}\right) = \frac{1}{2\pi}\int_0^{2\pi} e^{-im\psi} e^{-i(r_1 p\cos\psi + r_2 p\sin\psi} e^{in(\psi-\theta)}\, d\psi$$

$\forall m, n \in Z$ with the inner product $(\cdot, \cdot)$ defined as

$$(\varphi_1, \varphi_2) = \frac{1}{2\pi}\int_0^{2\pi} \overline{\varphi_1(\psi)}\varphi_2(\psi)\, d\psi$$

$U(g, p)$ is unitary with respect to this inner product since $(U(g, p)\varphi_1, U(g, p)\varphi_2) = (\varphi_1, \varphi_2)$.

The Fourier Matrix elements is expressed as an integral

$$\hat{f}_{mn}(p) = \int_{\mathbf{r}\in\mathbb{R}^2}\int_{\theta=0}^{2\pi}\int_{\psi=0}^{2\pi} f(\mathbf{r},\theta)e^{in\psi}e^{i(\mathbf{p}\cdot\mathbf{r})}e^{-im(\psi-\theta)}\, d^2r\, d\theta\, d\psi.$$

The algorithm is a band-limited approximation of the Fourier transform for $|m|, |n| \le S$ harmonics. We also assume that the order of sampling points in an $\mathbb{R}^2$ region is of order $S^2(N_r = \mathcal{O}(S^2))$ and the amount of sampling points of orientation angle θ is $N_R = \mathcal{O}(S)$, and the number of points along the p-interval is $N_p = \mathcal{O}(S)$. The total number of sample points in $SE(2)$ is in our way $N = \mathcal{O}(S^3)$. This order is the same as the order of sample points in the Fourier domain.

We introduce the notation

N_r	Number of samples on $\mathbb{R}^2$
N_R	Number of samples on $SO(2)$
N_p	Number of samples of p interval
N_u	Number of samples on $[0, 2\pi)$
N_F	Total number of harmonics.

Only matrix elements in the range $|s| < S$ and $l, l' < L$ are computed, since we have made the assumption that only a finite number of harmonics are required for an accurate approximation of the function $f(g)$. Therefore, if we make the assumption that $L = \mathcal{O}(S)$ we may make the following assumption of the number of sample points in terms of S

N_r	$\mathcal{O}(S^2)$
N_R	$\mathcal{O}(S)$
N_p	$\mathcal{O}(S)$
N_u	$\mathcal{O}(S)$
N_F	$\mathcal{O}(S^2)$.

We see from this definition that $N = N_r \cdot N_R = \mathcal{O}(S^3)$ and $N_p \cdot N_F = \mathcal{O}(N)$.

The first step in the 2D motion group Fourier transform is to perform $\mathbb{R}^2$ integration using the usual FFT

$$f_1(\mathbf{p},\theta) = \int_{\mathbb{R}^2} f(\mathbf{r},\theta) e^{i(\mathbf{p}\cdot\mathbf{r})}\, d^2r.$$

This is done in $\mathcal{O}(N_R N_r \log N_r)$ operations.

The next step is to interpolate the polar coordinate mesh. If N_s-point spline interpolation is used, the interpolation may be performed in $\mathcal{O}(N_s N_r N_R)$ operations.

Then we do integration on $SO(2)$

$$f_2^{(m)}(p,\psi) = \int_{SO(2)} f_1(p,\psi,\theta) e^{im\theta}\, d\theta,$$

which may be done in $\mathcal{O}(N_r N_R \log N_R)$ operations. The last step is ψ integration

$$\hat{f}_{mn}(p) = \int_0^{2\pi} \left[f_2^{(m]}(p,\psi) e^{-im\psi} \right] e^{in\psi}\, d\psi.$$

This may be done in $\mathcal{O}(SN_p S \log S) = \mathcal{O}(N_r N_R \log N_R)$ operations. The total number of samples on $SE(2)$ is $N = N_r N_R = \mathcal{O}(S^3)$. We may therefore compute the direct Fourier transform in $\mathcal{O}(N \log N) + \mathcal{O}(N\epsilon(N^{\frac{1}{2}}))$ arithmetic operations.

The inversion formula for the Fourier transform on $SE(2)$ with matrix elements $U_{mn}(g,p)$ is written in integral form as

$$f(g) = \frac{1}{2\pi} \int_0^{\infty} pdp \sum_{m,n=-\infty}^{\infty} \hat{f}_{nm}(p) \int_0^{2\pi} e^{i(n-m)\psi} e^{-i\mathbf{r}\cdot\mathbf{p}} e^{-in\theta}\, d\psi.$$

We may rewrite this as

$$f(g) = \frac{1}{2\pi} \sum_{n=-\infty}^{\infty} e^{-in\theta} \int_{\mathbb{R}^2} \tilde{f}_n(\mathbf{p}) e^{-i\mathbf{r}\cdot\mathbf{p}}\, d^2p$$

where

$$\tilde{f}_n(\mathbf{p}) = \sum_{m=-\infty}^{\infty} \hat{f}_{nm}(p) e^{i(n-m)\psi}.$$

The Fourier inversion may be performed in the same order as the set of FFTs in the forward transform if we assume that the sums over m and n above are truncated at $\pm S = \mathcal{O}(N_R)$ and $\tilde{f}(\mathbf{p})$ is band-limited for each value of n. This way is faster than if the ψ-integration is performed first, even thought that integrating over ψ first result in closed-form solutions for the matrix elements $U_{mn}(g,p)$.

4.6 The Discrete Motion Group of the plane

The *Discrete motion group* of the plane is the subgroup of $SE(2)$ where $\theta = 2\pi i/N_R$ for $i = 0, ..., N_R - 1$. It is the semidirect product of $\mathbb{R}^2$ and the group of rotational symmetries of a regular planar N_R-gon, C_{N_R}. That is, $G = \mathbb{R}^2 \rtimes_\varphi C_{N_R}$, where C_{N_R} is the N_R-element finite subgroup of $SO(2)$.

