Chapter 2

Basic Concepts of Group and Representation Theory

2.1 Introduction

From a mathematician’s view, a group is an object with a very precise meaning. It is a set of elements that must obey four group axioms. On these is based a very elaborate and fascinating theory, the Group theory. For signal processing researchers, group theory (Dresselhaus, 2008; Conway et. al., 1985; Chirikjian, G. S., and A. B. Kyatkin, 2001a; Chirikjian, G. S., and A. B. Kyatkin, 2001b; Duzhin, S. V., and B. D. Chebotarevsky, 2004; Eberly, D., and D. Wenzel, 1991; Fassler, A., and E. Stiefel, 1992; Hamermesh, 1970; Holmes, 1990; Scott, 1964) provides the mathematical foundation for studying any type of signal transformations. The theory allows for the study of a set of linear transformations, their relationships, and perspectives available (of the signal features) encapsulated in a group structure. It also allows for mapping the geometric structure of the group into a convenient algebraic structure where operations may be performed using well-established algebraic tools to extract signal features in the form of its structural symmetries. Linear algebra is used to build this bridge with the help of representation theory. When a group is defined as an abstract geometric structure, its representations form the foundation for an algebraic structure. A signal may be chosen as a function of vectors in a
vector space $V$. Then, group and representation theory show by linear algebra, how to obtain a group theoretical and data independent basis for the signal in the vector space $V$.

A review of group theory, its representations and examples of groups of transformations are presented in this chapter. For more details, the reader is referred to Dresselhaus (2008), Hamermesh (1970), Fassler (1992), Duzhin (2004), Serre (1997) and Kowalski (2011). Only a general description of group theoretical concepts is presented here. Chapter 3 presents a new framework for signal processing applying these concepts to build a new framework for signal processing and also shows how to derive a new signal processing algorithm from the framework. This is presented in the perspective of a signal processing researcher. Chapter 3 also summarizes how the characteristics of group theory have been utilized in the literature by various signal processing techniques, and currently what new opportunities exist to perform signal processing using group theory. For a reader familiar with basic group theoretical concepts, this chapter may be omitted without any loss of information.

2.2 Structure of Groups

The development of group theory does not depend on the nature of the group elements themselves, but in most physical applications these elements are transformations of one kind or another, which is why $T$ will be used to denote a typical group member.

Definition of a Group $G$:
A set $G$ of elements is called a “group” if the following four “group axioms” are satisfied:

- There exists an operation which associates with every pair of elements $T_1$ and $T_2$ of $G$ another element $T_3$ of $G$. This operation may be denoted as $\circ$ and is written as $T_3 = T_1 \circ T_2$, $T_3$ being described as the “operation of $T_1$ with $T_2$”. The operation may be chosen relevant to a particular type of group elements such that the following axioms are true.

- For any three elements $T_1, T_2$ and $T_3$ of $G$, $(T_1 \circ T_2)T_3 = T_1(T_2 \circ T_3)$. This is known as the “associative law” for group operation.

- There exists an identity element $T_e$ which is contained in $G$ such that $T^*E = E^*T = T$ for every element $T$ of $G$.
• For each element $T$ of $G$ there exists an inverse element $T^{-1}$ which is also contained in $G$ such that $T \circ T^{-1} = T^{-1} \circ T = T_e$

A group is called commutative or abelian if the binary operation is commutative, and is called non-abelian if the operation is non-commutative (Dresselhaus, 2008). An arbitrary collection of objects is not a useful entity when compared to any group which has structure and hence an identity. Some examples of groups and how each of the axioms are satisfied by the groups are given below.

### 2.2.1 Examples of Finite Groups

**Abelian (or Commutative) Groups:**

• **Group of real numbers by multiplication:** The simplest example, from which the concept of a group was generalized, is the set of all real numbers (excluding zero) that form a group. The group operation is ordinary multiplication of two numbers. The identity element is the number 1. Any number multiplied by 1 gives the same number. Each real number $t \neq 0$ has its reciprocal $1/t$ as its inverse, such that $T \circ T^{-1} = 1$. Also $T_1 \circ (T_2 \circ T_3) = (T_1 \circ T_2) \circ T_3$ for any three real numbers.

• **Group of real numbers by addition:** The set of all real numbers with ordinary addition as the group operation forms a group. The first, second and third axioms of a group are obviously satisfied. In this case, the identity is 0 since $(a + 0 = 0 + a = a)$, where $a$ and $b$ are two elements of the group. The inverse of a element $a$ is its negative $-a$ since $(a + (-a) = (-a) + a = 0)$.

• **Group of Rotations by composition:** The group of rotations of the plane around the origin through angles $2\pi k/n$, $0 \leq k \leq n - 1$, under composition.

• **Group of Complex Numbers:** The group of complex numbers $e^{2\pi ik/n}$, $0 \leq k \leq n - 1$ under multiplication.

