Dynamical Systems on Geometric Structures

Stephen Dzaka (stephen@aims.ac.za)
African Institute for Mathematical Sciences (AIMS)

Supervised by: Dr. Francesco G. Russo
Dr. David Erwin
University of Cape Town, South Africa

18 May 2017

Submitted in partial fulfillment of a structured masters degree at AIMS South Africa

African Institute for Mathematical Sciences
SOUTH AFRICA

Abstract

In this work, we first define the commutativity degree of a group in the finite case. We involve the notion of group actions under conjugation and of centralizer of an element, in order to compute the commutativity degree. Then we generalize to the infinite case involving the Haar measure on a compact group for the set of all pairs $(x, y) \in G \times G$ for which the commutator $[x, y] = 1$. Formally this is the probability that two elements picked randomly commute. This entails measure theory, group theory, topology and compact groups.

Declaration

I, the undersigned, hereby declare that the work contained in this research project is my original work, and that any work done by others or by myself previously has been acknowledged and referenced accordingly.

Stephen Dzaka, 18 May 2017

Contents

1. Introduction

In the present thesis we refer to the notion of “Dynamical System” in a way which is not very common. The intuitive idea is the following:

we will consider the universe of all finite groups and would like to characterize the condition of “being abelian” via a function of probability, which we will call “commutativity degree”.

This function will be very useful:

one of its extremal values characterizes the universe of all abelian groups.

Then we investigate more properly this function, showing the literature and some previous results.

In doing this, we will see that it is possible to have upper and lower bounds and they will describe large families of groups. For instance, Gustafson (Gustafson, 1973) answered an important problem of Paul Erdős (Erdős and Túran, 1968) about this topic. In fact he showed that, if G is a non-abelian finite group, then $d(G) \leq 5/8$; furthermore this bound is achieved if and only if $G/Z(G)$ is isomorphic to an elementary abelian 2-group of rank 2, where $Z(G)$ denotes the center of the group G.

We will see that the result of Gustafson, not only was generalized to the infinite case via compact groups, but may be interpreted in terms of some interesting infinite groups, called FC-groups. This is a more recent result, showed in Hofmann and Russo (2012).

On the other hand, there is a parallel approach, involving character theory, which we do not use, and we mention (Castelaz, 2010), since there are computational difficulties which may be solved better with one approach, instead of another.

Finally, we want to mention that the idea of studying algebraic structures and geometric structures via probabilistic invariants, is growing in the mathematical community, after a fundamental contribution of Mikhail Gromov.

In Gromov (1993), there is in fact the formulation of a deep theory, which correlates the growth of some topological invariants of infinite groups with structural properties of algebraic objects, generalizing the well-known notion of commutativity.

Many conjectures and open questions originated after this fundamental reference. Nowadays geometry, algebra, group theory and probability continue to be influenced by the same ideas and several new inter-connections are present. In particular, the role of the probability in group theory became more interesting for many authors in the last decades.

The ideas of Gromov join measure theory and algebra, so it is possible to investigate symmetries in groups via restrictions of numerical nature, and vice-versa.

The present project is devoted to study the property of being abelian and its generalizations, under the perspective of the probability of commuting pairs. The perspective of Gromov will fit perfectly in the present subject, even if not directly mentioned.

2. Commutativity Degree of a Finite Group

Given a finite group G, if we randomly select two elements, x and y of G,

what is the probability that x and y commute ?

We may give different answers to this question.

An intuitive perspective is to imaging

$$G \times G = \{(x, y) \mid x, y \in G\}$$

as a "dynamical system" in which we have a condition of "strong symmetry", when all the ordered pairs (x, y) satisfy the condition $xy = yx$. From this ideal case, one could have a series of more "chaotic configurations", in which the ordered pairs (x, y) do not satisfy the condition $xy = yx$.

If we would have a way to measure the gap between the ideal configuration and the real number of commuting pairs which we have in front of us (in an arbitrary group), then we would have a method to characterize abelian groups between all finite groups.

This intuitive (and apparently simple idea) goes back to some fundamental contributions of P. Erdős and W.H. Gustafson (Gustafson, 1973), who influenced several branches of combinatorics, group theory, measure theory and ergodic theory in the last 50 years.

Denoting by

$$c(G) = \{(x, y) \in G \times G : xy = yx\},$$

we have that the probability that two elements x and y are commuting, is given by

$$d(G) = \frac{|c(G)|}{|G \times G|}.$$

The probability $d(G)$ is also called *commutativity degree* of G (see (Castelaz, 2010)).

We will recall some notions from group actions, since they are very useful for the computation of $d(G)$.

Group Actions

Let G be a (finite or infinite) group and X an arbitrary non-empty set.

2.0.1 Definition. An (left) action of G on X is a map $\psi : G \times X \to X$ given by $(g, x) \mapsto g \cdot x = \psi(g, x)$ satisfying:

(i). $1 \cdot x = x$ for every $x \in X$;

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

Under these circumstances X is called a G-set, or, we say that G is acting on X.

There are various ways, in which a group may act on a set. We will focus on a particular type of action, which is the action by conjugation, because this is important for the study of the commutativity degree.

2.0.2 Example. Let G be a group and $X = G$. We may define an action of G on X by conjugation via the map $(g, x) \in G \times G \mapsto g \cdot x = gxg^{-1} \in G$. This defines an action of G on G, since:

(i). $1 \cdot x = 1x1^{-1} = x$ for all $x \in G$;

(ii). $(g_1 g_2) \cdot x = (g_1 g_2)x(g_1 g_2)^{-1} = g_1 g_2 x g_2^{-1} g_1^{-1} = g_1(g_2 x g_2^{-1})g_1^{-1} = g_1(g_2 \cdot x)g_1^{-1} = g_1 \cdot (g_2 \cdot x) = g_1(g_2 \cdot x)$, for all $g_1, g_2 \in G$ and $x \in G$.

We will give an example of an action, which is not by conjugation, in order to see that the notion is very general.

2.0.3 Example. Let $G = \mathbb{Z}$ be the additive group of the integers and $X = \mathbb{R}$. We may define $(n, x) \in \mathbb{Z} \times \mathbb{R} \mapsto n \cdot x = n + x \in \mathbb{R}$. This is an action, because $0 \cdot x = 0 + x = x$ is true and $(n + m) \cdot x = (n + m) + x = n + (m \cdot x) = n \cdot (m \cdot x)$ is true. But one has to be careful that the role of $\cdot$ must be properly interpreted as the action itself and/or the operation in the group.

For the following definition, G may be finite or infinite.

2.0.4 Definition. Let x and y be elements of a group G. The element x is conjugate to an element y if there exists an element $g \in G$ such that $gxg^{-1} = y$.

More precisely, we can say in Example 2.0.2 x is conjugate to y by g. The conjugation is an equivalence relation and we will denote as $x \sim y$. The equivalence classes are known as *conjugacy classes* and we denote the conjugacy class of x by $K(x)$:

$$K(x) = \{gxg^{-1} : g \in G\}.$$

Of course, if G is abelian, then $K(x) = \{x\}$ for all $x \in G$. More generally, if G is not abelian, we can always define the set

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

which turns out to be a subgroup of G. This is called the *center* of G and for all $z \in Z(G)$ we also have $K(z) = \{z\}$. Note that G is abelian if and only if $G = Z(G)$.

Let's prove this classical exercise.

2.0.5 Proposition. The conjugacy is an equivalence relation (in an arbitrary group).

Proof. We need to show that the relation $\sim$ is reflexive, symmetric and transitive.

Reflexive: $1\ x\ 1^{-1} = x$ shows that $x \sim x\ \forall x \in G$. Thus $\sim$ is reflexive.