4.6.1 IURs of the Discrete Motion Group

The irreducible unitary representations $U(\mathbf{a}, A)$ of $SE(2)$ which act on functions $f(\mathbf{u}) \in \mathrm{L}^2(S)[S$ is a unit circle,$\mathbf{u} = (\cos\Theta, \sin\Theta)^T$ is a vector to a point on the unit circle] are defined by the expression

$$(U_p(\mathbf{a}, A; p)\varphi)(\mathbf{u}) = e^{-ip\mathbf{u}\cdot\mathbf{a}}\varphi(A^{-1}\mathbf{u}) = e^{-i\mathbf{p}\cdot\mathbf{a}}\varphi(A^{-1}\cdot(\mathbf{p}/p)),$$

with the inner product defined as

$$(\varphi_1, \varphi_2) = \frac{1}{2\pi}\int_{S^1} \overline{\varphi_1(\Theta)}\varphi_2(\Theta)\, d\Theta$$

where $A \in SO(2)$, $p \in \mathbb{R}^+$, $\mathbf{p} = p\mathbf{u}$ is the vector to arbitrary points in the dual(frequency) space of $\mathbb{R}^2$(where p is the magnitude and $\mathbf{u}$ is the direction) and Θ is an angle on the unit circle.

We choose the same basis as [2], namely a pulse orthonormal basis $\varphi_{N_R,n}(\mathbf{u})$ on S^1. The circle is subdivided into identical segments F_n and the function φ is chosen to satisfy the orthonormality relation

$$\frac{1}{2\pi}\int_{S^1} \varphi_{N_R,n}(\mathbf{u})\varphi_{N_R,m}(\mathbf{u})\, d\Theta = \delta_{nm}.$$

A good choice for the orthonormal functions is

$$\varphi_{N_R,n}(\mathbf{u} = \begin{cases} (N_R)^{1/2} & \text{if } \mathbf{u} \in F_n\,, \\ 0 & \text{otherwise}\,. \end{cases}$$

where $n = 0, ..., N_R - 1$ corresponds to different segments. These pulse functions is denoted as δ-like functions $\varphi_{N_R,n}(\mathbf{u}) = (1/N_R)^{1/2})\delta_{N_R}(\mathbf{u}, \mathbf{u_n})$. Here $\mathbf{u}_n$ is the vector to the centre of the F_n segment.

The matrix elements of the IURs in this basis are

$$U_{mn}(A, \mathbf{r}; p) = \frac{1}{2\pi}\int_S \varphi_{N_R,m}(\mathbf{u})e^{-ip\mathbf{u}\cdot\mathbf{r}}\varphi_{N_R,n}(A^{-1}\mathbf{u})\, d\Theta, \tag{4.42}$$

and by using the δ-like notation it can be written as

$$U_{mn}(A, \mathbf{r}; p) = \frac{1}{2\pi N_R}\int_S \delta_{N_R}(\mathbf{u}, \mathbf{u_m})e^{-ip\mathbf{u}\cdot\mathbf{r}}\delta_{N_R}(A^{-1}\mathbf{u}, \mathbf{u_n})\, d\Theta, \tag{4.43}$$

The last integral, Equation (4.43), may be approximated as

$$U_{mn}(A, \mathbf{r}; p) \approx \frac{1}{N_R}e^{-ip\mathbf{u}_m\cdot\mathbf{r}}\delta_{N_R}(A^{-1}\mathbf{u}_m, \mathbf{u}_n), \tag{4.44}$$

and the δ-function is approximated as

$$1/N_R\delta_{N_R}(A^{-1}\mathbf{u}_m, \mathbf{u}_n) = \delta_{A^{-1}\mathbf{u}_m,\mathbf{u}_n} = \begin{cases} 1 & \text{if } A^{-1}\mathbf{u}_m = \mathbf{u}_n\,, \\ 0 & \text{otherwise} \end{cases}$$

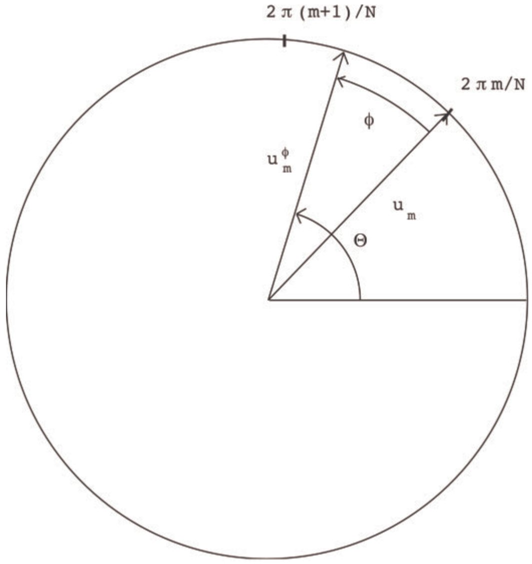


Figure 4.1: Illustration for vectors $\mathbf{u}_m^{\phi}$ in the matrix elements of IURs of the discrete motion group [17]

In other words rotations is restricted to the rotations A_j from the finite C_{N_R} subgroup of $SO(2)$, thus $A_j^{-1}\mathbf{u}_m = \mathbf{u}_{m-j} = \mathbf{u}_n$

Now, the matrix elements of the irreducible unitary representations of the group $G = \mathbb{R}^2 \rtimes_{\varphi} C_{N_R}$ are given as

$$U_{mn}(A_j, \mathbf{r}; p) = e^{-ip\mathbf{u}_m \cdot \mathbf{r}} \delta_{A_j^{-1}\mathbf{u}_m, \mathbf{u}_n}, \tag{4.45}$$

and in this case $\delta_{A_j^{-1}\mathbf{u}_m, \mathbf{u}_n} = \delta_{\mathbf{u}_{m-j}, \mathbf{u}_n}$.

4.6.2 Fourier Transform on the Discrete Motion Group

The approximation of the matrix elements in Equation (4.45) are in fact exact expressions for the matrix representations of the IURs of the discrete motion group. Unfortunately, this set of matrix elements in Equation (4.45) is, however, incomplete. Therefore, the direct and inverse Fourier transform, defined in this manner, introduces an $\mathcal{O}(1/N_R)$ error

$$\mathcal{F}^{-1}(\mathcal{F}(f(A_i, \mathbf{r})) = f(A_i, \mathbf{r})(1 + \mathcal{O}(\frac{1}{N_R})).$$

This is because that summing through all possible segments is not the same as integration over all possible angles on the circle. Therefore we need additional continuous parameters to enumerate possible angles inside each segment on the circle, which in turn gives us the complete set of the matrix elements. Thus we modify the matrix elements as

$$U_{mn}(A_j, \mathbf{r}; p, \Phi) = e^{-ip\mathbf{u}_m^{\Phi} \cdot \mathbf{r}} \delta_{A_j^{-1}\mathbf{u}_m, \mathbf{u}_n}, \tag{4.46}$$

where $\mathbf{u}_m^{\Phi}$ is the vector to the angle $\Theta = \Phi + 2\pi k/N_R$ on the unit circle on the interval

$$F_k = [2\pi k/N_R, 2\pi(k+1)/N_R],$$

where $k = 0, ..., N_R - 1$ and Φ measures the angle on this segment. See Figure 4.1 for illustration of the vector $\mathbf{u}_m^\Phi$.