For each of the above groups, with any two elements $a, b \in G$ and a group operation $\circ$, it is also true that $a \circ b = b \circ a$, called the ‘commutative property’. Such groups are called commutative groups. Groups where the commutative property does not hold true, are called
non-commutative groups. They may be understood better after learning about ‘action’ of a group.

For each of the above groups, with any two elements \(a, b \in G\) and a group operation \(\circ\), it is also true that \(a \circ b = b \circ a\), called the ‘commutative property’. Such groups are called commutative groups. Groups where the commutative property does not hold true, are called non-commutative groups. They may be understood better after learning about ‘action’ of a group.

### 2.2.2 Group Action

The ‘action’ of a group is performed by each member of the group on a set \(S\) of some elements. The action may be defined as:

**Definition 2.2.1.** Let \(G\) be a group and \(SS\) a nonempty set. Then \(G\) is said to act on \(SS\) if there is a function from \(G \times SS\) to \(SS\), usually denoted as \((g, s) \rightarrow gs\) for \(g \in G, s \in SS\), such that \(es = s\). Also for all \(g, h \in G\) and \(s \in SS\), the associative axiom \((gh)s = g(hs)\) holds true.

Consider an example. Let \(G\) be the group of nonzero real numbers under multiplication, and let \(S\) be the set of all vectors in \(R^3\) space. Thus \(S = f(a, b, c)|a, b, c \in R\). Then \(G\) acts on \(S\) via scalar multiplication. The group action is said to be scalar multiplication of vectors in the set \(S\), and the scalars are taken from the group of real numbers. That is, \(g(a, b, c) = (ga, gb, gc)\) if \(g\) is a nonzero real number. Then for any vector \(v\), we have \(1v = v\), the identity axiom. The associative axiom of the group also holds true, where \(g, h \in G\) and \((gh)v = g(hv)\), because, for \(v = (a, b, c)\), \((gh)v = (gha, ghb, ghc) = g(ha, hb, hc) = g(hv)\).

A ‘group action’ is different from a ‘group operation’. The axioms of a group structure are based on the ‘group operation’. Whereas the a ‘group action’ is defined as the change caused by elements of a group \(G\) on the members of a set \(SS\). A group \(G\) may also ‘act’ on another group \(G'\). Then the group action behaves as the mapping from group \(G\) to \(G'\). Once a group is defined, it is found that the group action is useful in exploring symmetries of a physical system. What kind of symmetries are explored depends on the choice of the group. It is intuitive that the nature of the group elements determines the group action and hence the study of the physical
system. With a signal chosen as the physical system, what happens with different groups and corresponding group actions on the signal, is elaborated in Chapter 3.

The above example is a case of commutative group action. Even for non-commutative groups, group actions are defined. Some examples of non-commutative groups are given below:

Non-Abelian (or Non-commutative) Groups:

- Symmetric group $S_n$: It is a group of permutations with the group operation as ‘composition’. The elements of the group satisfy the axioms of a group by ‘composition’. The group action for this group is permutations on a set $S$. A specific application of the symmetric group is its action on a set $S$ of size ‘$n$’. It is called the Galois group of a general polynomial of degree ‘$n$’ and plays an important role in Galois theory.

- Rotations: The 3D rotation group is the group of all rotations about the origin of three-dimensional Euclidean space $\mathbb{R}^3$ under the operation of composition. Composing two rotations results in another rotation. Every rotation has a unique inverse rotation, and there also an identity rotation. The group action is a rotation, may be on a set of vectors in the space $\mathbb{R}^3$. Symmetries of the set of vectors may be explored using this group.

- Dihedral group $D_n$: It is a group of rotations and reflection. This group contains ‘$n$’ rotations and ‘$n$’ reflections in the lines passing through the same centre, such that the angle between any two neighboring lines is $180^\circ/n$. This group is used to explore the symmetries of the plane preserving a regular $n$-sided polygon ($n \geq 3$).

- Linear transformation groups $GL(n)$: Some examples are cyclic, symmetric and octahedral transformation groups. The group that consists of rotations around a common centre through multiples of $360^\circ/n$, is called the cyclic group of order ‘$n$’. A symmetric group is a finite group $S(m)$ of all permutations on ‘$m$’ elements. The group $S(m)$ is abelian if and only if $m \leq 2$. The octahedral group is one of the finite subgroups of the rotation group in 3-D Euclidean space and a symmetry group of the cubic grid.