Symmetric: If $x \sim y$, then there is $g \in G$ such that $gxg^{-1} = y$. If we multiply by g from the right, then $gxg^{-1}g = yg$. Now if we multiply by g^{-1} from the left, we have $g^{-1}gxg^{-1}g = g^{-1}yg$, so $x = g^{-1}yg = g^{-1}y(g^{-1})^{-1} = zyz^{-1}$ for $z = g^{-1} \in G$. Therefore $y \sim x$. Thus $\sim$ is symmetric.

Transitive: If $x \sim y$ and $y \sim z$, then there are $g_1 \in G$ such that $g_1 x g_1^{-1} = y$ and $g_2 \in G$ such that $g_2 y g_2^{-1} = z$. By substituting, we have $g_2 g_1 x g_1^{-1} g_2^{-1} = (g_2 g_1)x(g_1^{-1} g_2^{-1}) = (g_2 g_1)x(g_2 g_1)^{-1} = z$ and so the element $g_2 g_1 = g_3$ is such that $g_3 x g_3^{-1} = z$, that is, $x \sim z$. Thus $\sim$ is transitive.

□

It is well known that any equivalence relation induces equivalence classes. From Proposition 2.0.5, we may partition G into equivalence classes with respect to $\sim$ and in fact

$$(\dagger) \quad G = \bigcup_{x \in G} K(x) = \left(\bigcup_{x \in Z(G)} K(x) \right) \cup \left(\bigcup_{x \in G - Z(G)} K(x) \right) = \left(\bigcup_{x \in Z(G)} \{x\} \right) \cup \left(\bigcup_{x \in G - Z(G)} K(x) \right),$$

but all these unions are disjoint and so we get the well known *Class Equation* (see (Robinson, 1980), pp. 38–40)

$$|G| = |Z(G)| + \sum_{x \in G - Z(G)} |K(x)|.$$

Note that one can prove something more, that is, $|K(x)| = |G : C_G(x)|$, where $C_G(x)$ will be properly defined later on.

2.1 Orbits and Stabilizers

Let's now study the conjugacy classes in terms of actions.

2.1.1 Definition. Let G be a group that acts on the set X (from the left). For $x \in X$, we define the orbit of x under the action of G by

$$\mathrm{Orb}_G(x) = \{g \cdot x \mid g \in G\}$$

Of course, $\mathrm{Orb}_G(x)$ is a subset of X and we note that the orbits induce a partition of X, because of the relation

$$y \approx x \;\Leftrightarrow\; y \in \mathrm{Orb}_G(x).$$

This means that two elements $x, y \in X$ are related by $\approx$ if and only if $y = g \cdot x$ for some $g \in G$. One can check that $\approx$ is an equivalence relation, overlapping the same argument that we gave in Proposition 2.0.5. More precisely,

Reflexive: $x = 1 \cdot x$ shows that $x \approx x$ for all $x \in X$.

Symmetric: If $y \approx x$, then there is $g \in G$ such that $g \cdot x = y$. If we multiply by g^{-1} from the left, then $x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot y$, and so $x \approx y$.

Transitive: If $y \approx x$ and $x \approx z$, then there are $g_1, g_2 \in G$ such that $g_1 \cdot x = y$ and $g_2 \cdot z = x$. By substituting, we have $y = g_1 \cdot (g_2 \cdot z) = (g_1 g_2) \cdot z$ and so $y \sim z$. Thus $\approx$ is transitive.

In particular, we will be interested in the action by conjugation and so

$$\mathrm{Orb}_G(x) = \{gxg^{-1} \mid g \in G\} = K(x)$$

so that (†) may be re-written as

$$|G| = |Z(G)| + \sum_{x \in G - Z(G)} |\mathrm{Orb}_G(x)|.$$

There is now another important notion, which is related to the group actions.

2.1.2 Definition. Given a left action of a group G on a non-empty set X, the *stabilizer* of x in G is given by

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

The stabiliser of x in G is the set of all elements of G fixing x under the given action. In particular, if the action is by conjugation, we introduce a special notation for $\mathrm{Stab}_G(x)$:

$$C_G(x) = \{g \in G \mid gxg^{-1} = x\}$$

and this set turns out to be a subgroup of G and is called *centralizer* of x in G. Of course, $C_G(x)$ may be described even as the subgroup of all elements of G commuting with x and we will see that it plays an important role in the study of the commutativity degree.

If $A = \langle x \rangle = \{1, x, x^2, x^3, \ldots\}$ is the subgroup generated by all the powers of x, then $C_G(x) = C_G(\langle x \rangle)$. More generally, if A is an arbitrary subgroup of G,

$$C_G(A) = \bigcap_{a \in A} C_G(a),$$

and, in particular, $C_G(G) = Z(G)$.

We may check by exercise that :

2.1.3 Proposition. $C_G(A)$ is a subgroup of G.

Proof. If $g_1, g_2 \in C_G(A)$, then $g_1 g_2 a (g_1 g_2)^{-1} = a$ forall $a \in A$, so

$$\begin{aligned} g_1 g_2 a (g_1 g_2)^{-1} &= g_1 \underbrace{g_2 a g_2^{-1}}_{a} g_1^{-1} \quad \text{by definition} \\ &= g_1 a g_1^{-1} \quad \text{by definition} \\ &= a. \end{aligned}$$

So $g_1 g_2 \in C_G(A)$. For $1 \in C_G(A)$, we have $1a1^{-1} = a$ for all $a \in A$ of course. Finally, if $g \in C_G(A)$ and $a \in A$, then $(g^{-1})a(g^{-1})^{-1} = g^{-1}ag$ but we have also $a = gag^{-1}$. Hence $g^{-1}a(g^{-1})^{-1} = a$, so $g^{-1} \in C_G(a) \subseteq C_G(A)$.

□

The stabilizers which we have seen until now may be specialized when the action of conjugation is given (not on elements but) on subgroup. In order to do this, we denote by $L(G)$ the set of all subgroups of G.

2.1.4 Definition. Given the (left) action $(g, A) \in G \times L(G) \mapsto g \cdot A = A^g \in L(G)$ by conjugation of G on $L(G)$, we may consider stabilizers and orbits. The stabilizer of A in G is called *normalizer* of A in G and is defined by

$$N_G(A) \quad = \quad \{g \in G : gAg^{-1} \subseteq A\} = \{g \in G : gag^{-1} \in A, \forall a \in A\}.$$

The orbit of A in G is called *conjugacy class* of A in G and is defined by

$$K(A) \quad = \quad \{gAg^{-1}, \forall g \in G\}.$$

Here, we will discuss a normal subgroup under action by conjugation.

Let H be a subgroup of G. Then H is called a *normal subgroup* of G (denoted by $H \lhd G$), if H is fixed under the action by conjugation in G. This means that

$$H \lhd G \;\Leftrightarrow\; ghg^{-1} \in H, \quad \forall h \in H, \forall g \in G.$$

Overlapping the ideas of Proposition 2.1.3, we can show that stabilizers of arbitrary (left) actions of groups on sets are always subgroups of the acting group. In fact the following fact is well known and is true even for actions which are not necessarily by conjugation.

2.1.5 Proposition. Let G be a group acting on a non-empty set X and $x \in X$. Then $\mathrm{Stab}_G(x)$ is a subgroup of G.

Proof. We know that the identity element, $1 \in \mathrm{Stab}_G(x)$ since it fixes every element in the set X. Let $g, h \in \mathrm{Stab}_G(x)$. Then $g \cdot x = x$ and $h \cdot x = x$ and also $(gh) \cdot x) = g \cdot (h \cdot x) = g \cdot x = x$, hence $gh \in \mathrm{Stab}_G(x)$. Finally, if we have

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

then $g^{-1} \in \mathrm{Stab}_G(x)$. Therefore $\mathrm{Stab}_G(x)$ is a subgroup of G. □

2.2 Examples of Conjugacy classes

In the present section, we give some examples of computational nature on the conjugacy classes of some groups of small order. We begin with the dihedral group of order six and then we generalize to groups of higher order.