We now get an exact completeness relation

$$\sum_{m=0}^{N_R-1} \sum_{n=0}^{N_R-1} \int_0^\infty \int_0^{2\pi/N_R} \overline{U_{mn}(A_i, \mathbf{r}_1; p, \Phi)} U_{mn}(A_j, \mathbf{r}_2; p, \Phi)\, p\, dp\, d\Phi$$
$$= (2\pi)^2 \delta^2(\mathbf{r}_1 - \mathbf{r}_2) \delta_{A_i, A_j} \tag{4.47}$$

($d\Phi = d\Theta$), since the integration is now over the entire space of $\mathbf{p}$ values. One way to prove this is to use the integral representation of the δ-function

$$\frac{1}{(2\pi)^2} \int_{\mathbb{R}^2} e^{-i\mathbf{p}\cdot\mathbf{r}}\, d^2p = \delta^2(\mathbf{r}).$$

We write the orthogonality relation as

$$\sum_{i=0}^{N_R-1} \int_{\mathbb{R}^2} \overline{U_{mn}(A_i, \mathbf{r}; p, \Phi)} U_{m'n'}(A_i, \mathbf{r}; p', \Phi')\, d^2r$$
$$= (2\pi)^2 \frac{\delta^2(p - p')}{p} \delta_{m,m'} \delta_{n,n'} \delta(\Phi - \Phi'), \tag{4.48}$$

and the direct Fourier Transform as

$$\hat{f}_{mn}(p, \Phi) = \sum_{i=0}^{N_R-1} \int_{\mathbb{R}^2} f(A_i, \mathbf{r}) U_{mn}^{-1}(A_i, \mathbf{r}; p, \Phi)\, d^2r. \tag{4.49}$$

The rotation A_m, which transform the segment F_0 to F_m, may be used to find the vector $\mathbf{u}_m^\Phi$ from $\mathbf{u}_0^\Phi$, i.e. $\mathbf{u}_m^\Phi = A_m \mathbf{u}_0^\Phi$. Again, the parameter Φ denotes the position inside the segment F_0.

The inverse Fourier transform is defined as

$$\mathcal{F}^{-1}(\hat{f}) = \frac{1}{4\pi^2} \sum_{m=0}^{N_R-1} \sum_{n=0}^{N_R-1} \int_0^\infty \int_0^{2\pi/N_R} \hat{f}_{mn}(p, \Phi) U_{nm}(A_i, \mathbf{r}; p, \Phi)\, p\, dp\, d\Phi. \tag{4.50}$$

This result is in agreement with [18].

4.6.3 Convolution on the Discrete Motion Group

Convolution on the discrete motion group is defined as

$$F(\mathbf{r}, A_j) = \frac{1}{2\pi N_R} \sum_{i=0}^{N_R-1} \int_{\mathbb{R}^2} f_1(\mathbf{a}, A_i) f_2(A_i^{-1}(\mathbf{r} - \mathbf{a}), A_{j-i})\, d^2a \tag{4.51}$$

As with the normal Fourier transform, the Fourier transform on the discrete motion group also transform convolution of functions into a product, in this case a product of Fourier matrices for each p and Φ

$$\hat{F}^{\Phi}_{mn}(p) = \frac{A}{2\pi N_R} \sum_{k=0}^{N_R-1} (\hat{f}_2)^{\Phi}_{mk}(p)(\hat{f}_1)^{\Phi}_{kn}(p) \tag{4.52}$$

Where A is the area of a compact region of $\mathbb{R} \ni \mathbf{r}$ where the FFT is applied. The support of the function must be inside A, and the function is considered periodic outside of this area. The reason that the factor A appears in Equation (4.52) is because the discrete Fourier transform is an approximation to the continuous one using

$$r_1 \to \frac{L}{N_r} i; \;\; p_1 \to \frac{2\pi}{L} i$$

(the same way goes for the 2nd component). L is here the length of the compact region in one of the direction x, y. Even though L cancels out of the equation if the direct and inverse Fourier transform is applied, it arises in the convolution defined in Equation (4.51).

4.6.4 SE(2) Convolution Computed Efficiently Using the Discrete-Motion-Group Fourier Transform

By using the Fourier transform on the discrete motion group we can compute the convolution integral in (4.51) efficiently. The finite rotation group has N_R elements, and N_r is the number of samples in the $\mathbb{R}^2$ region. It can then be shown that convolution of a function $f(\mathbf{r}, A_i)$ sampled at $N = N_R \cdot N_r$ may be performed in $\mathcal{O}(N \log N_r) + \mathcal{O}(N N_R)$ operations instead of $\mathcal{O}(N_g^2)$ computation which the direct integration in Equation (4.51) requires.

Because of the structure of the matrix elements in Equation (4.46) we may apply fast Fourier methods which reduce the amount of computations. Without the exploiting of the FFT the amount of computations using the Fourier transform method is $\mathcal{O}(N^2/N_R)$ which is still faster than the direct integration.

To estimate the amount of computations required to perform the direct and inverse Fourier transforms of $f(g)$, we assume that the p values are on a finite interval and is sampled at N_p points, and the Φ values is sampled at N_Φ points. The total number of harmonics is assumed to be $N_p N_\Phi N_R^2 = N = N_R N_r$.

Now we consider the direct Fourier transform in Equation (4.49). Each term i (i.e. A_i is fixed) gives one nonzero term in each row and column of the Fourier matrix $f^{\Phi}_{mn}(p)$ since only one element in each column and row of $U^{-1}_{mn}(g; p, \Phi)$ is nonzero. We may compute the standard FFT of $f(\mathbf{r}; A_i)$ for each fixed rotation i, this can be computed in $\mathcal{O}(N_r \log(N_r))$ operations. The FFT, however, are computed on a Cartesian square grid of $\mathbf{p}$ values. Thus, we interpolate the Fourier elements from the Cartesian grid to Fourier elements computed on a polar grid. The angular part of $\mathbf{p}$ determines the indices m, Φ, and the radial part p is determined by the length of $\mathbf{p}$. The last index n is determined uniquely for each given A_i. The Cartesian-to-polar interpolation may be performed in $\mathcal{O}(N_r\epsilon(N_r))$. So in $\mathcal{O}(N_R N_r \log(N_r))$ computations the whole Fourier matrix may be calculated.