- Finite matrix groups: Many of the groups appearing in physical problems consist of matrices with matrix multiplication as the group operation. As an example of such a group let $Q$ be the set of eight matrices that form a group by matrix multiplication:
\[
M_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},
M_2 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},
M_3 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix},
M_4 = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix},
M_5 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},
M_6 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},
M_7 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},
M_8 = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix},
\]

(2.2.1)

To proceed beyond an intuitive picture of the effect of symmetry operations or group actions, it is necessary to specify the actions in a precise algebraic form so that the results of successive operations can be easily deduced. This is what it means to map a geometric structure (i.e., group elements) to an algebraic structure (i.e., of group actions). The geometric structure of a group may be studied in different ways. It may be done using subgroups, cosets or conjugacy classes as described below.

2.2.3 Subgroups

A definition of a subgroup of a group G is given as:

**Definition 2.2.2.** If H is a subset of a group G (i.e. a subset of the set of elements of G) then it is called a ‘subgroup’, if it is also a group under the operation of G.

The subgroup H of group G is closed under products and inverses. Whenever a and b are in H, then ab and a\(^{-1}\) are also in H. These two conditions can be combined into one equivalent condition: whenever a and b are in H, then ab\(^{-1}\) is also in H. The number of elements in a group is called the order of the group.

**Theorem 2.2.1** (Lagrange’s theorem). The order of a subgroup of a finite group is a divisor of the order of the group.

This theorem can be used for finding the possible structures of groups of a given order. For example, consider a group of order 6. Then the order of each of its elements is 1, 2, 3, and 6, since they have to be factors of 6. The subgroup of orders 1, 2, and 3 are called ‘factor groups’. If one of the elements is of order 6, then the group is a cyclic group.
The identity $e$ must be a member of every subgroup of $G$. Indeed one subgroup of $G$ is the set $E$ consisting only of $E$. For every group $G$, the group as a whole is also called a subgroup and any other subgroup of $G$ is called a proper subgroup. A subset $S$ of a group $G$ may also fail to be a subgroup. For example, if $S$ does not contain the identity element, it violates one of the axioms of a group. If $S$ contains an element but not that element’s inverse, it would violate the inverse axiom. If $S$ contains two elements but not their product, then the group operation of $G$ cannot be said to be a group operation on $S$, because it maps some pairs from $S$ outside of $S$.

### 2.2.4 Cosets

Cosets of a group are found in relationship to a subset of the group $H$ which is also a subgroup. For any subgroup $H$ of a group $G$, left cosets are the sets $gH$ where $g$ is an element $\in G$. Similarly, the right cosets of $H$ are given by the sets $Hg$. Cosets (Hamermesh, 1970) of either type partition the elements of the group, and the union of left cosets of $H$ (or right cosets) make the group $G$. A subgroup is called a ‘normal’ subgroup when any of the following equivalent criteria are met.

1. A normal subgroup is one whose collection of left cosets is the same as its collection of right cosets, i.e., they are equal.

2. A normal subgroup is one which is self-conjugate, that is if $N$ is the subgroup, then for any element $g \in G$, the set $gNg^{-1} = N$. Here $gNg^{-1} = gng^{-1}$ where $n \in N$.

3. A normal subgroup $H$ in a group $G$ is one for which the quotient $G/H$ is defined.

The left cosets (or right cosets) themselves form a group by the group operation of $G$. Let $N$ be a normal subgroup of a group $G$. Then the set $G/N$ is defined to be the set of all left cosets of $N$ in $G$, i.e., $G/N = aN : a \in G$. The group operation on $G/N$ is the product of subsets defined above. In other words, for each $aN$ and $bN$ in $G/N$, the product of $aN$ and $bN$ is $(aN)(bN)$. This operation is closed, because $(aN)(bN)$ really is a left coset:

$$ (aN)(bN) = a(Nb)N = a(bN)N = (ab)NN = (ab)N. \quad (2.2.2) $$

Because the operation is derived from the product of subsets of $G$, the operation is well-defined (does not depend on the particular choice of group elements), associative, and has identity
element $N$. The inverse of an element $aN$ of $G/N$ is $a^{-1}N$. Thus, both the product and associative properties shown here are actions of group $G$ on the left cosets (or right cosets) of $H \in G$. The right cosets are given by $Hg$ subsets.

The final property of group actions will be to relate a group acting on a set with the group of permutations on a set. Let $G$ be a group acting on a set $S$. Let $S_n$ be the group of all permutations of $S$. Then a function is defined from $G$ to $S_n$ with the use of the action. Let $f : G \to S_n$ be given by $f(a)$ as the permutation that sends $s$ to $as$. Let this function be $fa$. First it needs to be shown that this function exists, i.e., show $fa$ is in fact a permutation of $S$.