2.2.1 Example. Take the group of all permutations on a three-element set $\{1, 2, 3\}$ and call it S_3. We want to compute all the conjugacy classes of S_3. By using the notation cycles, we have

$$1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \tau_1 = (12) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad \tau_2 = (13) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\tau_3 = (23) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \rho = (123) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \rho^2 = (132) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

We may give a different interpretation of S_3 in terms of reflections and rotations of a regular triangle of the usual plane. The following diagrams help to visualize.

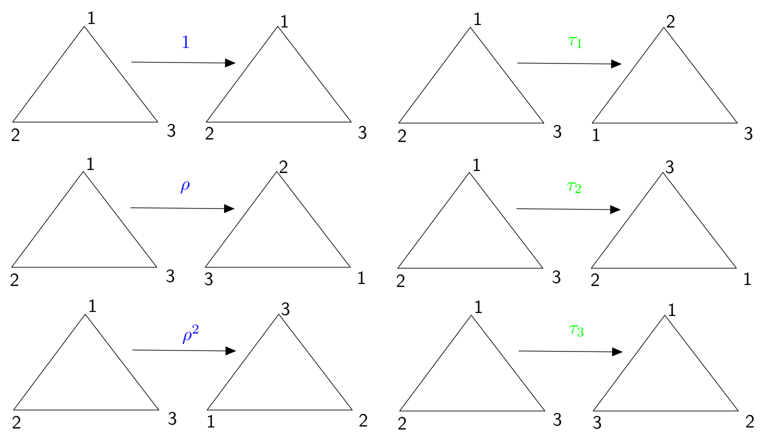


Figure 2.1: Geometric interpretations of S_3

We may describe the structure of $L(S_3)$ via the following diagram, in which $L(S_3) = \{\{1\}, S_3, A_3, H, K, L\}$, where $A_3 = \langle(123)\rangle = \langle\rho\rangle$, $H = \langle(12)\rangle = \langle\tau_1\rangle$, $K = \langle(13)\rangle = \langle\tau_2\rangle$, $L = \langle(23)\rangle = \langle\tau_3\rangle$. Note that $HK \neq KH$, $HL \neq LH$, $KL \neq LK$.

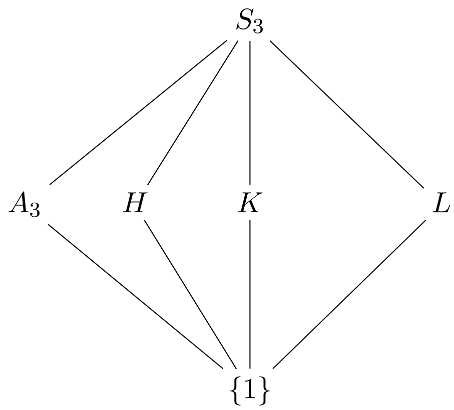


Figure 2.2: Lattice of subgroups of S_3

To find the conjugacy classes, we observe how the permutations are formed.

Firstly, we fix all the elements and we call this the identity, 1. Secondly, we observe 2 cycles such as $(12), (13), (23)$, they are formed through transposition and finally, 3 cycles $(123), (132)$, they are formed through "rotations". Hence, we have

$$\begin{aligned} K(1) &= \{1\} \\ K(\rho) &= K(\rho^2) = \{\rho, \rho^2\} \\ K(\tau_1) &= K(\tau_2) = K(\tau_3) = \{\tau_1, \tau_2, \tau_3\} \end{aligned}$$

At this point, it would be useful to recall the composition between elements of S_3.

$\circ$	1	ρ	ρ^2	τ_1	τ_2	τ_3
1	1	ρ	ρ^2	τ_1	τ_2	τ_3
ρ	ρ	ρ^2	1	τ_2	τ_3	τ_1
ρ^2	ρ^2	1	ρ	τ_2	τ_1	τ_2
τ_1	τ_1	τ_3	τ_2	1	ρ^2	ρ
τ_2	τ_2	τ_1	τ_3	ρ	1	ρ^2
τ_3	τ_3	τ_2	τ_1	ρ^2	ρ	1

Table 2.1: S_3 Group Table

The geometric interpretation, in terms of rotations and reflections of a regular triangle, allows us to identify S_3 as a group of symmetries of a regular triangle. There is a more general approach, in terms of groups of symmetries of regular polygons, which is related to the notion of semidirect product, which we will discuss later on. Another useful example of groups of symmetries, related to rotations and translations of a square, is given by the following group.

Here we will discuss its properties in an algebraic way and visualization which we gave in the previous example.

2.2.2 Example. In $D_8 = \langle a, b | a^4 = 1, b^2 = 1, bab^{-1} = a^{-1} \rangle$. We have $D_8 = \{1, a, a^2, a^3, b, ab, a^b, a^3b\}$

Element	1	a	a^2	a^3	b	ab	a^2b	a^3b
Order	1	4	4	4	2	2	2	2

We know that elements of the same conjugacy class have the same order. Secondly, we take the elements of order 4 that is $\{a, a^2, a^3\}$ and apply the definition of "conjugation of group". Thus, there exist $x \in D_8$ such that $xa = a^2x$ or $xa = a^3x$. From the definition of D_8, there does not exist $x \in D_8$ such that $xa = a^2x$ but there exist $x \in D_8$ such that $xa = a^3x$ where $x = b$. Hence a and a^3 belong to the same conjugacy class and a^2 stands alone as conjugacy class. We perform the same operation for elements of order 2, $\{b, ab, a^2b, a^3b\}$. We observed that there exist $x \in D_8$ such that $xb = a^2bx$ where $x = a$ and there exist $x \in D_8$ such that $xab = a^3bx$ where $x = a^2b$. Hence a, a^3 are in the same conjugacy class and ab, a^3b are in the same conjugacy class.

Therefore we can find 5 conjugacy classes and they are $\{1\}, \{a^2\}, \{b, a^2b\}, \{a, a^3\}, \{ab, a^3b\}$

$$
\begin{aligned}
K(1) &= \{1\} \\
K(a^2) &= \{a^2\} \\
K(a) &= = K(a^3) = \{a, a^3\} \\
K(b) &= K(a^2b) = \{b, a^2b\} \\
K(ab) &= K(a^3b) = \{ab, a^3b\}
\end{aligned}
$$

We may give a different interpretation of D_8 in terms of reflections and rotations of a square of the usual plane. The following diagrams help to visualize.

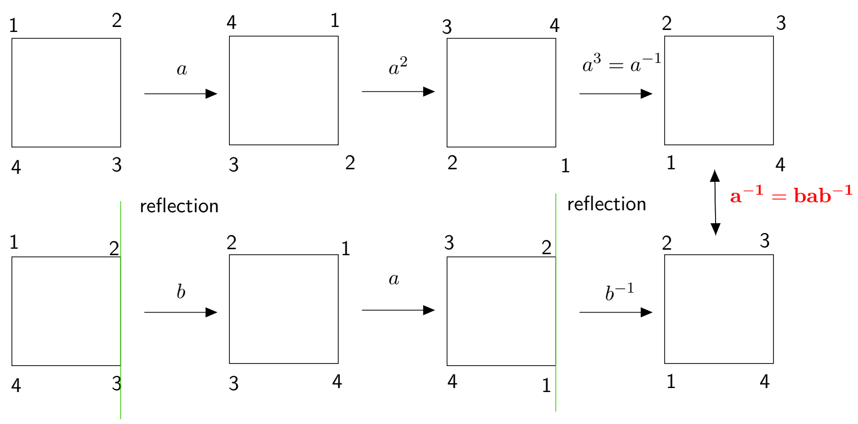


Figure 2.3: Geometric interpretations of $a^4 = 1$ and $bab^{-1} = a^{-1}$

We may describe the structure of $L(D_8)$ via the following diagram, in which

The normal subgroups are D_8, $\{1\}$, $B = \langle a \rangle$, $Z(D_8) = \langle a^2 \rangle$, $M_1 = \{1, a^2, b, a^2b\}$ and $M_2 = \{1, a^2, ab, a^3b\}$. Notice that $H = \langle a^2b \rangle$ and $K = \langle b \rangle$ are contained in M_1, while $U = \langle ab \rangle$ and $V = \langle a^3b \rangle$ in M_2.