As with the forward Fourier transform, only one element from each row and column is used in the computation of the inverse Fourier transform for each rotation element A_i. First, we do inverse interpolation from polar to Cartesian coordinates. This is done in $\mathcal{O}(N_r\epsilon(N_r))$ computations. Then, for each of the N_r nonzero matrix elements of U the inverse Fourier integration is performed in $\mathcal{O}(N_r \log(N_r))$ computations using the FFT. Therefore, we reproduce the function in $\mathcal{O}(N_R N_r \log(N_r))$ operations for all A_i.

In $\mathcal{O}(N_R^3)$ computations we calculate the matrix product directly of $\hat{f}^{\Phi}_{mn}(p)$ for each value p and Φ. Since convolution is a matrix product of Fourier matrices, it may be performed in $\mathcal{O}(N_R^3 N_p N_\Phi) = \mathcal{O}(N_R N)$ operations.

Thus, the total number of operation for the convolution of functions on the discrete motion group is $\mathcal{O}(N \log N_R) + \mathcal{O}(N N_R) + \mathcal{O}(N\epsilon(N_r))$ by using the Fourier method on the discrete motion group in the way defined above and the usual FFT. We have not assumed any special matrix multiplication technique.

Without the help of the FFT it is possible to show that the convolution may be performed in $\mathcal{O}(N^2/N_R)$ using the Fourier transform. This is still faster than the direct integration.

Chapter 5

Generalization of Phase Correlation to the Motion Group

In the field of image processing, phase correlation is a method used to perform image registration. Since it is a frequency-domain method, phase correlation is a fast method [19, 20]. Here we are going to present the algorithm for a simple translation case, and then use the theory from the previous chapters to generalize the method to the Euclidean motion group. As far as the author know, this has not been done earlier.

5.1 The Phase Correlation Method

Cross correlation for two functions f_1 and f_2 is defined as

$$(f_1 \star f_2)(\mathbf{x}) = \int_{-\infty}^{\infty} f_1^*(\mathbf{y}) f_2(\mathbf{x} + \mathbf{y})\, d\mathbf{y}, \tag{5.1}$$

and analogues to the convolution theorem it has Fourier properties

$$\mathcal{F}((f_1 \star f_2)) = \mathcal{F}(f_1)^* \mathcal{F}(f_2), \tag{5.2}$$

where $f_1^*, \mathcal{F}(f_1)^*$ denotes the complex-conjugated of $f_1, \mathcal{F}(f_1)$.

A problem with cross-correlation between two functions f_1 and f_2 in image registrations is that it always gives a maximum where the image has a region with maximum intensity value(a white region). Therefore, normalized cross-correlation was introduced , which is cross-correlation normalized at every step. The problem with this method is high complexity, and since it is normalized at every step the advantage of exploiting fast Fourier transforms is minimal. For this reason fast algorithms is not possible to achieve.

Phase correlation is cross-correlation scaled in the frequency domain. Given two images f_1 and f_2, take the 2D Fourier transform of each image, $F_1 = \mathcal{F}(f_1)$ and $F_2 = \mathcal{F}(f_2)$. Then, phase correlation is defined as [20]

$$R = \frac{F_1(\xi, \eta) F_2^*(\xi, \eta)}{|F_1(\xi, \eta) F_2^*(\xi, \eta)|} \tag{5.3}$$

By taking the inverse Fourier transform of Equation (5.3) we receive a normalized cross-correlation of f_1 and f_2

$$r = \mathcal{F}^{-1}(R) \tag{5.4}$$

5.2 Generalization to the Euclidean Motion Group

The general formula for cross-correlation on the Euclidean motion group is

$$(f_1 \star f_2)(g) = \sum_{h \in G} f_1^*(h) f_2(hg) \tag{5.5}$$

Analogous to convolution on groups we have a similar Fourier property for cross-correlation

Theorem 5.1. *The Fourier transform of the cross-correlation of two functions on a non-commutative group G is the matrix product of the Fourier transform matrices*

$$\mathcal{F}((f_1 \star f_2)(g))(p) = \hat{f}_2(p) f_1^\dagger(p)$$

where the order of the products matters.

Proof. By definition we have

$$\mathcal{F}((f_1 \star f_2)(g))(p) = \sum_{g \in G} \left(\sum_{h \in G} f_1^*(h) f_2\left(hg\right) \right) U\left(g^{-1}, p\right).$$

Setting $k = hg$ and substituting $g = h^{-1}k$, the expression becomes

$$\sum_{k \in G} \sum_{h \in G} f_1^*(h) f_2(k) U\left(k^{-1}h, p\right).$$

The homomorphism property of U and the commutative nature of the scalar-matrix multiplication and summation, and the fact that U is a unitary irreducible representations lets us split this into

$$\left(\sum_{k \in G} f_2(k) U\left(k^{-1}, p\right) \right) \left(\sum_{h \in G} f_1^*(h) U^\dagger\left(h^{-1}, p\right) \right) = \hat{f}_2(p) \hat{f}_1^\dagger(p).$$

□

By using Theorem 5.1 phase correlation of two functions on G, which in this case is the Euclidean motion group, may then be defined as

$$R(p) = \frac{F_2(p) F_1^\dagger(p)}{\|F_2(p) F_1^\dagger(p)\|}, \tag{5.6}$$

where $F_1(p), F_2(p)$ are the motion group Fourier transform for the functions $f_{1,2}$, and the norm in the denominator may be chosen to be the usual Frobenious norm for matrices. Again, the order of the products matters.

If the inverse motion group Fourier transform is taken of R we receive a normalized cross-correlation which now also includes rotation in addition to translation. The maximum is located at where the functions are translated and rotated accordingly to each other.