That $fa$ is a function from $S$ to $S$ is clear, but it needs to be checked that it is a mapping of one to one and onto. For one to one, suppose $s$ and $t$ are elements of $S$ with $fa(s) = fa(t)$. Then $as = at$. Also,

$$s = es = (a^{-1}a)s = a^{-1}(as) = a^{-1}(at) = (a^{-1}a)t = et = t \quad (2.2.3)$$

Therefore $fa$ is one to one. For onto, suppose $t \in S$. Let $s = a^{-1}t$. Then

$$fa(s) = as = a(a^{-1}t) = a(a^{-1}a)t = et = t \quad (2.2.4)$$

Thus the function $fa$ is also onto. Hence $fa$ is a permutation of $S$, so lies in $S_n$. Therefore $f$ is a function from $G$ to $S_n$. There exists a theorem on this,

**Theorem 2.2.2** (Cayley’s theorem). *Every group $G$ of order $n$ is isomorphic with a subgroup of the symmetric group $S_n$ acting on $G$.*

Hence, the above theorem can be understood as an example of a group action of $G$ on the elements of $G$ itself. Cayley’s theorem puts all groups on the same footing, by considering any group as a permutation group of some underlying set. Thus, theorems which are true for permutation groups are true for groups in general.

### 2.2.5 Conjugacy Classes

Let $G$ be a group and $S = G$. Conjugation may be defined as an action of $G$ on $S$. That is, if $g \in G$ and $s \in S$ (so $S \in G$), then a function is defined as $(g, s) \to gsg^{-1}$. This is an action of
G on S, because if \( s \in S \), then \( es = ese^{-1} = s \). So the first axiom is satisfied. Next, if \((g,h) \in G\) and \( s \in S \), then \(((gh),s) = (gh) s (gh)^{-1} = ghsh^{-1}g^{-1} \), and \((g,(h,s)) = g(hsh^{-1})g^{-1} \) which is the same as \(((gh),s)\). Therefore this is an action. Thus conjugation is an action of a group G onto itself.

**Theorem 2.2.3** (Class Equation). Let G be a finite group. Then a group \( G_1 \) may have a mapping to another group \( G_2 \) for every element in both the groups. This is homomorphism. If the mapping is a bijection, then it is called an isomorphism. An automorphism of a group is a mapping onto itself. Such a mapping is also called a conjugation.

Two elements that may be transformed into one another as in conjugation are called conjugate elements. Two elements that are transforms of the same elements are also transforms of one another. For example, if there is another element \( z \in G \) which is a transform of \( h \), then \( g \) and \( z \) are transforms of one another. Thus the entire set of elements \( g, h, z \) which are conjugate to \( g \) are said to form a class of conjugate elements. The order of this class is \( r \), which is the number of elements in this class. An identity element of any group \( G \) forms a class of order 1. Each conjugate set of elements are said to form a conjugacy class. The set of conjugacy classes of a group form a partition of the group \( G \). The internal structure of every conjugate element in a class is the same. These are called “classes” because they partition the group (i.e., form an equivalence relation).

**Theorem 2.2.4.** Conjugacy classes:

1. Every element of a group \( G \) is a member of some class of \( G \)

2. No element of group \( G \) can be a member of two different classes of \( G \)

3. The identity element \( E \) of \( G \) always forms a class of its own. For example, if \( G \) is an Abelian Group (i.e., commutative group), then every element makes a class on its own.

In the context of conjugate elements, another type of subgroup may be identified. A subgroup \( H \) of a group \( G \) is said to be an ‘invariant subgroup’ if \( ghg^{-1} \in H \) for every \( h \in H \) and every \( g \in G \). Thus normal subgroups are also called as invariant subgroups.
2.3 Group Representations


The theory of representations are used to describe the group actions discussed above. Group actions may be ‘represented’ by functions, polynomials or matrices. Through representations of groups, many group-theoretic problems are reduced to problems in linear algebra. They map the geometric structure of groups to the linear algebraic structure which is a better understood area. Therefore the term ‘representation’ of a group is also used in a more general sense to mean any “description” of a group as transformations of some mathematical object. More formally, a “representation” means a homomorphism from the group to the automorphism group of an object. Representation theory also depends heavily on the type of mathematical object on which the group acts. For example, a representation of a group $G$ on a vector space $L$ over a field $K$ is a group homomorphism from $G$ to $GL(L)$, the general linear group on $L$. Therefore, a representation is a map

$$\rho: G \to GL(L) \quad (2.3.1)$$

such that

$$\rho(g_1g_2) = \rho(g_1)\rho(g_2), \quad \text{for all } g_1, g_2 \in G. \quad (2.3.2)$$

Here $L$ is called the representation space and the dimension of $L$ is called the dimension of the representation. It is common practice to refer to $L$ itself as the representation when the homomorphism is clear from the context.

A representation $\rho : G \to GL(n, C)$ defines a group action of $G$ on the vector space $C^n$. Moreover this action completely determines $\rho$. Hence to specify a representation it is enough to specify how it acts on its representing vector space. Alternatively, the action of a group $G$
on a complex vector space \( L \) induces a left action of group algebra \( C[G] \) on the vector space \( L \), and vice-versa. Hence representations are equivalent to left \( C[G] \) modules.