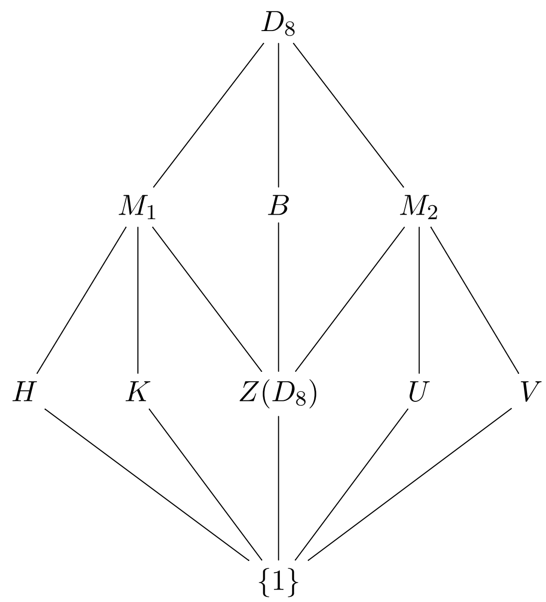


Figure 2.4: Lattice of subgroups of D_8

One could generalizes these arguments on S_3 and D_8 to dihedral groups of order D_{2n} since they have geometric interpretations in terms of regular polygons.

2.3 Commutativity Degree

In the present section, we want to see why the notion of centralizer and of group action is important in the context of our study. As we said before, the probability that two elements of a group, G commute is given by

$$d(G) = \frac{|\{(x, y) \in G \times G \mid [x, y] = 1\}|}{|G|^2}$$

where $[x, y] = xyx^{-1}y^{-1}$ is called *commutator* of x and y.

Of course, if G is an abelian group, then every element in the group commute with each other, hence the commutativity degree of an abelian group is 1. In fact, one can define the smallest subgroup of G containing all the elements $[x, y]$ fo4r $x, y \in G$, that is, the so-called *derived subgroup* (or, *commutator subgroup*)

$$G' = [G, G] = \langle [x, y] \mid x, y \in G \rangle$$

of G and this is trivial if and only if G is abelian. In fact

$$C_G(G) = G \quad \Leftrightarrow \quad G' = 1 \quad \Leftrightarrow \quad d(G) = \frac{|\{(x,y) \in G \times G : [x,y] = 1\}|}{|G|^2} = \frac{|G \times G|}{|G|^2} = 1$$

It is a first evidence that the computation of the commutativity degree involves strongly the notion of centralizer of element.

Another important consideration is related to (†). In (†), the elements of $Z(G)$ are isolated from the others, because their conjugacy classes are singleton. In some sense, this behaviour of the central elements may be found in a similar equation, which involves the commutativity degree (see (Castelaz, 2010; Gustafson, 1973)):

$$\begin{aligned}
d(G) &= \frac{|\{(x,y) \in G \times G \mid [x,y] = 1\}|}{|G|^2} \\
&= \frac{\left|\bigcup_{x \in G} \left(\{x\} \times \bigcup_{xy=yx} \{y\}\right)\right|}{|G|^2} \\
&= \frac{\left|\bigcup_{x \in G} \left(\{x\} \times \bigcup_{y \in C_G(x)} \{y\}\right)\right|}{|G|^2} \\
&= \frac{\left|\bigcup_{x \in G} \left|C_G(x)\right|\right|}{|G|^2} \\
&= \frac{1}{|G|^2} \sum_{x \in G} |C_G(x)| \\
&= \frac{1}{|G|^2} \left(\sum_{x \in Z(G)} |C_G(x)| + \sum_{x \in G - Z(G)} |C_G(x)| \right) \\
&= \frac{1}{|G|^2} \left(|Z(G)|\ |G| + \sum_{x \in G - Z(G)} |C_G(x)| \right) \\
d(G) &= \frac{|Z(G)|}{|G|} + \sum_{x \in G - Z(G)} \frac{|C_G(x)|}{|G|^2}.
\end{aligned}$$

Investigating the Commutativity Degree for some Special Groups

Let consider a dihedral group, D_{2n} is as the group that has two generators r and s with orders n (n odd) and 2 respectively such that $r^s = r^{-1}$. Thus

$$D_{2n} = \langle r, s : r^n = 1, s^2 = 1, r^s = r^{-1} \rangle$$

2.3.1 Theorem. *The group D_n has 2n elements.*

Proof. We show this theorem by listing all the possible elements in D_n. Thus

$$\begin{aligned} D_n &= \{\underbrace{1}_{1}, \underbrace{r, r^2, \ldots, r^{n-1}}_{n-1}, \underbrace{s}_{1}, \underbrace{rs, r^2s, \ldots, r^{n-1}s}_{n-1}\} \\ &= 1 + (n-1) + 1 + (n-1) \\ &= 2n \end{aligned}$$

□

The following properties are well known and can be found in Robinson (1980).

Given $y, z \in G$, we recall that

$$(yz)^{-1} = \begin{cases} y^{-1}z^{-1} & \text{if } G \text{ abelian,} \\ z^{-1}y^{-1} & \text{if not} \end{cases}$$

2.3.2 Proposition. Let $[x, y, z] = [[x, y], z]$ and $[x, y] = xyx^{-1}y{-}1$ where $x, y, z \in G$. The following are true:

(i) $[x, y] = 1$ if and only if $xy = yx$;

(ii) $[x, y]^{-1} = [y, x]$;

(iii) $y^x = [x, y]y = xyx^{-1}$;

(iv) $[x, zy] = [x, z][x, y]^z$;

(v) $[yx, z] = [x, z]^y[y, z]$;

(vi) $[z, y^{-1}, x]^y[y, x^{-1}, z]^x[x, z^{-1}, y]^z = 1$.

We sketch the proof of (iv) as useful exercise

Proof. We choose (iv) that is $[x, z] = [x, z][x, y]^z$ and show that is true.

$$\begin{aligned} [x, z][x, y]^z &= xzx^{-1}\underbrace{z^{-1}z}_{1}[x, y]z^{-1} \\ &= xz\underbrace{x^{-1}x}_{1}yx^{-1}y^{-1}z^{-1} \\ &= xzyx^{-1}y^{-1}z^{-1} \\ &= x(zy)x^{-1}(zy)^{-1} \\ &= [x, zy] \\ \therefore [x, z][x, y]^z &= [x, zy]. \end{aligned}$$

□

2.3.3 Theorem. *In D_{2n} (where n is odd) with the presentation $D_{2n} = \langle r, s : r^n = 1, s^2 = 1, r^s = r^{-1} \rangle$, we have $C_{D_{2n}}(\langle r \rangle) = \langle r \rangle$*

Proof. Of course, $C_{D_{2n}}(\langle r \rangle) \supseteq \langle r \rangle$ by definition. Vice versa

$[r, s] = r^2$ and $[r^j, s] = r^j s r^{-j} s^{-1} = r^{2j}$, this is enough to conclude that $C_{D_{2n}}(\langle r \rangle) \subseteq \langle r \rangle$. In fact

Case 1 : If g and h have order n. Then it is trivial.