Since functions $f_{1,2}(\mathbf{x}, A_i)$ is not depending on the orientations A_i [2], the matrix elements in the same column are identical, i.e.,

$$\left(\hat{f}_{1,2}\right)_{mn} = \left(\hat{f}_{1,2}\right)_{qn}$$

for any $m, q \in [0, N_R - 1]$. The reason for this may be observed from the expression of the unitary irreducible representations

$$U_{mn}\left(g^{-1}; p, \phi\right) = e^{-ip\mathbf{u}_n^{\phi}\cdot\mathbf{a}}\delta_{A_i^{-1}\mathbf{u}_n,\mathbf{u}_m} \tag{5.7}$$

where $g = (\mathbf{a}, A_i) \in G_{N_R}$, the definition of the forward discrete motion group transform, and the property that the functions do not depend on the orientation. Therefore it is only necessary to compute the Fourier matrix for one particular orientation

$$\left(\hat{f}_{1,2}\right)_{n} \triangleq \left(\hat{f}_{1,2}\right)_{nn}.$$

We also observe that the inverse Fourier transform is $\mathcal{O}(N_R)$ times more time-consuming then the forward transform. This is because we reproduce a function on the discrete motion group and not just on $\mathbb{R}^2$.

The total number of computations required for this method is $\mathcal{O}(N_R N_r \log(N_r))$ and this is for the most part the calculations of the inverse Fourier transform.

Chapter 6

Numerical Experiments

In this section some numerical experiments are performed. First the ordinary phase correlation method is tested, then the new proposed generalization of phase correlation to the discrete motion group is tested. The image used is one of the many Waldo-images (Figure 6.2), which can be found in children's books. The section of the image where Waldo is located is taken as the template image, see Figure 6.1. Afterwards we add some noise to the image and see how the proposed algorithm behaves compared to the ordinary phase correlation. All the algorithms are coded in MATLAB, therefore the performance of the algorithms would most likely be increased in a low level programming language like C/C++, Fortran etc. Parallel computing would also increase the performance drastically, so by exploiting the GPU with e.g CUDA (an acronym for Compute Unified Device Architecture) could be an efficiently way to increase the performance. The computer used to run this algorithm is a standard PC (Intel Core Duo Processor 2 GHz, 4 GB memory).

Figure 6.1: Template image of Waldo.

6.1 Phase Correlation Method, Including Translations

We compute the phase correlation function, Equation (5.3), and test how much Gaussian noise we may add before it gives a wrong location of Waldo.

We consider the image and template image depicted in Figure 6.2 and 6.1. The images are colour images, but only one of the channels are used in the phase correlation functions. The result is shown in Figure 6.3 where a frame indicates the location where Waldo is found. The noisy images are of size 200×200.

Now we test how much Gaussian noise we may add to the reference image before phase correlation gives a wrong maximum. The noise is added using MATLAB's inbuilt function

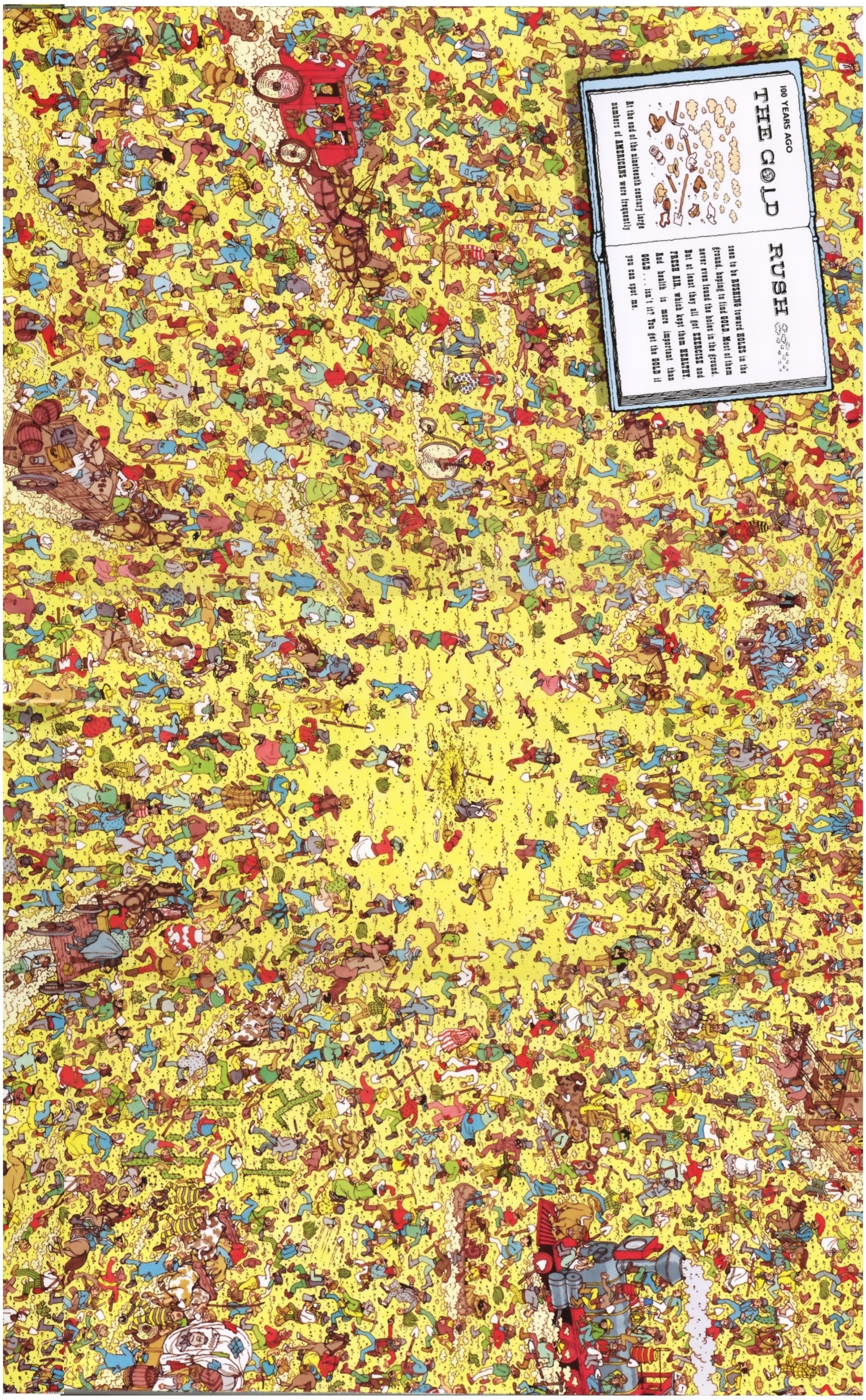


Figure 6.2: Waldo-image.