\( C[G] \) can also be considered as a representation of \( G \) in three different ways:

- Conjugation: \( g[h] = ghg^{-1} \)
- As a left action: \( g[h] = gh \) (a regular representation)
- As a right action: \( g[h] = hg^{-1} \) (also a regular representation).

For many groups it is entirely natural to represent the group through matrices. Consider for example a dihedral group \( D_4 \) of symmetries of a square. This is generated by the two reflection matrices.

\[
R_m = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \quad (2.3.3)
\]

\[
R_n = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (2.3.4)
\]

Here \( R_m \) is a reflection that maps \((x,y)\) to \((-x,y)\), while \( R_n \) maps \((x,y)\) to \((y,x)\). Multiplying these matrices together creates a set of 8 matrices that form a group. As discussed above, we can either think of the representation in terms of the matrices, or in terms of the action on the two-dimensional vector space \((x,y)\). Thus matrix representations are interesting to explore the vector space \( L \).

### 2.3.1 Matrix Representations

Let \( G \) be a group, a group \( GL(n) \) of \( n \times n \) matrices with complex entries is said to provide a \( n \)-dimensional representation or matrix representation of \( G \) if there is a homomorphism that assigns to each element \( g \in G \) a unique matrix \( \rho(g) \in GL(n) \) such that:

\[
\rho(g_1 \circ g_2) = \rho(g_1)\rho(g_2) \quad (2.3.5)
\]

\[
\rho(e) = id \quad (2.3.6)
\]

\[
\rho(g^{-1}) = \rho(g)^{-1} \quad (2.3.7)
\]
where ‘id’ is the identity matrix and ‘R’ is called the representation and ‘n’ is the dimension or degree of the representation. If ‘R’ is a representation of G on $C^n$, then for every ordered pair $(i, j)$, $1 \leq i \leq n, 1 \leq j \leq n$, the function $\rho_{ij} \in L^2(G)$ defined for each $g \in G$ to be the coefficient of the matrix $\rho(g)$ in the $i^{th}$ row and the $j^{th}$ column, $\rho_{ij}(g) \in C$, is called a matrix coefficient of $\rho$. These matrices are invertible.

A matrix representation $\rho$ is reducible if all matrices have the form:

$$\rho(g) = \begin{pmatrix} \rho_1(g) & \rho_{12}(g) \\ 0 & \rho_2(g) \end{pmatrix}$$

(2.3.8)

Thus a matrix representation looks like this:

$$\rho(R) = \begin{bmatrix} \rho_1(R) & 0 \\ \rho_2(R) & \rho_3(R) \\ 0 & \ddots \end{bmatrix}$$

(2.3.9)

The above matrix design is useful for generating transforms for signal processing. It may be noted that this matrix design creates orthonormal blocks which may capture structural symmetries of a signal depending on the nature of the block, i.e., irreducible representation. By choosing some random basis for the vector space $L$, matrix representations are obtained. Thus a mapping of the group $G$ on a group of $n \times n$ matrices is obtained. Then $\rho(G)$ is a matrix representation of the group $G$ such that if $R_1$ and $R_2$ are elements of $G$, then

$$\rho(R_1 R_2) = \rho(R_1) \rho(R_2)$$

(2.3.10)

$$\rho(R_1^{-1}) = [\rho(R_1)]^{-1}$$

(2.3.11)

$$\rho(E) = 1$$

(2.3.12)

The general procedure for constructing representations of a signal is as follows:

- Choose a group of operators, i.e., the transformation groups.

- Choose a linear vector space $L$ corresponding to the signal.

- Choose a basis for the space $L$. 
The standard basis is a convenient choice:

\[ B = B = \sum_{i=1}^{n} \sum_{j=1}^{n} e_{ij} \quad \text{where} \ e_{ij} = \begin{cases} 1 & \text{at } i = j, \\ 0 & \text{otherwise} \end{cases} \]  

(2.3.13)

For example, in matrix form, the basis \( B \) for space \( L \) of dimension \( n = 6 \) is given by,

\[
B = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 \\
\end{pmatrix}
\]  

(2.3.14)

where each \( i^{th} \) column of the matrix is the basis vector \( e_i \).

If the chosen \( d \times d \) matrices are unitary then the representation is called as a unitary representation of the group \( G \). If \( G \) is a finite group, then every representation of \( G \) is equivalent to a unitary representation.

**Theorem 2.3.1.** Every representation of a finite group is unitarizable.

Matrix representation are thus obtained by a homomorphic mapping of a group \( G \) onto a group of non-singular \( d \times d \) matrices with matrix multiplication as the group operation. If the mapping is one-to-one then it is said to be an isomorphic mapping and such a representation is termed as ‘faithful’ representation. Isomorphic groups may differ in the nature of their elements, but they have the same structure of subgroups, cosets and conjugacy classes. It may be noticed that the dimension of the representation \( \rho \) need not be the same as the dimension of a transformation group \( G \). If the dimension (or order) of \( G \) is \( n \), then the dimension of \( G \)'s matrix representations is \( n \times n \).