Case 2 : If g has order n and h has order 2, then we write $g = r^i$ and $h = r^j s$, and also $h^{-1} = h$. Hence

$$ghg^{-1}h^{-1} = ghg^{-1}h = r^i r^j s r^{-1} r^j s = r^{i+j} r^{-(j-i)} ss = r^{2i}$$

Case 3 : If g has order 2 and h has order n, then we write $g = r^i s$, $h = r^j$ and $g^{-1} = g$. Then we may apply the same argument of case 2 above.

$$(hgh^{-1}g^{-1})^{-1} = hgh^{-1}g^{-1} = hgh^{-1}g = r^j r^i s r^{-j} r^i s = r^{j+i} s r^{-(-j+i)} s = r^{2j}$$

Case 4 If both g and h have order 2, then $g = r^i s$, $h = r^j s$, $g^{-1} = g$ and $h^{-1} = h$. Hence, we compute

$$hgh^{-1}g^{-1} = ghgh = (gh)^2 = (r^i s r^j s)^2 = (r^{i-j} ss)^2 = r^{2(i-j)}$$

□

The following exercise is useful for our purposes.

2.3.4 Example. Let's take a dihedral group, D_6 and try and compute its commutativity degree. We define $D_6 = \langle r, s : r^3 = 1, s^2 = 1, srs^{-1} = r^{-1} \rangle$. The elements of $D_6 = \{1, r, r^2, s, rs, r^2 s\}$. Hence the order of D_6 is $|D_6| = 6$. The commutativity degree of D_6 is given by

$$d(D_6) = \frac{|\{(x, y) \in D_6 \times D_6 : [x, y] = 1\}|}{|D_6|^2} = \frac{1}{|G|^2} \sum_{x \in D_6} |C_{D_6}(x)|$$

From here, let compute the centralizer of each element in D_6.

$$\begin{aligned}
|C_{D_6}(x)| &= |\{g \in D_6 : gx = xg\}| \\
|C_{D_6}(1)| &= |\{1, r, r^2, s, rs, r^2 s\}| = |D_6| = 6 \\
|C_{D_6}(r)| &= |\{1, r, r^2\}| = 3 \\
|C_{D_6}(r^2)| &= |\{1, r, r^2\}| = 3 \\
|C_{D_6}(s)| &= |\{1, s\}| = 2 \\
|C_{D_6}(rs)| &= |\{1, rs\}| = 2 \\
|C_{D_6}(r^2 s)| &= |\{1, r^2 s\}| = 2
\end{aligned}$$

$$d(D_6) = \frac{1}{|D_6|^2} \sum_{x \in D_6} |C_{D_6}(x)| = \frac{6+3+3+2+2+2}{6^2} = \frac{18}{36} = \frac{1}{2}$$

Finally, we provide the computation of the commutativity degree of a nonabelian group of order eight, which is very important in theoretical physics. It is known as the group of the quaternions.

2.3.5 Example. The quaternion group, Q_8 is a nonabelian group of order eight and has the presentation

$$Q_8 = \langle a, b : a^4 = b^4 = 1, a^2 = b^2, ba = ab^3 \rangle.$$

We compute the commutativity degree. The elements of Q_8 are $\{1, a, a^2, a^3, b, ab.a^2b, a^3b\}$

	1	a	a^2	a^3	b	ab	a^2b	a^3b		$\|C_{Q_8}(x)\|$
1	1	1	1	1	1	1	1	1		8
a	1	1	1	1	0	0	0	0		4
a^2	1	1	1	1	1	1	1	1		8
a^3	1	1	1	1	0	0	0	0		4
b	1	0	1	0	1	0	1	0		4
ab	1	0	1	0	0	1	0	1		4
a^2b	1	0	1	0	0	0	1	1		4
a^3b	1	0	1	0	1	0	0	1		4

$$\begin{aligned}
|C_{D_8}(1)| &= |C_{D_8}(a^2)| = |\{1, a, a^2, a^3, b, ab, a^2b, a^3b\}| = 8 \\
|C_{D_8}(a)| &= |\{1, a, a^2, a^3\}| = 4 \\
|C_{D_8}(b)| &= |\{1, a^2, b, ab, a^2b\}| = 4 \\
|C_{D_8}(ab)| &= |\{1, a^2, ab, a^3b\}| = 4 \\
|C_{D_8}(a^2b)| &= |\{1, a^2, a^2b, a^3b\}| = 4 \\
|C_{D_8}(a^3b)| &= |\{1, a^2, b, a^3b\}| = 4
\end{aligned}$$

$$d(Q_8) = \frac{1}{|G|^2} \sum_{x \in Q_8} |C_{Q_8}(x)| = \frac{8+8+4+4+4+4+4+4}{8^2} = \frac{40}{64} = \frac{5}{8}$$

3. Direct and Semidirect Products

Given two groups G and H, the direct product $G \times H$ is the set $\{(g, h) : g \in G$ and $h \in H\}$.This is a new group containing copies of H and G, respectively. For abelian groups, the direct product is sometimes denoted by addition notation $G \oplus H$.

The operation on $G \times H$ is given by

$$(g_1, h_1)(g_2, h2) = (g_1 g_2, h_1 h_2)$$

We can take the direct product of more than two groups at once. Given a finite sequence $G_1, \ldots, G_n$ of groups, then our direct product is given by

$$\prod_{i=1}^{n} G_i = G_1 \times G_2 \times \ldots \times G_n$$

of a groups $G_1, G_2, \ldots, G_n$. If $G_1 = G_2 = \ldots = G_n$, then we write G^n.

3.0.6 Example. Let consider the group $\mathbb{Z}(2) = \langle a : 2 \cdot a = 0 \rangle$ and

$$\underbrace{\mathbb{Z}(2) \oplus \mathbb{Z}(2) \oplus \ldots \oplus \mathbb{Z}(2)}_{n- \text{ times}} = n\mathbb{Z}(2).$$

We may regard the group as a binary $n-$tuples of zeros and ones under operation "exclusive and". For example

$$(0011010110) \oplus (1000110011) = (0100011010)$$

This group is used in coding theory, cryptography and many areas in computer science.

Note that, if both G and H are finite, then $|G \times H| = |G||H|$.

The following is well known and can be found in Robinson (1980) and we report the proof below

3.0.7 Theorem. *Let* $(g_1, \ldots, g_n) \in \prod_{i=1}^{n} G_i$. *If* g_i *has finite order* r_i *in* G_i, *then the order of* $(g_1, \ldots, g_n) \in \prod_{i=1}^{n} G_i$ *is the least common multiple of the orders of* $r_1, \ldots, r_n$, *that is*

$$|(g_1, \ldots, g_n)| = lcm(|g_1|, \ldots, |g_n|)$$

Proof. Firstly, let consider two components. Let $(g_1, g_2) \in G_1 \times G_2$. If g_1 and g_2 have finite orders a and b respectively, then we say the order of $(g_1, g_2) \in G_1 \times G_2$ is the least common multiple of a and b. That is

$$|(g_1, g_2)| = lcm(a, b)$$

Let $m = lcm(a, b)$ and $n = |(g_1, g_2)|$. Then

$$(g_1, g_2)^m = (g_1^m, g_2^m) = (1_{G_1}, 1_{G_2})$$

Thus, n divides m, implies $n \leq m$. But also from $n = |(g_1, g_2)|$, we can write

$$(g_1^n, g_2^n) = (g_1, g_2)^n = (1_{G_1}, 1_{G_2})$$

This implies that a divides n and b divides n. Thus n is a common multiple of a and b. But since $n \leq m$ and $m = lcm(a, b)$. Then $n = m$. Therefore $|(g_1, g_2)| = lcm(|g_1|, |g_2|)$.