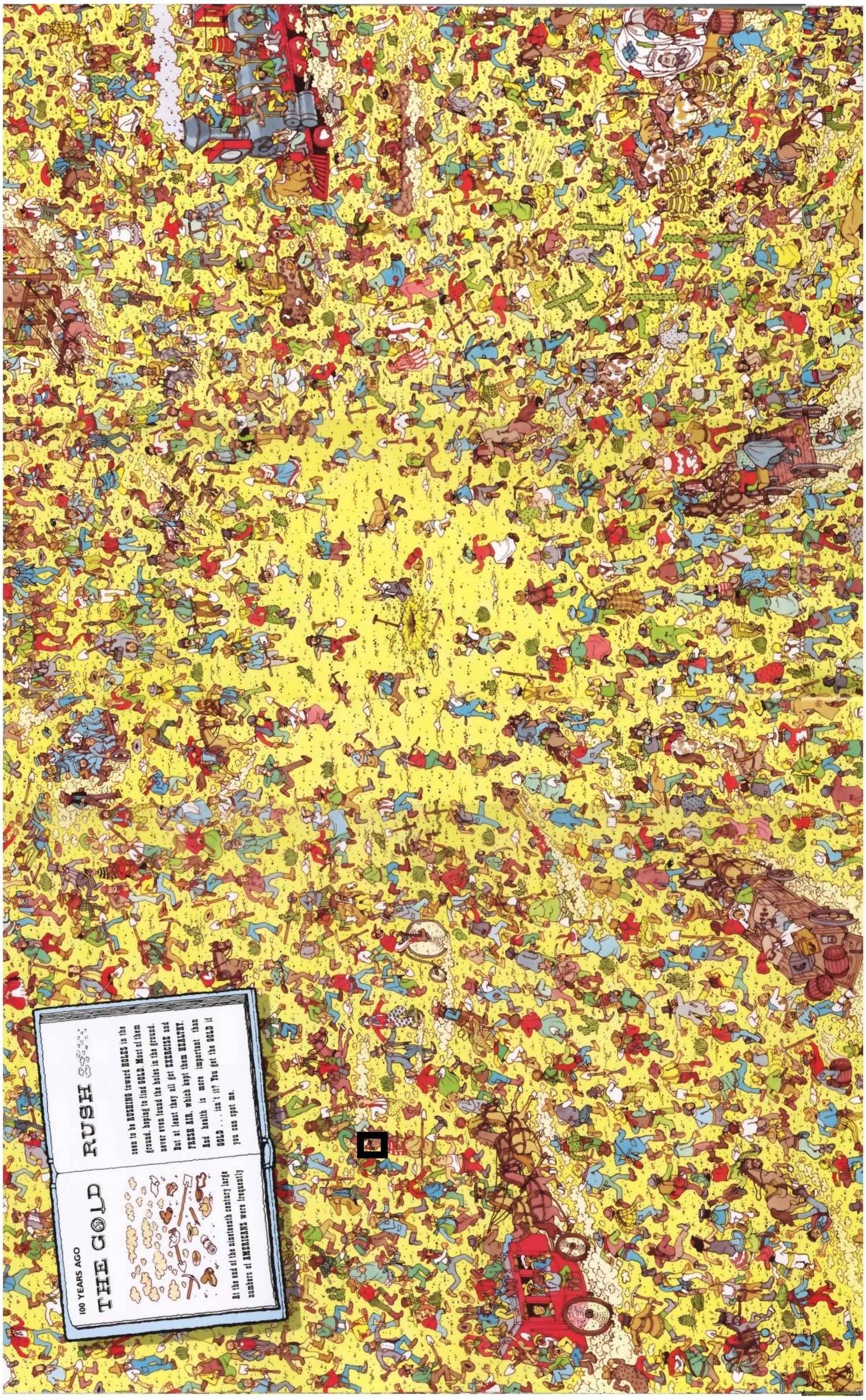
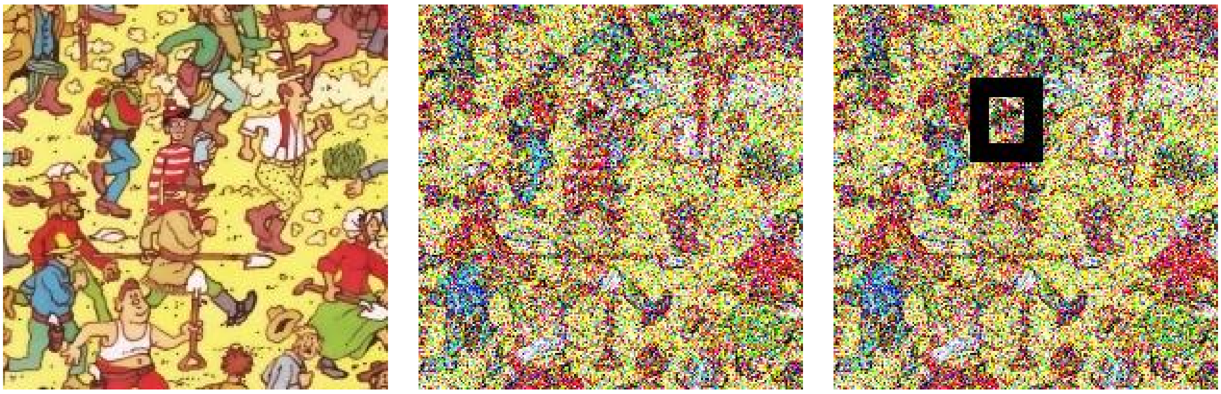


Figure 6.3: Waldo image. The frame shows the location of Waldo

`imnoise()`. Simple testing indicates that phase correlation may handle noise with mean $\mu = 0$ and standard deviation up to $\sigma = 0.19$, see Figure 6.4.



(a) (b) (c)

Figure 6.4: (a) Reference Waldo image. (b) Reference Waldo image with added Gaussian noise, $\mu = 0$ and $\sigma = 0.19$. (c) Image where Waldo is located.

The reason for using smaller images in the last case is for better comparison with the testing of the proposed algorithms in the next section, since memory then becomes an issue.