### 2.3.2 Irreducible Representations

Let a \( n \)-dimensional representation \( \rho(T) \) of a group \( G \) be partitioned such that the new representation contains diagonal blocks as in
\[
\rho(T) = \begin{pmatrix}
\rho_{11}(T) & \rho_{12}(T) \\
0 & \rho_{22}(T)
\end{pmatrix}
\]  
(2.3.15)

where the dimension ‘n’ is the sum of dimensions of \(\rho_{11}(T)\) and \(\rho_{22}(T)\). The representations \(\rho_{11}(T)\) and \(\rho_{22}(T)\) are individually different representations of \(G\) of smaller dimensions. Then the representation \(\rho(T)\) of the group \(G\) is said to be ‘reducible’. A representation of a group is said to be ‘irreducible’ if it is not reducible. A representation is called ‘completely reducible’ if it has the form

\[
\rho(T) = \begin{pmatrix}
\rho_{11}(T) & 0 & 0 & 0 \\
0 & \rho_{22}(T) & 0 & 0 \\
0 & 0 & \ldots & 0 \\
0 & 0 & 0 & \rho_{kk}(T)
\end{pmatrix}
\]  
(2.3.16)

Such a representation is a decomposable representation. For any finite group \(G\), every representation is completely reducible as stated by Maschke’s theorem (Holmes, 1990).

**Theorem 2.3.2.** (Maschkeş Theorem): Every finite-dimensional representation of a finite group is completely reducible.

**Proposition 2.3.1.** Every irreducible representation of a finite group is finite dimensional.

### 2.3.3 Characters

The ‘character’ of a matrix representation \(\rho(T)\) of a group element \(T \in G\) is defined to be the function \(tr(\rho(T))\), the trace of the representation. If two representations of a group \(G\) are considered to be equivalent then the set of all characters of their representation are identical. The characters are unchanged by any similarity transformations. Therefore on each conjugacy class of \(G\), the function \(\chi = tr(\rho(T))\) is a constant. The following theorems are stated in the work by Kowalski (2011), where \(\oplus\) denotes the dot product.

**Theorem 2.3.3.** Let \(G\) be a finite group.

1. If \(\rho_1(T)\) and \(\rho_2(T)\) are two inequivalent irreducible representations of the group \(G\), then the
The dot product of characters of the two representations is given as

\[(\text{tr}(\rho_1(T)) \odot \text{tr}(\rho_2(T))) = 0\] (2.3.17)

2. If \(\rho(T)\) is an irreducible representation of \(G\), then

\[(\text{tr}(\rho(T)) \odot \text{tr}(\rho(T))) = 1\] (2.3.18)

From the above theorem, the following theorem is derived:

**Theorem 2.3.4.** The irreducible characters of \(G\) form an orthonormal set in \(L^2(G)\).

**Corollary 2.3.2.** The inequivalent irreducible representations of a finite group \(G\) are finite in number.

Let the representation \(\rho(T)\) be noted as \(\rho\) and its character be taken as \(\chi\). Any reducible representation \(\rho\) may be written as a linear sum of its irreducible representations \(\rho_i\). If \(\odot\) denotes the dot product, the following theorems are true:

**Theorem 2.3.5.** Let \(\rho\) be any representation of a group \(G\) and let \(\chi_\rho\) be its character. Then,

\[\rho = \sum_{i=1}^{N} m_i \rho_i\] (2.3.19)

where

\[m = (\chi_{\rho_i} \odot \chi_\rho).\] (2.3.20)

Irreducible representation cannot be decomposed further into sub representations. Therefore there is only one character for such representations, which also implies

**Theorem 2.3.6.** A representation \(\rho(T)\) of a group \(G\) is irreducible only if

\[(\chi_\rho \odot \chi_\rho) = 1\] (2.3.21)

Also,

**Corollary 2.3.3.** The number of inequivalent irreducible representations of a group \(G\) is equal to the number of conjugacy classes of \(G\).
2.3.4 Basis of Conjugacy Class Functions

The vector space of class functions on G has for dimension the number of conjugacy classes of G. Let \((E, \rho)\) be a representation of G, and let \(f\) be a function on G. The endomorphism \(\rho f\) of E is defined by

\[
\rho f = \sum_{g \in G} f(g) \rho(g)
\]  (2.3.22)

Thus, by definition, for every \(x \in E\), \(\rho f(x) = \sum_{g \in G} f(g) \rho(g)(x)\).