By induction, the proof follows. □

As an application of Theorem 3.0.7, we report the following example.

3.0.8 Example. Let $(6,45) \in \mathbb{Z}(8) \oplus \mathbb{Z}(50)$. The $gcd(6,8) = 2$, hence the order of 6 is 4 in $\mathbb{Z}(8)$. Similarly, the $gcd(45,50) = 5$, the order of 45 is $50/5 = 10$ in $\mathbb{Z}(50)$. The least common multiple of 4 and 10 is 20. Thus $(6,45)$ has order 20 in $\mathbb{Z}(8) \oplus \mathbb{Z}(50)$.

Another application of Theorem 3.0.7 is the following

3.0.9 Example. Consider the following groups

$$\mathbb{Z}(2) \oplus \mathbb{Z}(2) = \{(0,0),(0,1),(1,0),(1,1)\}$$

$$\mathbb{Z}(2) \oplus \mathbb{Z}(3) = \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}$$

From the first equation, we get $\mathbb{Z}(2) \oplus \mathbb{Z}(2)$ and $\mathbb{Z}(4)$ are both containing four elements but they are not isomorphic since $\mathbb{Z}_(2) \oplus \mathbb{Z}(2)$ is not cyclic but $\mathbb{Z}(4)$ is cyclic with the generator 1 or 3 .

From the second equation, we get $\mathbb{Z}(2) \oplus \mathbb{Z}(3)$ and $\mathbb{Z}(6)$ are both containing six elements and they are isomorphic since $(1,1)$ is the generator of $\mathbb{Z})(2) \oplus \mathbb{Z}(3)$ and $\mathbb{Z}(6)$ has generator 1 or 5. Thus $\mathbb{Z}(2) \oplus \mathbb{Z}(3) \cong \mathbb{Z}(6)$

Now we report from Page 27 of Robinson (1980) the notion of semidirect product, which is a generalization of the notion fo direct product of two groups. Suppose N is a normal subgroup of G and there is a subgroup H such that

$$G = HN = \{hn \mid h \in H \text{ and } n \in N\}.$$

In general, we cannot conclude that the set product HN is a subgroup of G if both the subgroups H and N are not normal in G, but it is enough that one of them is normal, in order to conclude that HN is a subgroup of G. This is why we require N to be normal.

3.0.10 Definition. If G is a group and H and N two subgroups of G, G is called *(internal) semidirect product* of H and N, if

1. $H \cap N = \{1\}$;
2. N is normal in G;
3. $G = HN$.

If G is the semidirect product of H and N, we write briefly

$$G = N \rtimes H.$$

In this situation, every element of G is *uniquely expressed* in the form hn for $h \in H$ and $n \in N$. This is possible, because $H \cap N = \{1\}$.

There is an equivalent way to characterize the group G in terms of semidirect product, using the conjugation. This will give the notion of *external semidirect product*. Assume that N is a group and N is fixed under conjugation by elements of G. This means that the conjugation

$$\theta_g : n \in N \mapsto \theta_g(n) = gng^{-1} \in N$$

is a bijective homomorphism (i.e.: automorphism) of N for all $g \in G$. In fact $\theta = \theta_g$ is surjective and well-defined, because N is fixed by conjugation in G, but we have also

$$\theta_g(n_1\ n_2) = gn_1n_2g^{-1} = gn_1g^{-1}gn_2g^{-1} = \theta_g(n_1)\theta_g(n_2)$$

for all $n_1, n_2 \in N$ and also that $\theta_g(n_1) = \theta_g(n_2)$ if and only if $n_1 = n_2$.

Now H, N and $\theta\colon H \to \mathrm{Aut}(N)$ allows us to form a new group $N \rtimes_\theta H$, called the *(external) semidirect product of H and N with respect to θ*, via the multiplication

$$(*) \qquad (n,h)(n',h') = \Big(n\big(\theta_h(n')\big), hh'\Big) = \big(nhn'h^{-1}, hh'\big)$$

on the set of pairs $H \times N$. Here we can see that the multiplication is defined, on the second component, pointwise, but on the first component is not pointwise (in general). In fact the presence of θ influences the definition of the multiplication above on the first component only.

In the special case in which $g = 1$ and so $\theta_1 = \theta = id_N$, we get the case of the direct product $N \times H$.

Now one can check that the multiplication, defined above in the (external) semidirect product, is associative, there is an identity $(1_N, 1_H)$ and there is an inverse of $\big(n, h\big)$, which is $(\theta_{h^{-1}}(n^{-1}), h^{-1}\big)$. Therefore the structure of group is satisfied for the external semidirect product.

Finally, if we have an external semidirect product, then the sets $\{(1, h) \mid h \in H\} = H'$ and $\{(n, 1) \mid n \in N\} = N'$ are subgroups (with respect to the multiplication $(*)$) and N' is also normal. Moreover, $H' \cap N'$ is trivial and $H'N' = G$. This means that the axioms of Definition 3.0.10 are satisfied. Viceversa, we may start from subgroups H and N satisfying the axioms of Definition 3.0.10 and make the construction that we have just done. Therefore the two notions are equivalent. So there is no ambiguity in omitting the adjective "internal" or "external", saying just "semidirect product".

The following example shows an important relation between semidirect products and dihedral groups.

3.0.11 Example. Let consider dihedral group D_{2n} of order $2n$ and n is prime. Let a be a rotation and b be a reflection. Then we may consider $N = \langle a \rangle \simeq \mathbb{Z}(n)$ and $H = \langle b \rangle \simeq \mathbb{Z}(2)$ and we can form the semidirect product via the homomorphism

$$\theta_g : a^i \in \mathbb{Z}(n) \mapsto g a^i g^{-1} \in N,$$

where a^i (with $i \in \{0, 1, \ldots, n-1\}$) describes the general element of N, since N is cyclic. Now we may consider

$$\theta : b \in H \mapsto \theta_b \in \mathrm{Aut}(N).$$

Since n is prime, we can find in (Robinson, 1980) that $\mathrm{Aut}(N) \simeq \mathbb{Z}(n-1)$. But $b^2 = 1$, then θ either is the trivial homomorphism :

$$\theta : 1 \in H \mapsto \theta_1 \in \mathrm{Aut}(N)$$

or is the homomorphism that acts on elements of N sending in their inverses, and this is happening when $b \neq 1$. There are no more cases. In particular, this means that $\theta_b(a) = bab^{-1} = a^{-1}$. Then we have

$$D_{2n} = \langle a \rangle \rtimes \langle b \rangle \cong \mathbb{Z}(n) \rtimes \mathbb{Z}(2).$$

4. Elementary Notions on Topological Groups

In order to formulate the concept of commutativity degree in the infinite case, we need to involve topological groups and some properties of compact groups. We will refer to (Hofmann and Morris, 2006).

A topological group is a set equipped with two structures: that of a topological space and that of a group.Thus, one may discuss continuous functions, because of the topological structure and one may implement algebraic operations, because of the group structure. These structures are linked in a way that the topological properties of the space affect the algebraic properties of the group and vice versa. Two fundamental textbooks on topological groups are Hewitt and Ross (1979) and Hofmann and Morris (2006).

4.0.12 Definition. (Hewitt and Ross, 1979): Let G be a group and consider the topology τ on G (as set). Then G is said to be a topological group if

(i) the mapping $(x, y) \to xy\ G \times G \to G$ is a continuous mapping of the Cartesian product $G \times G$ onto G

(ii) the mapping $x \to x^{-1}$ of G onto G is continuous.