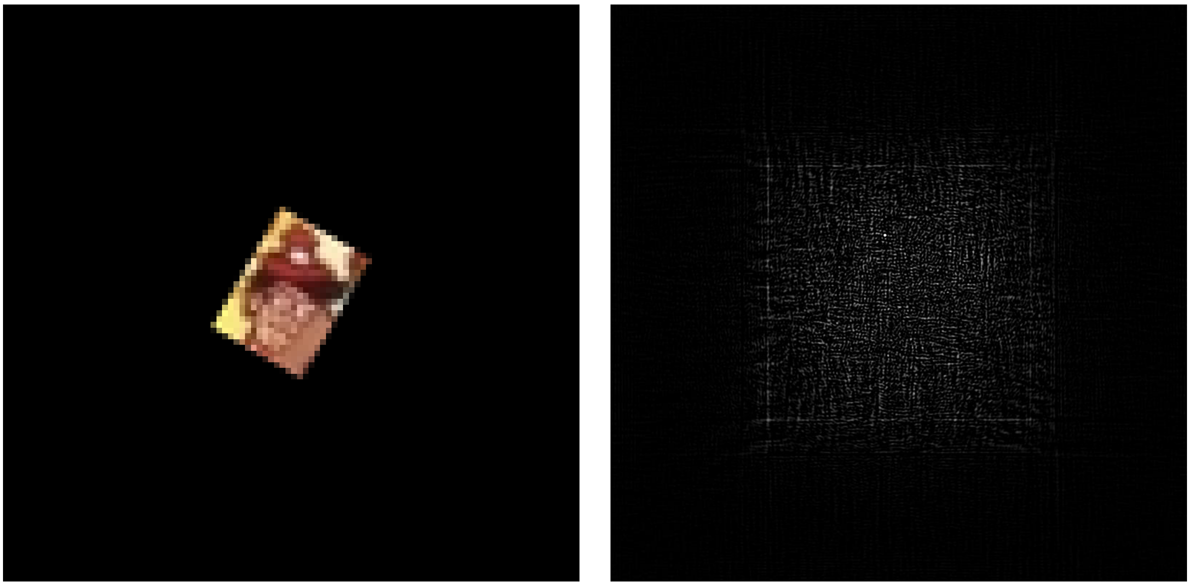
6.2 Phase Correlation Method, Including Rotations and Translations

In this section we compute the proposed generalization of the phase correlation function, Equation (5.6). All the examples are computed for images of size $N_r = 200 \times 200$ and for $N_R = 10, 12, 36, 60, 360$ (C_{N_R} groups). The result are tested for all rotations in each C_{N_R} subgroup of $SO(2)$ and for some rotations which are not in C_{N_R}. The reason for choosing smaller images is the limit of memory available. An array of for example $2000 \times 1400 \times 360$ corresponds to almost 8 GB of memory when double precision is used in MATLAB. To test the method we rotate the template image (by angle $\theta = -\pi/6$), see example in Figure 6.5, and compute the phase correlation function.

The testing of the method shows that if the template image is rotated with $\theta \in C_{N_R}$, then the rotation and translation is found correctly for all the discrete motion groups considered in this thesis (i.e., for $\mathbb{R}^2 \rtimes_\varphi C_{10}, C_{12}, C_{36}, C_{60}, C_{360}$).

If the rotation is not in C_{N_R}, the rotation found by the method is the closest corresponding rotation in C_{N_R}. For a template image rotated by an angle $\theta = -8\pi/45 \notin C_{60}$, depicted in Figure 6.6(a), the method gives a maximum at the orientation $\theta = \pi/6$ and at the correct translation.

The amount of noise which may be added before this method gives a wrong maximum is gaussian noise with $\mu = 0$ and $\sigma = 0.5$, depicted in Figure 6.6(b) which is considerable



(a) (b)

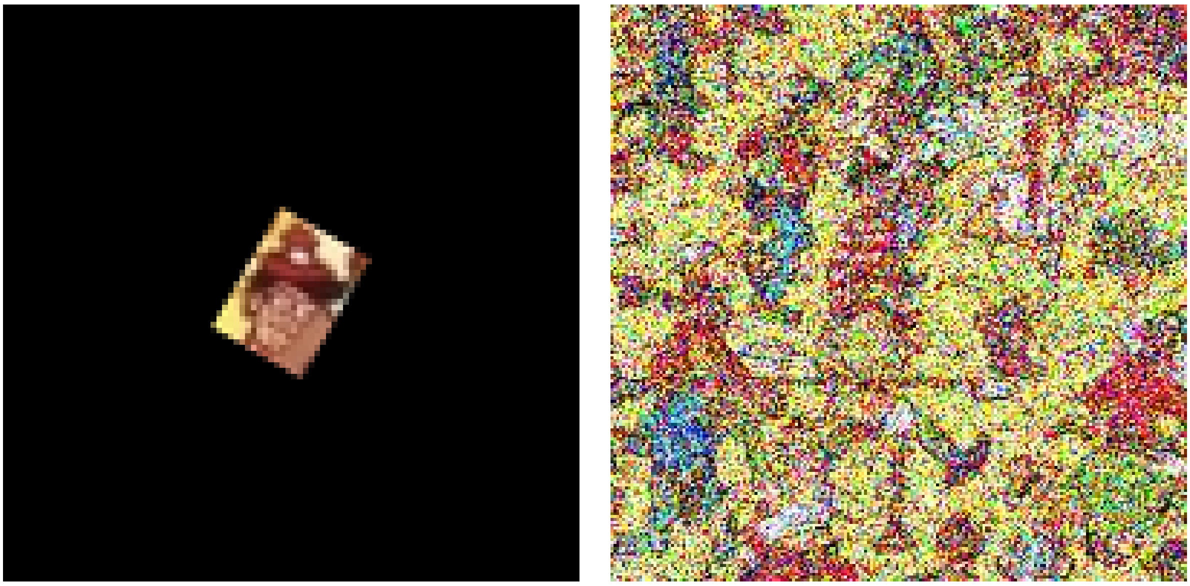
Figure 6.5: (a) Rotated template image by angle $\theta = -\pi/6$. (b) The phase correlation for the $\theta = \pi/6$ orientation angle. Notice the clear white dot, that is where the maximum is.

lower than in the ordinary phase correlation case. Still, the method shows good resilience against noise. It is worth mentioning that more zero padding would increase the robustness against noise, but then again, memory becomes an issue.

6.3 Discussion

In this implementation of the generalized phase correlation method, we have to be very careful handling the data, otherwise the method would give completely false results. If the template image is not completely symmetric around the origin the method will give the wrong translation and in the worst case also wrong rotation. We also have to zeropad to double size in the x, y direction in the spatial domain, and zeropad to double size in the r direction in the frequency domain, where r is the radii in polar coordinates, to be certain that the method gives the correct maximum.

If all the pitfalls are avoided and the implementation is done as described above, the method gives correct translation and rotation for every scenario tested in this thesis. One may argue that there exist faster and less memory intensive methods for image registration, but if a normalized cross-correlation which also includes rotation is needed, then this generalization of Phase correlation to the Euclidean motion group provides a very fast way for doing it.