**Theorem 2.3.7.** The irreducible characters form an orthonormal basis of the vector space of class functions.

It is known that the characters \(\{\chi_1, \chi_2, \ldots \chi_n\}\) of inequivalent irreducible representations of G form an orthonormal set in \(L^2(G)\).

2.3.5 Groups of Coordinate Transformations

If the elements of the group are coordinate transformations, then it is called a transformation group. A transformation group (Duzhin, 2004; Hamermesh, 1970; Holmes, 1990) is a set G of transformations of a certain set which has the following two properties:

- If two transformations \(f\) and \(g\) belong to G then their composition \(f \circ g\) also belongs to G;

- Together with every transformation \(f\) the set G also contains the inverse transformation \(f^{-1}\)

A transformation is also a one to one mapping \(f : x \rightarrow f(x)\) of some set SS onto itself. The set of all transformations with the law of combination defined as the composition of two transformations, \(i.e., f \circ g(x) = f(g(x)), \forall x \in SS\) forms a group, which is called the complete transformation group of SS.
2.3.6 Representations of Coordinate Transformation Groups

Consider a vector space L. If any vector $x \in L$ is mapped to another vector $y \in L$ by

$$ x = Ty $$

(2.3.23)

then T is called a mapping from x to y. T is also called an operator on the space L. Such operators can also form a group. If an arbitrary group G is mapped homomorphically to a group of operators $\rho(G)$ on the space L, the operator group $\rho(G)$ is a representation of the group G in the representation space L. If the group G is of order ‘n’, then the dimension of L is also ‘n’. The operator corresponding to the element R of G is given by $\rho(R)$. The dimension of the linear representation of the operator $\rho(R)$ is given by $n \times n$. A linear representation is a representation in terms of linear operators. If a representation for the operators is found, a representation for the group G is automatically obtained. If the operators of the group are unitary then the representation is also unitary. For a finite group G the representations are always unitary. For infinite groups, linear operators on Hilbert Space have to be used.

Let $\rho$ be a representation of G. A vector subspace $V \subseteq V$ is called invariant under G, if for every $g \in G$, $\rho(g)V \subseteq V$. Since V is finite-dimensional, automatically $\rho(g)V \subseteq V$ implies $\rho(g)V = V$. The representation $\rho$ is then restricted to V, which is a representation of G on V. The representation restricted to an invariant subspace is also called a subrepresentation. The representation $\rho$ of G is called irreducible if the only vector subspaces of V invariant under $\rho$ are 0 and $\rho$ itself. Otherwise $\rho$ is a reducible representation. A subrepresentation of $(x, V)$ is an invariant subspace $W \subseteq V$ under the action of G (also called a G-invariant subspace), which says that for all $w \in W$ and $g \in G$, $x(g)w \in W$. Finally, let ‘R’ be a representation of G. The character of $\rho$ is the function $\chi_g$ on G taking complex values defined by $\forall g \in G, \chi_g = tr(\rho(g))$. Equivalent representations have the same character.

2.3.7 Basis of Transformation Group Representations

Let $\rho$ be a n-dimensional representation of a group of coordinate transformation in the Euclidean space $R^3$. Let $\psi_1, \psi_2, \cdots, \psi_d$ be a set of basis functions of the representation $\rho$ and let M be any $n \times n$ non-singular matrix. Then the set of d linearly independent functions defined to be for $n = 1, 2, ..., d$
\[ \psi'_n(r) = \sum_{m=1}^{d} M_{mn} \psi_m(r) \]  

(2.3.24)

which form a basis for the equivalent representation for each transformation T of the group G. By Schur's orthogonality lemma (Kowalski, 2011) given below, the irreducible representations are orthonormal and form a basis for the \( n \) dimensional vector space \( L \) spanned by the non-singular representation matrices.

**Lemma 2.3.4** (Schur's orthogonality). *For finite dimensional representations of a finite group \( G \) in which inner products have been introduced to make the representations unitary*

- If \( \rho_1 \) and \( \rho_2 \) are two inequivalent irreducible representations, then every matrix column of \( \rho_1 \) is orthogonal to every matrix column of \( \rho_2 \) with respect to the inner product in the vector space \( V \).

- If \( \rho \) is another irreducible representation, then \( \left( \frac{\|G\| \text{trace}(\rho)}{\dim V} \right) \) is equal to the action of \( \rho \) on the other irreducible representations \( \rho_1, \rho_2 \).

As a consequence, the dimensions of the irreducible representations follow the rule:

\[ \sum_{i=1}^{m} d_i^2 = n \]  

(2.3.25)

where \( d_i \) = dimension of \( i^{th} \) irreducible representation, \( n \) = dimension of representation space and \( m \) = number of irreducible representations.