Some examples of topological groups are the following:

(1) Any finite group E with the discrete topology $\tau = P(E)$ is a topological group.

(2) The additive group of real numbers $\mathbb{R}$ form a topological group, with the usual topology that is with the topology in which the opens can be written by the unions of intervals $\mathbb{R}$.

On a group we may have both an algebraic structure and a topological structure and we want that these are preserved by quotients, products and subgroups. It is not difficult to check the following properties:

(i) Subgroups of a topological group are topological groups with respect to the induced topology.

(ii) Quotients of topological groups are topological groups with respect to the quotient topology.

(iii) The Cartesian product of topological groups is a topological group with respect to the product topology.

To understand what a compact group is, we need the notion of *open covering*, *finite subcovering* and compact space.

4.0.13 Definition. Let (X, τ) be a topological space. Let I be a set and $(M_i)_{i\in I}$, a family of open sets in a (X, τ). Let A be a subset of (X, τ). Then $(M_i)_{i\in I}$, is said to be *open covering* of A if $A \subseteq \bigcup_{i\in I} Mi$. A finite subfamily, $M_{i1}, M_{i2}, \ldots, M_{ij}$, of M_i, $i \in I$ is called a *finite subcovering* of A if $A \subseteq M_{i1} \cup M_{i2} \cup \ldots \cup M_{ij}$

Now we give the notion of compactness.

4.0.14 Definition. A subset A of a topological space (X, τ) is said to be *compact* if every open covering of A has a finite subcovering. If the compact subset A equals X, then (X, τ) is said to be a compact space. A *compact group* is a topological group whose topology is compact.

In general topology, compactness is a property that generalizes the notion of a subset of Euclidean space being closed and bounded

4.0.15 Remark. Compact groups are a natural generalization of finite groups with the discrete topology.

In the context of compact groups we should reformulate (i), (ii) and (iii) as follows:

(1) If H is a closed subgroup of a compact group G, then H is a compact group.

(2) If N is a closed normal subgroup of a compact group G, then G/N is a compact group.

(3) If G_i is a compact group for each $i \in I$, then $\prod_{i \in I} G_i$ is a compact group.

4.1 More Examples of Compact Groups

There are some interesting examples of compact groups, which may be embedded in direct products of finite groups. These sources of examples are the main motivation why one can generalize the notion of commutativity degree for infinite groups.

The *projective limit* is a process that allow us to "combine" several related objects and the process of combining is specified by *morphisms* between the objects.

Let I be a set directed by a partial ordering $\leq$, i.e.:

(1) $i \leq i$, for all $i \in I$;

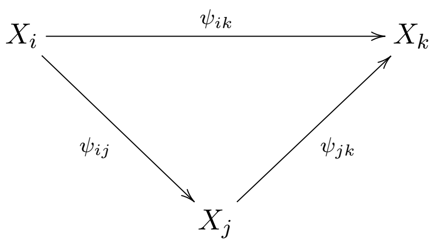
(2) If $i \leq j$ and $j \leq k$ the $i \leq k$, for all $i, j, k \in I$;

(3) If $i \leq j$ and $j \leq i$ then $i = j$, for all $i, j \in I$;

(4) If $i, j \in I$, there exists some $k \in I$ such that $i, j \leq k$ (Ribes and Zalesskii, 2010).

From (Ribes and Zalesskii, 2010), we have the following definition

4.1.1 Definition. A *projective system* of topological groups over I, consists of a collection $\{X_i : i \in I\}$ of topological groups indexed by I and a collection of a continuous group homomorphisms $\psi_{ij} : X_i \to X_j$, defined whenever $i \geq j$, such that the diagrams of the form



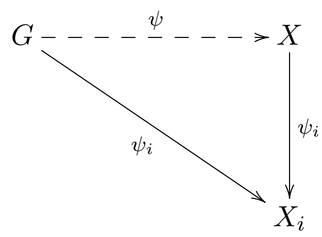
commute whenever $i, j, k \in I$ and $i \geq j \geq k$. We denote such a system by $\{X_i, \psi_{ij}, I\}$ (or by $\{X_i, \psi_{ij}\}$)

Let G be a topological group, $\{X_i, \psi_{ij}, I\}$ an projective system of topological groups over I and let $\psi_i : G \to X$ be a continuous group homomorphism for each $i \in I$. These mappings ψ_i are said to be *compatible* if $\psi_{ij}\psi_i = \psi_j$ whenever $j \leq i$

A topological group X together with compatible continuous homomorphism

$$\psi_i : X \to X_i \qquad (i \in I)$$

is a *projective limit* and is denoted by $\lim_{i\in\mathbb{N}} X_i = X$ of the projective system (X_i, ψ, I) if the following properties hold:



whenever G is a topological group and $\psi_i : G \to X_i$ for $i \in I$ is a set of compatible continuous homomorphism, then there is a unique continuous homomorphisms $\psi : G \to X$ such that $\psi_i \psi = \psi_i$ for al $i \in I$.

The maps $\psi_i : X \to X_i$ are called projections and they are not necessarily surjective.

The following example is a well known compact abelian groups and can be found in Hofmann and Morris (2006)

4.1.2 Example. Given a sequence $\psi_i : G_{i+1} \to G_i$, $i \in \mathbb{N}$ of morphisms of compact groups: then we obtain a projective system of compact groups by defining, for natural numbers $j \leq k$, the morphisms

$$f_{jk} = \psi_j \circ \psi_{j+1} \ldots \circ \psi_{k-1} : G_k \to G_j$$

Then $G = \lim_{i\in\mathbb{N}} G_i$ is given by $\{(g_n)_{i\in\mathbb{N}} : \text{ for all } i \in \mathbb{N} \quad \psi_i(g_{i+1}) = g_i\}$.

Now choose a natural number p and set $G_n = \mathbb{Z}(p^n) = \mathbb{Z}/p^n\mathbb{Z}$. We define $\psi_i : \mathbb{Z}(p^{n+1}) \to \mathbb{Z}(p^n)$ by $\psi_i(z + p^{n+1}\mathbb{Z}) = z + p^n\mathbb{Z}$.

$$\mathbb{Z}(p) \xleftarrow{\psi_1} \mathbb{Z}(p^2) \xleftarrow{\psi_2} \mathbb{Z}(p^3) \xleftarrow{\psi_3} \ldots$$

The projective limit $\lim_{i\in\mathbb{N}} \mathbb{Z}(p^n)$ of the system is called the group $\mathbb{Z}_p$ of $p-$*adic integers*

4.2 Haar Measure

Haar measure was introduced by Alfréd Haar in 1933. It assigns an "invariant volume" to a subset of locally compact group, as a result one can define an integral functions on those groups. To explicitly define Haar measure, we need some terminologies.

Let X be a nonempty set. A collection Σ of subsets of X is a σ-*algebra* when the following conditions are satisfied:

(1) $\emptyset \in \Sigma$ and $X \in \Sigma$

(2) If $B \in \Sigma$ then its complement $X \backslash B \in \Sigma$

(3) If (B_n) is a sequence of sets in Σ then the union $\bigcup_{n=1}^{\infty} B_n \in \Sigma$

The pair (X, Σ) is called *measurable space*. A function $\mu : \Sigma \to [0, \infty)$ is a *(positive nondegenerating) measure* (on the measurable space X) if the following properties are satisfied:

(1) $\mu(B) \geq 0$ for all $B \in \Sigma$;

(2) $\mu(\emptyset) = 0$;

(3) $\mu(\cup_{n\in\mathbb{N}} B_n) = \Sigma_{n\in\mathbb{N}} \mu(B_n)$ for all countable collections of pairwise disjoint $B_n \in \Sigma$.