(a) (b)

Figure 6.6: (a) Rotated template image by angle $\theta = -8\pi/45 \notin C_{60}$. (b) Reference Waldo image with added Gaussian noise, $\mu = 0$ and $\sigma = 0.05$.

Chapter 7

Conclusion and Further Work

In this thesis we have touched upon some beautiful pure mathematics, from group theory to representation theory and noncommutative harmonic analysis, and more well known applied theories in image science. We have used this theory to generalize two methods in image processing to the Euclidean motion group, namely cross-correlation and phase correlation. The Euclidean motion group has up until recently not been extensively used in image processing, but the amount of authors using it is increasing.

The generalization of the phase correlation method has very high complexity due to the amount of zero padding necessary for an accurate result. Because of the structure of the cross-correlation and the zero padding needed it is also very memory intensive. This could be improved by using a better and more accurate polar Fourier transform, or a better polar interpolation in the Fourier domain. Park and Chirikjian proposed a new algorithm for lossless conversion between Cartesian and polar coordinates [21] which should be implemented and tested with our method to improve the complexity and accuracy.

Furthermore, the new phase correlation method should be tested with “real“ data, e.g. medical imaging data, to see how well it behaves there. Despite its high complexity and memory usage, this method worked almost perfectly for our numerical experiments. The numerical testing indicates that if a big enough discrete motion group of $SE(2)$ is chosen, the method would give correct (within an ϵ for our needs) rotation and translation for every transformation of the template image in $SE(2)$. The method is also ”embarrassingly parallelizable”, and if implemented in a low level programming language and on a GPU, it should prove to be a very fast method for image registration.

Appendix A

Some Definitions Needed

Definition A.1. An **Equivalence relation** $\mathcal{R}$ on a set S is one that satifsfies these three properties for all $x, y, z \in S$

1. (Reflexive) $x\mathcal{R}x$.
2. (Symmetric) If $x\mathcal{R}y$ then $y\mathcal{R}x$.
3. (Transitive) If $x\mathcal{R}y$ and $y\mathcal{R}z$ then $x\mathcal{R}z$.

Definition A.2. A **ring** $\langle R, +, \cdot \rangle$ is a set R together with two binary operations $+$ and $\cdot$, which we call *addition* and *multiplication*, defined on R such that the following axioms are satisfied

1. $\langle R, + \rangle$ is an abelian group.
2. Multiplication is associative.
3. For all $a, b, c \in R$ the **left distributive law**, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and the **right distributive law** $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ hold.

Definition A.3. Let R be a ring with unity $1 \neq 0$. An element u in R is a **unit** of R if it has a multiplicative inverse in R. If Every nonzero element of R is a unit, then R is a **division ring** or **skew field**. A **field** is a commutative division ring. A noncommutative division ring is called a "**strictly skew field.**"

Definition A.4. If R is a ring, then an **R-module** M is an abelian group with an action of R, that is, a map $R \times M \to M$, written $(r, m) \to rm$, satisfying for all $r, s \in R$ and $m, n \in M$

1. $r(sm) = (rs)m$ (associativity)
2. $r(m + n) = rm + rn$
3. $(r + s)m = rm + sm$ (distributivity, or bilinearity)
4. $1m = m$ (identity)

Bibliography

[1] J.B. Fraleigh. *A First Course in Abstract Algebra*. Addison-Wesley publishing Company, Reading, 2003.

[2] G.S. Chirikjian and A.B. Kyatkin. *Engineering applications of noncommutative harmonic analysis: with emphasis on rotation and motion groups*. CRC, 2000.

[3] N.J. Vilenkin and AU Klimyk. Representation of Lie groups and special functions, Vols. 1, 2, 3. *Kluwer Academic*, 1993:1992, 1991.

[4] J.P. Serre. *Linear representations of finite groups*. Springer Verlag, New York, 1977.

[5] Y. Kosmann-Schwarzbach. *Groups and Symmetries: From Finite Groups to Lie Groups*. Springer Verlag, 2009.

[6] P. Diaconis and D. Rockmore. Efficient computation of the Fourier transform on finite groups. *Journal of the American Mathematical Society*, 3(2):297–332, 1990.

[7] D.N. Rockmore. Efficient computation of Fourier inversion for finite groups. *Journal of the ACM (JACM)*, 41(1):31–66, 1994.

[8] D.K. Maslen. *Fast transforms and sampling for compact groups*. Harvard University Cambridge, MA, USA, 1993.

[9] D.K. Maslen and D.N. Rockmore. Generalized FFTs-a survey of some recent results. Amer Mathematical Society, 1997.

[10] A. Orihara. Bessel functions and the Euclidean motion group. *Tohoku Math. J*, 13(1):66–74, 1961.

[11] J.D. Talman. *Special functions*. WA Benjamin, Inc., Amsterdam, 1968.

[12] N.Y. Vilenkin. Bessel functions and representations of the group of Euclidean motions. *Uspekhi Matematicheskikh Nauk*, 11(3):69–112, 1956.

[13] M. Sugiura. *Unitary representations and harmonic analysis: an introduction*. Elsevier Science, 1990.

[14] Alexander B. Kyatkin and Gregory S. Chirikjian. Algorithms for fast convolutions on motion groups. *Applied and Computational Harmonic Analysis*, 9(2):220 – 241, 2000.

[15] W. Miller. *Lie theory and special functions.* Academic Press Inc, 1968.

[16] M.N. Jones. *Spherical harmonics and tensors for classical field theory.* Research Studies Press Ltd, 1985.

[17] A.B. Kyatkin and G.S. Chirikjian. Pattern Matching as a Correlation on the Discrete Motion Group. *Computer vision and image understanding*, 74(1):22–35, 1999.

[18] J.-P. Gauthier, G. Bornard, and M. Silbermann. Motions and pattern analysis: harmonic analysis on motion groups and their homogeneous spaces. *Systems, Man and Cybernetics, IEEE Transactions on*, 21(1):159 –172, jan/feb 1991.

[19] E. De Castro and C. Morandi. Registration of translated and rotated images using finite Fourier transforms. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 9(5):700–703, 1987.

[20] BS Reddy and BN Chatterji. An FFT-based technique for translation, rotation, and scale-invariant image registration. *IEEE transactions on image processing*, 5(8):1266–1271, 1996.

[21] W. Park and GS Chirikjian. Interconversion between truncated cartesian and polar expansions of images. *IEEE Transactions on Image Processing*, 16(8):1946–1955, 2007.