The implications of the above rule are significant. Consider the basis of the representation \( \rho(T) \) be \( \psi_1, \psi_2, \cdots, \psi_d \) spanning a vector space \( L \) and the irreducible representations \( \rho_{kk} \) having dimensions \( d_1, d_2, \cdots, d_j \). As per Schur’s lemma, if \( d_k \) is the dimension of the irreducible representation \( \rho_{kk} \) and \( d \) represents the dimension of the representation \( \rho(T) \), a \( d \times d \) matrix, then \( \sum_{k=1}^{j} d_k = d \). The vector space \( L \) is thus a direct sum of the subspaces represented by the smaller irreducible representations. The representation \( \rho(T) \) may be treated as a direct sum of the irreducible representations. This implies that the basis vectors of irreducible representations are part of the whole set of basis vectors of \( \rho(T) \). If the set of irreducible representations are
\{\rho_{11}(T), \rho_{22}(T), \cdots, \rho_{kk}(T)\}, \text{ then the basis vectors } \psi_1, \psi_2, \cdots, \psi_{d_1} \text{ belong to the subspace of irreducible representation } R_{11}(T), \text{ the basis vectors } \psi_{d_1+1}, \psi_{d_1+2}, \cdots, \psi_{d_1+d_2} \text{ belong to the subspace of irreducible representation } \rho_{22}(T) \text{ and so on for } \rho_{kk}. \text{ This may be expressed as }

\rho(T) = \rho_{11}(T) \oplus \rho_{22}(T) \oplus \cdots \oplus \rho_{kk}(T) \tag{2.3.26}

where \( \oplus \) denotes a linear combination of the individual terms in the R.H.S. Since for a finite group G the representation \( \rho(T) \) is unitary, all the irreducible representations are also unitary. As unitary representations, the basis for irreducible representations are orthonormal within themselves, as well as mutually orthonormal because of their direct sum forming the total basis of the unitary representation \( \rho(T) \).

From the above discussion on representations, it may be seen that any function \( \phi_n(x) \in L^2 \) space, which is a space of square-integrable functions, may be written as the linear combination of the basis functions of the unitary irreducible representations of a group G of coordinate transformations in the space \( R^n \).

### 2.3.8 Dihedral Transformation Groups

This work uses dihedral groups (Viana, M., and V. Lakshminarayanan, 2010; Lenz, 1993) to illustrate the proposed signal processing algorithm as well as to examine its application to some problems in signal and image processing. Therefore, a brief discussion is provided below on dihedral groups. A dihedral group \( D_n \) consists of the reflections in any symmetry axes of the polygon and rotations of an angle \( 2\pi/n \) around the center of the polygon. Denoting the rotation of angle \( 2\pi/n \) by \( \rho \) and the reflection by \( \sigma \), all elements in \( D_n \) have the form \( \sigma^i \rho^j \) where \( i = 0, 1; j = 0, 1, \ldots, n - 1 \).

Thus the dihedral groups are defined by two linear transformations rotation and reflection. The rotations are taken around a common centre in a two dimensional space. The rotations for one set of coordinate axes are given by

\[ r_u = e^{(\theta)} \text{ where } \theta = (u \star 2 \star \pi)/\text{dim} \tag{2.3.27} \]

where \( \text{dim} \) = the dimension of the group. With respect to the irreducible representations both one and two dimensional cases, the rotation transform \( R_o \) is given by
where $id$ corresponds to one-dimensional irreducible representation and $r_u$ characterizes two-dimensional representations. Thus, a single rotation matrix embodies as many two-dimensional rotations as the number of conjugacy classes available for this transformation group. They are two-dimensional rotations because there are two members in each conjugacy class for a dihedral group. The one-dimensional representation also corresponds to single element conjugacy class. This kind of construction of rotation matrices show how to break a n-dimensional rotation into local two-dimensional rotations. This aspect is useful in making signal transforms whose action may be decomposed into local transforms.

Similarly the reflection transform $R_f$ is given by

\[
R_f = \begin{bmatrix}
id & 0 \\
R = r_v & R = r_v \\
0 & \ddots
\end{bmatrix}
\]  

(2.3.29)

where the reflections are given by

\[
r_v = S \ast e^{(\theta)} \text{ where } \theta = (v \ast \pi)/\text{dim}, \ S \text{ is an arbitrary reflection.}
\]  

(2.3.30)

Starting from Chapter 4, the proposed signal processing algorithm G-lets is illustrated using dihedral groups.

2.4 Conclusions

In this chapter, the mathematical basics of group theory useful for signal processing has been presented. How a new framework and a new signal processing algorithm is derived from group theory is presented in Chapter 3. Using group and representation theory how an existing signal processing algorithm may be described, and a classification of existing algorithms in
the new group theoretical framework is also presented in Chapter 3. It also presents how the inadequacies of existing algorithms are highlighted and the proposed research work called as G-lets, is introduced in a group theoretical perspective.