These notions are very common in functional analysis and can be found in Hewitt and Ross (1979). In general, one does not require the presence of a topology on X, but it is very common (as in our case) to connect the presence of a σ-algebra and the presence of a topology on the same set. If X is a topological space, we say that Σ is a *Borel algebra*, if it is the smallest σ-algebra containing all open subsets of X.

If μ_1 and μ_2 are two measures on the measurable spaces (X_1, Σ_1) and (X_2, Σ_2), then we may form a new σ-algebra $\Sigma_{X_1\times X_2}$ on the product $X_1 \times X_2$ given by subsets of the form $B_1 \times B_2$, where $B_1 \in \Sigma_1$ and $B_2 \in \Sigma_2$. It is possible to consider a new Borel algebra $\Sigma_{X_1\times X_2}$ on this product space, which has the product topology, and we get the so–called *Borel product algebra*. A measure on $(X_1 \times X_2, \Sigma_{X_1\times X_2})$ is called a *product measure* if the following property holds:

$$(\mu_1 \times \mu_2)(B_1 \times B_2) = \mu_1(B_1)\mu_2(B_2)$$

for all $B_1 \in \Sigma_1, B_2 \in \Sigma_2$

If g is an element of a compact group G and S a subset of G, then we define the *left translates* of S by

$$gS = \{g \cdot s \, : \, s \in S\}.$$

Now one can see that left translates map Borel sets into Borel sets, so they preserve the Borel algebra structure on G.

A measure μ on the Borel algebra of G is $left\ invariant$, if for all Borel subsets $S \subset G$ we have

$$\mu(gS) = \mu(S).$$

We report Haar's Theorem here:

There is, up to a positive multiplicative constant, a unique countably additive, non-trivial measure μ on the Borel subsets of the compact group G satisfying the following properties:

1. $\mu(gS) = \mu(S)$ for every $g \in G$ and all Borel sets $S \subset G$.
2. μ is finite on every compact set, that is, $\mu(K) < \infty$ for all compact $K \subset G$.
3. μ is outer regular on Borel sets,
4. μ is inner regular on open sets,

Such a measure is called *left Haar measure* on G.

It can be shown as a consequence of the above properties that then $\mu(G)$ is finite and positive, so we can uniquely specify a left Haar measure on G by adding the normalization condition $\mu(G) = 1$.

4.3 Commutativity Degree and Infinite Groups

One way to generalize the commutativity degree on infinite groups is to work on infinite compact groups. For infinite groups, the ratio of Section 2.3 is not longer meaningful. Compact groups with normalized Haar measure are good candidates for this procedure.

If G is a compact group with the Haar measure μ (described in the previous section), then we may define on the product measure space $G \times G$ the product measure $\mu \times \mu$, which is again a Haar measure on the new compact group $G \times G$. Then we may introduce the function

$$f : (x, y) \in G \times G \mapsto f(x, y) = [x, y] \in G$$

and this is (not a homomorphism in general) a continuous function so it sends preimages of closed subsets of G in closed subsets of $G \times G$. In particular,

$$f^{-1}(1) = C = \{(x, y) \in G \times G \mid xy = yx\},$$

is a compact and measurable subset of $G \times G$. Therefore it is possible to define

$$d(G) = (\mu \times \mu)(C).$$

Obviously if G is finite and has the discrete topology, then G is a compact group with the discrete topology and so the Haar measure of G is the counting measure. Then we find exactly the original notion of commutativity degree, given in Section 2.3.

From the point of view of the compact groups, many results of become special situations, since each finite group is trivially compact.

In 1970 Gustafson (Gustafson, 1973) proved that if G is a non-abelian finite group, then $d(G) \leq 5/8$; furthermore this bound is achieved if and only if $G/Z(G)$ is isomorphic to an elementary abelian 2-group of rank 2, where $Z(G)$ denotes the center of the group G, that is $G/Z(G) \cong \mathbb{Z}(2) \oplus \mathbb{Z}(2)$.

Given a group, G, an element $g \in G$ is called an FC-*element* if its number of conjugates is finite. This means that $|G : C_G(g)|$ is finite . FC-elements always form a subgroup. (Robinson, 1980). FC-element is known to be an element of the center of the group and for this reason the subgroup of all FC- elements is called FC-*center*.

4.3.1 Definition. Let G be a group. G is called FC-center, if $g \in G$ has only a finite number of conjugates in G. In other word, every conjugacy class of elements in G has a finite size. A group is FC- group if it agrees with its FC-center.

In particular:

4.3.2 Example. All abelian groups are FC-groups. All finite groups are FC-groups. All direct products $F = \prod_{i \in I} F_i$ of (eventually infinite) F_i finite groups is an FC-group: one can see from the previous section that such an F is in fact a compact group.

4.3.3 Theorem. *(Robinson, 1980)* $[G : Z(G)]$ *is finite, then* G *is an* $FC-$*group.*

Proof. $C_G(g) \supset Z(G)$, so $[G : C_G(g)] \leq [G : Z(G)]$ and so therefore each element of G is an $FC-$element. □

5. Conclusion

Now we end with a result (see (Hofmann and Russo, 2012)) which connects most of the notions which we have seen until now.

5.0.4 Theorem. *Let G be a compact group. Then the following conditions are equivalent:*

(i) $d(G) > 0$;

(ii) $|G : FC(G)| < \infty$.

This result, whose proof involves a lot of notions, shows that the commutativity degree of an infinite compact group influences the size index of the $FC-$center of G.

Since $FC-$groups have been completely characterized in Robinson (1980), this result shows in some sense how far a compact group us from being FC-groups.

More precisely, this is the first result which connects probabilistic methods with the theory of FC-groups and with the theory of compact groups.

Essentially the presence of a positive probability measure is quite natural, but, if it does not exist, that is, if the condition (i) of the above theorem is not satisfied, then, at least for compact groups, this means that pathological examples may arise.

There was not enough time to see here how the commutativity degree may be formulated in terms of a “random walk”, and so in the context of the theory in Gromov (1993).

This will be the subject of my future research in mathematics.

Acknowledgment

First and foremost, I thank God Almighty for His protection throughout this work which has finally come to a successful end.

I would like to express my sincerest gratitude to Dr. Francesco G. Russo and Dr. David Erwin for their supervision and motivation which has brought me this far.

Special appreciation goes to AIMS (African Institute for Mathematical Science) for granting me an opportunity to study Structured Masters. I would like to thank Prof. Jeff Sanders for his questions and guidance and also like to thank the AIMS tutors especially Andry Nirina Rabenantoandro for taking his time to work with me.

Finally, I would like to thank my mother and all of my family for their supports, love and prayers.

References

A. Castelaz. *Commutativity degree of finite groups*. Wake Forest University, 2010. MSc thesis.

P. Erdős and P. Túran. On some problems of statistical group theory. 19:413–435, 1968.

M. Gromov. *Asymtotic invariants of infinite groups*. Cambridge University Press, Cambridge, 1993.

W. Gustafson. What is the probability that two group elements commute? 80:1031–1034, 1973.

E. Hewitt and K. A. Ross. *Abstract harmonic analysis*, volume 1. Springer, Berlin, 2ed. edition, 1979.

K. H. Hofmann and S. A. Morris. *The Structure of Compact Groups: A Primer for Students - a Handbook for the Expert*. De Gruyter Studies in Mathematics. De Gruyter, Berlin, 2 revised edition, 2006.

K. H. Hofmann and F. G. Russo. The probability that x and y commute in a compact group. 153: 557–571, 2012.

L. Ribes and P. Zalesskii. *Profinite Groups*. Springer, Berlin, 2010.

D. Robinson. *A course in the theory of groups*. Springer, Berlin, 1980.